

HP Business Service Management

For the Windows® and Linux operating systems

Software Version: 9.20

Monitoring Automation for HP Operations Manager i Administrator Guide

Document Release Date: May 2013

Software Release Date: May 2013



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 2012-2013 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 software developed by the Apache Software Foundation (www.apache.org).

This product includes software developed by the JDOM Project (www.jdom.org).

This product includes software developed by the MX4J project (<http://mx4j.sourceforge.net>).

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

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

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

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

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

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

Contents

Monitoring Automation for HP Operations Manager i Administrator Guide ...	1
Contents	5
Monitoring	7
Management Templates and Aspects	9
Configuration Folders	13
Configuring Management Templates	17
Configuring Aspects	43
Viewing Details	70
Policy Templates	71
Configuring HP ArcSight Logger Policies	83
Configuring ConfigFile Policies	93
Configuring Flexible Management Policies	98
Configuring Log File Entry Policies	111
Configuring Measurement Threshold Policies	131
Configuring Node Info Policies	167
Configuring Open Message Interface Policies	171
Configuring Scheduled Task Policies	189
Configuring Service Auto-Discovery Policies	201
Configuring Service/Process Monitoring Policies	210
Configuring SNMP Interceptor Policies	228
Configuring Windows Event Log Policies	248
Configuring Windows Management Interface Policies	267
Configuring XML File Policies	286
Importing HP SiteScope Templates	311
Importing HP Operations Manager Policies and Instrumentation	320
Instrumentation Development	323
Validating HP Operations Manager Policies	330

ConfigExchange Command-Line Tool	332
Policy Objects for Scripts	336
Pattern Matching in Policy Rules	357
Pattern-Matching Details	357
User-Defined Variables in Patterns	361
Pattern Matching for Variables	363
Examples of Pattern Matching in Rule Conditions	364
Assignments and Tuning	366
Deployment Jobs	383
Settings for Monitoring Automation	385
Infrastructure Settings for Monitoring Automation	385
License Settings for Monitoring Automation	386
Logging and Tracing for Monitoring Automation	387
Exporting Configuration Data	389
Monitored Nodes	390

Chapter 1

Monitoring

Tip: To use Operations Management Administration areas, you must be granted permission to work with it.

Note: Monitoring Automation is divided into two levels:

Monitoring Automation for Servers is included with the HP Operations Management Event Foundation license. Monitoring Automation for Servers focuses on virtual and physical systems and server-centric applications.

HP Monitoring Automation for Composite Applications adds the capability to use management templates, facilitating the development of monitoring solutions for dynamic data centers. A license for HP Monitoring Automation for Composite Applications can be purchased as an add-on to the HP Operations Management Event Foundation. For more information, contact your local HP Sales Office.

The licensing structure affects the following aspects of the user interface:

- The choices for management templates mentioned in the UI Reference sections of the help are present only if you have an HP Monitoring Automation for Composite Applications license.
- Aspects and all underlying functionality such as nesting, conditional deployment and combining parameters are available with the Event Foundation license. If you do not have an HP Monitoring Automation for Composite Applications license, these should be used as the operator-facing elements. You can also assign policy templates directly to CIs and deploy them, but this is not the recommend approach. For more information see ["Assignments and Tuning" on page 366](#).

This part of the guide contains the following chapters:

- **"Configuration Folders" on page 13**

This chapter describes how to organize management templates and aspects into a hierarchical structure.

- **"Management Templates and Aspects" on page 9**

This chapter describes how to configure and use Management Templates & Aspects. A management template provides a complete management solution for an application or service. Management templates are containers for aspects. Each aspect provides the ability to monitor an aspect of a configuration item (CI). By grouping aspects together, you can create a management solution for several CIs that are related to each other.

- **"Policy Templates" on page 71**

This chapter describes how to configure policy templates. A policy template is a set of configuration information for HP Operations Agent, HP SiteScope, or HP ArcSight Logger. These products enable you to automate the configuration and monitoring of networks and computers. Policy templates define the details of specific configuration and monitoring tasks.

- **"Assignments and Tuning" on page 366**

This chapter describes how to assign management templates, aspects, and policy templates.

- **"Deployment Jobs" on page 383**

This chapter describes how to manage deployment jobs. Whenever you assign a management template, aspect, or policy template to a CI, Operations Management creates a deployment job to transfer the monitoring configuration to the relevant monitoring software (HP Operations Agent, HP SiteScope, or HP Arcsight Logger).

- **"Settings for Monitoring Automation" on page 385**

This chapter provides an overview of the settings required for Monitoring Automation.

- **"Exporting Configuration Data" on page 389**

This chapter describes how to export configuration data.

Chapter 2

Management Templates and Aspects

The Management Templates & Aspects screen has the following panes:

- **Configuration Folders Pane**

The Configuration Folders pane (left pane) is used to create and manage configuration folders. A configuration folder structure is used to organize management templates and aspects.

If you select a subfolder, any management templates or aspects it contains are listed in the Management Templates & Aspects pane (middle pane). If no folder or a folder containing only subfolders is selected the pane is empty.

For detailed information about creating and using configuration folders, see "[Configuration Folders](#)" on page 13.

- **Management Templates & Aspects Pane**

The Management Templates & Aspects Pane pane (middle pane) is used to create and manage both management templates and aspects. To view management templates or aspects, browse to the relevant configuration folder in the Configuration Folders pane (left pane).

For detailed information about creating and using management templates, see "[Configuring Management Templates](#)" on page 17. For detailed information about creating and using aspects, see "[Configuring Aspects](#)" on page 43.

- **Details Pane**

The Details pane (right pane) contains details about the management template or aspect selected in the Management and Aspects pane (middle pane). If no management template or aspect is selected, the pane is empty.

Which details are shown depends on whether a management template or an aspect is selected in the Management Templates & Aspects pane. For detailed information about viewing details, see "[Viewing Details](#)" on page 70.

Tasks

How to Generate Reports


You can generate the following types of reports:

- **Inventory Report**

The inventory report lists which management templates, aspects and policy templates are available on the server. To generate the inventory report, go to the Management Templates & Aspects screen and click **Generate Report**  in the Configuration Folders pane (left pane).

Note: There is only one inventory report. Therefore, the report is the same, no matter which configuration folder is selected when you generate the report. You can only generate the inventory report from the Management Templates & Aspects screen.









• Assignment Report




Assignment reports list which CIs are assigned to a selected management template, aspect or policy template. To generate an assignment report from the Management Templates & Aspects screen, select a management template or aspect and click **Generate Report**  in the Management Templates & Aspects pane (middle pane).

You can also generate assignment reports, as well as other types of reports, from the "Assignments and Tuning" on page 366 screen.









UI Reference







Configuration Folders Pane

UI Element	Description
	Refresh: Reload the tree of configuration folders.
	New Configuration Folder: Open the Create Folder Dialog Box to create a new configuration folder, which will be created as a subfolder of the selected folder.
	Edit Item: Open the Edit Folder Dialog Box to edit the selected configuration folder.
	Delete Item: Delete the selected configuration folder. A message box will prompt you to Confirm or Cancel deletion.
	Show Item Properties: Show the name, description and ID of the selected configuration folder in a message box. Click OK to close the message.
	Search: Open the Search Dialog Box to search for folders or items contained in them.
	Cut Item: Copy the selected configuration folder and its content to the clipboard. It is not possible to accidentally delete a configuration folder: <ul style="list-style-type: none"> • The item that was cut remains in place until it is pasted. • When the paste command is used, the configuration folder cut to the clipboard is moved from its original location to the paste location.
	Paste Item: Paste the last configuration folder that was cut to the clipboard and its content as a subfolder to the selected folder.

UI Element	Description
	You can move configuration folders to a different location in the hierarchy using drag-and-drop.
	Generate Inventory Report: The inventory shows which Management Templates, Aspects and Policy Templates are available on a server. When clicking this icon, a new Browser window opens, prompting you to select a report template. After selecting the template, the browser window shows a report listing details about all elements in the selected configuration folders.
	Help: Open the relevant help in a new browser window.



Management Templates & Aspects Pane

UI Element	Description
	Refresh: Reload all management templates and aspects and refreshes the list..
	<p>New: Provides the following options:</p> <ul style="list-style-type: none">  Management Template: Open the Create/Edit Management Template wizard, which is used to create a new management template.  Aspect: Open the Create/Edit Aspect wizard, which is used to create a new aspect.
	Edit Item: Open the Create/Edit Management Template or Create/Edit Aspect dialog box to edit the selected management template or aspect.
	<p>Delete Item: Delete the selected item(s).</p> <ul style="list-style-type: none"> If a management template or aspect is selected, the item and all its versions are deleted. If a version is selected, only the selected version of the item is deleted. To access the available versions of an item, expand it by clicking the  icon in front of it. <p>You can select multiple items by holding down the Ctrl or Shift key while selecting them.</p> <p>You cannot delete aspects or aspect versions that are referenced by a management template or aspect.</p>
	<p>Update to Latest: Update the selected management template or aspect and all aspects contained in it to their latest version.</p> <p>Note: Update to latest can only be used when a single management template or aspect is selected.</p>





UI Element	Description
	Copy Item: Copy the selected management template or aspect to the clipboard.
	Cut Item: Cut the selected management template or aspect to the clipboard.
	Paste Item: Paste a management template or aspect from the clipboard. Before you can paste the item, you must select a configuration folder that is different to the configuration folder containing the item you cut or copied.
	Assign and Deploy Item: Open the Assign and Deploy wizard, which enables you to assign the selected management template or aspect to a configuration item, and then deploy it.
	Generate Assignment Report: Display a report listing the CIs to which the selected management template or aspect is assigned in a new browser window.
	Help: Open the relevant help in a new browser window.

Details Pane

—Attributes Screen

UI Element	Description
Attribute Categories	The attributes are organized in the following categories: <ul style="list-style-type: none"> • General • Topology View (management templates only) • CI Type (aspects only) • Instrumentation (aspects only) • Aspects • Policy Templates (aspects only)
	Expand: Expand the category to show the attributes contained in it.
	Collapse: Collapse the category to hide the attributes contained in it.

—Structure Screen

UI Element	Description
	Expand All: Expand the structure element to show the entire tree of contained elements. Possible structure elements contained in the element are: <ul style="list-style-type: none"> • Aspects (for aspects, these are nested aspects) • Policy templates assigned to the aspects
	Expand Branch: Expand this branch only.
	Collapse All: Collapse the entire structure tree.
	Collapse Branch: Collapse this branch only.

Configuration Folders








A configuration folder is used to organize management templates and aspects into a hierarchical structure.

Tasks


How to Organize Management Templates and Aspects

Management templates and aspects are stored in a hierarchically structured tree of configuration folders. The root folder is called `Configuration Folders`.


To organize your management templates and aspects:

1. In the root folder `Configuration Folders`, create a set of subfolders that reflects the structure of the cloud you are managing. To create a subfolder, select an existing folder and click **New Configuration Folder** . The new subfolder is created as a subfolder to the selected folder.
2. You can rearrange configuration folders, management templates and aspects using either of the following methods:
 - a. Drag-and-drop.
 - b. Cut-and-paste using the **Cut**  and **Paste**  icons.
3. Create the additional management templates and aspects you need to manage your cloud:
 - a. To create an aspect, select an appropriate folder, click **New...**  in the Management Templates & Aspects pane, and select  **Create Management Template**. For details about how to create aspects, see "Configuring Aspects" on page 43.
 - b. To create a management template, select an appropriate folder, click **New...**  in the Management Templates & Aspects pane, and select  **Create Aspect**. The aspects you created in the previous step are part of the information you need to provide when creating


the management template. For details about how to create management templates, see "Configuring Management Templates" on page 17.

You assign a version number to any new items you create manually. You can view all versions of an item by clicking the expand icon  in front of it. For more information about versioning see "Management Templates and Aspects" on page 9.



How to Browse for a Management Template or Aspect

1. Click the expand icon  to expand the appropriate folders and subfolders. All elements it contains are listed in the Management Templates and Aspects pane (middle pane).
2. Select an element in the Management Templates and Aspects pane. The element's relevant details are displayed in the [Details](#) pane (right pane). The content and UI elements for the [Details](#) pane depend on which type of element is selected. For more information on management templates see "Configuring Management Templates" on page 17, and for aspects see "Configuring Aspects" on page 43.

How to Search for a configuration folder, management template or aspect

1. Click **Search**  to open the [Search Dialog Box](#). You can search for any element in the tree: the search finds both subfolders and the elements they contain.
2. Enter search criteria, observing the following principles:
 - All criteria you specified are combined using logical AND.
 - The search finds all elements with the strings specified in the **Name** and **Description** fields in their name and description.
 - You must specify at least part of the name or the description to be able to do a search. Until you specify one of these criteria the **Search** button is inactive.
 - Use the character * as a wildcard. For example, to search for any aspect, select `Aspect` as the **Type**: criterion, and type * in the **Description** field. The **Search** button is activated and clicking it returns all aspects in the database.

If you specify words separated by spaces, the entire string, including the spaces, is taken literally. Example: If you specify the string `Oracle Server` in the **Description** field, the search returns an item with the description `This aspect is for Oracle Servers`. It will not, however, return an item with the description `This aspect is for Oracle 11 Servers`. (Note that the search string `Oracle* Server` returns both.)


3. Click **Search** to perform the search. All elements conforming to the search criteria are listed.
4. Select one of the elements in the list. You can take the following actions:
 - a. Click **Show Item**  to select the selected element in the Management Templates & Aspects pane. The selection is performed in the background immediately after you click the button, without closing the dialog box.
 - b. Click **Edit Item**  to open an edit dialog box for the selected element. (At the same time the search dialog box is closed and the selected element is selected in the Management Templates & Aspects pane in the background.) Edit the element and click **OK** to return to

the main screen.

- c. Click **Close** to close the dialog box.
5. For more information see [Search Dialog Box](#).

Note: If you specify a search string for **Name** only, the search returns only the currently assigned versions of an aspect or management template. If you specify a **Description**, all versions are returned, whether a **Name** is specified or not.

How to Display an Inventory Report

Click **Generate Inventory Report**  in the Configuration Folders pane (left pane).

The preconfigured inventory report, which is shown in a new web browser window, lists all management templates, aspects and policy templates that are available on a server.

UI Reference


Create Folder Dialog Box





UI Element	Description
Name	Provide a name for the new folder.
Description	Provide a description for the new folder.
ID	Left blank until the folder is created.
OK	Create the folder, assign an ID and close the dialog box.
Cancel	Close the dialog box without creating a folder.

Edit Folder Dialog Box

UI Element	Description
Name	The name of the folder.
Description	The description of the folder.
ID	The unique ID number of the folder. The ID is assigned by the system and cannot be changed.
OK	Change the folder attributes to the new values and close the dialog box.
Cancel	Close the dialog box without creating a folder.



Reports Window

UI Element	Description
	Expand all: Expand all CIs.

UI Element	Description
	Collapse all: Collapse all CIs.
	Filter On/Off: Toggle between Show Customized Values Only and Show All Values .
	Expand Category: Expand the category to show the attributes contained in it.
	Collapse Category: Collapse the category to hide the attributes contained in it.

Search Dialog Box

UI Element	Description
Name	Name or part of the name of the configuration folder, management template or aspect you want to work with.
Description	Description or part of the description of the configuration folder, management template or aspect you want to work with.
Type	Select one of the element types to narrow down the results to the selected element type, or select nothing to return all element types.
Ignore Case	When checked, the search is not case-sensitive. When unchecked, the case of the search strings is taken into account exactly as specified.
Search	List all elements conforming to the specified search criteria. When more than one search criterion is specified, only elements for which all criteria are true are listed. <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note: If you specify a search string for Name only, the search returns only the currently assigned versions of an aspect or management template. If you specify a Description, all versions are returned, whether a Name is specified or not.</p> </div>

UI Element	Description
Search Results Table	 <p>Show Item: Select the selected item in the main window. A message informing you that the item has been selected is displayed, and the relevant details are displayed in the Details pane in the background.</p>  <p>Edit Item: Open the edit dialog for the selected item:</p> <ul style="list-style-type: none"> • If a management template is selected, the Edit Management Template Dialog Box opens. For details, see Configuring Management Templates. • If an aspect is selected, the Edit Aspect Dialog Box opens. For details, see Configuring Aspects. <p>Name The name of the item.</p> <p>Version The elements for which the search criteria are true.</p> <p>Con-figuration Folder The lowest-level configuration folder where the aspect is stored.</p> <p>Path The higher-level configuration folders where the aspect is stored, separated with '/' and starting with the root.</p>
Close	Close the dialog box.

Configuring Management Templates

A management template provides a complete management solution for an application or service. Management templates are containers for aspects. Each aspect provides the ability to monitor an aspect of a configuration item (CI). By grouping aspects together, you can create a management solution for several CIs that are related to each other.

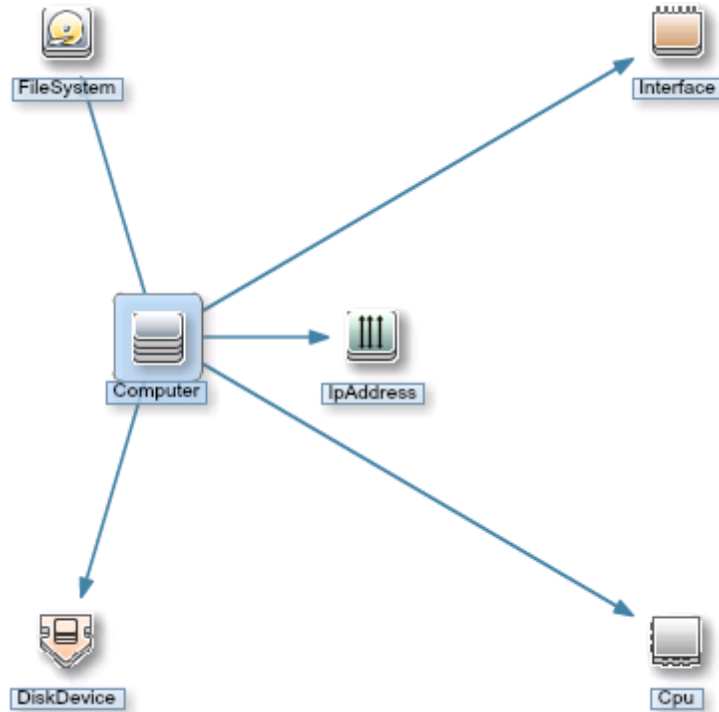
Learn More

Topology Views for Management Templates

BSM Run-time Service Model (RTSM) is a database of the physical and logical entities in your managed environment (for example hardware, software, services, and so on). The entities are represented in RTSM as configuration items (CIs), of which there are many different types (for example, Computer, CPU, DiskDevice, WebServer, Oracle).

RTSM can be populated with CIs automatically using data flow probes and with data from external data providers (for example HP Operations Manager, HP BSM Integration Adapter). The number of CIs in RTSM can be large, but you can focus on specific CIs using views. Views are queries that select CIs from RTSM based on their CI type and their relations with other CIs of other types.

The following graphic shows one of the default views that BSM provides, called Systems_Infrastructure.

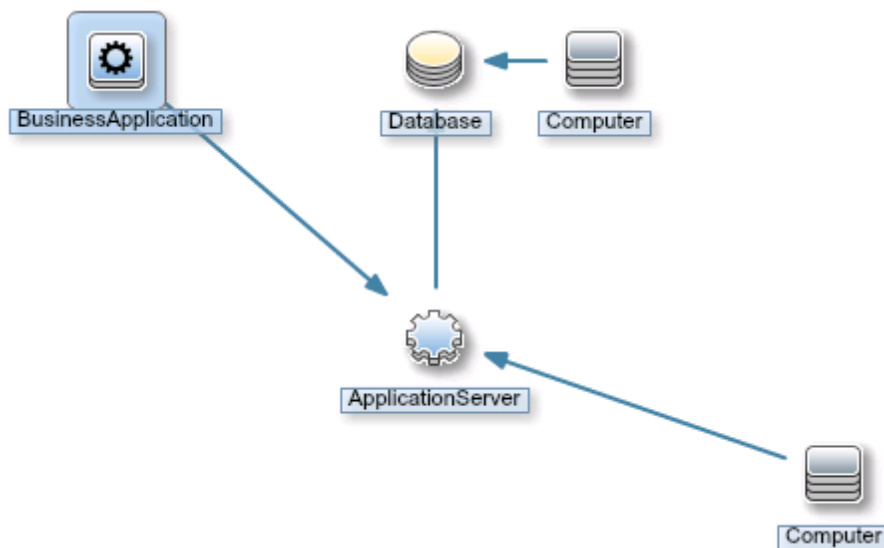


The Systems_Infrastructure view selects CIs of the type Computer, and related CIs of the types Cpu, IPAddress, DiskDevice, Interface, and FileSystem.

When you create a management template, you create a complete management solution for an application or service that consists of several related CIs.

When creating a management template, start with a view that selects the CIs associated with the application or service to be managed.

The following graphic shows an example of a view that selects CIs of the type Business Application, and the related CIs of the types Application Server, Database, and Computer.



Before you create a management template, make sure you have a view that selects the appropriate types of CIs. If necessary, you can create a new view using the Modeling Studio.

Each aspect that you add to a management template is applied to one or more of the CI types in the topology view. For example, a management template for an insurance application could include three aspects that monitor the application database: Database performance, Database process health, and Database connections. In this case, those three aspects are added to the management template and applied to the CI type Database in the topology view.

Version Numbers

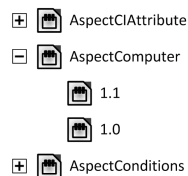
All the items in a management template are versioned. Note the following with respect to version numbers:

- The version number consists of a major and minor version number, separated by a period, for example: 1.2.
- If you modify an existing management template, you create a new version of the management template in the database with a unique version number and version ID. By default, the minor version number increases to the next available higher number automatically after you modify the management template.
- If the version numbers contained in content to be uploaded already exist on the system (for example when applying a Management Pack), the conflicting content is not uploaded and the upload process reports an error.
- Only one version of an item is assigned to a management template at any one time. You can use the **Update to Latest** feature to update all items in a management template to the latest version.

Note: If you modify a management template that is part of an HP Operations Management Pack, HP recommends increasing the minor version number only. The next version of the Management Pack normally uses the next major version number, so adhering to this principle preempts potential version clashes when updating the Management Pack.

To facilitate keeping track of versions it is good practice to specify **Change Log** information. For detailed information about managing versions see the relevant tasks in section *Tasks*.

All versions of an item are visible in the Management Templates & Aspects pane. Expand an item to open a list of all its available versions with the latest version at the top, as shown below for the aspect AspectComputer, which has the two versions 1.0 and 1.1:



When creating a template or aspect, the system proposes version number 1.0 by default, but you can set the version number of the item and all items contained in it as desired. If you want to save the management template with a specific version number, you can select the major and minor version number that you want. It is not possible, however, to replace an existing version of a management template.

Parameterization

Aspects use parameters, which correspond to variables in policy templates, to control how CIs of a certain type are monitored. The value of the parameter is set by an operator for the CI type the aspect is assigned to. The corresponding variable is set and passed to the CI according to the definition in the policy template.

A parameter decouples a value from its physical definition in a policy template. This has the following advantages:

- A value can be set at deployment time in the application, rather than having to change hard-coded variables in a policy template.
- A parameter can be deployed conditionally so the value it represents can be used in multiple situations, but needs to be set only once.
- Parameter values can be set at various levels, allowing defaults to be used on the lower levels. This can greatly reduce the number of values to be set by an operator.
- It is possible to override any configured values by tuning assignments when the monitoring process is started.
- Parameters can be combined to reuse a value occurring multiple times, removing the need to specify values repetitively. A typical example is a password parameter that is used by several policy templates in an aspect to log on to the same service.

Conditional Deployment

You can use the following criteria for the conditional deployment of a policy template:

- *OS type*

You can configure a policy template to be deployed for specific operating systems. Conditional deployment of several policy templates in a single aspect allows for creating platform-neutral aspects.

As an example, consider MySQL, which can run on several platforms. An aspect monitoring process health is configured with conditionally deployed policy templates for Windows, Linux and Solaris. When the aspect is assigned to a MySQL CI that is hosted on a Linux node, Operations Management automatically deploys the Linux variant of the policy template.

- *CI type*

You can configure a policy template to be deployed for specific CI types. Conditional deployment allows you to create aspects monitoring CIs governed by the same parameters, but having CI type-specific policy templates, enabling Operations Management to automatically select the correct policy template for the CI type of a CI when the aspect is assigned to it.

- *CI attribute*

You can configure a policy template to be deployed when a CI attribute has a specific value. Conditional deployment allows you to create aspects that are assigned only to CIs for which certain attributes have a specific value.

Specifying a Default Value

Parameter values are set in the monitoring agents when a policy template is deployed. Parameter values can be defined and changed in the following places:

- The policy template contains a default value for the parameter.
- You can override any policy template defaults at aspect level in the aspect's policy template configuration.
- You can override any aspect-level values at management template level in the management template's aspect configuration.
- You can override any management template- or aspect-level value when deploying a management template or aspect, unless the parameter is configured as `hidden` or `read-only`.

Combining Parameters


You can combine several parameters to create a single combined parameter. The value of a combined parameter is passed to all its constituent parameters, enabling using a single value definition for multiple CIs, making it easier to assign and maintain the management template or aspect using it.



Example: Consider an aspect used to manage MySQL performance which contains several policy templates using the username and password to access MySQL. In this case it is useful to combine the parameters passing the credentials at aspect level, so that they can be defined in one go when the aspect is assigned.



For details, see task Combining Parameters and the UI Reference section for the Edit/Combine Parameters dialog box.

Tasks

How to Create or Edit Management Templates

1. In the Configuration Folders pane, select the configuration folder in which you want to create a new management template, or create a new folder. For details about creating and managing configuration folders, see "[Configuration Folders](#)" on page 13.
2. To edit an existing management template, select it in the list of management templates in the Management Templates & Aspects pane and click the Edit Item button . The Edit Management Template dialog box opens on the General page.

To create a new management template, click the **New** button  in the Management Templates & Aspects pane and select  **Create Management Template**. The Create Management Template wizard opens on the General page.

Note: Do not use the **New** button  to create a new *version* of an existing management template rather than creating a new management template from scratch. To create a new version of an existing management template, use the **Edit** button , select a new version in the General page, make any required changes, and click **OK**.

3. The General page allows you to enter general information about the management template.

Note: Required fields are marked with a red asterisk *****; until all the required fields have




been filled in, the **Next** button is inactive. Fields filled in by the system are marked with a blue background. These fields do not require manual interaction.

- a. Enter a unique **Name** for the management template
- b. *Optional.* Enter a **Description** for the management template.
- c. If required, set the major and minor version numbers for the management template. By default, the major version number of the latest version is selected for new management templates.
- d. *Optional.* Enter your motivation for creating the new management template in the **Change Log** field.
- e. Click the **Topology View** tab or **Next** to accept the values, generate the ID and go to the Topology View page.
- f. The Topology View page is used to define the CI type to which the management template can be assigned, and the application topology for the management template. The CI type to which the management template can be assigned is called the root CI type.

Observe the following:

- The root CI type should occur only once in the topology view to ensure consistency with respect to auto-assignments.
- All CI types present in the application you want to monitor using the management template must be present in the selected topology view. If such a view does not exist, you must create one.


To configure the CI types:

- i. Select a view containing the items you want to manage using one of the following methods:
 - Select an existing view from the drop-down list associated with the **Topology View** field.
 - If you need more choices, click the **Browse** button The *Browse Views* dialog box opens. Browse the views on the system or, if a suitable view does not exist, click the **Model** button  to start the Modeling Studio and create a new view.
- ii. Select a convenient layout from the drop-down list associated with the **Layout** field. If not all the CIs are clearly visible, you can scroll down the graphic and zoom in or out using the zoom buttons  and .
- iii. In the topology view, click the CI type to which the management template is to be assigned. The CI type of the selected CI is selected in the **CI Type** field and highlighted with a blue background in the topology view.

Note: If multiple CIs of the root CI type exist in the assigned topology view, a message warns you of possible inconsistencies but the CI type is nevertheless configured as root CI type. Therefore, if inconsistencies could occur make sure you select a different CI type that occurs only once before continuing.

Alternatively, you can select a CI type from the drop-down list associated with the **CI Type** field. The list contains the CI types of all CIs in the topology view.


Click the **Aspects** tab or **Next** to accept the values and go to the Aspects page.


4. The Aspects page is used to define aspects for the management template.
 - a. Identify the Aspects to be included:
 - Select a node in the Topology View on the left. All aspects that can be assigned to the selected node's CI type are listed in the list of available aspects on the right, at the top of the pane.
 - To include aspects in the management template, select them in the list of available aspects and click . The selected aspects are added to the list of selected aspects, at the bottom of the pane. The target is automatically set to the CI type of the node selected to list the available aspects.


Note: Each aspect must be associated with at least one target node with a matching CI type in the view.

- By default, the latest version of an aspect is added. If you need to use an older version, select the required **Version** after adding it.

Note: To update all aspects in a management template and the parameters and instrumentation contained in them in one go, use the **Update to Latest** feature from the Management Templates & Aspects pane.

- To remove any selected aspects, select them in the list of selected aspects and click .
- b. Click the **Parameters** tab or **Next** to accept the values and go to the Parameters page.
5. The Parameters page lists all parameters contained in the aspects you added in the Aspects tab or screen.

To facilitate monitoring, it may be useful to combine parameters as described in task *How to Combine Parameters*. To combine parameters, make sure at least two parameters are selected and click the  button. The *Edit/Combine Parameters* dialog box opens.

You can also set parameter values at management template level. To edit a parameter, make sure a single parameter is selected and click the  button. The *Edit/Combine Parameters* dialog box opens.

6. Click **OK** or **Finish** to save the management template and close the wizard. The changed or new management template appears in the Management Templates & Aspects pane.

How to Start Monitoring Using a Management Template

There are two places where you can start the monitoring process:





1. The Assignments & Tuning screen at **Admin > Operations Management > Monitoring > Assignments & Tuning**

You would use this location when applying already configured solutions to your cloud. For more information, see "Assignments and Tuning" on page 366.

2. The Management Templates & Aspects pane described in this section.

You would use this place when configuring a solution.

To assign and deploy a management template from the Management Templates & Aspects pane:

1. Select the management template to be deployed in the Management Templates & Aspects pane and then click the **Assign and Deploy** button . The Assign and Deploy wizard opens.
2. In the Configuration Item page, click the configuration item(s) to which you want to assign the aspect. You can select multiple aspects by holding down the **Ctrl** or **Shift** key while selecting. Click **Next** to assign the CIs and go to the Parameter page..
3. In the Parameter page, specify a value for each parameter:
 - a. *Optional.* By default, the list shows only mandatory parameters. To see optional parameters, click the  button. You can also click the  button to see expert parameters.
 - b. Select a parameter in the list, and then click the  button. The Edit Parameter dialog box opens.
 - c. Click **Value**, specify the value, and then click **OK**.

Click **Next** to assign the parameters and go to the Configuration Options screen, or **Finish** to assign the parameters and close the wizard.

4. *Optional.* In the Configuration Options screen, clear the **Enable Assigned Objects** check box if you do not want to enable the assignment immediately. (You can enable assignments later using the Assignments & Tuning manager at **Admin > Operations Management > Monitoring > Assignments & Tuning**.) Click **Finish** to close the wizard.

Operations Management creates deployment jobs to transfer the monitoring configuration to the nodes. After a policy template has been deployed, the BSM server specified in the **Default Virtual Gateway Server for Data Collectors URL** infrastructure setting becomes the owner of the policy on the node.


How to Update a Management Template or Aspect

If you make changes to policy templates or aspects (for example when updating a Management Pack or customizing a policy template or aspect), the policy templates and aspects it contains are added to the database as new versions. Management templates and aspects reference specific versions of aspects, so Management Pack updates require all management templates and aspects referencing the updated aspects and policy templates to be updated as well.


Operations Management features an Update to Latest wizard that helps you to update your management templates and aspects automatically. The Update to Latest wizard supports several different ways of versioning the updated items. Your use case determines which way works best in a particular situation.

To update all items in a management template or aspect to the latest version in the database:



1. Browse to the appropriate configuration folder and select the management template or aspect to be updated in the *Management Templates & Aspects* pane. Select a single management template or aspect; updates can only be done on single management templates or aspects.

2. Click **Update to Latest** . The Update to Latest wizard opens.
3. Set the following options to suit your use case:
 - a. Versioning alternatives:
 - i. **Update to the latest major and minor version** causes both major and minor versions to reflect the latest version.
 - ii. **Update to the Latest Minor Version, Keeping All Major Versions** limits changes to the minor version number only. If the latest version of an item has a higher major number than the current item, the new version will have the lowest available minor number for the same major number as the current version.


For example, if the current version is 1.5 and there are two newer versions with version numbers 1.6 and 2.1:

- i. **Update to the latest major and minor version** will update the version number to 2.1.
 - ii. **Update to the Latest Minor Version, Keeping All Major Versions** will update the version number to 1.6.
 - b. Scope of update:
 - i. **Only Update This Object, Not the Contained Object** causes only the selected object to be updated to the latest version. Any objects further down in the tree structure are left as the current version.
 - ii. **Update this object and all containing objects** causes all objects in the entire tree represented by the management template or aspect to be updated to the latest version.
4. Click **Next**. A preview of the update is shown as an expanded tree view of the management template or aspect, where items that will be updated are labeled "*(old version > new version)* ", and items that will not be updated are labeled "*(current version)*".


If you want to keep certain items from being updated you can use the Preview screen exclude them:

- a. Select the item you want to exclude from the update.
- b. Click **Exclude From Update** . Although the versioning label for the item is not changed, the selected item is now excluded from the update as indicated by the label being followed by the **Exclude From Update**  icon.

Note: Exclude From Update is only activated for items to be updated, as indicated by the label "*(old version > new version)* .


- c. Click **Reload Preview** to apply the manual exclusions. The list is refreshed.
- To include a manually excluded item again, select it, and click **Include in Update**  followed by **Reload Preview**.
5. Click **Finish** to apply the update as shown in the preview.

How to Automatically Assign Management Templates or Aspects




1. Go to the Assignments & Tuning screen.
2. In the drop-down list at the top of the **Browse Views** tab of the View Browser (left pane), select the view for which you want to configure auto-assignment. The view and the first level of assigned COs are shown in the View Browser.
3. Select the view itself, which is the top level item labeled  <view name>. The list of assignments (at the top of the right-hand pane) now shows the auto-assignments for the view, as indicated by the header **Auto-Assignments**.

Note: Make sure that the view you selected for auto-assignment contains the root CI type of the management template or, in case an aspect is auto-assigned, the CI type of the aspect.

It is not necessary for the view to contain all CI types of the aspects contained in a management template to be auto-assigned.

4. Click **New Assignment...**  in the toolbar of the list of auto-assignments and select the appropriate option. The Assign and Deploy Wizard is shown.
5. In the Select Configuration Object page, click the **Name** of the management template or aspect that you want to automatically assign.

The list shows only the management templates that have a root CI type that appears in the view that you selected or, in case an aspect is auto-assigned, compatible aspects.
6. Select the **Version** of the management template or aspect that you want to assign.

Click **Next**.
7. In the Parameter page, specify a value for each parameter:
 - a. *Optional.* By default, the list shows only mandatory parameters. To see all parameters, click the  button. You can also click the  button to see expert parameters.
 - b. Select a parameter in the list, and then click the  button.
 - For standard parameters, the Edit Parameter dialog box opens.


Click **Value**, specify the value, and then click **OK**.
 - For instance parameters, the Edit Instance Parameter dialog box opens.

Add instance values, and then for each instance value, specify dependent parameter values. After you specify the instances and dependent parameter values, click **OK**.
In the Parameter page, click **Next**.
8. *Optional.* In the Configure Options page, if you do not want to enable the assignment immediately, clear the **Enable Assigned Objects** check box. You can then enable the assignment later.
9. Click **Finish**. The management template or aspect is added to the list of auto-assignments.




Operations Management creates deployment jobs to transfer the monitoring configuration to the nodes. After a policy template has been deployed, the BSM server specified in the **Default Virtual**

Gateway Server for Data Collectors URL infrastructure setting becomes the owner of the policy on the node.

How to Display an Assignment Report for a Management Template

1. Select the Management Template you want to create the report for.
2. Click **Generate Assignment Report**  in the Management Templates & Aspects (middle) pane.



The preconfigured Assignment Report is displayed.

You can use the **Expand** () and **Collapse** () buttons to expand or collapse the assigned CI information. The **Show** () button toggles between displaying all values or only the customized values.

You can display additional types of reports from the "[Assignments and Tuning](#)" on page 366 screen.


UI Reference

Add Existing Aspect

UI Element	
	Refresh: Reload the list of aspects that are available to nest within this aspect.
	Search: Specifying a string restricts the aspects list to aspects having the string in their name.
Name	The name of the aspect. The list shows only those aspects that can be assigned to the aspect's CI type or to more generic CI types.
Description	The description of the aspect.
OK	Add all selected aspects as nested aspects and close the dialog box. You can select multiple items by holding down the Ctrl or Shift key while selecting them.
Cancel	Close the dialog box without adding aspects.
Help	Help: Open the relevant help in a new browser window.


Assign and Deploy Wizard









—Configuration Item Screen

UI Element	Description
	Search: Specifying a string restricts the CI list to CIs having the string in their name.
Name	The name of a configuration item. The list contains only the types of

UI Element	Description
	<p>configuration for to which it is possible to deploy the selected management template, aspect, or policy template:</p> <ul style="list-style-type: none"> • For management templates, the list contains all CIs of the root CI type that have been discovered. • For aspects, the list can contain the following CIs: <ul style="list-style-type: none"> ▪ All CIs of the aspect's assigned CI types that have been discovered. ▪ Any CIs of the aspect's assigned CI types that have not been discovered but are flagged as Node Compatible. • For policy templates, the list can contain all CIs that have been discovered, and any CIs that have been flagged as Node Compatible.
Type	The type of configuration item.
Also Show CIs of Type Node (Node compatible aspects only)	When checked, all CIs compatible with the aspect are shown. When not checked, only CIs of the type with which the CI is node compatible are shown. For more information, see <i>Create Aspect Wizard/Edit Aspect Dialog—CI Type Screen/Tab</i> , UI element Node Compatible .

—Parameter Screen

UI Element	Description
Parameter List	<p>Lists all parameters in the management template^{Cpst}, aspect or policy template you are assigning to the configuration object.</p> <p>The toolbar provides the following controls:</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;">  </div> <div> <p>Edit: Open a dialog box that enables you to specify the value of the selected parameter for this assignment.</p> <ul style="list-style-type: none"> • For standard parameters, the Edit Parameter dialog box opens. <ul style="list-style-type: none"> ▪ If you select Value you must specify or select a value in the range that is valid for the parameter. The value you specify overrides any default values defined in the policy template, aspect, or management template. ▪ Select Use Default Value if you want to use the default value defined in the policy template, aspect, or management template. <p>Click OK to apply the values and close the Edit</p> </div> </div>

UI Element	Description
	<p>Parameter dialog box, or Cancel to close the dialog box without making changes.</p> <ul style="list-style-type: none"> For instance parameters, the Edit Instance Parameter dialog box opens. For details, see the UI Reference section for the Edit Instance Parameter dialog box. <p> Show Only Mandatory Parameters: Show or hide optional parameters in the table of parameters.</p> <p> Show Expert Parameters: Show or hide expert parameters in the table of parameters.</p> <p> Sort According to UI Order: Sort the list of parameters according to their UI order values (lowest to highest).</p> <p>The parameter list has the following columns:</p> <p>Target (Management Template only) The CI type of the aspect using the parameter.</p> <p>Defined In (Management Template only) The management template, aspect or policy template in which the parameter is defined.</p> <p>Name The name of the parameter.</p> <p>Value The value for this parameter in this assignment. If the value is dimmed, it is the default value.</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String <p>If the icon is dimmed, the value is read-only.</p> <p>If the invalid icon appears () , the parameter is mandatory, and you need to specify a value.</p> <p>Description A description of the parameter.</p>

UI Element	Description
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.

—Configure Options Screen






UI Element	Description
Enable Assigned Objects	If you do not want to enable an assignment immediately, clear the Enabled Assigned Objects check box for that assignment. You can then enable the assignment later using the Assignments & Tuning manager.

Create Management Template Wizard/Edit Management Template Dialog

—General Screen/Tab







UI Element	Description
Name	The name of the management template.
Description	A description of the management template.
ID	A unique identifier for the management template.
Version ID	A unique identifier for this version of the management template.
Version	The current version of the management template. The version is formatted as follows: <i><Major Version Number>. <Minor Version Number></i> The major version number is specified in the left-hand field, the minor version number in the right-hand field.
Change Log	Text that describes what is new or modified in this version of the management template.
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.






—Topology View Screen/Tab


UI Element	Description
Topology View	<p>The topology view that this management template is linked to. Select a topology view that contains all the CI types to be managed with this management template.</p> <p>You can select a topology view from the Topology View drop-down list, or click the ... button to open the Browse Views dialog box. If a suitable view does not exist, you can click the  button to go to the Modeling Studio and create a suitable view.</p>
Topology Map	<p>A graphical representation of the selected topology view.</p> <p>The toolbar provides the following controls:</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;">  </div> <div> <p>Refresh: Refresh the topology map.</p> </div> </div> <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="margin-right: 20px;">  </div> <div> <p>Zoom In: Enlarge the topology map.</p> </div> </div> <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="margin-right: 20px;">  </div> <div> <p>Zoom Out: Show a larger part of the topology map.</p> </div> </div> <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="margin-right: 20px;">  </div> <div> <p>Display Edge Labels: Switch the label associated with the arrows connecting the topology elements on and off.</p> </div> </div> <p>Layout Change the format of the topology view.</p>
CI Type	<p>The root CI type for assignment. To set the root CI type, click the node to which Operations Management should auto-assign the management template in the Topology View, or select it from the drop-down list. The selected root CI type is highlighted with a blue background.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Note: The root CI type should occur only once in the topology view to ensure consistency with respect to auto-assignments.</p> </div> <p>For more information about auto-assignment, see task <i>How to Configure Auto-Assignment of Management Templates and Aspects</i>.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Caution: If the management template already has aspects selected in the Aspects screen or tab, clicking a different root CI type causes the aspects to lose their targets. Therefore, only select a different root CI type if you are certain you want to change it, or else you'll have to delete and reselect the aspects manually in the Aspects screen or tab.</p> </div>

UI Element	Description
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.


—Aspects Screen/Tab




UI Element	Description
Topology View	<p>Shows the topology view for the management template.</p> <p>The toolbar provides the following controls:</p> <p> Refresh: Refresh the topology map.</p> <p> Zoom In: Enlarge the topology map.</p> <p> Zoom Out: Show a larger part of the topology map.</p> <p> Display Edge Labels: Switch the label associated with the arrows connecting the topology elements on and off.</p> <p>Layout Change the format of the topology view.</p> <p>When you click a node in the topology map all aspects matching the CI type of the selected node are listed in the list of available aspects (upper list on the right).</p>
List of Available Aspects (upper list on the right)	<p>Lists all aspects matching the CI type selected in the Topology View.</p> <p>To add aspects to the management template:</p> <ol style="list-style-type: none"> 1. Select the aspect to be added. 2. Click . The selected aspect is added to the list of selected aspects (lower list on the right). <p>The toolbar provides the following controls:</p> <p>Information bar above toolbar Lists all aspects compatible with the CI Type selected in the topology view.</p> <p> Search: Specifying a string restricts the aspect list to aspects having the string in their name.</p> <p>The list has the following columns:</p>




UI Element	Description
	<p>Name The name of the aspect.</p> <p>Description The description of the aspect.</p> <p>The toolbar below the list provides the following controls:</p> <p> Add the aspect selected in the list of available aspects (upper list on the right) to the management template.</p> <p> Remove the aspect selected in the list of selected aspects (lower list on the right) from the management template.</p>
List of Selected (lower list on the right)	<p>Lists all aspects contained in the management template.</p> <p>To assign aspects to the management template:</p> <ol style="list-style-type: none"> 1. Click Add Aspect and select or create the aspects to be assigned (for details see below). The aspects are added to the list. 2. If you need to change the used version of an aspect, select the desired version in its Version column. 3. Assign target CI types by selecting all aspects to have the same target CI type, and clicking a CI of the desired target CI type in the topology map. The CI type of the clicked CI is entered in the Target CI Type column of all selected aspect. <p>To remove an aspect from the template:</p> <ol style="list-style-type: none"> 1. Select the aspect to be removed. 2. Click . The selected aspect is removed from the list. <p>The toolbar provides the following controls:</p> <p> Refresh: Reload the list of aspects.</p> <p> Edit Aspect: Open the Edit Aspect dialog box for the selected aspect.</p> <p>The list has the following columns:</p> <p>Name The name of a contained aspect.</p>

UI Element	Description
	<p>Version The version of the nested aspect.</p> <p>To change to a different version, select the desired version from the drop-down list.</p> <p>Note: Operations Management does not automatically update aspect versions. If new versions of aspects are available, either use the Update to Latest for the parent management template, or update the version manually. See also "Configuring Management Templates" on page 17, task <i>How to Update a Management Template After a Management Pack Update</i>.</p> <p>Target The CI type the aspect can be assigned to. This is also the CI type used to match CIs to the topology view for auto-assignment.</p> <p>Note: This column cannot be empty for any selected aspect. Empty fields are marked with the error icon .</p>
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.

—Parameters Screen/Tab

UI Element	Description
List of Parameters	<p>Lists all parameters defined in the policy templates assigned to the aspects contained in the management template or aspect.</p> <p>The toolbar provides the following controls:</p> <p> Edit/Combine...:</p> <ul style="list-style-type: none"> • To Edit a Parameter <ol style="list-style-type: none"> a. Select a single parameter.

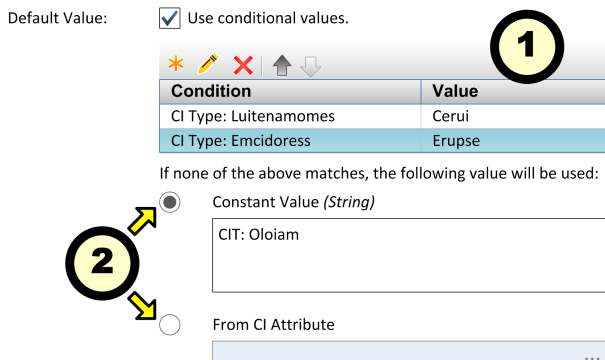
UI Element	Description
	<p>b. Click the Edit/Combine button . The Edit/Combine Parameters Dialog Box opens, where you can edit parameter settings.</p> <div data-bbox="852 401 1357 577" style="background-color: #f0f0f0; padding: 5px;"> <p>Note: Changes made here are applied at aspect level. They overrule the definitions in the policy template, but do not change the policy template itself.</p> </div> <ul style="list-style-type: none"> • To Combine Parameters <ol style="list-style-type: none"> a. Select a number of parameters of the same type (such as string values or numeric values). b. Click the Edit/Combine button . The Edit/Combine Parameters Dialog Box opens, where you can specify the parameter settings for the new parameter that is the combination of the selected parameters. <div data-bbox="852 940 1357 1461" style="background-color: #f0f0f0; padding: 5px;"> <p>Note: You can combine parameters only if they meet the following criteria:</p> <ul style="list-style-type: none"> ○ Parameters to be combined must be of the same type. ○ Parameters to be combined must not have conditional values. ○ The range of allowed values of numeric parameters to be combined must overlap. ○ Enumeration parameters to be combined must have at least one common value. </div> <p> Uncombine/Undo Changes:</p> <p>Undo parameter changes and combinations for all selected parameters.</p> <ul style="list-style-type: none"> • If any parameters that are not combined parameters are selected, Uncombine/Undo Changes undoes all changes that have been made to the selected parameters.






UI Element	Description
	<ul style="list-style-type: none"> If any combined parameters are selected, Uncombine/Undo Changes restores the single parameters making up the selected combined parameters, <i>and</i> undoes any changes that were made to them, including changes made before the parameters were combined. <p> Show Parameter Details: Expand the table of parameters to show the extra columns Defined In, Description, Type and Instance Parameter.</p> <p> Refresh: Reload the list of parameters.</p> <p> Search: Specifying a string restricts the parameter list to parameters having the string in their name.</p> <p>The list has the following columns:</p> <p>I Instance Parameter: ✓ indicates that the parameter is an instance parameter, — indicates it is not.</p> <p>C Combined Parameter: ✓ indicates that the parameter is a combined parameter or that the parameter is changed, — indicates it is not.</p> <p>UI Order The position of this parameter in the list of parameters.</p> <p>Name The name of the parameter. The list initially contains all the parameters from the policy templates and nested aspects that this aspect includes. However, you can edit parameters at aspect level and give them alternative names. You can also specify a name when you combine parameters.</p> <p>Defined In (detail) The name of the policy template or aspect that contains the parameter. If the parameter was combined in this aspect, it is the name of this aspect. If the parameter is part of a nested aspect, it is the name of the nested aspect.</p> <p>Description (detail) The description of the parameter.</p>

UI Element	Description
	<p>Type(detail) The type of value that you can specify for the parameter. The variable type can be a string, numeric, an enumeration (of several options), or a password.</p> <p>Instance Parameter (detail) The name of the instance parameter that this parameter depends on (if any).</p> <p>Target (Management Template only) The CI type of the management template's root CI.</p> <p>Default Value The default value of the parameter. Parameters can have a default value that is defined in the policy template. You can also set a default value at the management template or aspect level, which then overrides the default in the policy template.</p>
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.

Edit/Combine Parameters Dialog

UI Element	Description
Name	The name of the parameter. The parameter list contains parameters defined in any aspect in the management template or aspect structure. You can review the structure of a management template or aspect in the Structure tab of the Details pane.
Instance Parameter	<i>Read-only.</i> If the checkbox is checked the parameter is an instance parameter, if it is unchecked it is not.
Description	A description of the parameter.
UI Order	The position of this parameter in the list of parameters.
Flags	<p>Provides the following options:</p> <ul style="list-style-type: none"> • Mandatory: <i>Read-only.</i> If the checkbox is checked the parameter is mandatory, if it is unchecked it is not. <p>Read Only: Select this check box to prevent changes to the</p>

UI Element	Description
	<p>parameter value when the management template is assigned to a configuration item. If you select this check box, the default value is used when the management template is assigned.</p> <ul style="list-style-type: none"> • Expert Setting: Select this check box to hide the parameter by default when the management template is assigned to a configuration item. Users can choose whether to show expert settings when they make an assignment. • Hidden: Select this check box to hide the parameter during assignment to a configuration item. If you select this check box, the default value is used when the management template is assigned.
<p>Default Value</p>	<p>The default value of the parameter.</p> <p>The default value used by Operations Management observes the following priorities:</p> <ul style="list-style-type: none"> • A default value defined at aspect level overrides any corresponding default value in a policy template. • A default value defined at management template level overrides any corresponding default value defined at aspect level (and therefore any corresponding default value defined in a policy template). <p>A default value is assigned using the control in the default value group shown in the following figure for a parameter using conditional values:</p>  <ol style="list-style-type: none"> 1. If any conditional values exist in the conditional value list 1, the conditions are evaluated in the order in which they are listed, and the value corresponding to the first condition evaluating to true is used as default value. 2. If no conditions exist or none evaluate to true a constant value or the value of a CI attribute is used as default value, depending on which of these is selected with the radio button 2. <p>The following table describes how to use the controls in the default value group:</p>



UI Element	Description
	<p>Use Conditional Values After checking this checkbox the conditional value list ① is shown, with the following UI elements:</p> <ul style="list-style-type: none">  New Item: Open the Edit Conditional Value Dialog Box, which is used to define a new condition.  Edit Item...: Open the Edit Conditional Value Dialog Box, which is used to edit the selected condition.  Delete Item: Delete the selected condition.  Move Up: Increase the priority of the condition.  Move Down: Decrease the priority of the condition. <p>Condition A semicolon-separated string listing all expressions used in the condition.</p> <p>Value The value used as default when the condition is the first to evaluate to true.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: At management template level you cannot add, remove, or rearrange conditions, but you can change the values used to evaluate them.</p> </div> <p>Constant Value When selected, the value specified in the text box is used as default value if no conditional values are defined, or if none of the conditional values evaluates to true.</p> <p>From CI Attribute When selected and a CI attribute is selected, the value of the selected attribute is used as default value if no conditional values are defined, or if none of the conditional values evaluates to true.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: The value used to evaluate this condition is always the value of the aspect CI from where the value will be resolved, even if it is overwritten on management template level.</p> </div> <p>To use a default value from a CI attribute:</p>












UI Element	Description
	<ol style="list-style-type: none"> 1. Select the From CI Attribute radio button. 2. Click the ... button to the right of the input field. The Available Attributes dialog box is shown. 3. The Attribute CI Type list contains all CI types assigned in the CI Types screen for the current aspect or any contained and nested aspects. Select the appropriate attribute(s).

Edit Conditional Value Dialog Box

UI Element	Description
Constant Value	A specific value to use when the condition is true. You can type or select a value (depending on the type of parameter).
From CI Attribute	<p>A CI attribute to use when the condition is true. To choose a CI attribute, click the ... button. The Available Attributes dialog box opens. If the aspect can be assigned to more than one CI type, select the Attribute CI Type and then select a CI attribute. If the aspect can be assigned to only one CI type, it is not necessary to select the Attribute CI Type first.</p> <p>If you specify a CI attribute, Operations Management sets the parameter value automatically during the deployment of the underlying policy templates, using the actual value of this attribute from the CI.</p>






Edit Instance Parameter Dialog Box

UI Element	
Instance Values List	<p>The toolbar provides the following controls:</p> <div style="display: flex; flex-direction: column; gap: 10px;"> <div data-bbox="573 1339 1373 1541">  <p>Create Instance Parameter: Open the Edit Parameter Dialog Box. To create a new value, select Value and specify a value in the text box. Click OK to close the dialog box and add the new value to the Instance Values list, or click Cancel to close the dialog box without making changes.</p> </div> <div data-bbox="573 1566 1373 1768">  <p>Edit Instance Parameter: Open the Edit Parameter Dialog Box. To change the instance value, edit the value in the text box. Click OK to close the dialog box and replace the value in the Instance Value list with the new value, or click Cancel to close the dialog box without making changes.</p> </div> </div>

UI Element									
	<div style="display: flex; flex-direction: column; gap: 10px;"> <div style="display: flex; align-items: flex-start;">  <p>Delete Instance Parameter: Delete the selected instance value.</p> </div> <div style="display: flex; align-items: flex-start;">  <p>Move Up: Move the selected instance value up in the list.</p> </div> <div style="display: flex; align-items: flex-start;">  <p>Move Down: Move the selected instance value down in the list.</p> </div> </div>								
Dependent Values List	<p>The Dependent Value list lists the dependent values for the instance value selected in the Instance Values list.</p> <p>The toolbar provides the following controls:</p> <div style="display: flex; flex-direction: column; gap: 10px;"> <div style="display: flex; align-items: flex-start;">  <p>Edit... Show the Edit Parameter Dialog Box to specify a value for the parameter.</p> </div> <div style="display: flex; align-items: flex-start;">  <p>Show Only Mandatory Parameters: Show or hide optional parameters.</p> </div> <div style="display: flex; align-items: flex-start;">  <p>Show/Hide Expert Parameters: Show or hide expert parameters.</p> </div> <div style="display: flex; align-items: flex-start;">  <p>Sort According to UI Order: Sort the list of dependent values according to the order as shown in the Operations Management console.</p> </div> </div> <p>The list has the following columns:</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Defined In</td> <td>Policy template containing the definition of the value.</td> </tr> <tr> <td>Target CI Type</td> <td>Name of the CI type to which this value applies..</td> </tr> <tr> <td>Name</td> <td>The name of the dependent value.</td> </tr> <tr> <td>Value</td> <td>The value of the dependent value.</td> </tr> </table> <p>If the value is dimmed, it is the default value.</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none"> •  Enumeration (of several options) •  Number •  Password •  String 	Defined In	Policy template containing the definition of the value.	Target CI Type	Name of the CI type to which this value applies..	Name	The name of the dependent value.	Value	The value of the dependent value.
Defined In	Policy template containing the definition of the value.								
Target CI Type	Name of the CI type to which this value applies..								
Name	The name of the dependent value.								
Value	The value of the dependent value.								

UI Element	
	<p>If the icon is dimmed, the value is read-only.</p> <p>If the invalid icon appears (❌) when you select the value, the value is mandatory needs to be specified.</p> <p>Description A description of the dependent value.</p>
OK	<p>Add all selected aspects as nested aspects and close the dialog box.</p> <p>You can select multiple items by holding down the Ctrl or Shift key while selecting them.</p>
Cancel	Close the dialog box without making changes.

Reports Window

UI Element	Description
	Expand all: Expand all CIs.
	Collapse all: Collapse all CIs.
	Filter On/Off: Toggle between Show Customized Values Only and Show All Values .
	Expand Category: Expand the category to show the attributes contained in it.
	Collapse Category: Collapse the category to hide the attributes contained in it.





Update to Latest Wizard

—Options Screen

UI Element	Description
Update to the Latest Major and Minor Version	Allow the system to update both major and minor version numbers to the latest version.
Update to the Latest Minor Version, Keeping All Major Versions	Allow changes to the minor version number only. If the latest version of an item has a higher major number than the current item, the new version will have lowest available minor number for the same major number as the current version.
Only Update This Object, Not the Contained Object	Update the version of the selected object only, but not the object further down in the tree structure.

UI Element	Description
Update This Object and All Containing Objects, Recursively	Update all objects in the entire tree.
Next	Go to the <i>Preview</i> screen.
Cancel	Close the wizard without making any changes.
Help	Open the relevant help in a new browser window.

—Preview Screen

UI Element	Description
	Expand All: Expand the structure element to show the entire tree of contained elements.
	Collapse All: Collapse the entire structure tree.
	Include in Update: Force a manually excluded policy template to be included in the update.
	Exclude from Update: Force a policy template to be excluded from the update.
Reload Preview	Recalculate the version numbers to be applied and refresh the preview after manually excluding or re-including policy templates
Back	Go back to the <i>Options</i> screen.
Finish	Apply all proposed changes and close the wizard.
Cancel	Close the wizard without making any changes.
Help	Open the relevant help in a new browser window.

Configuring Aspects

Aspects are containers for policy templates, instrumentation, and parameters. Each aspect provides the ability to monitor a configuration item (CI). Aspects can be designed to work independently of other aspects, and can be included in multiple management templates. You can also nest one or more aspects within another aspect to avoid duplication and make them easier to maintain.

Learn More

Nested Aspects

In some cases, you may want to create an aspect that extends existing aspects. In these cases, you can nest one or more aspects within another aspect.

For example, you may want to create two reusable aspects that define monitoring configurations for servers:

- **Basic server monitoring**

An aspect that contains policy templates for monitoring ten server performance metrics.

- **Detailed server monitoring**

An aspect that provides the same monitoring configuration as the basic server monitoring aspect, plus additional policy templates for monitoring a further twenty server performance metrics.

In the above example, you could first configure the basic server monitoring aspect, and then nest it within the detailed server monitoring aspect. By nesting one aspect within another, you can avoid duplication and make aspects easier to maintain.

When you create an aspect, you must select one or more CI types to which the aspect can be assigned. Nested aspects must be configured to be assignable to either the same or more generic types of CI. An aspect for the CI type `Computer`, for example, may contain nested aspects for the CI type `Computer` or the more generic CI type `Node`.

Parameterization

Aspects use parameters, which correspond to variables in policy templates, to control how CIs of a certain type are monitored. The value of the parameter is set by an operator for the CI type the aspect is assigned to. The corresponding variable is set and passed to the CI according to the definition in the policy template.

A parameter decouples a value from its physical definition in a policy template. This has the following advantages:

- A value can be set at deployment time in the application, rather than having to change hard-coded variables in a policy template.
- A parameter can be deployed conditionally so the value it represents can be used in multiple situations, but needs to be set only once.
- Parameter values can be set at various levels, allowing defaults to be used on the lower levels. This can greatly reduce the number of values to be set by an operator.
- It is possible to override any configured values by tuning assignments when the monitoring process is started.
- Parameters can be combined to reuse a value occurring multiple times, removing the need to specify values repetitively. A typical example is a password parameter that is used by several policy templates in an aspect to log on to the same service.

Conditional Deployment

You can use the following criteria for the conditional deployment of a policy template:

- *OS type*

You can configure a policy template to be deployed for specific operating systems. Conditional deployment of several policy templates in a single aspect allows for creating platform-neutral aspects.

As an example, consider MySQL, which can run on several platforms. An aspect monitoring process health is configured with conditionally deployed policy templates for Windows, Linux and Solaris. When the aspect is assigned to a MySQL CI that is hosted on a Linux node, Operations Management automatically deploys the Linux variant of the policy template.

- *CI type*

You can configure a policy template to be deployed for specific CI types. Conditional deployment allows you to create aspects monitoring CIs governed by the same parameters, but having CI type-specific policy templates, enabling Operations Management to automatically select the correct policy template for the CI type of a CI when the aspect is assigned to it.

- *CI attribute*

You can configure a policy template to be deployed when a CI attribute has a specific value. Conditional deployment allows you to create aspects that are assigned only to CIs for which certain attributes have a specific value.

Specifying a Default Value

Parameter values are set in the monitoring agents when a policy template is deployed. Parameter values can be defined and changed in the following places:

- The policy template contains a default value for the parameter.
- You can override any policy template defaults at aspect level in the aspect's policy template configuration.
- You can override any aspect-level values at management template level in the management template's aspect configuration.
- You can override any management template- or aspect-level value when deploying a management template or aspect, unless the parameter is configured as `hidden` or `read-only`.

Combining Parameters

You can combine several parameters to create a single combined parameter. The value of a combined parameter is passed to all its constituent parameters, enabling using a single value definition for multiple CIs, making it easier to assign and maintain the management template or aspect using it.

Example: Consider an aspect used to manage MySQL performance which contains several policy templates using the username and password to access MySQL. In this case it is useful to combine the parameters passing the credentials at aspect level, so that they can be defined in one go when the aspect is assigned.


For details, see task Combining Parameters and the UI Reference section for the Edit/Combine Parameters dialog box.

Tasks



How to Create or Edit Aspects

1. In the Configuration Folders pane, select the configuration folder in which you want to create a

new aspect, or create a new folder. For details about creating and managing configuration folders, see "Configuration Folders" on page 13.

2. To edit an existing aspect, select it in the list of aspects in the Management Templates & Aspects pane and click the Edit Item button . The Edit Aspect dialog box opens on the General page.

To create a new aspect, click the **New** button  in the Management Templates & Aspects pane and select  **Create Aspect**. The Edit Aspect wizard opens on the General page.


Note: Do not use the **New** button  to create a new *version* of an existing aspect rather than creating a new aspect from scratch. To create a new version of an existing aspect, use the **Edit** button , specify a new version number in the General page, make any required changes, and click **OK**.

3. The General page allows you to enter general information about the aspect.


Note: Required fields are marked with a red asterisk *****; until all the required fields have been filled in, the **Next** button is inactive. Fields filled in by the system are marked with a blue background. These fields do not require manual interaction.

- a. Enter a unique **Name** for the aspect.
- b. *Optional.* Enter a **Description** for the aspect.
- c. If required, set the major and minor version numbers for the aspect. By default, the major version number of the latest version is selected for new aspects.
- d. *Optional.* Enter your motivation for creating the new aspect in the **Change Log** field.

Click the **CI Type** tab or **Next** to accept the values, generate the ID and go to the CI Type page.

4. Each aspect enables you to monitor one specific characteristic of one or more types of configuration items having the same characteristic. In the CI Types page, select one or more **Available CI Type(s)** to which you need to be able to assign the aspect, and click the  button. The selected CI types are added to the list of assigned CI types. You can select multiple items by holding down the **Ctrl** or **Shift** key while selecting them. If you need the aspect to be assignable to CIs of the type node, check **Node Compatible**.





Click the **Instrumentation** tab or **Next** to accept the values and go to the Instrumentation page.

5. In the Instrumentation page, click the **Add Instrumentation** button  to add instrumentation to the aspect. The Add Instrumentation dialog box opens, which enables you to select the instrumentation that you want to add.

Instrumentation includes scripts and executables executed by the HP Operations Agent as defined in policies for managed nodes that have the agent installed on them.


Click the **Aspects** tab or **Next** to accept the values and go to the Aspects page.


6. *Optional.* The Aspects page allows you to include nested aspects.

- To create a new aspect from scratch, click the **Add Aspect** button  and select  **Add New Aspect**. The Create Aspect wizard opens. Create a new aspect in the same way as the parent aspect. After clicking **Finish** at the end of the process, the Create Aspect wizard closes and the new aspect is added to the list of nested aspects.
- To include an aspect created earlier, click the **Add Aspect** button , and select  **Add Existing Aspect**. The Add Existing Aspect dialog box opens. To add and nest an existing aspect:
 - i. For those aspects to be added, select the appropriate version in the **Version** drop-down list.
 - ii. Create or select the aspect(s) that you want to nest within this aspect from the list. You can select multiple aspects by holding down the **Ctrl** or **Shift** key while selecting them.
 - iii. Click **OK** to accept the aspects and close the Add Existing Aspect dialog box.

Click the **Policy Templates** tab or **Next** to accept the values and go to the Policy Templates page.

7. The Policy Templates page allows you to assign policy templates defining the parameters and instrumentation needed to monitor the configured CI types.

To assign a policy template, Click the **Add Policy Template** button . The Add Policy Template to Aspect dialog box opens, listing all policy templates installed on the system.

- To create a new policy template from scratch, click the **New** button . The Create New Policy Template wizard opens. Create a new policy template as described in "[Policy Templates](#)" on page 71. After clicking **Finish** at the end of the process, the Create New Policy Template wizard closes and the new policy template is added to the list of policy templates.
- To include policy templates created earlier:
 - i. Select all policy templates you want to assign to the aspect. You can select multiple policy templates by holding down the **Ctrl** or **Shift** key while selecting them.
 - ii. Click **OK** to accept the values and return to the Policy Templates page of the wizard.
- To make changes to a policy template, click the **Edit Item** button and select the appropriate option. For more information about changing policy templates, see "[Policy Templates](#)" on page 71.

Click the **Parameters** tab or **Next** to accept the values and go to the Parameters page.

8. The Parameters page lists all parameters defined in the policy templates you added in the Add Policy Templates page.



Sometimes it is useful to change parameter behavior:


- You can set the value of a parameter at aspect level.
- You can combine parameters (see task *How to Combine Parameters*).
- You can undo changes or split combined parameters.

For details, see the UI Reference section on the Edit/Combine Parameters dialog box and the Learn More section on Aspect Parameterization.

9. Click **OK** or **Finish** to save the values in all screens and close the dialog box. The changed or new aspect is shown in the Management Templates & Aspects pane.

How to Edit or Combine Parameters

To edit a parameter, select a *single* parameter to be edited and click the  button. To combine parameters into a single new parameter, select *several* parameters to be combined while holding down the **Ctrl** or **Shift** key and click the  button. The Edit/Combine Parameters dialog box opens, allowing you to specify the following information for the existing or combined parameter:

1. If necessary, type a **Name** for the parameter.
2. *Optional.* Specify a **Description**.
3. *Optional.* Specify a **Default Value**. You can set the default value in one of the following ways:
 - Specify a conditional value by checking **Conditional value** and clicking the **New** button  to open the Edit Conditional Value dialog box.
 - Set a specific value by selecting **Constant Value** and selecting a value from the list.
 - Obtain a value corresponding to a CI attribute by selecting **From CI Attribute** and then browse for a CI attribute. When you specify a CI attribute, Operations Management sets the parameter value automatically during deployment of the policy templates, using the actual value of this attribute from the aspect's CI. You can also set conditional parameter values [here](#).

If you specify a conditional value but none of the defined conditions apply the constant value or the value from the CI attribute (whichever is selected) is used.
4. *Optional.* Set the **Read Only**, **Expert Setting**, and **Hidden** options as appropriate.
 - Checking **Read Only** prevents changes to the parameter value when the aspect is assigned to a configuration item.
 - Checking **Hidden** also prevents changes, but additionally makes the parameter invisible.
 - Checking **Expert Settings** enables the expert settings when assigning the parameter. For more information, see task *How to Deploy Aspects* below.
5. Click **OK** to combine the parameters and close the Edit/Combine Parameters dialog box.





How to Deploy Aspects

Note: To start monitoring an application or service you can assign an aspect directly to a CI. If you have a Monitoring Automation for Composite Applications add-on license, however, HP recommends to deploy the management template containing the aspect instead. For details about deploying management templates, see "[Configuring Management Templates](#)" on [page 17](#) task *How to Deploy Management Templates*.

Users who have not installed the add-on license and developers may choose to deploy aspects anyway. The Assign and Deploy Wizard is described in "[Configuring Management Templates](#)" on [page 17](#), UI Reference section *Assign and Deploy Dialog Box*, but omitted from the UI

reference section in this topic. You can also deploy aspects in the "Assignments and Tuning" on page 366 screen.

How to Display an Assignment Report


1. Select the aspect you want to create the report for.
2. Click the **Report** button  in the Management Templates & Aspects (middle) pane. A new browser window listing all management templates and aspects opens.
3. Select the management template or aspect for which you want to create the report. The assignment report is displayed.
 - Use the **Expand**  and **Collapse**  buttons to expand or collapse the list of assigned CIs.
 - Use the **Show** button  to switch between all values and customized values only being displayed.

How to Update a Management Template or Aspect

If you make changes to policy templates or aspects (for example when updating a Management Pack or customizing a policy template or aspect), the policy templates and aspects it contains are added to the database as new versions. Management templates and aspects reference specific versions of aspects, so Management Pack updates require all management templates and aspects referencing the updated aspects and policy templates to be updated as well.


Operations Management features an Update to Latest wizard that helps you to update your management templates and aspects automatically. The Update to Latest wizard supports several different ways of versioning the updated items. Your use case determines which way works best in a particular situation.

To update all items in a management template or aspect to the latest version in the database:



1. Browse to the appropriate configuration folder and select the management template or aspect to be updated in the *Management Templates & Aspects* pane. Select a single management template or aspect; updates can only be done on single management templates or aspects.
2. Click **Update to Latest** . The Update to Latest wizard opens.
3. Set the following options to suit your use case:
 - a. Versioning alternatives:
 - i. **Update to the latest major and minor version** causes both major and minor versions to reflect the latest version.
 - ii. **Update to the Latest Minor Version, Keeping All Major Versions** limits changes to the minor version number only. If the latest version of an item has a higher major number than the current item, the new version will have the lowest available minor number for the same major number as the current version.

For example, if the current version is 1.5 and there are two newer versions with version numbers 1.6 and 2.1:


- i. **Update to the latest major and minor version** will update the version number to 2.1.

- ii. **Update to the Latest Minor Version, Keeping All Major Versions** will update the version number to 1.6.
 - b. Scope of update:
 - i. **Only Update This Object, Not the Contained Object** causes only the selected object to be updated to the latest version. Any objects further down in the tree structure are left as the current version.
 - ii. **Update this object and all containing objects** causes all objects in the entire tree represented by the management template or aspect to be updated to the latest version.
4. Click **Next**. A preview of the update is shown as an expanded tree view of the management template or aspect, where items that will be updated are labeled "*(old version > new version)* ", and items that will not be updated are labeled "*(current version)*".


If you want to keep certain items from being updated you can use the Preview screen exclude them:

- a. Select the item you want to exclude from the update.
- b. Click **Exclude From Update** . Although the versioning label for the item is not changed, the selected item is now excluded from the update as indicated by the label being followed by the **Exclude From Update**  icon.

Note: Exclude From Update is only activated for items to be updated, as indicated by the label "*(old version > new version)* .


- c. Click **Reload Preview** to apply the manual exclusions. The list is refreshed.
- To include a manually excluded item again, select it, and click **Include in Update**  followed by **Reload Preview**.
5. Click **Finish** to apply the update as shown in the preview.

How to Automatically Assign Management Templates or Aspects

1. Go to the Assignments & Tuning screen.
2. In the drop-down list at the top of the **Browse Views** tab of the View Browser (left pane), select the view for which you want to configure auto-assignment. The view and the first level of assigned COs are shown in the View Browser.
3. Select the view itself, which is the top level item labeled  <view name>. The list of assignments (at the top of the right-hand pane) now shows the auto-assignments for the view, as indicated by the header **Auto-Assignments**.

Note: Make sure that the view you selected for auto-assignment contains the root CI type of the management template or, in case an aspect is auto-assigned, the CI type of the aspect.




It is not necessary for the view to contain all CI types of the aspects contained in a management template to be auto-assigned.

4. Click **New Assignment...**  in the toolbar of the list of auto-assignments and select the appropriate option. The Assign and Deploy Wizard is shown.
5. In the Select Configuration Object page, click the **Name** of the management template or aspect that you want to automatically assign.

The list shows only the management templates that have a root CI type that appears in the view that you selected or, in case an aspect is auto-assigned, compatible aspects.

6. Select the **Version** of the management template or aspect that you want to assign.

Click **Next**.

7. In the Parameter page, specify a value for each parameter:
 - a. *Optional.* By default, the list shows only mandatory parameters. To see all parameters, click the  button. You can also click the  button to see expert parameters.
 - b. Select a parameter in the list, and then click the  button.
 - For standard parameters, the Edit Parameter dialog box opens.
Click **Value**, specify the value, and then click **OK**.
 - For instance parameters, the Edit Instance Parameter dialog box opens.
Add instance values, and then for each instance value, specify dependent parameter values. After you specify the instances and dependent parameter values, click **OK**.



In the Parameter page, click **Next**.

8. *Optional.* In the Configure Options page, if you do not want to enable the assignment immediately, clear the **Enable Assigned Objects** check box. You can then enable the assignment later.
9. Click **Finish**. The management template or aspect is added to the list of auto-assignments.

Operations Management creates deployment jobs to transfer the monitoring configuration to the nodes. After a policy template has been deployed, the BSM server specified in the **Default Virtual Gateway Server for Data Collectors URL** infrastructure setting becomes the owner of the policy on the node.

UI Reference

Add Existing Aspect Dialog Box





UI Element	
	Refresh: Reload the list of aspects that are available to nest within this aspect.
	Search: Specifying a string restricts the aspects list to aspects having the string in their name.
Name	The name of the aspect. The list shows only those aspects that can be assigned to the aspect's CI type or to more generic CI types.


UI Element	
Description	The description of the aspect.
OK	Add all selected aspects as nested aspects and close the dialog box. You can select multiple items by holding down the Ctrl or Shift key while selecting them.
Cancel	Close the dialog box without adding aspects.
Help	Help: Open the relevant help in a new browser window.

Add Instrumentation Dialog Box


UI Element	Description
Name	The name of an instrumentation category that is installed on the system.
Description	A description of the instrumentation category.
Refresh	Retrieve the installed instrumentation from the system and refresh the list.
OK	Add all selected instrumentation to the aspect. You can select multiple items by holding down the Ctrl or Shift key while selecting them.
Cancel	Close the dialog box without adding any instrumentation.

Add Policy Template to Aspect Dialog Box


UI Element	Description
	Refresh: Reload the list of policy templates that are available to add to this aspect.
	<p>New...: Provides the following options:</p> <ul style="list-style-type: none">  Add New Policy Template: Open the Select Type for New Policy Template Dialog Box, which enables you to select the policy template type for the policy template that you want to create. Click OK to open the policy template editor and create a new policy template in normal mode.  Add New Policy Template (Raw Mode): Open the Select Type for New Policy Template Dialog Box, which enables you to select the policy template type for the policy template that you want to create. Click OK to open the policy template editor and create a new policy template using raw mode. <p>The following policy template types are available:</p>








UI Element	Description
	<ul style="list-style-type: none"> • Arcsight Logger • ConfigFile • Flexible Management • Logfile Entry • Measurement Threshold • Node Info • Open Message Interface • Scheduled Task • Service Auto-Discovery • Service/Process Monitoring • SiteScope • SNMP Interceptor • Windows Event Log • Windows Management Interface • XML File
	Search: Specifying a string restricts the list of policy templates to policy templates having the string in their name.
Name	Name of the policy.
OS Type	Types of operating system with which the policy is compatible.
Description	The description of the policy.
Type	The policy template type.
OK	<p>Add all selected policy templates and close the dialog box.</p> <p>You can select multiple items by holding down the Ctrl or Shift key while selecting them.</p>
Cancel	Close the dialog box without adding policy templates.
Help	Help: Open the relevant help in a new browser window.

Assign and Deploy Wizard
—Configuration Item Screen

UI Element	Description
	Search: Specifying a string restricts the CI list to CIs having the string in their name.
Name	<p>The name of a configuration item. The list contains only the types of configuration for to which it is possible to deploy the selected management template, aspect, or policy template:</p> <ul style="list-style-type: none"> • For management templates, the list contains all CIs of the root CI type that have been discovered. • For aspects, the list can contain the following CIs: <ul style="list-style-type: none"> ▪ All CIs of the aspect's assigned CI types that have been discovered. ▪ Any CIs of the aspect's assigned CI types that have not been discovered but are flagged as Node Compatible. • For policy templates, the list can contain all CIs that have been discovered, and any CIs that have been flagged as Node Compatible.
Type	The type of configuration item.
Also Show CIs of Type Node (Node compatible aspects only)	When checked, all CIs compatible with the aspect are shown. When not checked, only CIs of the type with which the CI is node compatible are shown. For more information, see <i>Create Aspect Wizard/Edit Aspect Dialog—CI Type Screen/Tab</i> , UI element Node Compatible .

—Parameter Screen

UI Element	Description
Parameter List	<p>Lists all parameters in the management template^{Cpst}, aspect or policy template you are assigning to the configuration object.</p> <p>The toolbar provides the following controls:</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;">  </div> <div> <p>Edit: Open a dialog box that enables you to specify the value of the selected parameter for this assignment.</p> <ul style="list-style-type: none"> • For standard parameters, the Edit Parameter dialog box opens. <ul style="list-style-type: none"> ▪ If you select Value you must specify or select a value in the range that is valid for the parameter. The value you specify overrides any default values defined in the policy template, aspect, or management template. ▪ Select Use Default Value if you want to use </div> </div>

UI Element	Description								
	<p>the default value defined in the policy template, aspect, or management template.</p> <p>Click OK to apply the values and close the Edit Parameter dialog box, or Cancel to close the dialog box without making changes.</p> <ul style="list-style-type: none"> For instance parameters, the Edit Instance Parameter dialog box opens. For details, see the UI Reference section for the Edit Instance Parameter dialog box. <p> Show Only Mandatory Parameters: Show or hide optional parameters in the table of parameters.</p> <p> Show Expert Parameters: Show or hide expert parameters in the table of parameters.</p> <p> Sort According to UI Order: Sort the list of parameters according to their UI order values (lowest to highest).</p> <p>The parameter list has the following columns:</p> <table border="0"> <tr> <td data-bbox="573 1018 743 1115">Target (Management Template only)</td> <td data-bbox="773 1018 1295 1045">The CI type of the aspect using the parameter.</td> </tr> <tr> <td data-bbox="573 1142 743 1239">Defined In (Management Template only)</td> <td data-bbox="773 1142 1268 1203">The management template, aspect or policy template in which the parameter is defined.</td> </tr> <tr> <td data-bbox="573 1266 646 1293">Name</td> <td data-bbox="773 1266 1081 1293">The name of the parameter.</td> </tr> <tr> <td data-bbox="573 1320 646 1348">Value</td> <td data-bbox="773 1320 1333 1381">The value for this parameter in this assignment. If the value is dimmed, it is the default value.</td> </tr> </table> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String <p>If the icon is dimmed, the value is read-only.</p>	Target (Management Template only)	The CI type of the aspect using the parameter.	Defined In (Management Template only)	The management template, aspect or policy template in which the parameter is defined.	Name	The name of the parameter.	Value	The value for this parameter in this assignment. If the value is dimmed, it is the default value.
Target (Management Template only)	The CI type of the aspect using the parameter.								
Defined In (Management Template only)	The management template, aspect or policy template in which the parameter is defined.								
Name	The name of the parameter.								
Value	The value for this parameter in this assignment. If the value is dimmed, it is the default value.								

UI Element	Description
	<p>If the invalid icon appears (✘), the parameter is mandatory, and you need to specify a value.</p> <p>Description A description of the parameter.</p>
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.

—Configure Options Screen

UI Element	Description
Enable Assigned Objects	If you do not want to enable an assignment immediately, clear the Enabled Assigned Objects check box for that assignment. You can then enable the assignment later using the Assignments & Tuning manager.



Create Aspect Wizard/Edit Aspect Dialog

—General Screen/Tab


UI Element	Description
Name	The name of the aspect.
Description	A description of the aspect.
ID	A unique identifier for the aspect.
Version ID	A unique identifier for this version of the aspect.
Version	<p>The current version of the aspect. The version is formatted as follows: <i><Major Version Number>. <Minor Version Number></i></p> <p>The major version number is specified in the left-hand field, the minor version number in the right-hand field.</p>
Change Log	Description of what is new or modified in this version of the aspect.


UI Element	Description
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.

—CI Type Screen/Tab



UI Element	Description
Node Compatible	In certain situations it is useful to be able assign an aspect to a CI of the type node, rather than a CI type related to a topology view. To enable an aspect to be assigned to nodes, check Node Compatible .
Available CI Type(s)	A list of all available CI types.
Assigned CI Type(s)	The CI types the user wants to assign the aspect to.
	Add CI Type: Move the selected CI types from the list of available CI types to the list of assigned CI types.
	Delete CI Type: Remove the selected CI types from the list of assigned CI types.
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.

—Instrumentation Screen/Tab

UI Element	Description
List of Instrumentation Categories	 <p>Add Instrumentation: Open the Add Instrumentation Dialog Box, which enables you to select the categories of instrumentation that you want to include in this aspect.</p> <p>Instrumentation includes scripts and executables executed by the HP Operations Agent as defined in policies for managed nodes that have the agent</p>



UI Element	Description
	<p>installed on them.</p> <p> Delete Instrumentation: Remove the selected categories of instrumentation from this aspect.</p> <p>You can select multiple items by holding down the Ctrl or Shift key while selecting them.</p> <p>Name The name of an instrumentation category that is included in this aspect.</p> <p>Description A description of the instrumentation category.</p>
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.






—Aspects Screen/Tab



UI Element	Description
List of Aspects	<p>Lists the aspects assigned to management template.</p> <p>Note: You cannot add any of the following types of aspects:</p> <ul style="list-style-type: none"> • Aspects containing the current aspect as a nested aspect. • Aspects with nested aspects already present as a nested aspect in the aspect itself. • Aspects containing a policy template that is already included somewhere else in the aspect structure. <p>The toolbar provides the following controls:</p> <p> Refresh: Reload the list of aspects.</p> <p> Edit Aspect: Open the Edit Aspect dialog box for the selected aspect.</p> <p>The list has the following columns:</p>

UI Element	Description
	<p>Name The name of a first-level nested aspect. (For a fully recursive list of aspects, activate the Structure tab in the Details pane.)</p> <p>Version The version of the nested aspect.</p> <p>To change to a different version, select the desired version from the drop-down list.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: Operations Management does not automatically update aspect versions automatically. If new versions of aspects are available, either use the Update to Latest for the parent management template or aspect, or update the version manually. See also "Configuring Management Templates" on page 17, task <i>How to Update a Management Template After a Management Pack Update</i>.</p> </div> <p>Description A description of the nested aspect.</p>
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.



—Policy Templates Screen/Tab






UI Element	Description
List of Policy Templates	<p> Refresh: Reload the list of policy templates in this aspect.</p> <p> Add Policy Template: Open the Add Policy Template to Aspect dialog box, which enables you to either add an existing policy template or create a new policy templates.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: You cannot add a policy template to an aspect if one of the following conditions exists:</p> <ul style="list-style-type: none"> • The aspect has nested aspects using the </div>

UI Element	Description
	<p data-bbox="800 300 1117 331">policy template to be added.</p> <ul data-bbox="768 352 1312 415" style="list-style-type: none"> • The aspect is a nested aspect, and its parent aspect uses the policy template to be added. <p data-bbox="573 468 605 499"></p> <p data-bbox="743 468 1222 499">Edit Item: Provides the following options:</p> <ul data-bbox="751 520 1352 741" style="list-style-type: none"> •  Edit Policy Template: Open the selected policy template in the policy template editor in normal mode. •  Edit Policy Template (Raw Mode): Open the selected policy template in the policy template editor in raw mode. <p data-bbox="573 772 605 804"></p> <p data-bbox="743 772 1360 898">Edit Deployment Condition: Open the Edit Deployment Condition Dialog Box, which enables you to specify deployment conditions for the selected policy template.</p> <p data-bbox="573 930 605 961"></p> <p data-bbox="743 930 1360 993">Delete Policy Template: Remove the selected policy template(s) from this aspect.</p> <p data-bbox="743 1014 1360 1077">You can select multiple items by holding down the Ctrl or Shift key while selecting them.</p> <p data-bbox="573 1108 646 1140">Name</p> <p data-bbox="743 1108 1092 1140">The name of a policy template.</p> <p data-bbox="573 1161 670 1192">Version</p> <p data-bbox="743 1161 1133 1192">The version of the policy template.</p> <p data-bbox="743 1213 1320 1276">To change to a different version, select the desired version from the drop-down list.</p> <p data-bbox="768 1329 1336 1623">Note: Operations Management does not update policy template versions automatically. If new versions of policy templates are available, either use the Update to Latest Wizard for the parent management template, or update the version manually. See also "Configuring Management Templates" on page 17, task <i>How to Update a Management Template After a Management Pack Update</i>.</p>

UI Element	Description
	<p>Deployment Condition The deployment conditions for the policy template. To specify deployment conditions for a policy template, select it, click the Edit Item button  and select the  Edit Deployment Condition option to open the Edit Deployment Condition Dialog Box.</p> <p>Type The type of the policy template.</p>
Type	The type of the policy template.
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.

—Parameters Screen/Tab

UI Element	Description
List of Parameters	<p>Lists all parameters defined in the policy templates assigned to the aspects contained in the management template or aspect.</p> <p>The toolbar provides the following controls:</p> <p> Edit/Combine...:</p> <ul style="list-style-type: none"> • To Edit a Parameter <ol style="list-style-type: none"> a. Select a single parameter. b. Click the Edit/Combine button . The Edit/Combine Parameters Dialog Box opens, where you can edit parameter settings. <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Note: Changes made here are applied at aspect level. They overrule the definitions in the policy template, but do not change the policy template itself.</p> </div> • To Combine Parameters <ol style="list-style-type: none"> a. Select a number of parameters of the same type (such as string values or numeric values).

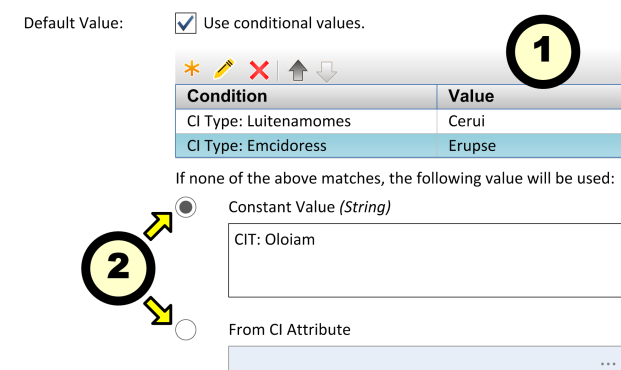









UI Element	Description
	<p>b. Click the Edit/Combine button . The Edit/Combine Parameters Dialog Box opens, where you can specify the parameter settings for the new parameter that is the combination of the selected parameters.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: You can combine parameters only if they meet the following criteria:</p> <ul style="list-style-type: none"> ○ Parameters to be combined must be of the same type. ○ Parameters to be combined must not have conditional values. ○ The range of allowed values of numeric parameters to be combined must overlap. ○ Enumeration parameters to be combined must have at least one common value. </div> <p> Uncombine/Undo Changes:</p> <p>Undo parameter changes and combinations for all selected parameters.</p> <ul style="list-style-type: none"> ● If any parameters that are not combined parameters are selected, Uncombine/Undo Changes undoes all changes that have been made to the selected parameters. ● If any combined parameters are selected, Uncombine/Undo Changes restores the single parameters making up the selected combined parameters, <i>and</i> undoes any changes that were made to them, including changes made before the parameters were combined. <p> Show Parameter Details: Expand the table of parameters to show the extra columns Defined In, Description, Type and Instance Parameter.</p> <p> Refresh: Reload the list of parameters.</p> <p> Search: Specifying a string restricts the parameter list to parameters having the string in their name.</p> <p>The list has the following columns:</p>



UI Element	Description
	<p>I Instance Parameter: ✓ indicates that the parameter is an instance parameter, — indicates it is not.</p>
	<p>C Combined Parameter: ✓ indicates that the parameter is a combined parameter or that the parameter is changed, — indicates it is not.</p>
UI Order	The position of this parameter in the list of parameters.
Name	The name of the parameter. The list initially contains all the parameters from the policy templates and nested aspects that this aspect includes. However, you can edit parameters at aspect level and give them alternative names. You can also specify a name when you combine parameters.
Defined In (detail)	The name of the policy template or aspect that contains the parameter. If the parameter was combined in this aspect, it is the name of this aspect. If the parameter is part of a nested aspect, it is the name of the nested aspect.
Description (detail)	The description of the parameter.
Type(detail)	The type of value that you can specify for the parameter. The variable type can be a string, numeric, an enumeration (of several options), or a password.
Instance Parameter (detail)	The name of the instance parameter that this parameter depends on (if any).
Target (Management Template only)	The CI type of the management template's root CI.
Default Value	The default value of the parameter. Parameters can have a default value that is defined in the policy template. You can also set a default value at the management template or aspect level, which then overrides the default in the policy template.

UI Element	Description
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.

Edit/Combine Parameters Dialog Box

UI Element	Description
Name	The name of the parameter. The parameter list contains parameters defined in any aspect in the management template or aspect structure. You can review the structure of a management template or aspect in the Structure tab of the Details pane.
Instance Parameter	<i>Read-only.</i> If the checkbox is checked the parameter is an instance parameter, if it is unchecked it is not.
Description	A description of the parameter.
UI Order	The position of this parameter in the list of parameters.
Flags	Provides the following options: <ul style="list-style-type: none"> • Mandatory: <i>Read-only.</i> If the checkbox is checked the parameter is mandatory, if it is unchecked it is not. • Read Only: Select this check box to prevent changes to the parameter value when the management template is assigned to a configuration item. If you select this check box, the default value is used when the management template is assigned. • Expert Setting: Select this check box to hide the parameter by default when the management template is assigned to a configuration item. Users can choose whether to show expert settings when they make an assignment. • Hidden: Select this check box to hide the parameter during assignment to a configuration item. If you select this check box, the default value is used when the management template is assigned.
Default Value	The default value of the parameter. The default value used by Operations Management observes the following priorities: <ul style="list-style-type: none"> • A default value defined at aspect level overrides any corresponding default value in a policy template.

UI Element	Description				
	<ul style="list-style-type: none"> A default value defined at management template level overrides any corresponding default value defined at aspect level (and therefore any corresponding default value defined in a policy template). <p>A default value is assigned using the control in the default value group shown in the following figure for a parameter using conditional values:</p>  <ol style="list-style-type: none"> If any conditional values exist in the conditional value list (1), the conditions are evaluated in the order in which they are listed, and the value corresponding to the first condition evaluating to true is used as default value. If no conditions exist or none evaluate to true a constant value or the value of a CI attribute is used as default value, depending on which of these is selected with the radio button (2). <p>The following table describes how to use the controls in the default value group:</p> <table border="1"> <thead> <tr> <th data-bbox="560 1228 722 1333">Use</th> <th data-bbox="722 1228 1385 1333">After checking this checkbox the conditional value list (1) is shown, with the following UI elements:</th> </tr> </thead> <tbody> <tr> <td data-bbox="560 1333 722 1438">Conditional Values</td> <td data-bbox="722 1333 1385 1438"> <ul style="list-style-type: none">  New Item: Open the Edit Conditional Value Dialog Box, which is used to define a new condition.  Edit Item...: Open the Edit Conditional Value Dialog Box, which is used to edit the selected condition.  Delete Item: Delete the selected condition. </td> </tr> </tbody> </table>	Use	After checking this checkbox the conditional value list (1) is shown, with the following UI elements:	Conditional Values	<ul style="list-style-type: none">  New Item: Open the Edit Conditional Value Dialog Box, which is used to define a new condition.  Edit Item...: Open the Edit Conditional Value Dialog Box, which is used to edit the selected condition.  Delete Item: Delete the selected condition.
Use	After checking this checkbox the conditional value list (1) is shown, with the following UI elements:				
Conditional Values	<ul style="list-style-type: none">  New Item: Open the Edit Conditional Value Dialog Box, which is used to define a new condition.  Edit Item...: Open the Edit Conditional Value Dialog Box, which is used to edit the selected condition.  Delete Item: Delete the selected condition. 				

UI Element	Description
	<div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 15%; text-align: center;">   </div> <div style="width: 85%;"> <p>Move Up: Increase the priority of the condition.</p> <p>Move Down: Decrease the priority of the condition.</p> <p>Condition A semicolon-separated string listing all expressions used in the condition.</p> <p>Value The value used as default when the condition is the first to evaluate to true.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p>Note: At management template level you cannot add, remove, or rearrange conditions, but you can change the values used to evaluate them.</p> </div> <p>Move Up: Increase the priority of the condition.</p> <p>Move Down: Decrease the priority of the condition.</p> <p>Condition A semicolon-separated string listing all expressions used in the condition.</p> <p>Value The value used as default when the condition is the first to evaluate to true.</p> </div> </div>
Constant Value	<p>When selected, the value specified in the text box is used as default value if no conditional values are defined, or if none of the conditional values evaluates to true.</p>
From CI Attribute	<p>When selected and a CI attribute is selected, the value of the selected attribute is used as default value if no conditional values are defined, or if none of the conditional values evaluates to true.</p>
	<div style="background-color: #f0f0f0; padding: 5px;"> <p>Note: The value used to evaluate this condition is always the value of the aspect CI from where the value will be resolved, even if it is overwritten on management template level.</p> </div>
	<p>To use a default value from a CI attribute:</p>
	<ol style="list-style-type: none"> 1. Select the From CI Attribute radio button.

UI Element	Description
	<ol style="list-style-type: none"> Click the ... button to the right of the input field. The Available Attributes dialog box is shown. The Attribute CI Type list contains all CI types assigned in the CI Types screen for the current aspect or any contained and nested aspects. Select the appropriate attribute(s).

Edit Conditional Value Dialog Box






UI Element	Description
Constant Value	A specific value to use when the condition is true. You can type or select a value (depending on the type of parameter).
From CI Attribute	<p>A CI attribute to use when the condition is true. To choose a CI attribute, click the ... button. The Available Attributes dialog box opens. If the aspect can be assigned to more than one CI type, select the Attribute CI Type and then select a CI attribute. If the aspect can be assigned to only one CI type, it is not necessary to select the Attribute CI Type first.</p> <p>If you specify a CI attribute, Operations Management sets the parameter value automatically during the deployment of the underlying policy templates, using the actual value of this attribute from the CI.</p>

Edit Deployment Condition dialog box

UI Element	Description
OS type	<p>The operating systems for which this policy template is suitable. To include a condition for the OS, check the OS Type checkbox, then check all operating systems for which the policy template should be deployed.</p> <p>Note: An aspect can contain policy templates for multiple operating systems. Operations Management automatically deploys the policy templates that are suitable for the operating system of the node that hosts the CI.</p> <p>To configure a platform-independent policy template, create a platform-specific variation of the same policy for each platform, and include all variations in a single aspect.</p>
CI type	<p>A policy template can be made to be applied to a certain CI type only.</p> <p>To include a condition for the CI type, check the CI Type checkbox, then check the appropriate CI type.</p>
CI attribute	When including information from several CI types in a single aspect, a

UI Element	Description
	<p>CI attribute condition allows selective deployment of the policy template based on the value of a CI attribute.</p> <p>To include a condition for a CI attribute:</p> <ol style="list-style-type: none"> 1. Check the CI Attribute checkbox. 2. Click the Browse button ... to the right of the attribute (left-most) field. The Available Attributes dialog box is shown. The left pane lists all CI types contained in the view assigned to the aspect. 3. Select the CI type with the attribute you want to use as a filter. All attributes available for the selected CI type are shown in the list. 4. Select the appropriate attribute in the list and click Insert. The Available Attributes dialog box closes and the selected attribute is entered in the attribute field. 5. Select a value from the drop-down list in the operator (middle) field. Select Equals if you want the condition to match an exact value, or MatchesRegexp if you want to match a regular expression. 6. Enter an appropriate value in the value (right) field. 7. Click OK. All deployment conditions are entered in the Deployment Condition column in the Policy Templates pane.
OK	<p>Apply all conditions.</p> <p>Note: All conditions must be true for the item to be deployed.</p>
Cancel	Close the dialog box without adding any conditions.

Reports Screen





UI Element	Description
	Expand all: Expand all CIs.
	Collapse all: Collapse all CIs.
	Filter On/Off: Toggle between Show Customized Values Only and Show All Values .
	Expand Category: Expand the category to show the attributes contained in it.
	Collapse Category: Collapse the category to hide the attributes contained in it.

Update to Latest Wizard

—Options Screen

UI Element	Description
Update to the Latest Major and Minor Version	Allow the system to update both major and minor version numbers to the latest version.
Update to the Latest Minor Version, Keeping All Major Versions	Allow changes to the minor version number only. If the latest version of an item has a higher major number than the current item, the new version will have lowest available minor number for the same major number as the current version.
Only Update This Object, Not the Contained Object	Update the version of the selected object only, but not the object further down in the tree structure.
Update This Object and All Containing Objects, Recursively	Update all objects in the entire tree.
Next	Go to the <i>Preview</i> screen.
Cancel	Close the wizard without making any changes.
Help	Open the relevant help in a new browser window.

—Preview Screen

UI Element	Description
	Expand All: Expand the structure element to show the entire tree of contained elements.
	Collapse All: Collapse the entire structure tree.
	Include in Update: Force a manually excluded policy template to be included in the update.
	Exclude from Update: Force a policy template to be excluded from the update.
Reload Preview	Recalculate the version numbers to be applied and refresh the preview after manually excluding or re-including policy templates
Back	Go back to the <i>Options</i> screen.
Finish	Apply all proposed changes and close the wizard.
Cancel	Close the wizard without making any changes.
Help	Open the relevant help in a new browser window.

Viewing Details

Management templates and aspects have a number of properties and a structure. The Details pane (right pane) contains details about the management template or aspect selected in the Management and Aspects pane (middle pane). If no management template or aspect is selected, the pane is empty.

Which details are shown depends on whether a management template or an aspect is selected in the Management Templates & Aspects pane. In the UI reference section below, details categories appearing for management templates or aspects only are marked accordingly.

Chapter 3

Policy Templates

A policy template is a set of configuration information for HP Operations Agent, HP SiteScope, or HP ArcSight Logger. These products enable you to automate the configuration and monitoring of networks and computers. Policy templates define the details of specific configuration and monitoring tasks.

You can develop and deploy individual policy templates to computers that run HP Operations Agent, HP SiteScope, or HP Arcsight Logger. Furthermore, you can group policy templates together within aspects and management templates to create complete management solutions for applications or services.

Learn More

This section includes:

- "Policy Template Types" below
- "Policy Template Groups" on the next page
- "Policy Template Versions" on the next page
- "Policy Template Parameterization" on the next page
- "Instance Parameters" on page 73

Policy Template Types

The following types of policy template are available:

- Arcsight Logger
- ConfigFile
- Flexible Management
- Logfile Entry
- Measurement Threshold
- Node Info
- Open Message Interface
- Scheduled Task
- Service Auto-Discovery
- Service/Process Monitoring
- SiteScope
- SNMP Interceptor

- [Windows Event Log](#)
- [Windows Management Interface](#)
- [XML File](#)

Policy Template Groups

Policy template groups are used to organize policy templates. You can define your own policy template groups and place policies within them. This links a policy template to the policy template group. A policy template can be placed in more than one group.

The **Templates grouped by type** template group is used to automatically organize templates according to their `Type` value.

Policy Template Versions

If you modify an existing policy template, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.

Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.

Policy Template Parameterization

Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.

For example, if you have a policy template that monitors the level of CPU usage, you could have parameters for a minor event threshold, a major event threshold, and a critical event threshold. Consumers of the policy template set the parameters to specify for themselves what level of CPU usage is a minor, major, or critical event on the computer that they want to monitor. The user does not need to modify the policy template, and does not need detailed knowledge of how the policy template monitors the CPU. The user needs to know only what monitoring functionality the policy template provides and the purpose of the parameters.

Parameters also enable you to create policy templates that use values you could not specify in advance.

For example, a policy template that monitors database performance might need a user name and password to connect to the database. Appropriate parameters would make it possible to provide a generic policy template, without hard-coded user credentials.

After a policy template is assigned and deployed, an application expert can change the value of parameters as often as necessary to tune their monitoring solution.

You can specify a variable in any text field of a policy template in the format `%%<variable_name>%%` (for example `%%CriticalThreshold%%`). Variable names can include alphanumeric

characters (a-z, A-Z, 0-9) and underscores (_). No other characters (or spaces) are valid in variable names.

Each variable is internal to the policy template, and not visible to consumers of the template. Consumers see the corresponding parameter and can set the value.

You can specify the types of parameter value that are acceptable. Parameter values can be strings, numbers, passwords, or you can set up an enumeration of acceptable values to select from. You can set a default value for a parameter. A value is always mandatory for password and enumeration parameters, but you can control whether a value is mandatory for string and numeric parameters. For numeric parameters you can specify a range of acceptable values. You can also specify the order in which the parameters are listed.

Instance Parameters

An instance parameter enables you to create policy templates that monitor multiple instances of the same type of object (for example multiple database instances or multiple hard disks).

Each policy template can have only one instance parameter. When you add an instance parameter to a policy template, all other parameters become dependent on it. The user can specify separate values for the dependent parameters of each instance.


For example, if you have a policy template that monitors the percentage of disk space in use, you could create an instance parameter called 'Disks', and dependent parameters called 'Minor disk usage threshold', 'Major disk usage threshold', and 'Critical disk usage threshold'. A user of this policy template can specify multiple disk instances using the 'Disks' parameter (for example, by adding the instance values C:, D:, and E:). For each disk instance, the user can then set different values for the dependent parameters (for example, the value of 'Critical disk usage threshold' could be 85% for disk C:, 90% for disk D:, and 95% for disk E:).



Tasks

This section includes:

- ["How to Deploy Policy Templates" below](#)
- ["How to Create a Template Group" on the next page](#)
- ["How to Search for Policy Templates" on page 75](#)

How to Deploy Policy Templates

1. Open the Policy Templates manager:
Admin > Operations Management > Monitoring > Policy Templates
2. In the Policy Template Groups pane, expand the tree and navigate to the policy template that you want to deploy.
3. In the Policy Templates pane, select the policy template that you want to deploy and click the  button. The Assign and Deploy wizard opens.
4. In the Configuration Item page, click the configuration item to which you want to assign the policy template, and then click **Next**.
5. In the Parameter page, specify a value for each parameter:

- a. *Optional.* By default, the list shows only mandatory parameters. To see all parameters, click the  button.
- b. Select a parameter in the list, and then click the  button.
 - For standard parameters, the Edit Parameter dialog box opens.
Click **Value**, specify the value, and then click **OK**.
 - For instance parameters, the Edit Instance Parameter dialog box opens.
Change the instance values if necessary, and then for each instance value, change dependent parameter values. After you change the instances and dependent parameter values, click **OK**.

Click **Next**.



6. *Optional.* If you do not want to enable the assignment immediately, clear the **Enable Assigned Objects** check box. You can then enable the assignment later using the Assignments & Tuning manager.
7. Click **Finish**. Operations Management creates deployment jobs, which deploy the policy template to the nodes.



After a policy template has been deployed, the BSM server specified in the **Default Virtual Gateway Server for Data Collectors URL** infrastructure setting becomes the owner of the policy on the node.

How to Create a Template Group


1. Open the Policy Templates manager:

Admin > Operations Management > Monitoring > Policy Templates




2. In the Policy Template Groups pane, select **Template Groups** and click the  button. Alternatively, to create a nested template group, select an existing group and click the  button. The New Template Group dialog box opens.
3. Type the name and description of the new template group and click **OK**. The new template group is added below the selected template group.
4. Add policy templates to the template group by selecting them in the Policy Templates pane and dragging them to the template group.

Alternatively, select a policy template and click the  button. Then select the template group to which you want to add the policy templates and click  button in the Policy Templates pane.

Note:

- Template groups always contain the latest version of a policy template.
- When you add policy templates to a template group, the templates are linked to the group. To delete templates from a group, select the templates and click  **Delete Item (s) From Group**. This deletes the template links from the group; the actual policy templates continue to exist under **Templates grouped by type**.

How to Search for Policy Templates

1. Open the Policy Templates manager:
Admin > Operations Management > Monitoring > Policy Templates
2. In the Policy Template Groups pane, click the  button. The Search dialog box opens.
3. Type a search string in either or both **Name** and **Description**. You can also use wildcards (*).
 If you search for both the name and the description, the search returns only policy templates that match both search strings.
4. Select where to search. Select **Policy Template Groups** to search for policy templates that are assigned to template groups. Select **Policy Templates** to search for all policy templates.
5. Click **Search**. The search results are displayed in the lower half of the dialog box.
6. *Optional.* Select a policy template in the search results and click  to highlight the template version in the Policy Templates pane.
Optional. Select a policy template and click  to open the corresponding policy editor for the template.

UI Reference





This section includes:






- "Assign and Deploy—Configuration Item" below
- "Assign and Deploy—Parameters" on the next page
- "Assign and Deploy—Configure Options" on page 77
- "Policy Parameters Dialog Box" on page 78
- "Policy Template Details Pane" on page 81
- "Policy Template Groups Pane" on page 81
- "Policy Templates Pane" on page 81
- "Search Dialog Box" on page 82
- "Template Group Dialog Box" on page 83

Assign and Deploy—Configuration Item

UI	
Element	Description
Name	The name of a configuration item. The list contains only the types of configuration to which it is possible to deploy the selected management template, aspect, or policy template.
Type	The type of configuration item.

Assign and Deploy—Parameters

UI Element	Description				
Parameter List	<p data-bbox="558 302 1305 365">Lists all parameters in the management template, aspect or policy template you are assigning to the configuration object.</p> <p data-bbox="558 390 1045 422">The toolbar provides the following controls:</p> <div data-bbox="570 457 602 489">  </div> <p data-bbox="769 457 1349 552">Edit: Open a dialog box that enables you to specify the value of the selected parameter for this assignment.</p> <ul data-bbox="776 569 1360 915" style="list-style-type: none"> • For standard parameters, the Edit Parameter dialog box opens. <ul data-bbox="805 632 1360 915" style="list-style-type: none"> ▪ If you select Value you must specify or select a value in the range that is valid for the parameter. The value you specify overrides any default values defined in the policy template, aspect, or management template. ▪ Select Use Default Value if you want to use the default value defined in the policy template, aspect, or management template. <p data-bbox="805 936 1341 1031">Click OK to apply the values and close the Edit Parameter dialog box, or Cancel to close the dialog box without making changes.</p> <ul data-bbox="776 1058 1357 1184" style="list-style-type: none"> • For instance parameters, the Edit Instance Parameter dialog box opens. For details, see the UI Reference section for the Edit Instance Parameter dialog box. <div data-bbox="570 1213 602 1245">  </div> <p data-bbox="769 1213 1354 1276">Show Only Mandatory Parameters: Show or hide optional parameters in the table of parameters.</p> <div data-bbox="570 1304 602 1335">  </div> <p data-bbox="769 1304 1317 1367">Show Expert Parameters: Show or hide expert parameters in the table of parameters.</p> <div data-bbox="570 1394 602 1425">  </div> <p data-bbox="769 1394 1279 1491">Sort According to UI Order: Sort the list of parameters according to their UI order values (lowest to highest).</p> <p data-bbox="558 1524 1073 1556">The parameter list has the following columns:</p> <table data-bbox="570 1587 1295 1812"> <tr> <td data-bbox="570 1587 743 1688">Target (Management Template only)</td> <td data-bbox="769 1587 1295 1619">The CI type of the aspect using the parameter.</td> </tr> <tr> <td data-bbox="570 1713 743 1812">Defined In (Management Template only)</td> <td data-bbox="769 1713 1268 1776">The management template, aspect or policy template in which the parameter is defined.</td> </tr> </table>	Target (Management Template only)	The CI type of the aspect using the parameter.	Defined In (Management Template only)	The management template, aspect or policy template in which the parameter is defined.
Target (Management Template only)	The CI type of the aspect using the parameter.				
Defined In (Management Template only)	The management template, aspect or policy template in which the parameter is defined.				

UI Element	Description
	<p>Name The name of the parameter.</p> <p>Value The value for this parameter in this assignment. If the value is dimmed, it is the default value.</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String <p>If the icon is dimmed, the value is read-only.</p> <p>If the invalid icon appears () , the parameter is mandatory, and you need to specify a value.</p> <p>Description A description of the parameter.</p>
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.






Assign and Deploy—Configure Options

UI Element	Description
Enable Assigned Objects	If you do not want to enable an assignment immediately, clear the Enabled Assigned Objects check box for that assignment. You can then enable the assignment later using the Assignments & Tuning manager.

Policy Parameters Dialog Box

UI Element	Description
Name	<p>Label for the parameter. This name appears to consumers of the policy template in the user interface.</p> <p>Tip: Aspects and management templates can contain many policy templates. Therefore, it may be helpful to use specific parameter names rather than general names.</p> <p>For example, "Critical disk usage threshold" may be better than "Critical threshold".</p>
Variable Name	<p>Name of the corresponding variable in the policy template.</p> <p>You can specify a variable in any text field within a condition or an event definition in a policy template. Type the variable in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>). Variable names can include alphanumeric characters (a-z, A-Z, 0-9) and underscores (_). No other characters (or spaces) are valid in variable names.</p> <p>Each variable is internal to the policy template, and not visible to consumers of the template. The variable name must be unique within the policy template.</p>
Instance Parameter	<p>Defines that this parameter is an instance parameter. An instance parameter enables you to create policy templates that monitor multiple instances of the same type of object (for example multiple database instances or multiple hard disks).</p> <p>Each policy template can have only one instance parameter. When you add an instance parameter to a policy template, all other parameters become dependent on it. The user can specify separate values for the dependent parameters of each instance.</p> <p>Tip: In measurement threshold policy templates, use the instance parameter's variable to define the <code>OBJECT</code> attribute.</p> <p>For example, if you have a policy that monitors multiple instances of hard disks, you could create an instance parameter with the variable name <code>DISK</code>, you could use it in the policy template as follows:</p> <pre>OBJECT "^%%DISK%%\$" SEPARATORS " "</pre> <p>The following policy types do not support instance parameters:</p> <ul style="list-style-type: none"> • Flexible Management • Node Info • Open Message Interface • Service Auto-Discovery









UI Element	Description
	<ul style="list-style-type: none"> • Service/Process Monitoring • SNMP Interceptor • Windows Event Log • Windows Management Interface
UI Order	Position of this parameter in the list of parameters.
Description	Description of the parameter. This description appears to consumers of the policy template in the user interfaces. Provide a description that enables users to understand the purpose of the parameter.
Variable Type	<p>Defines the type of value that consumers can specify for the parameter. The following variable types are available:</p> <ul style="list-style-type: none"> • String The value can be a string of any characters. • Numeric The value must be a number. You can specify minimum and maximum values. • Enumeration The value must be one of a specified list of acceptable values. • String (Password) The value can be a string of any characters, but the user interface does not display the value. Operations Management encrypts the value before storing it in the database.
Minimum Value	Defines the minimum value that is acceptable (if the variable type is numeric).
Maximum Value	Defines the maximum value that is acceptable (if the variable type is numeric).
Acceptable Values	Defines a list of acceptable values (if the variable type is enumeration). Specify each value on a separate line.

UI Element	Description
Default Value	<p>Defines the default value of the parameter.</p> <p>Select the Use conditional values check box to add a list of conditional default values. You can configure conditional default values based on the type of operating system of the host node to which the policy template is deployed.</p> <p>If you use conditional values, Operations Management evaluates the conditions in the specified order before the policy template is deployed, and uses the value that corresponds to the first condition that is true. If no conditions are true, Operations Management uses the default value. If you use conditional parameter values, you must therefore set an unconditional default value for the parameter too.</p> <p>The following options are available for conditional values:</p> <ul style="list-style-type: none">  New Item: Opens the Edit Conditional Value dialog box to add a new conditional value.  Edit Item: Opens the Edit Conditional Value dialog box, so that you can edit the condition for the selected conditional value.  Delete Item: Deletes the selected conditional value.  Move Up: Moves the selected conditional value up the list.  Move Down: Moves the selected conditional value down the list.
Password	Defines a password.
Verify Password	Repeat the password to verify it.
Mandatory	<p>Specifies that a default or user-specified value is required before assigning the policy. If you select this check box and any of Read Only, Expert Setting, or Hidden, you must also specify a default value.</p> <p>Enumeration and password parameters are always mandatory.</p>
Read Only	Prevents users from overriding the parameter value in aspects and management templates. This setting also prevents users from changing the value when the policy template is assigned to a configuration item (either directly, or as part of an aspect or management template).
Expert Setting	Hides the parameter by default when the policy template is assigned to a configuration item. Users can choose whether to show expert settings when they make an assignment.
Hidden	Hides the parameter completely in aspects and management templates, and during assignment to a configuration item. If you select this check box, the default value is used when the aspect is assigned to a CI.





Policy Template Details Pane









UI Element	Description
General	Provides an overview of the policy template's general attributes.
Parameters	Provides an overview of the parameters that the policy template contains.

Policy Template Groups Pane

UI Element	Description
	Refresh: Reloads the tree of policy templates.
	Add New Template Group: Opens the Add New Template Group dialog box.
	Edit Template Group: Opens the Edit Template Group dialog box for the selected template group.
	<p>Delete Item: Deletes the selected template group. Any policy templates and template groups contained in the template group are also deleted.</p> <p>Note: The policy templates are only deleted from the group and can be accessed again under Templates grouped by type.</p>
	Show Item Properties: Opens the Template Group Properties dialog box for the selected template group.
	Search: Opens the Search dialog box.
	Cut Item: Cuts the selected template group to the clipboard.
	Paste Item: Pastes a previously cut template group to a new location.



Policy Templates Pane

UI Element	Description
	Refresh: Reloads the list of policy templates.
	<p>New: Provides the following options:</p> <ul style="list-style-type: none">  Add New Policy Template: Opens the appropriate editor for the selected policy template type. If a native editor is not available, the policy template opens in a policy template raw editor instead.  Add New Policy Template (Raw Mode): Opens the new policy template in a policy template raw editor for the selected policy template type.

UI	
Element	Description
	<p>Edit Item: Provides the following options:</p> <ul style="list-style-type: none">  Edit Policy Template: Opens the appropriate editor for the selected policy template. If a native editor is not available, the policy template opens in a policy template raw editor instead.  Edit Policy Template (Raw Mode): Opens the policy for editing in a policy template raw editor.
	<p>Delete Item(s) From Group: Deletes the selected policy templates from the current template group. The policy templates are only deleted from the group and can be accessed again under Templates grouped by type as well as in any other template groups that contain them.</p> <p>Delete Item(s): Deletes the selected policy templates or policy versions from Operations Management. If you select a policy template and a policy version or if you select all versions of a policy, the policy template including all versions is deleted.</p>
	Copy Item: Copies the selected policy template to the clipboard.
	Paste as Item Link: Pastes a link to the previously copied policy template into the selected policy template group.
	Paste Item: Pastes a previously copied policy template to a new location.
	Assign and Deploy Policy Template: Opens the Assign and Deploy wizard, which enables you to assign the selected policy template to a configuration item, and then deploy it.

Search Dialog Box

UI Element	Description
Name	<p>String to search for in policy template names. You can type one or more characters and combine them with asterisks (*) to match zero or more characters.</p> <p>When searching by name but not by description, only the latest matching versions are returned as a result.</p>
Description	String to search for in policy template descriptions. You can type one or more characters and combine them with asterisks (*) to match zero or more characters.
Search in	<p>Policy Template Groups: Searches only in policy templates that are assigned to template groups.</p> <p>Policy Templates: Searches in all policy templates.</p>
Ignore case	<p>Clear to make the search string case sensitive.</p> <p>Default value: selected</p>

UI Element	Description
Search	Starts the search.
Search Results	
	Show Item: Highlights the selected version of the policy template in the Policy Templates pane.
	Edit Item: Opens the appropriate editor for the selected policy template version. If a native editor is not available, the policy template opens in a policy template raw editor instead.
Name	Name of the policy template.
Version	Version of the policy template
Template Group	Name of the template group to which the policy template is assigned.
Path	Path to the template group to which the policy template is assigned.

Template Group Dialog Box

UI Element	Description
Name	Name of the template group.
Description	Description of the template group.
ID	GUID ¹ assigned to the template group when it is first created.

Configuring HP ArcSight Logger Policies

HP ArcSight Logger (ArcSight Logger) is a log management solution that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. ArcSight Logger receives and stores events; supports search, retrieval, and reporting; and can optionally forward selected events.

ArcSight Logger Receiver Configuration policy templates configure one or more receivers in ArcSight Logger. Receivers in ArcSight Logger listen for and capture event data locally or on remote systems.


To access

You can create or edit an ArcSight Logger template using the ArcSight Logger Template Editor, which you can open in the following ways.








- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:

Admin > Operations Management > Monitoring > Management Templates & Aspects

¹(globally unique identifier)




- b. In the Configuration Folders pane, expand the configuration folders.
- c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.

The Edit Aspect dialog box opens.




- d. Click the **Policy Templates** tab, and then do one of the following:
 - o To add a new policy template:
 - o Click the  button. The Add Policy Template to Aspect dialog box opens.
 - o Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - o Select the type **ArcSight Logger Template**, and then click **OK**.
 - o To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The ArcSight Logger Template Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:

Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **ArcSight Logger Receiver Configuration Templates** folder, and then do one of the following:
 - o To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New ArcSight Logger Template Editor opens.

- o To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit ArcSight Logger Template Editor opens.

Learn More

This section includes:

- ["ArcSight Logger Configuration Syntax" on the next page](#)
- ["Example ArcSight Logger Receiver Configuration Policy" on page 88](#)
- ["Assigning and Deploying ArcSight Logger Policy Templates" on page 88](#)

ArcSight Logger Configuration Syntax

ArcSight Logger policies configure ArcSight Logger receivers on the system to which they are deployed. The policies must use the following syntax:

- **Receiver name, type, and state syntax**

The policy name determines the name of the receiver in ArcSight. The policy parameters `_logger_receiver_type` and `_logger_receiver_state` define the receiver type and state.

For example, the policy "Audit Log", which contains the policy parameter `_logger_receiver_type` with the value `localfile` and the parameter `_logger_receiver_state` with the value `true` creates a receiver named "Audit Log" of the type "File Receiver" that is enabled in ArcSight Logger after deployment.

If the policy parameters `_logger_receiver_type` and `_logger_receiver_state` are not defined, the policy template by default creates a receiver of the type File Receiver and enables it after deployment.

Parameter Name	Parameter Type	Parameter Value										
<code>_logger_receiver_type</code>	Enumeration	<p>Defines the receiver type. Supported values are:</p> <table border="0"> <tr> <td><code>udp</code></td> <td>Creates a receiver for UDP messages (for example, SYSLOG).</td> </tr> <tr> <td><code>tcp</code></td> <td>Creates a receiver for TCP messages (for example, SYSLOG, which can also be sent with TCP).</td> </tr> <tr> <td><code>localfile</code></td> <td>Creates a receiver to read logs from a local or remote file system (for example, NFS, CIFS, or SAN).</td> </tr> <tr> <td><code>filetransfer</code></td> <td>Creates a receiver to read remote logs using scp, sftp or ftp.</td> </tr> <tr> <td><code>smartmsg</code></td> <td>Creates a receiver for encrypted SmartMessage messages sent by SmartConnectors.</td> </tr> </table>	<code>udp</code>	Creates a receiver for UDP messages (for example, SYSLOG).	<code>tcp</code>	Creates a receiver for TCP messages (for example, SYSLOG, which can also be sent with TCP).	<code>localfile</code>	Creates a receiver to read logs from a local or remote file system (for example, NFS, CIFS, or SAN).	<code>filetransfer</code>	Creates a receiver to read remote logs using scp, sftp or ftp.	<code>smartmsg</code>	Creates a receiver for encrypted SmartMessage messages sent by SmartConnectors.
<code>udp</code>	Creates a receiver for UDP messages (for example, SYSLOG).											
<code>tcp</code>	Creates a receiver for TCP messages (for example, SYSLOG, which can also be sent with TCP).											
<code>localfile</code>	Creates a receiver to read logs from a local or remote file system (for example, NFS, CIFS, or SAN).											
<code>filetransfer</code>	Creates a receiver to read remote logs using scp, sftp or ftp.											
<code>smartmsg</code>	Creates a receiver for encrypted SmartMessage messages sent by SmartConnectors.											

Parameter Name	Parameter Type	Parameter Value
		<p><code>cefudp</code> Creates a receiver for CEF (Common Event Format) messages sent through UDP.</p> <p><code>ceftcp</code> Creates a receiver for CEF (Common Event Format) messages sent through TCP.</p>
<code>_logger_receiver_state</code>	String	<p>Defines the receiver state. Supported values are:</p> <p><code>true</code> Sets the receiver state to enabled in ArcSight Logger.</p> <p><code>false</code> Sets the receiver state to disabled in ArcSight Logger.</p>

• Receiver parameter syntax

The data part of an ArcSight Logger policy template defines the details of a receiver. Each receiver property is defined by a receiver parameter name-value pair. You can optionally create policy parameters for each receiver parameter and insert them as variables in place of the values.

For more information about the receiver parameters, see the ArcSight Logger Administrator's Guide.

Tip: You can add as many different parameter name-value pairs to your ArcSight Logger policy template as you want. ArcSight Logger ignores parameters that are not relevant to the receiver configured by the policy template.

UDP, TCP, CEF UDP, and CEF TCP Receiver parameters

Parameter Name	Receiver Property
<code>ip</code>	IP/Host
<code>PORT</code>	Port
<code>Encoding</code>	Encoding

File Receiver parameters

Parameter Name	Receiver Property
rfsname	RFS Names
folder	Folder
sourcetype	Source Type
wildcard	Wildcard (regex)
mode	Mode
renameext	Rename extension
charencoding	Character encoding
delayafterfirstseen	Delay after seen
datetimelocale	Date/time locale
datetimezone	Date/time zone
datetimelocregex	Date/time loc regex
datetimeformat	Date/time format
singlelinestart	Event start (regex)

File Transfer Receiver parameters

Parameter Name	Receiver Property
protocol	Protocol
port	Port
host	Ip/Host
username	User
password	Password
filepath	File path
schedule	Schedule
zipformat	Zip Format
sourcetype	Source Type
charencoding	Character encoding
delayafterfirstseen	Delay after seen

Parameter Name	Receiver Property
datetimelocale	Date/time locale
datetimezone	Date/time zone
datetimelocregex	Date/time loc regex
datetimeformat	Date/time format
singlelinestart	Event start (regex)

Smart Message Receiver parameters

Parameter Name	Receiver Property
Encoding	Encoding

Example ArcSight Logger Receiver Configuration Policy

The following policy data creates an enabled ArcSight Logger receiver of the type "File Receiver". The receiver reads all files in the folder /home/arcsight/filereceiver01 on the ArcSight Logger system.

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<ParameterValues>
  <Parameter Name="_logger_receiver_type" Value="localfile"/>
  <Parameter Name="_logger_receiver_state" Value="true"/>
  <Parameter Name="rfsname" Value="LOCAL"/>
  <Parameter Name="folder" Value="/home/arcsight/filereceiver01"/>
  <Parameter Name="sourcetype" Value="Other"/>
  <Parameter Name="wildcard" Value=".*"/>
  <Parameter Name="mode" Value="persist"/>
  <Parameter Name="renameext" Value=".done"/>
  <Parameter Name="charencoding" Value="US-ASCII"/>
  <Parameter Name="delayafterfirstseen" Value="10"/>
  <Parameter Name="datetimelocale" Value="en_US"/>
  <Parameter Name="datetimezone" Value="Europe/Berlin"/>
  <Parameter Name="datetimelocregex" Value=""/>
  <Parameter Name="datetimeformat" Value=""/>
  <Parameter Name="singlelinestart" Value=""/>
</ParameterValues>
```

Assigning and Deploying ArcSight Logger Policy Templates

You assign ArcSight Logger policy templates to the remote systems from which you want to receive data in ArcSight Logger. Based on the connected server configuration, Operations Management then selects an ArcSight Logger server and deploys the policy template to that server. The ArcSight Logger server finally creates the corresponding receivers and starts receiving data from the corresponding hosts.

To be able to assign and deploy an ArcSight Logger policy template, the ArcSight Logger system must be set up as a connected server in Operations Management and a node CI must exist for the

system in Monitored Nodes. In addition, the remote systems that send data to ArcSight Logger must be represented as node CIs in the RTSM.

If the ArcSight Logger policy template contains parameters, you can choose to deploy the policy template with the default values or provide custom values during the assignment or tuning. For example, even if the default value of the `_logger_receiver_type` parameter is `localfile`, you can tune this parameter before deployment and change it to `udp`.

Tasks

This section includes:

- ["Prerequisites" below](#)
- ["How to Install the HP Operations Subagent for ArcSight Logger" below](#)
- ["How to Create an HP ArcSight Logger Policy" below](#)

Prerequisites

Before you can collect log data from a node using ArcSight Logger, you must complete the following steps:

- Install HP Operations Agent and the HP Operations Subagent for ArcSight Logger on the ArcSight Logger system. For details, see ["How to Install the HP Operations Subagent for ArcSight Logger" below](#).
- Set up the ArcSight Logger system as a connected server in Operations Management. For details, see "Connected Servers" in the BSM Application Administration Guide.
- Verify that a node CI has been created for the ArcSight Logger system, access:
Admin > Operations Management > Setup > Monitored Nodes
- Make sure the systems that send data to ArcSight Logger are represented as node CIs in the RTSM, access:
Admin > Operations Management > Setup > Monitored Nodes

How to Install the HP Operations Subagent for ArcSight Logger

1. *Prerequisite:* Make sure HP Operations Agent is installed on the ArcSight Logger system.
2. On the BSM Data Processing Server, navigate to the subagent installation files:
`<HPBSM root directory>/opr/subagents/arcsight_logger`
3. Copy the subagent installation files from the BSM Data Processing Server to a temporary directory on the ArcSight Logger system.
4. On the ArcSight Logger system, execute the installation script `install_asloggersubagent.sh`.

The script prompts you for the installation directory on the ArcSight Logger system. Type `/opt/arcsight/`, for example.

How to Create an HP ArcSight Logger Policy

1. In the HP ArcSight Logger Policy Editor, in the Properties page, type a **Name** for the policy.


You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "Properties Page" on the next page.

2. Use the Policy Parameters tab to create the `_logger_receiver_state` and the `_logger_receiver_type` parameters.

For more details, see "Receiver name, type, and state syntax" on page 85 and "Policy Parameters Tab" below.

3. In the Policy Data page, type the details of the receiver using name-value pairs. If you are creating a new policy, copy and paste template data from an existing policy template.

Alternatively, click the  button to load policy data from a policy template file on your computer.

For details, see "Receiver parameter syntax" on page 86.



4. Click **OK** to save the policy template.
5. *Optional.* If the receiver state has been set to false (disabled), enable the receiver in ArcSight Logger (**Configuration > Event Input/Output**) after the deployment.

UI Reference



This section includes:







- "Policy Data Page" below
- "Policy Parameters Tab" below
- "Properties Page" on the next page

Policy Data Page

UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	HP ArcSight Logger policies do not support syntax checking. You can click Check Syntax but the check fails to perform.
<policy data>	Policy data in text form. For details, see "ArcSight Logger Configuration Syntax" on page 85.

Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.

UI Element	Description
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Properties Page

UI Element	Description
Name	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).

UI Element	Description
Policy ID	GUID ¹ assigned to the policy when it is first created.
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

¹(globally unique identifier)

Configuring ConfigFile Policies


HP Operations Smart Plug-ins (SPIs) provide predefined monitoring and management functionality for infrastructure, operating systems and applications. SPIs may include scripts or programs called instrumentation, which enable specific management and monitoring tasks. In some cases, it is necessary to configure the instrumentation after it is deployed. ConfigFile policies contain rules or instructions to configure SPI instrumentation.

Note:








- This release of Operations Management does not encrypt ConfigFile policies. It is therefore not recommended to insert passwords in the data part of these policies.
- This release of Operations Management does not support ConfigFile templates.

To access

You can create or edit a ConfigFile policy using the ConfigFile Policy Editor, which you can open in the following ways.




- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:
Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.




The Edit Aspect dialog box opens.

- d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **ConfigFile Template**, and then click **OK**.
 - To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The ConfigFile Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:
Admin > Operations Management > Monitoring > Policy Templates

- b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
- c. Click the **ConfigFile Templates** folder, and then do one of the following:
 - To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New ConfigFile Policy Editor opens.
 - To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit ConfigFile Policy Editor opens.

Learn More

This section includes:

- ["ConfigFile Definition" below](#)
- ["ConfigFile Data" below](#)
- ["Example ConfigFile Policy" on the next page](#)

ConfigFile Definition

The first part of a ConfigFile policy (also known as ConfigFile variety) defines the path and file name of the configuration file that is associated with the policy. The ConfigFile definition contains the following attributes:

`Application`

Specifies the name of the managed application. This is usually the name of the SPI (for example `dbspi`).

`SubGroup`

Additional grouping mechanism that helps the SPI to manage configuration files by grouping them according to custom categories. For example, `dbspi` has one subgroup for every supported database vendor.

`Filename`

Specifies the file name of the configuration file (for example, `dbmon.cfg`).

ConfigFile Data

The data part of a ConfigFile policy contains the rules or instructions that configure the instrumentation on the node and begins with the following keyword:

`Data:`

The following generic keywords can be used after `Data:`

```
#$Installcommand=<command>
#$Deinstallcommand=<command>
```

`<command>` contains the command to be run, including any required parameters. If necessary, use quotation marks to handle all platforms. `$Installcommand` runs when the policy is deployed or enabled. `$Deinstallcommand` runs when the policy is removed or disabled.

`#$Commandtype=<value>`

`<value>` specifies the type of command to be used:

1—Executable (default)

If you do not specify the command type, the Config File policy assumes that the command is an executable.

2—VBScript or shell script

You do not need to add a `.vbs` or `.sh` extension to the command. Operations Management automatically appends the appropriate extension so that a single policy can be run on both Windows and UNIX nodes.

3—Perl script

Example ConfigFile Policy

When you deploy or enable the following example ConfigFile policy, the file `acme.cfg` is created, the last three lines are added to the file, and the file `install.bat` runs. When you remove or disable the policy, the file `acme.cfg` is removed and the file `deinstall.bat` runs.

Example:

```
Application=acme
SubGroup=acme_application
Filename=acme.cfg

Data:
#$Installcommand="C:\data\install.bat"
#$Deinstallcommand=C:\data\deinstall.bat"

AcmeSystemID = ACME
AcmeUserName = acme_root
AcmePassword = acme_password
```


Tasks

How to Create a ConfigFile Policy

1. In the ConfigFile Policy Editor, in the Properties page, type a **Name** for the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "[Properties Page](#)" on page 97.

2. In the Policy Data page, type the ConfigFile definition and data using the HP Operations Agent ConfigFile policy syntax. If you are creating a new policy, copy and paste template data from an existing policy template. Alternatively, click the  button to load policy data from a policy template file on your computer.

For details, see "ConfigFile Definition" on page 94 and "ConfigFile Data" on page 94.

You can also use policy parameters. For more details, see "Policy Parameters Tab" below.



3. Click **OK** to save the policy template.

UI Reference





This section includes:





- "Policy Data Page" below
- "Policy Parameters Tab" below
- "Properties Page" on the next page

Policy Data Page

UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	ConfigFile policies do not support syntax checking. You can click Check Syntax but the check fails to perform.
<code><policy data></code>	Policy data in text form. For details, see "ConfigFile Definition" on page 94 and "ConfigFile Data" on page 94.

Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.
	Delete Parameter: Delete the selected parameter from the list.
	Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter. Also checks for unused parameters, for which no corresponding variable exists in the policy template. If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore . If you click Change , the missing parameters are automatically created, and unused parameters are automatically deleted.

UI Element	Description
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Properties Page

UI Element	Description
Name	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.

¹(globally unique identifier)

UI Element	Description
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>


Configuring Flexible Management Policies

Flexible management policies enable you to configure HP Operations agents to send events to different servers based on the time of day and the event attributes. They also enable you to configure secondary servers, and servers that can start actions on the agent.








To access

You can create or edit a flexible management policy using the Flexible Management Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:




Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.

The Edit Aspect dialog box opens.




- d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **Flexible Management Template**, and then click **OK**.
 - To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Flexible Management Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:

Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **Flexible Management Templates** folder, and then do one of the following:
 - To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New Flexible Management Policy Editor opens.

- To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit Flexible Management Policy Editor opens.

Learn More

This section includes:

- ["Flexible Management Policies" below](#)
- ["Flexible Management Policy Syntax and Keywords" below](#)
- ["Time Templates" on page 105](#)
- ["Event Target Rules" on page 106](#)
- ["Action-Allowed and Secondary Servers" on page 107](#)

Flexible Management Policies

A flexible management policy, enables you to configure the following:

- Action-allowed and secondary servers that define which servers can run actions on the node.
- Date-and-time rules that define when the node sends events to which server.
- Event attribute rules that define when the node sends events to which server.

If you want the configuration to apply to all nodes in a given environment, you would develop one policy for all nodes. If you want varying configuration on different nodes, you would develop one policy for each configuration type.

Flexible Management Policy Syntax and Keywords

You can use the syntax described in the following sections as a basis for configuring flexible management policies.

- Special Characters Used in the Syntax

The syntax uses the following special characters:

- **e.** Denotes an empty string.
- **# (number sign).** Comment. Example: # This is a comment
- **\ (backslash).** Escape character. Use a backslash to escape quotation marks in a syntax string. Example: \"quotation\"

- Syntax for Responsible Server Configuration policies

Use the following syntax for responsible server configuration policies:

```

respmgrconfigs ::= <respmgrconfigs> RESPMGRCONFIG DESCRIPTION
<string> <respmgrconds> | e
respmgrconds  ::= SECONDARYMANAGERS <secondmgrs>
ACTIONALLOWMANAGERS <actallowmgrs>
                [MSGTARGETRULES <msgtargetrules>]
secondmgrs    ::= <secondmgrs> SECONDARYMANAGER NODE <node>
[DESCRIPTION <string>] | e
actallowmgrs  ::= <actallowmgrs> ACTIONALLOWMANGER NODE <node>
[DESCRIPTION <string>] | e
msgtargetrules ::= <msgtargetrules> MSGTARGETRULE DESCRIPTION
<string> <msgtargetrule> | e

```

```

msgtargetrule ::= MSGTARGETRULECONDS <mtrconditions>
MSGTARGETMANAGERS <msgtargetmgrs>
                | MSGTARGETRULECONDS <mtrconditions>
MSGTARGETMANAGERS <msgtargetmgrs> ACKNONLOCALMGR
mtrconditions ::= <mtrconditions> MSGTARGETRULECOND DESCRIPTION
<string> <mtrcond> | e
mtrcond       ::= <mtrcond> SEVERITY <severity> |
                <mtrcond> NODE <nodelist> |
                <mtrcond> APPLICATION <string> |
                <mtrcond> MSGGRP <string> |
                <mtrcond> OBJECT <string> |
                <mtrcond> MSGTYPE <string> |
                <mtrcond> TEXT <pattern> |
                <mtrcond> SERVICE_NAME <pattern> |
                <mtrcond> MSGCONDTYPE <msgcondtype> | e
severity      ::= Unknown | Normal | Warning | Critical |
                Minor | Major
msgcondtype   ::= Match | Suppress
nodelist      ::= <node> | <nodelist> <node>
node          ::= IP <ipaddress> | IP <ipaddress> <string> | IP
<ipaddress> <string> ID <string>
string        ::= "any alphanumeric string"
ipaddress     ::= <digits>.<digits>.<digits>.<digits>
pattern       ::= <string> <separators> <icase>
separators    ::= SEPARATORS <string>
icase         ::= ICASE

```

- Syntax for Time Templates

Use the following syntax for time templates:

```

timetmpls     ::= <timetmpls> TIMETEMPLATE <string>
                DESCRIPTION
                <string> <conditions> | e
conditions    ::= TIMETMPLCONDS <timetmplconds> | e
timetmplconds ::= <timetmplconds> TIMETMPLCOND <timetmplcond>
timetmplcond  ::= [TIMECONDTYPE <timecondtype>] [TIME FROM
                <time> TO <time>] [WEEKDAY <weekday>]
                [DATE <exact_date>] | e
timecondtype  ::= Match | Suppress
time          ::= <hh>:<mm>
weekday       ::= ON <day> | FROM <day> TO <day>
exact_date    ::= ON <date> | FROM <date> TO <date>
day           ::= Monday | Tuesday | Wednesday | Thursday
                | Friday | Saturday | Sunday
date          ::= <mm>/<dd>/<yyyy> | <mm>/<dd>/*

```

Note: The time template is compared with the creation time of the event on the node. Event creation time is always defined in GMT.

- Syntax for Management Responsibility Switching

Use the following syntax for templates that switch server responsibility:

```
configfile ::= [TIMETEMPLATES <timetmpls>] RESPMGRCONFIGS
            <respmgrconfigs>
```

- Syntax for Message Target Rules

Use the following syntax for templates that define message target rules:

```
msgtargetmgrs ::= <msgtargetmgrs> MSGTARGETMANAGER
                 TIMETEMPLATE <string> OPCMGR <node> |
                 <msgtargetmgrs> MSGTARGETMANAGER
                 TIMETEMPLATE <string> OPCMGR <node>
                 MSGCONTROLLINGMGR | <msgtargetmgrs>
                 MSGTARGETMANAGER TIMETEMPLATE <string>
                 OPCMGR <node> NOTIFYMGR | e
```

Note: You can replace <string> with \$OPC_ALWAYS to specify that the time condition is always true. To specify that the current primary server is always used as the event target server, replace <node> with \$OPC_PRIMARY_MGR. Pattern matching is only available in <string>.

- Keywords in Flexible Management Policies

Keyword	Definition
RESPMGRCONFIG	Responsible manager configuration.
DESCRIPTION	Short description of the manager.
SECONDARYMANAGERS	<p>Secondary managers of an agent. Each of these servers have permission to take over responsibility and become the primary manager for an agent.</p> <ul style="list-style-type: none"> ■ SECONDARYMANAGER: Name of the secondary manager. ■ NODE <node>: Node name of the secondary manager. ■ DESCRIPTION: Description of the secondary manager.

ACTIONALLOWMANAGERS	<p>Servers that are allowed to execute actions on the node. The action response is sent to this manager. Only the primary manager can configure action-allowed managers for an agent.</p> <ul style="list-style-type: none"> ■ ACTIONALLOWMANAGER: Name of the manager allowed to execute actions on the node. ■ NODE: Node name of the action-allowed manager. You can use the variable \$OPC_PRIMARY_MGR to specify that this node name is always the node name of the primary manager. ■ DESCRIPTION: Short description of the action-allowed manager.
MSGTARGETRULES	<p>Event target rules.</p> <ul style="list-style-type: none"> ■ MSGTARGETRULE: Rule to configure the event target conditions and the event target manager. ■ DESCRIPTION: Description of the event target rule.

MSGTARGETMANAGERS	<p>Event target managers. Server to which the agents send events, as well as the action responses to those events. The result of an event is sent to only one server. The keyword is also used to escalate events from one server to another.</p> <ul style="list-style-type: none">■ MSGTARGETMANAGER: Event target manager. Server to which you forward an event. Always specify the IP address of the target server as 0.0.0.0. The real IP address is then resolved by the domain name server (DNS).■ TIMETEMPLATE: Time template. Name of the time template corresponding to the target manager. If the time condition is always true, you can use the variable \$OPC_ALWAYS. If you use this keyword, event transfers to the target manager will not depend on the time.■ OPCMGR: Node name of the target manager. You can use the keyword \$OPC_PRIMARY_MGR to indicate that this will always be the primary manager.■ MSGCONTROLLINGMGR: Event-controlling manager. Enables event target manager to transfer control of a message.■ NOTIFYMGR: Notify manager. Enables the event target manager to notify itself. This attribute is set by default if no attribute is defined for the event target manager.■ ACKNONLOCALMGR: Enables an event rule to force a direct acknowledgment of a notification event on a source server.
-------------------	--

MSGTARGETRULECONDS	<p>Event target rule conditions.</p> <ul style="list-style-type: none"> ■ MSGTARGETRULECOND: Condition that tells the agent to which server to send specific events. Events are sent based on event attributes or time. The agent evaluates the event target conditions by reading the file mgrconf. If the mgrconf file does not exist, the events are sent to the server name stored in the primmgr file. If the primmgr file does not exist, events are sent according to instructions set using the ovconfchg command-line tool. ■ DESCRIPTION: Description of the event target rule condition. ■ SEVERITY: Severity level of the event. Can be Unknown, Normal, Warning, Minor, Major, Critical. ■ NODE <node>: One or more node names, separated by spaces. You can specify a node in different ways (for example, <code>NODE IP 0.0.0.0 hpbbn</code>). If the node is defined using the format <code>IP <ipaddress></code> or <code>IP <ipaddress> <string></code>, you should use the IP address "0.0.0.0." The real IP address is then resolved by the domain name server (DNS). ■ APPLICATION: Application name. ■ MSGGRP: Category name (also known as message group name in HP Operations Manager). ■ OBJECT: Object name. ■ MSGTYPE: Description of the type. ■ MSGCONDTYPE: Event condition type: <ul style="list-style-type: none"> ○ Match Condition is true if the specified attributes are matched. ○ Suppress Condition is true if the specified attributes are not matched. ■ TEXT: A string containing all or part of the event title. Pattern-matching may be used. ■ SERVICE_NAME: A string containing the unique identifier of the service. Pattern-matching may be used, for example: <code>SERVICE_NAME "Service<*> [A B]"</code> ICASE
--------------------	--

Time Templates

A time template is a set of conditions (or rules) that tells the agent to which server and at what time a given node should send specific events. You create time conditions and save them in time templates. You can combine simple rules to set up more complex constructions (for example, "on Monday, Wednesday and Thursday from 10 am to 11:35 am from January to March"). Time

conditions are defined using the 24-hour clock notation (for example, for 1:00 p.m., you would enter "13:00").

- Setting Time Intervals

You can set several different time intervals as follows:

- **No Time.** If you specify no particular time, day of the week, or year, HP Operations Agent assumes you want the condition to be true from 00:00 to 24:00 every day of the year, every year. If you specify a condition, HP Operations Agent assumes the condition should apply continually for the time and day specified.

For example, specifying "Tuesdays" triggers a condition every Tuesday from 00:00 to 24:00 throughout the year, every year.

- **Span of Time.** Specify a time range (for example, "from 7:00 to 17:00").
- **Wildcard (*) Date or Period.** Use wildcards (*) in dates or periods of time (for example, to set a condition for January 31 every year, you would enter "1/31/*").

- Configuring Time-Indifferent Templates

HP Operations Agent requires that you set up a time template for the event target rules even if your scheduled action is time-indifferent. Use the variable \$OPC_ALWAYS to configure time-indifferent templates.

Event Target Rules

You can use a list of event target rules to determine to which server an event should be sent.

An event target rule consists of three parts:

- Event attribute rule
- Time template
- Defined server
- Example of an Event Target Rule for Printing Group

An event target rule for a printing group would have the following conceptual structure:

Example:

category = "printing"

current time fits time template 2(event) --> mgr 2

current time fits time template 1(event) --> mgr 1

current time fits time template 3(event) --> mgr 3

In this example, HP Operations Agent forwards all events with the category "printing" that meet the time conditions in template 1 to the server 1. All events that meet the time conditions in template 2 will be forwarded to server 2. Time template 3 functions the same.

- Example of an Event Target Rule for a Database Group

An event target rule for a database group would have the following conceptual structure:

Example:

```
category = "database"
```

```
current time fits time template 1 .....(event) --> mgr 2
```

```
current time fits time template 2 .....(event) --> mgr 3
```

```
current time fits time template 3 .....(event) --> mgr 1
```

In this example, HP Operations Agent forwards all events with the category "database" that meet the time conditions in template 1 to the server 2. All events that meet the time conditions in template 2 are sent to the server 3. And so on.

Action-Allowed and Secondary Servers

By default, only a node's primary server can start actions on the node. To enable other servers to start actions on a node, you must specify action-allowed servers in a flexible management policy and deploy it to the node. This policy is important if you forward events that have automatic and operator-initiated actions to other servers.

The primary server is initially set during the agent installation. To enable other servers to become a node's primary server, you can specify secondary servers in the same policy. The secondary servers can deploy policies and packages to the node, without first becoming the primary management server.

A flexible management policy that configures action-allowed and secondary servers must contain the following statements:

```
RESPMGRCONFIGS
  RESPMGRCONFIG DESCRIPTION "Policy description"
  SECONDARYMANAGERS
  ACTIONALLOWMANAGERS
```

You can add to this minimal policy as many secondary servers and action-allowed managers as you need. You can specify the IP address or host name, followed by the core ID of each server. To specify only a host name, use the IP address 0.0.0.0.

To get a server's core ID, open a command prompt and then type the following command:

```
bbcutil -ping <server>
```

The response includes the core ID of the server.

Example:

```
RESPMGRCONFIGS
  RESPMGRCONFIG DESCRIPTION "Enable manager1, manager2, and 192.168.1.3"
  SECONDARYMANAGERS
    SECONDARYMANAGER NODE IP 0.0.0.0 "manager1.example.com"
                          ID "e77b4992-5d78-753f-1387-c01230fe2648"
    SECONDARYMANAGER NODE IP 0.0.0.0 "manager2.example.com"
                          ID "68f01602-8bfa-7557-0403-8467ba97477a"
  ACTIONALLOWMANAGERS
    ACTIONALLOWMANAGER NODE IP 0.0.0.0 "manager1.example.com"
```

```

ACTIONALLOWMANAGER NODE IP 0.0.0.0 "manager2.example.com"
                                ID "e77b4992-5d78-753f-1387-c01230fe2648"
ACTIONALLOWMANAGER NODE IP 192.168.1.3
                                ID "68f01602-8bfa-7557-0403-8467ba97477a"
                                ID "bc180332-d338-7557-0384-a10be68caa36"

```

The example policy specifies manager1.example.com and manager2.example.com as secondary and action-allowed managers. It also specifies that the management server with IP address 192.168.1.3 is an action-allowed manager.


Tasks

How to Create a Flexible Management Policy

1. In the Flexible Management Policy Editor, in the Properties page, type a **Name** for the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "[Properties Page](#)" on page 110.

2. In the Policy Data page, type the flexible management policy data using the flexible management policy syntax. If you are creating a new policy, copy and paste template data from an existing policy template. Alternatively, click the  button to load policy data from a policy template file on your computer.

For details, see "[Flexible Management Policy Syntax and Keywords](#)" on page 100.

You can also use policy parameters. For more details, see "[Policy Parameters Tab](#)" on the next page.



3. Click **OK** to save the policy template.

UI Reference

This section includes:









- "[Policy Data Page](#)" below
- "[Policy Parameters Tab](#)" on the next page
- "[Properties Page](#)" on page 110

Policy Data Page

UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Flexible Management policies do not support syntax checking. You can click Check Syntax but the check fails to perform.

UI Element	Description
<policy data>	Policy data in text form. For details, see "Flexible Management Policy Syntax and Keywords" on page 100.

Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Properties Page

UI Element	Description
Name	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.

¹(globally unique identifier)

UI Element	Description
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>


Configuring Log File Entry Policies

Log file entry policies enable you to monitor log files for entries that match specific rules. You can configure policies to create events and launch commands whenever a log file entry matches one of your rules.








To access

You can create or edit a log file entry policy using the Logfile Entry Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:

Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.

The Edit Aspect dialog box opens.

 - d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **Logfile Entry Template**, and then click **OK**.
 - To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.




The Logfile Entry Policy Editor opens.
- To open the editor from the Policy Templates manager:

- a. Open the Policy Templates manager:




Admin > Operations Management > Monitoring > Policy Templates

- b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.

- c. Click the **Logfile Entry Templates** folder, and then do one of the following:

- To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New Logfile Entry Policy Editor opens.

- To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit Logfile Entry Policy Editor opens.

Tasks

How to Create a Log File Entry Policy

1. In the Log File Entry Policy Editor, in the Properties page, type a **Name** for the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "[Properties Page](#)" on page 126.

2. In the Source page, define the log file that the policy reads (for example, the path and name of the log file).

- a. In **Log File Path / Name**, type the full path to the log file on nodes.

- b. *Optional.* Preprocess the log file.

If you want to reformat an original log file before the agent reads it, you can preprocess it using a command or program that you provide. For example, you can preprocess a binary log file to produce a text file in a format that the agent can then read.

To preprocess a log file:

- i. Select the **Preprocessing** check box.
- ii. In **File to be executed**, type the complete path and extension of the command or program that preprocesses the log file. The file that you specify must exist on the node.

If **Log file path \ name** is empty, the agent runs the command at the polling interval that you specify. If **Log file path \ name** contains the path of a log file, the agent runs the command at the specified polling interval only if the log file has changed.

- iii. *Optional.* In **File to be read**, type the full path of the log file that the preprocessing command creates or updates.

If you specify a path in **File to be read**, the agent reads this log file. If you leave **File to be read** empty, the agent reads the log file that you specify in **Log file path \ name** instead.


- c. Click **Logfile Character Set** and select the character set of the log file that you want to monitor.

For more details, see "[Source Page](#)" on page 127.

3. *Optional.* In the Defaults page, set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

Note: You can set defaults for only a subset of event attributes. You can set the other event attributes within individual rules.

For more details, see "[Event Attributes Tab](#)" on page 119, "[Event Correlation Tab](#)" on page 120, "[Instructions Tab](#)" on page 121, and "[Advanced Tab](#)" on page 117.

4. In the Rules page, define one or more policy rules.
 - a. In the Policy Rules list, click the  button, and then click one of the following options:
 - **Event on matched rule:** Use this option if you want to send an event to BSM when the conditions are met.
 - **Suppress on matched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are met.
 - **Suppress on unmatched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are *not* met.
 - b. Click the **Rule Description** and type a brief description of the rule.

For more details, see "[Policy Rules List](#)" on page 124.

5. In Rule Content, use the Condition tab to specify a string that the policy searches for in the log file that the policy monitors.

You can use policy variables and policy parameters in most text boxes. Pattern matching expressions can only be entered in the **Logfile line matches** text boxes.

For example, set these conditions to match the following log file line:

```
Warning: too many users on node celery.example.com
```

- **Node equals:** celery.example.com
- **Logfile line matches:** ^Warning:<*.text>on node<@.node>\$

This pattern matches any message that starts with `Warning` and assigns `too many users` to `text` and `celery.example.com` to `node`.

For more details, see "[Condition Tab](#)" on page 117 and "[Pattern Matching in Policy Rules](#)" on page 357.

6. *Optional.* If you are creating a rule of the type 'event on matched rule', set attributes for events that you want the policy to send. You can override the default event attributes here. You can also write instructions that help operators handle the associated event and configure actions to

solve problems automatically or manually.

In text boxes, you can use indicators, policy variables, and policy parameters.

For more details, see "Event Attributes Tab" on page 119, "Event Correlation Tab" on page 120, "Custom Attributes Tab" on page 118, "Instructions Tab" on page 121, "Advanced Tab" on page 117, and "Actions Tab" on the next page.

7. *Optional.* In the **Options** page, configure options for local event logs, unmatched events, and pattern matching.

For more details, see "Options Page" on page 121.

8. Click **OK** to save the policy template.

UI Reference

This section includes:

- "Actions Tab" on the next page
- "Advanced Tab" on page 117
- "Condition Tab" on page 117
- "Custom Attributes Tab" on page 118
- "Defaults Page" on page 119
- "Event Attributes Tab" on page 119
- "Event Correlation Tab" on page 120
- "Indicators Tab" on page 120
- "Instructions Tab" on page 121
- "Options Page" on page 121
- "Policy Data Page" on page 123
- "Policy Parameters Tab" on page 123
- "Policy Rules List" on page 124
- "Policy Variables Tab" on page 125
- "Properties Page" on page 126
- "Rules Page" on page 127
- "Source Page" on page 127

Actions Tab

UI Element	Description
Automatic command	Automatic command that runs when the rule is matched. For example, you could configure a log file entry policy to automatically delete the contents of C:\Temp when the log file contains "The C: disk is at or near capacity."
Command	Command and parameters to run when the command is started for this event. The command runs on the node you specify in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information on <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (\$AGENT_USER). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.
Send event immediately	Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.

UI Element	Description
Wait until local command completes and then	Options that can help to reduce the amount of unnecessary network traffic to the BSM server. For example, if an automatic command solves the problem that generated the event, you may choose not to inform the BSM server. <ul style="list-style-type: none"> • Send the event • Send the event if the local command fails • Send the event only if the local command is successful
Operator-initiated command	Operator-initiated command that is attached to the event that the rule sends to the Event Browser. This command can be started by the BSM user from the Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.
Command	Command and parameters to run when the command is started for this event. The command runs on the node specified in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information about <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.

Advanced Tab

Note: In the default event attributes, you cannot set the Event Drilldown URL attribute. You can set this event attribute within individual rules.



UI Element	Description
Application	Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM, 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 RTSM, the object attribute is a simple string-type attribute (for example, C:, and /dev/spool).
HPOM Service ID	ID of the service associated with 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.
Enable Agent MSI	<p>The message stream interface (MSI) allows external applications to interact with the internal event flow of HP Operations Agent. The external application can be a read-write application, for example, an event processing program that can read events, modify attributes, and generate new events for retransmission to the server. The application could also read events, or send its own events.</p> <p>Divert events. Divert an event to the MSI instead of to the server when an event is requested by an external application.</p> <p>Copy events. Send the event to the server, and a copy of the event to the MSI.</p> <p>If the agent MSI is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Agent MSI. Applies the agent MSI settings configured in the event defaults to this rule.</p> <p>Override default settings for Agent MSI: Enables you to configure specific agent MSI settings for this policy rule.</p>

Condition Tab

UI Element	Description
Node equals	<p>Fully qualified domain name, node name, or IP address that the policy compares with the node in the log file line. Type a value in this field to match the log file line from a specific node.</p> <p>Separate multiple entries with the OR operator () or leave blank to match all nodes.</p> <p>Example: <code>celery.example.com broccoli.example.com</code></p>

UI Element	Description
Logfile line matches	<p>Pattern that you want the policy to compare with the log file line.</p> <p>Note: Log file policies read each line of a log file individually. Therefore, you cannot match patterns that span multiple lines in the log file.</p> <p>Tip: You can use standard HP Operations Agent pattern-matching rules when matching values. Click ► to open the pattern matching expression toolbox. The toolbox displays the following:</p> <ul style="list-style-type: none"> • Pattern Matching Expressions. Click an expression to insert it in the pattern. • Variable Bindings Options. Variable bindings options include 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.

Custom Attributes Tab

UI Element	Description
	Create New Custom Attribute: Creates a new custom attribute with the default name CA_n. To rename the custom attribute, double-click the name to select it and type the new name.
	Delete Custom Attribute: Deletes an existing custom attribute.

UI	
Element	Description
Name	<p>The name of the custom attribute. The name is case-insensitive.</p> <p>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.</p> <p>The following custom attribute names cannot be used because they are reserved for internal use:</p> <p>Description</p> <p>EtiHint</p> <p>HP_OPR_SAAS_CUSTOMER_ID</p> <p>NoDuplicateSuppression</p> <p>RelatedCiHint</p> <p>SourceCiHint</p> <p>SourcedFromExternalId</p> <p>SourcedFromExternalUrl</p> <p>SubCategory</p> <p>SubCiHint</p>
Value	Value of the custom attribute.

Defaults Page

The Defaults page enables you to set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

For more details, see ["Event Attributes Tab"](#) below, ["Event Correlation Tab"](#) on the next page, ["Instructions Tab"](#) on page 121, and ["Advanced Tab"](#) on page 117.

Event Attributes Tab

Note: In the default event attributes, you can set only the Severity, Category, and Node attributes. You can set the other event attributes within individual rules.

UI	
Element	Description
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.

UI Element	Description
Send with closed status	Sets the event's lifecycle status to Closed before sending it to the Event Browser in Operations Management.

Event Correlation Tab



Note: In the default event attributes, you cannot set the following attributes:




- Close Events with Key
- Suppress Deduplication on Server

You can set these event attributes within individual rules.

UI Element	Description
Event Key	An identifier used to identify duplicates and for Close Events with Key.
Enable Event Suppression	<p>Enables event suppression for the events generated by this policy.</p> <p>If event suppression is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Event Suppression. Applies the event suppression settings configured in the event defaults to this rule.</p> <p>Override default settings for Event Suppression: Enables you to configure specific event suppression settings for this policy rule.</p>

Indicators Tab

UI Element	Description
	<p>Refresh. Loads the configured indicators from the BSM server.</p> <p>Note: Loading indicators from the BSM server may take a few seconds.</p>
	<p>Shows or hides the Select drop target format drop-down panel:</p> <ul style="list-style-type: none"> • Use Indicator States. Click to change the drop target format to indicator states only. • Use Indicator Names and States. Click to change the drop target format to indicator names and states.

UI Element	Description
<Search ...>	<p>Entered search string is used to search the indicators and highlight only the indicators containing the specified string.</p> <p>To search for indicators with specific text strings in the name, type the string in the <Search ...> field and click the  button. The first matching indicator is selected in the list of rules. Click the  and  buttons to move to the previous and next matching indicator.</p>
<Indicators>	<p>Hierarchy of configuration item types with associated health indicators (HIs) and event type indicators (ETIs). To insert an indicator in a policy, drag and drop the indicator from the Indicators tab to the relevant field in the policy.</p>

Instructions Tab

UI Element	Description
Instructions	<p>Instructions that you want to accompany the event.</p> <p>Events generated by a policy can include instructions that explain what to do when the event is generated. This instruction text can often help an operator to solve a problem when a particular type of event is received. The operator can view the instructions included with an event by viewing the Event Details pane in the Event Browser. You can define default instructions for all rules in a policy. You can also override the default with different instructions for any rule.</p> <p>You can type URLs in the text, and the Event Browser automatically converts them into clickable hyperlinks. For example, you can add URLs of external Web sites, support sites, documentation repositories, troubleshooting information, and similar sites.</p> <p>To add a link, type any URL that begins with one of the following URI scheme names:</p> <ul style="list-style-type: none"> • http:// • https:// • ftp:// • ftps://



Options Page

UI Element	Description
Log Local Events	<p>Defines 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:</p> <p>Windows: %OvDataDir%\log\OpC\opcmsglg</p> <p>AIX, HP-UX, Linux, and Solaris: /var/opt/OV/log/OpC/opcmsglg</p>



UI Element	Description
that match a rule and trigger an event	Logs any events in the event source that match the policy rules.
that match a rule and are ignored	Logs any events in the event source that are suppressed. (Suppressed events are not sent to the Event Browser.)
that do not match any rule	Logs any events that do not match any of the rules in the policy.
Unmatched Events	<p>Send an event to the 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.</p> <p>Each policy that sends unmatched events to the Event Browser creates an event with the default values of the policy.</p> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p>
are sent to the Event Browser	Sends unmatched events to the Event Browser.
are sent to the Closed Events Browser	Sends unmatched events to the Closed Events Browser.
are ignored	Ignores unmatched events.
Pattern Matching Options	Defines case sensitivity and field separators for all rules.
Case sensitive check	Defines whether the case (uppercase or lowercase) of a text string is considered when the pattern of a rule is compared with the source data. When switched on, a match only occurs if the use of uppercase and lowercase letters is exactly the same in both the source data and the pattern. This is the default setting.







UI Element	Description
Field Separators	<p>Defines 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:</p> <ul style="list-style-type: none"> • \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 (\) <p>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).</p> <p>If you leave this box empty, the default separators (a blank and the tab character) are used by default.</p> <p>You can set case sensitivity and separator characters for individual rules in a policy by clicking the ▶ button in rule's match condition.</p>
Apply to All	<p>Applies the pattern matching options to all existing rules in a policy. This overwrites any modifications made to the pattern matching options in individual rules.</p> <p>If you change the pattern matching options and do not click Apply to all, they only apply to all new rules in a policy.</p>

Policy Data Page


UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Check Syntax: Validates the syntax of the policy data. If the policy syntax is incorrect, the validation tool reports an error and points to the corresponding line and position of the unexpected token (for example the incorrect keyword).
<policy data>	Policy data in text form. The data uses the HP Operations Agent policy syntax.










Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.

UI Element	Description
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Policy Rules List

UI Element	Description
	<p>Create New Rule: Provides the following options:</p> <ul style="list-style-type: none"> Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM.

UI Element	Description
	Copy Rule. Copies the selected rule. You can then rewrite the description of the copied rule and edit the rule.
	Delete Rule. Deletes the selected rule.
	Move Up. Moves the selected rule higher in the rule order.
	Move Down. Moves the selected rule lower in the rule order.
<Move to>	Entered number is used to select the rule with that sequence number in the list of rules. To select a specific rule in the rule list, type the rule's sequence number in the <Move to> field and click the  button.
<Search rules>	Entered search string is used to search the rule descriptions and highlight only the rules containing the specified string. To search for rules with specific text strings in the rule description, type the string in the <Search rules> field and click the  button. The first matching rule is selected in the list of rules. Click the  and  buttons to move the previous and next matching rule.
	Activate/Deactivate Rule Filter. Activates and deactivates the rule filter.
Seq.	Sequence number of the rules. Rules are evaluated in a specific order. When one condition is matched, no additional rules are evaluated.
Rule Description	Description of the rule. It is good practice to use a description that helps you remember what the rule does
Rule Type	<ul style="list-style-type: none"> • Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. • Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. • Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM. <p>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.</p>

Policy Variables Tab

You can use the following variables in log file entry policies. If a variable returns values that contain spaces, surround the variable with quotation marks.

Variable	Description
<\$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-event basis. If the policy is reading 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. Sample output: SU 03/19 16:13 + tty7 bill-root

Properties Page

UI Element	Description
Name	Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed. The name is set when the policy is created and cannot be changed in new versions of a policy.
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.
Version	The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy. Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.
Change Log	Text that describes what is new or modified in this version of the policy.

¹(globally unique identifier)

UI Element	Description
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	<p>Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.</p>
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

Rules Page

The Rules page enables you to define one or more policy rules.

For more details, see ["Policy Rules List" on page 124](#), ["Condition Tab" on page 117](#), ["Event Attributes Tab" on page 119](#), ["Event Correlation Tab" on page 120](#), ["Custom Attributes Tab" on page 118](#), ["Advanced Tab" on page 117](#), and ["Actions Tab" on page 115](#).

Source Page

UI Element	Description
------------	-------------

Log File Path / Name	<p>Path and name of the log file that the policy reads. Type the drive letter and the full path for the location of this file on the node.</p> <p>Tip:</p> <ul style="list-style-type: none"> You can use Windows environment variables (for example <code>winnt</code> or <code>clusterlog</code>) to make your policies more flexible. The proper syntax for these variables is <code><\$variablename></code>, for example <code><\$winnt></code>. You can also call a script or command that returns the path and name of the log file you want to access. For example, type <pre><`command`></pre> <p>where <code>command</code> is the name of a script that returns the path and name of the log file you want the policy to read. The command can also return more than one log file path separated by spaces. The HP Operations Agent processes 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 process multiple instances of a log file.</p> <p>Caution: You must ensure that the log file can be processed. For example, log files that contain binary data cannot be read by the policy and may cause the policy to stop responding or even quit. If your log files contain binary data, use log file preprocessing to preprocess your files.</p>
Preprocessing	<p>If you want to reformat an original log file before the agent reads it, you can preprocess it using a command or program that you provide. For example, you can preprocess a binary log file to produce a text file in a format that the agent can then read.</p>
File to be executed	<p>Path and name with extension of the command or program that preprocesses the log file. The file that you specify must exist on the node.</p> <p>If Log File Path \ Name is empty, the agent runs the command at the polling interval that you specify. If Log File Path \ Name contains the path of a log file, the agent runs the command at the specified polling interval only if the log file has changed.</p>
File to be read	<p>Path of the log file that the preprocessing command creates or updates.</p> <p>If you specify a path in File to be read, the agent reads this log file. If you leave File to be read empty, the agent reads the log file that you specify in Log File Path \ Name instead.</p>

Polling Interval	<p>Determines how often the policy reads 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 <i>after</i> the first polling interval passes. A shorter polling interval is better when you are testing a policy.</p> <p>To modify the time, click the ▼ button and use the drop-down lists to specify increments of hours, minutes, or seconds.</p> <p>To insert a parameter in a time field, type the parameter in the format <code>%%<variable_name>%%</code> or drag and drop the parameter from the Policy Parameters tab.</p> <p>Default value: 5 minutes</p>
Logfile Character Set	<p>Name of the character set used by the log file that the policy reads.</p> <div data-bbox="488 783 1370 1031" style="background-color: #f0f0f0; padding: 10px;"> <p>Note: 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 BSM. If you are unsure of which character set is used by the log file that the policy reads, consult the documentation of the program that writes the file.</p> </div> <p>Default value: UTF-8</p>
Send event if log file does not exist	<p>The agent sends an event if the specified log file does not exist.</p> <p>Default value: not selected</p>
Close after reading	<p>The policy keeps the log file open (and retains its file handle) after reading it. Do not use a polling interval of less than one minute when this option is selected.</p> <p>If you do not select this option and the name of the log file changes, the policy continues to read the original log file instead of processing any new log file with the specified name. Consider the following example: a policy reads the log file <code>syslog.log</code>. Mondays at 23:59, the file is renamed to <code>syslog.monday</code>, and a new version of <code>syslog.log</code> is created for the Tuesday log. Without Close after reading being selected, the policy continues to read <code>syslog.monday</code> because the file handle refers to the original, renamed file.</p> <p>Default value: not selected</p>

Read Mode	The read mode of an log file policy indicates whether the policy processes the entire file or only new entries.	
	<p>Read from last position. The policy reads only new—appended—entries written in the log file while the policy is activated. If the file decreases in size between readings, then the entire file is read. Entries that are added to the file when the policy is disabled are not processed by the policy.</p> <p>Choose this option if you are concerned only with entries that occur when the policy is enabled.</p>	<p>Advantage: No chance of reading the same entry twice. (Unless the file decreases in size because some entries were deleted.)</p> <p>Disadvantage: Entries written to file while the policy is disabled or the agent is not running are not processed by the policy.</p>
	<p>Read from beginning (first time). The policy reads the complete log file each time the policy is activated or the agent restarts. This ensures that all entries in the file are compared with the rules in the policy. Each successive time that the policy reads the file, only new (appended) entries in the file are processed.</p> <p>Choose this option if you want to ensure that every existing and future entry in the file is processed by the policy while it is activated.</p>	<p>Advantage: Every existing and future entry in the file will be processed by the policy.</p> <p>Disadvantage: Duplicate entries can occur if an activated policy is deactivated and reactivated, or if the agent stops and restarts.</p>
	<p>Read from beginning (always). The policy reads the complete log file every time it detects that the file has changed. The policy scans the file at the specified polling interval. If no change is detected, the file is not processed. Any 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 the policy reads a file that is overwritten, rather than appended.</p>	<p>Advantage: Ensures that files that are overwritten are correctly processed.</p> <p>Disadvantage: Only valid for files that are overwritten, rather than appended.</p>
<p>Note: Every policy reads the same log files independently from any other policies. This means, for example, that if "Policy 1" with read mode Read</p>		

	<p>from beginning (first time) is activated and "Policy 2" with the same read mode already exists, "Policy 1" still reads the entire file after it has been activated.</p> <p>Default value: Read from last position</p>
--	---


Configuring Measurement Threshold Policies

Measurement threshold policies enable you to monitor performance metrics from various sources. You can configure policies to create events and launch commands whenever a performance metric crosses a threshold that you specify.








To access

You can create or edit a measurement threshold policy using the Measurement Threshold Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:

Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.




The Edit Aspect dialog box opens.




- d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **Measurement Threshold Template**, and then click **OK**.
 - To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Measurement Threshold Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:

Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.

- c. Click the **Measurement Threshold Templates** folder, and then do one of the following:
 - To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New Measurement Threshold Policy Editor opens.
 - To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit Measurement Threshold Policy Editor opens.

Learn More

This section includes:

- ["Measurement Threshold Policies" below](#)
- ["Instance Filters" below](#)
- ["opcmon Command" on the next page](#)
- ["Java API" on the next page](#)
- ["C API" on the next page](#)

Measurement Threshold Policies

Measurement threshold policies can monitor values received from the Embedded Performance Component (Coda), from external processes (opcmon), or from programs that the policies run. They can also monitor values in a Management Information Base, in the Windows Real Time Performance Monitor, and in a Windows Management Instrumentation database.

Measurement threshold policies provide predefined minimum and maximum processing rules, which set a threshold limit under which the monitored value must drop or that the monitored value must exceed for a rule to match. However, you can also write your own Perl or VB scripts to evaluate the sources you are monitoring and determine the threshold limit.

You need to use a script to determine the threshold for your measurement threshold policy if the source that you choose delivers something other than a number or a Boolean value, or if you want to evaluate multiple sources. A script makes it possible for you to perform your own calculations and decide if the threshold has been crossed.

Policies with only one data source can process data using the predefined minimum or maximum rules, or using scripts. Policies with more than one data source require you to write scripts to evaluate the threshold levels.

Instance Filters

Instance filters provide a way for the policy to apply different sets of threshold levels to different instances of the object being monitored. For example, a threshold policy that monitors disk usage will apply the same threshold to all disks, but if you specify instance filters, you can specify one set of threshold levels for disk C:, another set for disk D: and so on.

Instance filters can be used with policies that evaluate the threshold based on a minimum, maximum, or scripts. Instance filters are not available for threshold policies based on the source MIB. Switching a policy to instance filters cannot be reverted.

opcmon Command

The `opcmon` command enables you to submit monitored values to the HP Operations Agent from a command prompt or script. HP Operations Agent evaluates and processes the submitted values based on measurement threshold policy configurations.

```
opcmon [-help]
        <object_name>[-<shortname>]=<value>
        [-object <object>]
        [-option <var>=<value>]
```

`opcmon` is available in one of the following locations.

- AIX, HP-UX, Linux, and Solaris: `/opt/OV/bin/opcmon`
- Windows 32-bit: `%OvInstallDir%\bin\opcmon`
- Windows 64-bit: `%OvInstallDir%\bin\win64\opcmon`

For more details, see the *HP Operations Agent Reference Guide*.

Java API

The Java API enables you to create Java programs that submit monitored values to the HP Operations Agent. The required JAR files (`jopcagtbase.jar` and `jopcagtmsg.jar`) are installed with the HP Operations Agent in one of the following locations:

- AIX: `/usr/lpp/OV/java/`
- HP-UX, Linux, and Solaris: `/opt/OV/java/`
- Windows: `%OvInstallDir%\java\`

Javadoc style class documentation is available in the following location:

- AIX: `/usr/lpp/OV/www/htdocs/jdoc_agent/index.html`
- HP-UX, Linux, and Solaris: `/opt/OV/www/htdocs/jdoc_agent/index.html`
- Windows: `%OvInstallDir%\www\htdocs\jdoc_agent\index.html`

For more details, see the *HP Operations Agent Reference Guide*.

C API

The C API enables you to create C programs that submit monitored values to the HP Operations Agent. The required header file (`opcapi.h`) is installed with the HP Operations Agent in one of the following directories:

- AIX: `/usr/lpp/include/`
- HP-UX, Linux, and Solaris: `/opt/OV/include/`
- Windows: `%OvInstallDir%\include\`

The required libraries (`libopcagtapi`, and on UNIX and Linux `libOvXp1`) are installed with the HP Operations Agent in one of the following directories:

- AIX 32-bit: /usr/lpp/OV/lib/
- AIX 64-bit: /usr/lpp/OV/lib64/
- HP-UX Itanium: /opt/OV/lib/hpux32
- HP-UX PA-RISC: /opt/OV/lib/
- Linux and Solaris 32-bit: /opt/OV/lib/
- Linux and Solaris 64-bit: /opt/OV/lib64/
- Windows 32-bit: %OvInstallDir%\bin\
- Windows 64-bit: %OvInstallDir%\bin\win64\

For more details about the C API and required compiler options, see the *HP Operations Agent Reference Guide*.


Tasks

How to Create a Measurement Threshold Policy

1. In the Measurement Threshold Policy Editor, in the Properties page, type a **Name** for the policy.


You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "[Properties Page](#)" on page 154.

2. In the Source page, define the sources that you want to monitor.
 - a. Click  **Add Source** and select one of the following source types:
 - **Add Embedded Performance Component Source:** Use this option if you want to monitor performance counter and instance data collected by the Embedded Performance (Coda) component.
 - **Add External Source:** Use this option if you want to monitor data sent from an external program (the opcmn command line tool, for example). HP Operations Agent does not poll the external program but waits for values to arrive.
 - **Add Management Information Base Source:** Use this option if you want to monitor data stored in a Management Information Base (MIB).
 - **Add Program Source:** Use this option if you want to monitor data sent from an external program. HP Operations Agent runs the external program at each polling interval.
 - **Add Real Time Performance Measurement Source:** Use this option if you want to monitor data gathered by the Windows performance monitor.
 - **Add Windows Management Instrumentation Source:** Use this option if you want to monitor data stored in the WMI database.
 - b. Type a **Short Name** and optionally a **Description** of the source. These labels can help you recognize the value or metric for the threshold source.

- c. *Optional.* Click **Store in Coda** to configure the policy to store the collected data in the Embedded Performance Component (Coda). Other users can then consume the data from Coda (for example, to create graphs in Performance Graphing).

You can enter a **Data Source**, **Object** and **Metric** of your own invention here. The policy will create them in the Embedded Performance Component (Coda) and will store the data from the policy's source each polling interval.

- d. *Optional.* Click  and add another source to the policy. You can add as many sources as required.
- e. Accept the default **Polling Interval** of five minutes or set another interval.

For more details, see ["Source Page" on page 156](#).

3. *Optional.* In the Defaults page, set default attributes for all events that the policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

Note: You can set defaults for only a subset of event attributes. You can set the other event attributes within individual rules.

For more details, see ["Event Attributes Tab" on page 144](#), ["Instructions Tab" on page 149](#), and ["Advanced Tab" on page 142](#).

4. In the Processing page, set options that determine how the collected data is processed by the policy.


- a. Select how you want to set the threshold level:
 - o **Minimum:** Sets a minimum threshold level under which the monitored value must drop for a rule to match.
 - o **Maximum:** Sets a maximum threshold level that the monitored value must exceed for a rule to match.
 - o **Perl Script:** Configures the policy to use a Perl script that evaluates the sources you are monitoring and determines the threshold limit.
 - o **VB Script:** Configures the policy to use a VB script that evaluates the sources you are monitoring and determines the threshold limit.
- b. *Optional.* Click **Use Instance Filter** to enable instance filters for the policy. Switching to instance filters cannot be reverted.
- c. *Optional.* If you are using scripts to set and evaluate the threshold level, you can choose how the policy processes multiple instances of the value being measured.

Click **Process each instance separately** if you want each instance to be processed by the policy separately. For example, if the policy monitors each CPU in a multiple CPU server, and the activity of all CPUs exceeds the threshold, an event will be generated for each CPU.

Alternatively, accept the default, which is to process all instances once.

For more details, see ["Processing Page" on page 153](#).

5. If instance filters are not enabled, define one or more threshold rules in the Rules page.

- a. Click  **Create New Threshold** to add a new threshold rule.
- b. In Threshold Definition, use the Definition tab to define the threshold value that you want to evaluate against the monitored value:
 - i. In **Threshold Level Description**, type a description of the rule to help you identify it.
 - ii. Define the threshold limit:
 - o Minimum thresholds: **<= (less than or equal to)**: Set the value that triggers an event if the monitored value is equal or lower.
 - o Maximum thresholds: **>= (greater than or equal to)**: Set the value that triggers an event if the monitored value is equal or higher.
 - o Scripts: Write a script that evaluates the sources you are monitoring and sets the Rule Object to either TRUE or FALSE.

The script should use the short names and the policy objects to access the value for each source, and should perform some calculation to determine if a threshold has been crossed. The script should set the Rule Object to TRUE if the threshold has been crossed or FALSE if it has not been crossed.

When the policy is deployed, the script will evaluate the sources and sets the rule object to TRUE or FALSE after each polling interval. If rule object is set to TRUE, the policy will carry out the start, continue, or end actions depending on how long the threshold has been crossed. You can also use the script to send events or run commands directly if you require more flexibility than the start, continue, and end actions provide.
 - iii. *Optional.* Click **Ignore single short-term peaks occurring within:** and set a value that is a multiple of the policy's polling interval. If the duration is set to 0 or the box is left empty, an alarm is generated as soon as HP Operations Agent detects that the threshold has been equaled or crossed.
 - iv. *Optional.* Click **Specify a special reset value for the threshold level** and set the reset value. For minimum and maximum rules, type the value in the field; for scripts write a script that evaluates the sources and determines the reset value. Alternatively, use the same value as the threshold limit.


For more details, see "[Threshold Rules—Definition Tab](#)" on page 162.

- c. *Optional.* Click **Actions** and indicate what the policy should do after evaluating the threshold level. The policy can send an event, start a command, prepare a command for the operator to start, or any combination or none of these actions.
 - o Start actions are always carried out.
 - o Continue actions are optional; they are carried out at each polling interval if the start action of the rule was carried out at a previous polling interval, and the reset value is not reached. To configure continue actions, click **Define special "Continue Actions"**.
 - o End actions are also optional; they are carried out after the threshold crosses the reset value, only if the start action for that rule was carried out. To configure end actions, click **Start the specified "End Actions"**.

Complete the following steps to configure start, continue, and end actions:

- i. *Optional.* Click **Start Actions** and use the tabs to configure the event that the agent sends when the threshold is crossed for the first time. If you do not configure details of the event, the event defaults are used.
- ii. *Optional.* Click **Continue Actions** and use the tabs to configure the event that the agent sends at each polling interval if the reset value is not reached. If you do not configure details of the event, the event defaults are used.
- iii. *Optional.* Click **End Actions** and use the tabs to configure the event that the agent sends after the threshold crosses the reset value. If you do not configure details of the event, the event defaults are used.

For more details, see ["Threshold Rules—Actions Tab"](#) on page 165.

6. If instance filters are enabled, define one or more instance rules in the Rules page.
 - a. Click  **Create New Rule**, and then choose one of the following rule types:
 - o **Evaluate thresholds if matched.** If the instance matches the condition, all thresholds are evaluated and an event is sent to BSM.
 - o **Stop evaluation if matched.** If the instance matches the condition, the agent stops processing and does not send an event to BSM.
 - o **Stop evaluation if not matched.** If the instance does not match the condition, the agent stops processing and does not send an event to BSM.

For more details, see ["Instance Rules—Overview"](#) on page 146.

- b. In Instance Rule Definition, use the Definition tab to define the condition that the instance must match:
 - i. Provide a **Rule Description** (for example, *matches the C drive*).
 - ii. *Optional.* Check the **Rule Type**. This is the type you selected in the previous step. If necessary, select another type from the drop-down list.
 - iii. Specify the instances that you want to monitor:
 - o Minimum and maximum:

In **Object Name**, type a pattern matching string that will match the instance (or instances) for which you want to write specific rules.

- o Scripts:

Click **Filter using object name pattern** if you want to use a pattern matching string to match the instance (or instances) for which you want to write specific rules.


Alternatively, click **Filter using script** and type a VB Script or Perl Script that filters the object instances.

For a VB Script threshold, set `Rule.Status = True` if the object instance matches the condition. Otherwise set `Rule.Status = False`.

For a Perl Script threshold, set `$Rule->Status(TRUE)` ; if the object instance matches the condition. Otherwise set `$Rule->Status(FALSE)` ;.

For more details, see ["Instance Rules—Definition"](#) on page 147.

- c. *Optional.* If you are creating a rule of the type 'evaluate thresholds if matched', create the threshold values that you want to evaluate against the instance values.

In Instance Rule Definition, click **Thresholds**, and then click  **Create New Threshold** to add a new threshold rule.

- d. In Threshold Definition, use the Definition tab to define the threshold value that you want to evaluate against the instance value:

- i. In **Threshold Level Description**, type a description of the rule to help you identify it.

- ii. Define the threshold limit:

- o Minimum thresholds: **<= (less than or equal to)**: Set the value that triggers an event if the monitored value is equal or lower.
- o Maximum thresholds: **>= (greater than or equal to)**: Set the value that triggers an event if the monitored value is equal or higher.
- o Scripts: Write a script that evaluates the sources you are monitoring and sets the Rule Object to either TRUE or FALSE.

The script should use the short names and the policy objects to access the value for each source, and should perform some calculation to determine if a threshold has been crossed. The script should set the Rule Object to TRUE if the threshold has been crossed or FALSE if it has not been crossed.

When the policy is deployed, the script will evaluate the sources and sets the rule object to TRUE or FALSE after each polling interval. If rule object is set to TRUE, the policy will carry out the start, continue, or end actions depending on how long the threshold has been crossed. You can also use the script to send messages or execute commands directly if you require more flexibility than the start, continue, and end actions provide.

- iii. *Optional.* Click **Ignore single short-term peaks occurring within:** and set a value that is a multiple of the policy's polling interval. If the duration is set to 0 or the box is left empty, an alarm is generated as soon as HP Operations Agent detects that the threshold has been equaled or crossed.

- iv. *Optional.* Click **Specify a special reset value for the threshold level** and set the reset value. For minimum and maximum rules, type the value in the field; for scripts write a script that evaluates the sources and determines the reset value.

Alternatively, use the same value as the threshold limit.

For more details, see "[Threshold Rules—Definition Tab](#)" on page 162.

- e. *Optional.* Click **Actions** and indicate what the policy should do after evaluating the threshold level. The policy can send an event, start a command, prepare a command for the operator to start, or any combination or none of these actions.
- o Start actions are always carried out.
 - o Continue actions are optional; they are carried out at each polling interval if the start action of the rule was carried out at a previous polling interval, and the reset value is not reached. To configure continue actions, click **Define special "Continue Actions"**.
 - o End actions are also optional; they are carried out after the threshold crosses the reset

value, only if the start action for that rule was carried out. To configure end actions, click **Start the specified "End Actions"**.

Complete the following steps to configure start, continue, and end actions:

- i. *Optional.* Click **Start Actions** and use the tabs to configure the event that the agent sends when the threshold is crossed for the first time. If you do not configure details of the event, the event defaults are used.
- ii. *Optional.* Click **Continue Actions** and use the tabs to configure the event that the agent sends at each polling interval if the reset value is not reached. If you do not configure details of the event, the event defaults are used.
- iii. *Optional.* Click **End Actions** and use the tabs to configure the event that the agent sends after the threshold crosses the reset value. If you do not configure details of the event, the event defaults are used.

For more details, see "Threshold Rules—Actions Tab" on page 165.

- f. Repeat for each object instance.
7. *Optional.* In the **Options** page, configure options for local event logs, unmatched events, and pattern matching.

For more details, see "Options Page" on page 149.

8. Click **OK** to save the policy template.

UI Reference

This section includes:

- "Actions Tab" on the next page
- "Advanced Tab" on page 142
- "Custom Attributes Tab" on page 143
- "Defaults Page" on page 144
- "Event Attributes Tab" on page 144
- "Event Correlation Tab" on page 145
- "Indicators Tab" on page 145
- "Instance Rules—Overview" on page 146
- "Instance Rules—Definition" on page 147
- "Instance Rules—Thresholds" on page 148
- "Instructions Tab" on page 149
- "Options Page" on page 149
- "Policy Data Page" on page 151
- "Policy Parameters Tab" on page 151
- "Policy Variables Tab" on page 152

- "Processing Page" on page 153
- "Properties Page" on page 154
- "Rules Page" on page 156
- "Script API Tab" on page 156
- "Source Objects Tab" on page 156
- "Source Page" on page 156
- "Threshold Rules—Overview" on page 161
- "Threshold Rules—Definition Tab" on page 162
- "Threshold Rules—Actions Tab" on page 165
- "Threshold Rules—Start Actions Tab" on page 165
- "Threshold Rules—Continue Actions Tab" on page 166
- "Threshold Rules—End Actions Tab" on page 166

Actions Tab

UI Element	Description
Automatic command	Automatic command that runs when the rule is matched.
Command	Command and parameters to run when the command is started for this event. The command runs on the node you specify in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information on <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.

UI Element	Description
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.
Send event immediately	Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.
Wait until local command completes and then	Options that can help to reduce the amount of unnecessary network traffic to the BSM server. For example, if an automatic command solves the problem that generated the event, you may choose not to inform the BSM server. <ul style="list-style-type: none"> • Send the event • Send the event if the local command fails • Send the event only if the local command is successful
Operator-initiated command	Operator-initiated command that is attached to the event that the rule sends to the Event Browser. This command can be started by the BSM user from the Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.
Command	Command and parameters to run when the command is started for this event. The command runs on the node specified in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information about <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.

UI Element	Description
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.

Advanced Tab

Note: In the default event attributes, you cannot set the following attributes:



- Event Drilldown URL
- Type

You can set these event attributes within individual rules.

UI Element	Description
Application	Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM, 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 RTSM, the object attribute is a simple string-type attribute (for example, C:, and /dev/spool).
HPOM Service ID	ID of the service associated with 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.

UI Element	Description
Enable Agent MSI	<p>The message stream interface (MSI) allows external applications to interact with the internal event flow of HP Operations Agent. The external application can be a read-write application, for example, an event processing program that can read events, modify attributes, and generate new events for retransmission to the server. The application could also read events, or send its own events.</p> <p>Divert events. Divert an event to the MSI instead of to the server when an event is requested by an external application.</p> <p>Copy events. Send the event to the server, and a copy of the event to the MSI.</p> <p>If the agent MSI is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Agent MSI. Applies the agent MSI settings configured in the event defaults to this rule.</p> <p>Override default settings for Agent MSI: Enables you to configure specific agent MSI settings for this policy rule.</p>

Custom Attributes Tab

UI Element	Description
	Create New Custom Attribute: Creates a new custom attribute with the default name CA_ <i>n</i> . To rename the custom attribute, double-click the name to select it and type the new name.
	Delete Custom Attribute: Deletes an existing custom attribute.

UI	
Element	Description
Name	<p>The name of the custom attribute. The name is case-insensitive.</p> <p>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.</p> <p>The following custom attribute names cannot be used because they are reserved for internal use:</p> <p>Description</p> <p>EtiHint</p> <p>HP_OPR_SAAS_CUSTOMER_ID</p> <p>NoDuplicateSuppression</p> <p>RelatedCiHint</p> <p>SourceCiHint</p> <p>SourcedFromExternalId</p> <p>SourcedFromExternalUrl</p> <p>SubCategory</p> <p>SubCiHint</p>
Value	Value of the custom attribute.

Defaults Page

The Defaults page enables you to set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

For more details, see ["Event Attributes Tab"](#) below and ["Advanced Tab"](#) on page 142.

Event Attributes Tab

Note: In the default event attributes, you can set only the following attributes:

- Severity
- Category
- Node

You can set the other event attributes within individual rules.

UI Element	Description
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.
Send with closed status	Sets the event's lifecycle status to Closed before sending it to the Event Browser in Operations Management.

Event Correlation Tab






Note: In the default event attributes, you cannot set the following attributes:

- Close Events with Key
- Suppress Deduplication on Server

You can set these event attributes within individual rules.











UI Element	Description
Event Key	An identifier used to identify duplicates and for Close Events with Key.

Indicators Tab

UI Element	Description
	<p>Refresh. Loads the configured indicators from the BSM server.</p> <p>Note: Loading indicators from the BSM server may take a few seconds.</p>
	<p><i>Event integration policies only:</i> Shows or hides the Select drop target format drop-down panel:</p> <ul style="list-style-type: none"> • Use Indicator States. Click to change the drop target format to indicator states only. • Use Indicator Names and States. Click to change the drop target format to indicator names and states.
<Search ...>	<p>Entered search string is used to search the indicators and highlight only the indicators containing the specified string.</p> <p>To search for indicators with specific text strings in the name, type the string in the <Search ...> field and click the  button. The first matching indicator is selected in the list of rules. Click the  and  buttons to move to the previous and next matching indicator.</p>

UI Element	Description
<Indicators>	Hierarchy of configuration item types with associated health indicators (HIs) and event type indicators (ETIs). To insert an indicator in a policy, drag and drop the indicator from the Indicators tab to the relevant field in the policy.

Instance Rules—Overview







UI Element	Description
	<p>Create New Rule: Provides the following options:</p> <ul style="list-style-type: none"> • Evaluate thresholds if matched. If the instance matches the condition, all thresholds are evaluated and an event is sent to BSM. • Stop evaluation if matched. If the instance matches the condition, the agent stops processing and does not send an event to BSM. • Stop evaluation if not matched. If the instance does not match the condition, the agent stops processing and does not send an event to BSM.
	Copy Rule: Copies the selected instance rule. You can then rewrite the description of the copied rule and edit the rule.
	Delete Item: Deletes the selected instance rule.
	Move Up. Moves the selected instance rule higher in the rule order.
	Move Down. Moves the selected instance rule lower in the rule order.
<Move to>	<p>Entered number is used to select the instance rule with that sequence number in the list of rules.</p> <p>To select a specific instance rule in the rule list, type the rule's sequence number in the <Move to> field and click the  button.</p>
<Search Thresholds>	<p>Entered search string is used to search the instance rule descriptions and highlight only the rules containing the specified string.</p> <p>To search for instance rules with specific text strings in the rule description, type the string in the <Search Rules> field and click the  button. The first matching rule is selected in the list of rules. Click the  and  buttons to move the previous and next matching rule.</p>
	Activate/Deactivate Threshold Filter. Activates and deactivates the instance rule filter.
Seq.	Sequence number of the instance rules. Rules are evaluated in a specific order. When one condition is matched, no additional rules are evaluated.
Rule Description	Description of the instance rule. It is good practice to use a description that helps you remember what the rule does.

UI Element	Description
Rule Type	<p>The three rule types are:</p> <ul style="list-style-type: none"> • Evaluate thresholds if matched. If the monitored object matches the condition, all thresholds are evaluated and an event is sent to BSM. • Stop evaluation if matched. If the monitored object matches the condition, the agent stops processing and does not send an event to BSM. • Stop evaluation if not matched. If the monitored object does not match the condition, the agent stops processing and does not send an event to BSM.
Amount Thresholds	The number of thresholds configured for the selected instance rule.

Instance Rules—Definition

UI Element	Description
Rule Description	This is a name you give to the rule to help you identify it. This name is visible in the rules list.
Rule Type	<p>The three rule types are:</p> <ul style="list-style-type: none"> • Evaluate thresholds if matched. If the monitored object matches the condition, all thresholds are evaluated and an event is sent to BSM. <p>Stop evaluation. Cancels evaluation of the remaining rules.</p> <ul style="list-style-type: none"> • Stop evaluation if matched. If the monitored object matches the condition, the agent stops processing and does not send an event to BSM. • Stop evaluation if not matched. If the monitored object does not match the condition, the agent stops processing and does not send an event to BSM.
Object name	<p><i>Minimum and maximum processing rules only:</i></p> <p>Type a pattern matching string that will match the instance (or instances) for which you want to write specific rules.</p>
Filter using object name pattern	<p><i>Script processing only:</i></p> <p>Type a pattern matching string that will match the instance (or instances) for which you want to write specific rules.</p>
Filter using script	<p><i>Script processing only:</i></p> <p>Type a VB Script or Perl Script that filters the object instances:</p> <p>For a VB Script threshold, set <code>Rule.Status = True</code> if the object instance matches the condition. Otherwise set <code>Rule.Status = False</code>.</p> <p>For a Perl Script threshold, set <code>\$Rule->Status(TRUE)</code> ; if the object instance matches the condition. Otherwise set <code>\$Rule->Status(FALSE)</code> ;.</p>

Instance Rules—Thresholds

UI Element	Description
	Create New Threshold: Adds an empty threshold rule to the list for you to edit.
	Copy Threshold: Copies the selected threshold rule. You can then rewrite the description of the copied rule and edit the rule.
	Delete Item: Deletes the selected threshold rule.
	Move Up. Moves the selected threshold rule higher in the rule order.
	Move Down. Moves the selected threshold rule lower in the rule order.
<Move to>	Entered number is used to select the threshold rule with that sequence number in the list of rules. To select a specific threshold rule in the rule list, type the rule's sequence number in the <Move to> field and click the ▶ button.
<Search Thresholds>	Entered search string is used to search the threshold rule descriptions and highlight only the rules containing the specified string. To search for threshold rules with specific text strings in the rule description, type the string in the <Search Thresholds> field and click the 🔍 button. The first matching rule is selected in the list of rules. Click the ◀ and ▶ buttons to move the previous and next matching rule.
	Activate/Deactivate Threshold Filter. Activates and deactivates the threshold rule filter.
Seq.	Sequence number of the threshold rules. Rules are evaluated in a specific order. When one condition is matched, no additional rules are evaluated.
Threshold Level Description	Description of the threshold rule. It is good practice to use a description that helps you remember what the rule does.

Instructions Tab

UI Element	Description
Instructions	<p>Instructions that you want to accompany the event.</p> <p>Events generated by a policy can include instructions that explain what to do when the event is generated. This instruction text can often help an operator to solve a problem when a particular type of event is received. The operator can view the instructions included with an event by viewing the Event Details pane in the Event Browser. You can define default instructions for all rules in a policy. You can also override the default with different instructions for any rule.</p> <p>You can type URLs in the text, and the Event Browser automatically converts them into clickable hyperlinks. For example, you can add URLs of external Web sites, support sites, documentation repositories, troubleshooting information, and similar sites.</p> <p>To add a link, type any URL that begins with one of the following URI scheme names:</p> <ul style="list-style-type: none"> • http:// • https:// • ftp:// • ftps://



Options Page

UI Element	Description
Log Local Events	<p>Defines 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:</p> <p>Windows: %OvDataDir%\log\OpC\opcmsglg AIX, HP-UX, Linux, and Solaris: /var/opt/OV/log/OpC/opcmsglg</p>
that match a rule and trigger an event	Logs any events in the event source that match the policy rules.
that match a rule and are ignored	Logs any events in the event source that are suppressed. (Suppressed events are not sent to the Event Browser.)
that do not match any rule	Logs any events that do not match any of the rules in the policy.



UI Element	Description
Unmatched Events	<p>Send an event to the 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.</p> <p>Each policy that sends unmatched events to the Event Browser creates an event with the default values of the policy.</p> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p>
are sent to the Event Browser	Sends unmatched events to the Event Browser.
are sent to the Closed Events Browser	Sends unmatched events to the Closed Events Browser.
are ignored	Ignores unmatched events.
Pattern Matching Options	Defines case sensitivity and field separators for all rules.
Case sensitive check	Defines whether the case (uppercase or lowercase) of a text string is considered when the pattern of a rule is compared with the source data. When switched on, a match only occurs if the use of uppercase and lowercase letters is exactly the same in both the source data and the pattern. This is the default setting.







UI Element	Description
Field Separators	<p>Defines 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:</p> <ul style="list-style-type: none"> • \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 (\) <p>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).</p> <p>If you leave this box empty, the default separators (a blank and the tab character) are used by default.</p> <p>You can set case sensitivity and separator characters for individual rules in a policy by clicking the ► button in rule's match condition.</p>
Apply to All	<p>Applies the pattern matching options to all existing rules in a policy. This overwrites any modifications made to the pattern matching options in individual rules.</p> <p>If you change the pattern matching options and do not click Apply to all, they only apply to all new rules in a policy.</p>

Policy Data Page

UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Check Syntax: Validates the syntax of the policy data. If the policy syntax is incorrect, the validation tool reports an error and points to the corresponding line and position of the unexpected token (for example the incorrect keyword).
<policy data>	Policy data in text form. The data uses the HP Operations Agent policy syntax.

Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.

UI Element	Description
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Policy Variables Tab

Variable	Description
<code><\$INSTANCE></code>	Returns the name of the current instance Sample output: C ;
<code><\$MSG_NODE></code>	Returns the IP address of the node on which the original event took place. Sample output: 192.168.1.123
<code><\$MSG_NODE_NAME></code>	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-event basis.

Variable	Description
<\$MSG_OBJECT>	Returns the name of the object associated with the event. This is set in the Event Defaults section of the policy editor.
<\$MSG_TEXT>	Returns the full text of the event. Sample output: SU 03/19 16:13 + ttyp7 bill-root
<\$NAME>	Returns the name of the policy that sent the event. Sample output: cpu_util
<\$OPTION (N) >	Returns the value of an optional variable that is set by opcmsg or opcmon (for example, <\$OPTION (A) >, < \$OPTION (B) >, and so on.).
<\$THRESHOLD>	Returns value for the threshold limit set in the Threshold Definition tab. If the threshold is determined with a script, the name of the scripting language is returned, for example, VBScript. Sample output: 95.00
<\$VALUE>	Returns the value measured by a Measurement Threshold policy. Sample output: 100.00
<\$VALAVG>	Returns the average value of all messages reported by the Measurement Threshold policy. Sample output: 100.00
<\$VALCNT>	Returns the number of times that the threshold monitor has delivered a message to the browser. Sample output: 1

Processing Page

UI Element	Description
Script Type	<ul style="list-style-type: none"> • Minimum: Sets a minimum threshold level under which the monitored value must drop for a rule to match. • Maximum: Sets a maximum threshold level that the monitored value must exceed for a rule to match. • Perl Script: Configures the policy to use a Perl script that evaluates the sources you are monitoring and determines the threshold limit. • VB Script: Configures the policy to use a VB script that evaluates the sources you are monitoring and determines the threshold limit. <p>Caution: A measurement threshold policy can only contain one of these types of rules. A conversion between threshold types is not always possible:</p> <ul style="list-style-type: none"> • Changing between minimum and maximum: rules are not deleted. • Changing from minimum or maximum to VisualBasic or Perl: the rules are converted to script. • Changing from VisualBasic or Perl to minimum or maximum: rules are deleted.

	<ul style="list-style-type: none"> • Changing between VisualBasic and Perl: no conversion occurs, you must rewrite the script. <p>Tip: You need to use a script to determine the threshold for your measurement threshold policy if the source that you choose delivers something other than a number or a Boolean value, or if you want to evaluate multiple sources. A script makes it possible for you to perform your own calculations and decide if the threshold has been crossed.</p>
<p>Instance Filter</p>	<p>Instance filters provide a way for the measurement threshold policy to apply different sets of threshold levels to different instances of the object being monitored. For example, a threshold policy that monitors disk usage will apply the same threshold to all disks, but if you specify instance filters, you can specify one set of threshold levels for disk C:, another set for disk D: and so on.</p> <p>Instance filters can be used with policies that evaluate the threshold based on a minimum, maximum, or scripts. Instance filters are not available for threshold policies based on the source MIB.</p> <p>Use Instance Filter: Enables instance filters for the policy. Switching to instance filters cannot be reverted.</p>
<p>Processing Options</p>	<p>You can choose how a policy processes multiple instances of the value being measured. For example, if a policy monitors disk space, then each disk in the monitored node is one instance, and you can choose whether to treat each disk separately or all disks as a whole.</p> <ul style="list-style-type: none"> • Process each instance separately: Select this option if you want each instance to be processed by the policy separately. For example, if the policy monitors each CPU in a multiple CPU server, and the activity of all CPUs exceeds the threshold, an event will be generated for each CPU. • Process all instances once: This option can only be used if the threshold rules use the output of a script as the threshold (instead of minimum or maximum). Select this option if the script evaluates all instances and delivers one value to be tested by the policy. (Make sure that the scripting language that you choose is supported on the platform where you plan to distribute your policy.)

Properties Page

UI Element	Description
<p>Name</p>	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>

UI Element	Description
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

¹(globally unique identifier)

Rules Page

The Rules page enables you to define one or more instance or threshold rules.

For more details on instance rules, see "Threshold Rules—Overview" on page 161, "Threshold Rules—Definition Tab" on page 162, "Threshold Rules—Actions Tab" on page 165, "Threshold Rules—Start Actions Tab" on page 165, "Threshold Rules—Continue Actions Tab" on page 166, and "Threshold Rules—End Actions Tab" on page 166.

For more details on threshold rules, see "Instance Rules—Overview" on page 146, "Instance Rules—Definition" on page 147, "Instance Rules—Thresholds" on page 148, "Threshold Rules—Definition Tab" on page 162, "Threshold Rules—Actions Tab" on page 165, "Threshold Rules—Start Actions Tab" on page 165, "Threshold Rules—Continue Actions Tab" on page 166, and "Threshold Rules—End Actions Tab" on page 166.


Script API Tab



UI Element	Description
<Source Objects>	List of policy objects that can be used in VB and Perl scripts. For details, see "Policy Objects for Scripts" on page 336.

Source Objects Tab

UI Element	Description
<Source Objects>	List of sources that the policy monitors. You can insert the source objects in the event attribute fields using drag and drop.

Source Page

UI Element	Description
Sources	<p> Add Source: Provides the following options:</p> <ul style="list-style-type: none"> • Add Embedded Performance Component Source: The Embedded Performance (Coda) component collects performance counter and instance data. • Add External Source: Uses the data sent from an external program (the opcmn command line tool, for example) as the source for a threshold alarm. HP Operations Agent does not poll the external program but waits for values to arrive. • Add Management Information Base Source: Uses entries in a Management Information Base as the source for a threshold alarm. • Add Program Source: Uses the data sent from an external program as the source for a threshold alarm. HP Operations Agent runs the external program at each polling interval. • Add Real Time Performance Measurement Source: Uses data gathered by the performance monitor as the source for a threshold alarm. • Add Windows Management Instrumentation Source: Uses

	<p>information in the WMI database as the source for the threshold alarm.</p> <p>Policies with multiple sources require you to write scripts to evaluate the threshold levels. Note that switching from single to multiple sources automatically converts the rules to Perl Script.</p> <p>Make sure that the scripting language that you choose will run on the operating system where you intend to use the policies.</p> <p> Copy Source: Copies and inserts the copy below the selected source for editing.</p> <p> Delete Source: Deletes the selected source.</p> <p>Short Name and Description are labels that you choose to help you recognize the value or metric for a threshold source. These labels are visible in the Source Page and are helpful if you write a policy with multiple sources. When using a script to determine the threshold level, these names are used in the script to identify the sources.</p> <p>Store in Coda: You can enter a Data Source, Object and Metric of your own invention here. The policy will create them in the Embedded Performance Component (Coda) and will store the data from the policy's source each polling interval. The data is then available for other uses. For example, you can use data stored in the Embedded Performance Component to create graphs with Performance Graphing.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Caution: For each WMI instance class, you must specify a dedicated CODA object. For example, you can store all WMI instance classes of the type Win32_SystemUsers in a CODA object "users", but you cannot store WMI instance classes of the type Win32_LogicalDisk in the same CODA "users" object. For Win32_LogicalDisk instance classes, use the CODA object "logical_disk", for example.</p> </div>
<p>Embedded Performance Component</p>	<p>The Embedded Performance Component collects performance counter and instance data. You can use these metrics in defining event/action thresholds that generate alarms in real time based on availability, response time, and throughput measurements.</p> <ul style="list-style-type: none"> • Data Source: CODA • Object: GLOBAL, CPU, NETIF, FILESYSTEM, DISK • Metric: metric to be collected (for example GBL_CPU_TOTAL_UTIL) <p>You can view a list of available metrics in the <i>HP Performance Agent Dictionary of Operating System Performance Metrics</i>, which is available at HP Software Product Manuals. (Select the product Operations Agent, the required version, OS, and language.)</p> <p>About Metrics</p> <p>The Embedded Performance Component collects the following types of</p>


	<p>metrics:</p> <ul style="list-style-type: none"> • Basic (golden) metrics. These are approximately 30 metrics that are collected for all supported platforms. They can be used to answer most of your questions about a system's global configuration, CPU, disk, swap, and memory usage and have been chosen to offer the best information for the widest number of platforms. • Additional metrics. The data collection component also provides you with additional performance metrics on each of the supported platforms. Although these metrics vary by platform, they are available on most platforms and are generally useful for drill down and diagnosis on a particular system. <p>The collection interval is five minutes. All metrics, including golden metrics and the additional metrics, are collected. The data is kept in the data store for up to five weeks, at which time a week's worth of data is rolled out.</p> <p>Note: The embedded performance component must have the Physical Disk Object available to report the disk metrics. To get the disk metrics reported on a node, you must run diskperf -Y to enable the counters under the Physical Disk Object.</p>
External	<p>Select External if you want to use the data sent from an external program as the source for a threshold alarm. The program must produce and deliver values to the policy (see <code>opcmon</code>). If you choose this source, the program will not be started or stopped by the HP Operations Agent. If you want HP Operations Agent to run the external program, choose Program instead.</p>
Management Information Base	<p>Select Management Information Base if you want to use entries in a Management Information Base as the source for a threshold alarm. You must specify the MIB ID and the node where the ID is produced.</p> <ul style="list-style-type: none"> • MIB ID: Object ID assigned to the MIB (for example, 1.3.6.1.4.1.11.2.3.9.4.2.1.1). • On Node: Fully qualified domain name of the node where the OID is produced. <p>HP Operations Agent used the default community <code>public</code> for SNMP queries. If the MIB object resides in another community, the community name must be set on the node where the MIB monitoring takes place. (Use <code>ovconfchg</code> to set the parameter <code>SNMP_COMMUNITY <community></code> in the <code>eaagt</code> namespace.)</p> <p>Note: Instance filters are not available for threshold policies based on the source MIB.</p>
Program	<p>Select Program if you want to use the data sent from an external program as the source for a threshold alarm.</p>










	<p>The external program will be started by HP Operations Agent, and must produce and deliver values to the policy. If you do not want HP Operations Agent to control when the external program runs, choose External instead.</p> <p>Program: Type the complete path and extension of the program that you want to run on the managed node (for example, %OvDataDir%\bin\instrumentation\collector.exe). The file that you specify should exist on the node.</p> <p>If you want to automatically deploy the program that runs on the managed node, configure it as instrumentation for this policy</p> <p>You can use the following policy name variables in Program:</p> <p><\$FULLNAME></p> <p>Returns the name of the policy and the source, concatenated with a hyphen (-). Sample output: example_policy_name-example_source_name</p> <p><\$NAME></p> <p>Returns the name of the policy, which you specify when you save the policy. Sample output: example_policy_name</p> <p><\$SRCNAME></p> <p>Returns the name of the source, which you specify in Short Name. Sample output: example_source_name</p> <p>The agent resolves these variables before it starts the program. This enables you to rename the policy without modifying the program name.</p> <p>If you precede a variable with a backslash (\), the agent ignores the variable.</p> <p>It is possible to disable policy name variables by setting the parameter OPC_MON_DISABLE_PROG_VARS to TRUE in the eaagt namespace on the monitored node.</p>
<p>Real Time Performance Measurement</p>	<p>Select Real Time Performance Management if you want to use data gathered by the performance monitor as the source for a threshold alarm.</p> <ul style="list-style-type: none"> • Object: Object entry in the Performance Manager. • Counter: Counter entry in the Performance Manager. • Instance: Instance entry in the Performance Manager. <p>For a complete listing and description of all default object counters, see the documentation that Microsoft provides.</p> <p>Additional Configuration</p> <ul style="list-style-type: none"> • If the counter has a percent sign (%), it can be omitted if you want to receive the raw value instead of a percent • For instances which have parent instances, a question mark (?) can be

	<p>used as a wildcard to match any parent instance. For example: <code>?/C:</code> matches <code>0/C</code> and <code>1/C</code></p> <p>Examples</p> <ul style="list-style-type: none">• The percentage of free disk space on a C drive on SCSI port 0: Object: LogicalDisk Counter: % Free Space Instance: <code>0/C:</code>• The number of free megabytes on any C: drive: Object: LogicalDisk Counter: Free Megabytes Instance: <code>?/C:</code>• The available bytes of RAM: Object: Memory Counter: Available Bytes Instance: <code>empty</code>• The amount of CPU time used by a specific process: Object: Process Counter: % Processor Time Instance: <code>process name</code>• The paging file utilization: Object: Paging File Counter: % Usage Instance: <code>/DosDevices/C:/pagefile.sys</code>
--	--

<p>Windows Management Instrumentation</p>	<p>Select Windows Management Instrumentation if you want to use information in the WMI database as the source for the threshold alarm.</p> <ul style="list-style-type: none"> • WMI Namespace: The namespace that contains the data that you want to monitor. • Instance Class Name: The instance that contains the property that you want to monitor. • Property Name: The property that you want to monitor. The property should in most cases be either an integer or a Boolean value. If you choose any other type of property (for example, a string), the policy will automatically restrict the choice of threshold level to VB Script, or Perl Script and you will need to write a script that interprets the string and sets the Rule object to True or False. • Non Agent User: If selected, the agent accesses the node's WMI database using the following account information. This account must exist on the agentless node and must have local administrator privileges. If not selected, the agent account is used. <ul style="list-style-type: none"> ▪ Username. User name of the account that the agent will use to connect to the WMI database. ▪ Password. Password of the specified user account. ▪ Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
<p>Polling Interval</p>	<p>How often the policy checks the source for new information. To increase performance, the polling interval should be as large as possible, while still being frequent enough to monitor data at the rate that it is expected to change. A policy begins to evaluate data <i>after</i> the first polling interval passes. A shorter polling interval is better when you are testing a policy.</p> <p>To modify the time, click the ▼ button and use the drop-down lists to specify increments of hours, minutes, or seconds.</p> <p>To insert a parameter in a time field, type the parameter in the format <code>%%<variable_name>%%</code> or drag and drop the parameter from the Policy Parameters tab.</p> <p>Default value: 5 minutes</p>

Threshold Rules—Overview

UI Element	Description
	<p>Create New Threshold: Adds an empty threshold rule to the list for you to edit.</p>

UI Element	Description
	Copy Threshold: Copies the selected threshold rule. You can then rewrite the description of the copied rule and edit the rule.
	Delete Item: Deletes the selected threshold rule.
	Move Up. Moves the selected threshold rule higher in the rule order.
	Move Down. Moves the selected threshold rule lower in the rule order.
<Move to>	Entered number is used to select the threshold rule with that sequence number in the list of rules. To select a specific threshold rule in the rule list, type the rule's sequence number in the <Move to> field and click the  button.
<Search Thresholds>	Entered search string is used to search the threshold rule descriptions and highlight only the rules containing the specified string. To search for threshold rules with specific text strings in the rule description, type the string in the <Search Thresholds> field and click the  button. The first matching rule is selected in the list of rules. Click the  and  buttons to move the previous and next matching rule.
	Activate/Deactivate Threshold Filter. Activates and deactivates the threshold rule filter.
Seq.	Sequence number of the threshold rules. Rules are evaluated in a specific order. When one condition is matched, no additional rules are evaluated.
Threshold Level Description	Description of the threshold rule. It is good practice to use a description that helps you remember what the rule does.

Threshold Rules—Definition Tab

UI Element	Description
Threshold Level Description	This is a name you give to the rule to help you identify it. This name is visible in the rules list.
Threshold Limit (Minimum or Maximum)	Minimum thresholds: <= (less than or equal to): Set the value that triggers an event if the monitored value is equal or lower. Maximum thresholds: >= (greater than or equal to): Set the value that triggers an event if the monitored value is equal or higher. Use the following syntax guidelines when specifying the minimum or maximum threshold:

UI Element	Description
	<p>Sequence of Digits: May include a decimal separator. (The character used as the separator is determined by the operating system language.) For example: 0.5, 100.1</p> <p>Sign (optional): Plus sign (+). For example: +50 Minus sign (-). For example: -730</p> <p>Exponent (optional): Exponent character: e or E. For example: 15e2, 7E4 Exponent sign. For example: 8e+2, 4E-2 One or more decimal digits. For example: 25.88e4</p> <p>Tip: If you set a minimum or maximum threshold limit, you can override it for individual nodes.</p> <p>To override a threshold limit on an individual node, set a parameter locally on the node in the eaagt.thresholds namespace. Specify the parameter value in the following format:</p> <pre><policy_name>/<threshold_level_description>/<limit>:<reset_value></pre> <p>For example, if you have a policy called <code>cpu load</code> with a threshold level called <code>condition critical</code> that you want to override with the limit 75 and the reset value 70, set a parameter with the following value:</p> <pre>cpu load/condition critical/75:70</pre> <p>The following limitations apply:</p> <ul style="list-style-type: none"> Specify <code><policy_name></code> and <code><threshold_level_description></code> exactly as they appear in the policy editor. The first and last slash marks (/) delimit the <code><threshold_level_description></code>, which can itself contain slash marks. <code><reset_value></code> is required, even if it is the same as <code><limit></code>. <p>Set the parameter using one of the following methods:</p> <ul style="list-style-type: none"> Deploy a node info policy that contains the following line: <pre><parameter_name>(thresholds) <parameter_value></pre> <p>The <code><parameter_name></code> can be any alphanumeric string that is unique within the eaagt.thresholds namespace. Adding <code>(thresholds)</code> after <code><parameter_name></code> ensures that the node info policy sets the parameter in the eaagt.thresholds namespace.</p> Use the command <code>ovconfpar</code> with the following syntax: <pre>ovconfpar -change -host <node_hostname> -ns eaagt.thresholds -set <parameter_name> <parameter_</pre>

UI Element	Description
	<p><i>value</i>></p> <p>The <<i>parameter_name</i>> can be any alphanumeric string that is unique within the eaagt.thresholds namespace.</p>
<p>Threshold Limit (Perl or VB Script)</p>	<p>Write a script that evaluates the sources you are monitoring and sets the Rule Object to either TRUE or FALSE.</p> <p>The script should use the short names and the policy objects to access the value for each source, and should perform some calculation to determine if a threshold has been crossed. The script should set the Rule Object to TRUE if the threshold has been crossed or FALSE if it has not been crossed.</p> <p>Note:</p> <ul style="list-style-type: none"> • HP Operations Agent uses a generic Microsoft scripting engine to run VBScript scripts. You can therefore use standard VBScript objects (for example, the FileSystemObject object) in your scripts. Objects that are specific to wscript or cscript (for example, the WScript object) are not supported. • The agent runs as a service that has no standard input, standard output, or standard error streams. Therefore, the predefined file handles STDIN, STDOUT, and STDERR are not available for Perl scripts in measurement threshold policies. It is also not possible to open file handles that use command pipes or capture the standard output from commands within backticks (`).
<p>Short-Term Peaks</p>	<p>Since it may not be reasonable to create an event when a threshold is exceeded only for a short time, you can define a minimum time period over which the monitored value must exceed the threshold before generating an event. For an event to be sent, the value must be greater than the threshold each time the value is measured during a duration that you select.</p> <p>Ignore single short-term peaks occurring within: Select a value that is a multiple of the policy's polling interval. For example, if the polling interval is 2m (two minutes), set the short-term peak duration to 4m, 6m, 8m, or 10m (and so on). If the duration is set to 0 or the box is left empty, an alarm is generated as soon as HP Operations Agent detects that the threshold has been equaled or crossed.</p> <p>To modify the time, click the ▼ button and use the drop-down lists to specify increments of hours, minutes, or seconds.</p> <p>To insert a parameter in a time field, type the parameter in the format <code>%%<variable_name>%%</code> or drag and drop the parameter from the Policy Parameters tab.</p>

UI Element	Description
Reset	<p>The reset value is a limit below which the monitored value must drop (or exceed, for minimum thresholds) to return the status of the monitored object to normal. After the status of a monitored object returns to normal, a new start event can be issued if the monitored value again crosses the threshold value. You can either use the same value as the threshold limit, or specify a different reset value.</p> <ul style="list-style-type: none"> • Reset value is same value as threshold limit • Specify a special reset value for the threshold level <ul style="list-style-type: none"> ▪ Minimum thresholds: <source name> < (less than) ▪ Maximum thresholds: <source name> > (greater than) ▪ Script thresholds: Write a script that evaluates the sources and determines the reset value.

Threshold Rules—Actions Tab

UI Element	Description
Start Actions	<p>Start actions are carried out the first time that the threshold is met or crossed.</p> <p>Edit the "Start Actions" event: Opens the Start Action tab, which enables you to define what the policy should do after evaluating a particular threshold level.</p>
Continue Actions	<p>Continue actions are carried out at each polling interval if the start action of the rule was carried out at a previous polling interval, and the reset value is not reached.</p> <p>Define special "Continue Actions": Enables continue actions for this rule.</p> <p>Edit the "Continue Actions event: Opens the Continue Action tab.</p>
End Actions	<p>End actions are carried out after the threshold crosses the reset value, only if the start action for that rule was carried out. If the value drops below two thresholds within one polling interval, the end actions of the lowest rule that performed start actions are carried out.</p> <p>Start the specified "End Actions": Enables end actions for this rule.</p> <p>Edit the "End Actions event: Opens the End Action tab.</p>

Threshold Rules—Start Actions Tab

UI Element	Description
Event Attributes	Enables you to set the attributes of the start event.
Event Correlation	Enables you to set correlation options for the start event.

UI Element	Description
Custom Attributes	Enables you to add custom attributes to the start event.
Instructions	Enables you to add instruction information to help operators handle the continue event.
Advanced	Enables you to set the advanced attributes of the start event.
Actions	Enables you to add automatic and operator-initiated commands to the start event.

Threshold Rules—Continue Actions Tab

UI Element	Description
Event Attributes	Enables you to set the attributes of the continue event.
Event Correlation	Enables you to set correlation options for the continue event.
Custom Attributes	Enables you to add custom attributes to the continue event.
Instructions	Enables you to add instruction information to help operators handle the continue event.
Advanced	Enables you to set the advanced attributes of the continue event.
Actions	Enables you to add automatic and operator-initiated commands to the continue event.

Threshold Rules—End Actions Tab


UI Element	Description
Event Attributes	Enables you to set the attributes of the end event.
Event Correlation	Enables you to set correlation options for the end event.
Custom Attributes	Enables you to add custom attributes to the end event.
Instructions	Enables you to add instruction information to help operators handle the continue event.
Advanced	Enables you to set the advanced attributes of the end event.
Actions	Enables you to add automatic and operator-initiated commands to the end event.

Configuring Node Info Policies








Node info policies enable you to change configuration parameters of HP Operations Agent on managed nodes.

To access




You can create or edit a node info policy using the Node Info Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:
Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.

The Edit Aspect dialog box opens.




- d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **Node Info Template**, and then click **OK**.
 - To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Node Info Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:
Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **Node Info Templates** folder, and then do one of the following:
 - To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New Node Info Policy Editor opens.

- To edit an existing policy template, click the policy template in the Policy Templates

pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit Node Info Policy Editor opens.

Learn More

This section includes:

- "Node Info Policy Syntax" below
- "Example Node Info Policy" below

Node Info Policy Syntax

Node info policies use the following syntax:

```
;XPL config  
[<namespace>  
<parameter_name>=<parameter_value>
```

```
[<namespace>
```

The HP Operations Agent configuration namespace to be updated.

```
<parameter_name>
```

The name of the HP Operations Agent configuration parameter.

```
<parameter_value>
```

The value of the HP Operations Agent configuration parameter. Only ASCII characters are supported. New line characters are not permitted.

For a list of supported configuration parameters and their namespaces, see the HP Operations Agent Reference Guide.

Example Node Info Policy

The following example node info policy enables the message stream interface (MSI) on the managed node and allows MSI instances to create or modify events with automatic actions. The policy also configures the agent to redirect all communication to the proxy proxy1.example.com at port 8080.

Example:

```
;XPL config  
[eaagt]  
OPC_AGTMSI_ENABLE=TRUE  
OPC_AGTMSI_ALLOW_AA=FALSE  
[bbc.http]  
PROXY=proxy1.example.com:8080
```


Tasks

How to Create a Node Info Policy

1. In the Node Info Policy Editor, in the Properties page, type a **Name** for the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see ["Properties Page" on the next page](#).

- In the Policy Data page, type the configuration parameters and their values using the HP Operations Agent node info policy syntax. If you are creating a new policy, copy and paste template data from an existing policy template. Alternatively, click the  button to load policy data from a policy template file on your computer.

For details, see ["Node Info Policy Syntax" on the previous page](#).

You can also use policy parameters. For more details, see ["Policy Parameters Tab" below](#).



- Click **OK** to save the policy template.

UI Reference




This section includes:






- ["Policy Data Page" below](#)
- ["Policy Parameters Tab" below](#)
- ["Properties Page" on the next page](#)

Policy Data Page

UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Node Info policies do not support syntax checking. You can click Check Syntax but the check fails to perform.
<code><policy data></code>	Policy data in text form. For details, see "Node Info Policy Syntax" on the previous page .

Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.
	Delete Parameter: Delete the selected parameter from the list.

UI Element	Description
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Properties Page

UI Element	Description
Name	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.

¹(globally unique identifier)

UI Element	Description
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>


Configuring Open Message Interface Policies

The HP Operations Agent provides a command (called `opcmmsg`), a Java API, and a C API, which enable you to submit messages to the agent's message interface. Open message interface policies enable you to filter these messages through rules. Each rule consists of a condition definition, and








optionally an event definition. Whenever a message matches your conditions, you can create an event.

To access




You can create or edit an open message interface policy using the Open Message Interface Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:
Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.




The Edit Aspect dialog box opens.

- d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **Open Message Interface Template**, and then click **OK**.
 - To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Open Message Interface Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:
Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **Open Message Interface Templates** folder, and then do one of the following:
 - To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New Open Message Interface Policy Editor opens.

- To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit Open Message Interface Policy Editor opens.

Learn More

This section includes:

- "opcmmsg Command" below
- "Java API" below
- "C API" on the next page

opcmmsg Command

The `opcmmsg` command enables you to submit messages to the open message interface from a command prompt or script.

```
opcmmsg [-help]
        [-id]
        [severity=normal|warning|minor|major|critical]
        application=<application>
        object=<object>
        msg_text=<text>
        [msg_grp=<message group>]
        [node=<node>]
        [service_id=<svcid>]
        [-option <var>=<value>]
```

`opcmmsg` is available in one of the following locations.

- AIX, HP-UX, Linux, and Solaris: `/opt/OV/bin/opcmmsg`
- Windows 32-bit: `%OvInstallDir%\bin\opcmmsg`
- Windows 64-bit: `%OvInstallDir%\bin\win64\opcmmsg`

For more details, see the *HP Operations Agent Reference Guide*.

Java API

The Java API enables you to create Java programs that submit messages to the open message interface. The required JAR files (`jopcagtbase.jar` and `jopcagtmsg.jar`) are installed with the HP Operations Agent in one of the following locations:

- AIX: `/usr/lpp/OV/java/`
- HP-UX, Linux, and Solaris: `/opt/OV/java/`
- Windows: `%OvInstallDir%\java\`

Javadoc style class documentation is available in the following location:

- AIX: `/usr/lpp/OV/www/htdocs/jdoc_agent/index.html`
- HP-UX, Linux, and Solaris: `/opt/OV/www/htdocs/jdoc_agent/index.html`
- Windows: `%OvInstallDir%\www\htdocs\jdoc_agent\index.html`

For more details, see the *HP Operations Agent Reference Guide*.

C API

The C API enables you to create C programs that submit messages to the open message interface. The required header file (`opcapi.h`) is installed with the HP Operations Agent in one of the following directories:

- AIX: `/usr/lpp/include/`
- HP-UX, Linux, and Solaris: `/opt/OV/include/`
- Windows: `%OvInstallDir%\include\`

The required libraries (`libopcagtapi`, and on UNIX and Linux `libOvXpl`) are installed with the HP Operations Agent in one of the following directories:

- AIX 32-bit: `/usr/lpp/OV/lib/`
- AIX 64-bit: `/usr/lpp/OV/lib64/`
- HP-UX Itanium: `/opt/OV/lib/hpux32`
- HP-UX PA-RISC: `/opt/OV/lib/`
- Linux and Solaris 32-bit: `/opt/OV/lib/`
- Linux and Solaris 64-bit: `/opt/OV/lib64/`
- Windows 32-bit: `%OvInstallDir%\bin\`
- Windows 64-bit: `%OvInstallDir%\bin\win64\`

For more details about the C API and required compiler options, see the *HP Operations Agent Reference Guide*.

Tasks

How to Create an Open Message Interface Policy

1. In the Message Interceptor Policy Editor, in the Properties page, type a **Name** for the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.


For more details, see "[Properties Page](#)" on page 188.

2. *Optional.* In the Defaults page, set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

Note: You can set defaults for only a subset of event attributes. You can set the other event attributes within individual rules.

For more details, see "[Event Attributes Tab](#)" on page 181, "[Event Correlation Tab](#)" on page 182, "[Instructions Tab](#)" on page 183, and "[Advanced Tab](#)" on page 178

3. In the Rules page, define one or more policy rules.

- a. In the Policy Rules list, click the  button, and then click one of the following options:
 - **Event on matched rule:** Use this option if you want to send an event to BSM when the conditions are met.
 - **Suppress on matched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are met.
 - **Suppress on unmatched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are *not* met.
- b. Click the **Rule Description** and type a brief description of the rule.

For more details, see ["Policy Rules List" on page 186](#).

4. In Rule Content, use the Condition tab to define values that you want to evaluate against messages that arrive at the agent's message interface. The attributes that are available in the Condition tab correspond to the attributes that you can set when you submit a message to the message interface.

In text boxes, you can use policy variables, policy parameters, and pattern-matching.

For example, to match all such fatal error messages for the insurance application's server process, set the following attributes:

- **Application:** Insurance Application
- **Object:** Server Process
- **Message Text:** FATAL ERROR<*>

This condition would match a message that you send to the message interface using the following command:

```
opcmsg application="Insurance Application" object="Server Process"
msg_text="FATAL ERROR: The server process failed to start."
```

For more details, see ["Condition Tab" on page 179](#).

5. *Optional.* If you are creating a rule of the type 'event on matched rule', set attributes for events that you want the policy to send. You can override the default event attributes here. You can also write instructions that help operators handle the associated event and configure actions to solve problems automatically or manually.

In text boxes, you can use indicators, policy variables, and policy parameters.

For more details, see ["Event Attributes Tab" on page 181](#), ["Event Correlation Tab" on page 182](#), ["Custom Attributes Tab" on page 180](#), ["Instructions Tab" on page 183](#), ["Advanced Tab" on page 178](#), and ["Actions Tab" on the next page](#).

6. *Optional.* In the **Options** page, configure options for local event logs, unmatched events, and pattern matching.

For more details, see ["Options Page" on page 183](#).

7. Click **OK** to save the policy template.

UI Reference

This section includes:

- "Actions Tab" below
- "Advanced Tab" on page 178
- "Condition Tab" on page 179
- "Custom Attributes Tab" on page 180
- "Defaults Page" on page 181
- "Event Attributes Tab" on page 181
- "Event Correlation Tab" on page 182
- "Indicators Tab" on page 182
- "Instructions Tab" on page 183
- "Options Page" on page 183
- "Policy Data Page" on page 185
- "Policy Parameters Tab" on page 185
- "Policy Rules List" on page 186
- "Policy Variables Tab" on page 188
- "Properties Page" on page 188
- "Rules Page" on page 189

Actions Tab

UI Element	Description
Automatic command	Automatic command that runs when the rule is matched.
Command	Command and parameters to run when the command is started for this event. The command runs on the node you specify in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information on <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.

UI Element	Description
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.
Send event immediately	Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.
Wait until local command completes and then	Options that can help to reduce the amount of unnecessary network traffic to the BSM server. For example, if an automatic command solves the problem that generated the event, you may choose not to inform the BSM server. <ul style="list-style-type: none"> • Send the event • Send the event if the local command fails • Send the event only if the local command is successful
Operator-initiated command	Operator-initiated command that is attached to the event that the rule sends to the Event Browser. This command can be started by the BSM user from the Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.
Command	Command and parameters to run when the command is started for this event. The command runs on the node specified in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information about <code>cmd</code> .

UI Element	Description
Non Agent User	<p>By default, the command runs as the agent user (\$AGENT_USER). Alternatively, select Non Agent User and specify a user account and password that exists on the node:</p> <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.

Advanced Tab

Note: In the default event attributes, you cannot set the following attributes:

- Event Drilldown URL
- Type

You can set these event attributes within individual rules.

UI Element	Description
Application	Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM, 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 RTSM, the object attribute is a simple string-type attribute (for example, C:, and /dev/spool).



UI Element	Description
HPOM Service ID	ID of the service associated with 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.
Enable Agent MSI	<p>The message stream interface (MSI) allows external applications to interact with the internal event flow of HP Operations Agent. The external application can be a read-write application, for example, an event processing program that can read events, modify attributes, and generate new events for retransmission to the server. The application could also read events, or send its own events.</p> <p>Divert events. Divert an event to the MSI instead of to the server when an event is requested by an external application.</p> <p>Copy events. Send the event to the server, and a copy of the event to the MSI.</p> <p>If the agent MSI is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Agent MSI. Applies the agent MSI settings configured in the event defaults to this rule.</p> <p>Override default settings for Agent MSI: Enables you to configure specific agent MSI settings for this policy rule.</p>

Condition Tab

UI Element	Description
Node	<p>Fully qualified domain name, node name, or IP address that the policy compares with the node in the source message.</p> <p>Separate multiple entries with the OR operator () or leave blank to match all nodes.</p> <p>This field corresponds to the <code>node</code> option of the <code>opcmsg</code> command.</p>
Message Group	<p>Message group that the policy compares with the message group in the source message.</p> <p>Separate multiple entries with the OR operator () or leave blank to match all message groups.</p> <p>This field corresponds to the <code>msg_grp</code> option of the <code>opcmsg</code> command.</p>
Application	<p>Application that the policy compares with the application in the source message.</p> <p>Separate multiple entries with the OR operator () or leave blank to match all applications.</p> <p>This field corresponds to the <code>application</code> option of the <code>opcmsg</code> command.</p>

UI Element	Description
Object	<p>Object that the policy compares with the object in the source message.</p> <p>Separate multiple entries with the OR operator () or leave blank to match all objects.</p> <p>This field corresponds to the <code>object</code> option of the <code>opcmsg</code> command.</p> <p>Note: Although the term <i>application</i> generally refers to a general program name and <i>object</i> generally refers to a process or sub-program, you should use these values to assist your own organizational scheme.</p>
Severity	<p>Severity that the policy compares with the severity in the source message. At least one severity must be selected.</p> <p>This field corresponds to the <code>severity</code> option of the <code>opcmsg</code> command.</p>
Message Text	<p>Message text or pattern that the policy compares with the message text in the source message.</p>

Custom Attributes Tab

UI Element	Description
	Create New Custom Attribute: Creates a new custom attribute with the default name <code>CA_n</code> . To rename the custom attribute, double-click the name to select it and type the new name.
	Delete Custom Attribute: Deletes an existing custom attribute.

UI	
Element	Description
Name	<p>The name of the custom attribute. The name is case-insensitive.</p> <p>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.</p> <p>The following custom attribute names cannot be used because they are reserved for internal use:</p> <p>Description</p> <p>EtiHint</p> <p>HP_OPR_SAAS_CUSTOMER_ID</p> <p>NoDuplicateSuppression</p> <p>RelatedCiHint</p> <p>SourceCiHint</p> <p>SourcedFromExternalId</p> <p>SourcedFromExternalUrl</p> <p>SubCategory</p> <p>SubCiHint</p>
Value	Value of the custom attribute.

Defaults Page

The Defaults page enables you to set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

For more details, see ["Event Attributes Tab"](#) below, ["Event Correlation Tab"](#) on the next page, and ["Advanced Tab"](#) on page 178.

Event Attributes Tab

Note: In the default event attributes, you can set only the Category attribute. You can set the other event attributes within individual rules.

UI	
Element	Description
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.

UI Element	Description
Send with closed status	Sets the event's lifecycle status to Closed before sending it to the Event Browser in Operations Management.

Event Correlation Tab



Note: In the default event attributes, you cannot set the following attributes:




- Close Events with Key
- Suppress Deduplication on Server

You can set these event attributes within individual rules.

UI Element	Description
Event Key	An identifier used to identify duplicates and for Close Events with Key.
Enable Event Suppression	<p>Enables event suppression for the events generated by this policy.</p> <p>If event suppression is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Event Suppression. Applies the event suppression settings configured in the event defaults to this rule.</p> <p>Override default settings for Event Suppression: Enables you to configure specific event suppression settings for this policy rule.</p>

Indicators Tab

UI Element	Description
	<p>Refresh. Loads the configured indicators from the BSM server.</p> <p>Note: Loading indicators from the BSM server may take a few seconds.</p>
	<p><i>Event integration policies only:</i> Shows or hides the Select drop target format drop-down panel:</p> <ul style="list-style-type: none"> • Use Indicator States. Click to change the drop target format to indicator states only. • Use Indicator Names and States. Click to change the drop target format to indicator names and states.

UI Element	Description
<Search ...>	<p>Entered search string is used to search the indicators and highlight only the indicators containing the specified string.</p> <p>To search for indicators with specific text strings in the name, type the string in the <Search ...> field and click the  button. The first matching indicator is selected in the list of rules. Click the  and  buttons to move to the previous and next matching indicator.</p>
<Indicators>	<p>Hierarchy of configuration item types with associated health indicators (HIs) and event type indicators (ETIs). To insert an indicator in a policy, drag and drop the indicator from the Indicators tab to the relevant field in the policy.</p>

Instructions Tab

UI Element	Description
Instructions	<p>Instructions that you want to accompany the event.</p> <p>Events generated by a policy can include instructions that explain what to do when the event is generated. This instruction text can often help an operator to solve a problem when a particular type of event is received. The operator can view the instructions included with an event by viewing the Event Details pane in the Event Browser. You can define default instructions for all rules in a policy. You can also override the default with different instructions for any rule.</p> <p>You can type URLs in the text, and the Event Browser automatically converts them into clickable hyperlinks. For example, you can add URLs of external Web sites, support sites, documentation repositories, troubleshooting information, and similar sites.</p> <p>To add a link, type any URL that begins with one of the following URI scheme names:</p> <ul style="list-style-type: none"> • http:// • https:// • ftp:// • ftps://



Options Page

UI Element	Description
Log Local Events	<p>Defines 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:</p> <p>Windows: %OvDataDir%\log\OpC\opcmsglg</p> <p>AIX, HP-UX, Linux, and Solaris: /var/opt/OV/log/OpC/opcmsglg</p>



UI Element	Description
that match a rule and trigger an event	Logs any events in the event source that match the policy rules.
that match a rule and are ignored	Logs any events in the event source that are suppressed. (Suppressed events are not sent to the Event Browser.)
that do not match any rule	Logs any events that do not match any of the rules in the policy.
Unmatched Events	<p>Send an event to the 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.</p> <p>Each policy that sends unmatched events to the Event Browser creates an event with the default values of the policy.</p> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p>
are sent to the Event Browser	Sends unmatched events to the Event Browser.
are sent to the Closed Events Browser	Sends unmatched events to the Closed Events Browser.
are ignored	Ignores unmatched events.
Pattern Matching Options	Defines case sensitivity and field separators for all rules.
Case sensitive check	Defines whether the case (uppercase or lowercase) of a text string is considered when the pattern of a rule is compared with the source data. When switched on, a match only occurs if the use of uppercase and lowercase letters is exactly the same in both the source data and the pattern. This is the default setting.







UI Element	Description
Field Separators	<p>Defines 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:</p> <ul style="list-style-type: none"> • \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 (\) <p>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).</p> <p>If you leave this box empty, the default separators (a blank and the tab character) are used by default.</p> <p>You can set case sensitivity and separator characters for individual rules in a policy by clicking the ▶ button in rule's match condition.</p>
Apply to All	<p>Applies the pattern matching options to all existing rules in a policy. This overwrites any modifications made to the pattern matching options in individual rules.</p> <p>If you change the pattern matching options and do not click Apply to all, they only apply to all new rules in a policy.</p>

Policy Data Page


UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Check Syntax: Validates the syntax of the policy data. If the policy syntax is incorrect, the validation tool reports an error and points to the corresponding line and position of the unexpected token (for example the incorrect keyword).
<policy data>	Policy data in text form. The data uses the HP Operations Agent policy syntax.










Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.

UI Element	Description
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Policy Rules List

UI Element	Description
	<p><i>Event policies:</i> Create New Rule: Provides the following options:</p> <ul style="list-style-type: none"> Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM.

UI Element	Description
	Copy Rule. Copies the selected rule. You can then rewrite the description of the copied rule and edit the rule.
	Delete Rule. Deletes the selected rule.
	Move Up. Moves the selected rule higher in the rule order.
	Move Down. Moves the selected rule lower in the rule order.
<Move to>	Entered number is used to select the rule with that sequence number in the list of rules. To select a specific rule in the rule list, type the rule's sequence number in the <Move to> field and click the  button.
<Search rules>	Entered search string is used to search the rule descriptions and highlight only the rules containing the specified string. To search for rules with specific text strings in the rule description, type the string in the <Search rules> field and click the  button. The first matching rule is selected in the list of rules. Click the  and  buttons to move the previous and next matching rule.
	Activate/Deactivate Rule Filter. Activates and deactivates the rule filter.
Seq.	Sequence number of the rules. Rules are evaluated in a specific order. When one condition is matched, no additional rules are evaluated.
Rule Description	Description of the rule. It is good practice to use a description that helps you remember what the rule does
Rule Type	The three rule types of event policies are: <ul style="list-style-type: none"> • Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. • Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. • Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM. <p>The three rule types of metrics policies are:</p> <p>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.</p>

Policy Variables Tab

Variable	Description
<\$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-event basis.
<\$MSG_TEXT>	Returns the full text of the event. For open message interface policies, this value is the <code>msg_text</code> parameter submitted by the <code>opcmsg</code> command. Sample output: <code>SU 03/19 16:13 + tty7 bill-root</code>
<\$OPTION (N) >	Returns the value of an optional variable that is set by <code>opcmsg</code> (for example, <code><\$OPTION (A) ></code> , <code>< \$OPTION (B) ></code> , and so on.).

Properties Page

UI Element	Description
Name	Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed. The name is set when the policy is created and cannot be changed in new versions of a policy.
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.
Version	The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy. Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.
Change Log	Text that describes what is new or modified in this version of the policy.

¹(globally unique identifier)

UI Element	Description
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 Web browser 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 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.
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.
OS Types	Types of operating system with which this policy is compatible. To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify. If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.

Rules Page

The Rules page enables you to define one or more policy rules.

For more details, see "Policy Rules List" on page 186, "Condition Tab" on page 179, "Event Attributes Tab" on page 181, "Event Correlation Tab" on page 182, "Custom Attributes Tab" on page 180, "Advanced Tab" on page 178, and "Actions Tab" on page 176.

Configuring Scheduled Task Policies


Scheduled task policies enable you to start commands and scripts on nodes that have the HP Operations Agent. You can start a task once, or regularly according to a schedule. You can configure the policies to create events when the task starts and if it succeeds or fails.

To access








You can create or edit a scheduled task policy using the Scheduled Task Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:

Admin > Operations Management > Monitoring > Management Templates & Aspects




- b. In the Configuration Folders pane, expand the configuration folders.
- c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.




The Edit Aspect dialog box opens.

- d. Click the **Policy Templates** tab, and then do one of the following:
 - o To add a new policy template:
 - o Click the  button. The Add Policy Template to Aspect dialog box opens.
 - o Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - o Select the type **Scheduled Task Template**, and then click **OK**.
 - o To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Scheduled Task Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:

Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **Scheduled Task Templates** folder, and then do one of the following:
 - o To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New Scheduled Task Policy Editor opens.
 - o To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit Scheduled Task Policy Editor opens.

Tasks

How to Create a Scheduled Task Policy

1. In the Scheduled Task Policy Editor, in the Properties page, type a **Name** for the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "[Properties Page](#)" on page 197.

2. In the Task page, click Task Type, and then click one of the following options:
 - **Command:** Use this option if you want to start a command or program that already exists on the node.
 - **VB Script:** Use this option if you want to start a VB Script, which you embed in the policy.
 - **Perl Script:** Use this option if you want to start a Perl Script, which you embed in the policy.For more details, see ["Task Page" on page 200](#).
3. In the Schedule page, specify when you want the task to run. The following options are available:
 - **Once:** Use this option when you want to run the task at one specific date and time.
 - **Once per interval:** Use this option when you want to run the task at regular intervals.
 - **Advanced:** Use this option when you want the task to run to a complex schedule. You have full control over the year, months, days, hours, and minutes at which the task runs.For more details, see ["Schedule Page" on page 198](#).
4. *Optional.* In the **Start Event**, **Success Event**, and **Failure Event** pages, set attributes for events that you want the policy to send when the task starts, succeeds, or fails. You can also write instructions that help operators handle the associated event.

In text boxes, you can use policy variables, and policy parameters.

For more details, see ["Event Attributes Tab" on page 193](#), ["Event Correlation Tab" on page 193](#), ["Custom Attributes Tab" on the next page](#), ["Instructions Tab" on page 194](#), and ["Advanced Tab" on the next page](#).
5. Click **OK** to save the policy template.

UI Reference

This section includes:



- ["Advanced Tab" on the next page](#)
- ["Custom Attributes Tab" on the next page](#)
- ["Event Attributes Tab" on page 193](#)
- ["Event Correlation Tab" on page 193](#)
- ["Indicators Tab" on page 194](#)
- ["Instructions Tab" on page 194](#)
- ["Policy Data Page" on page 195](#)
- ["Policy Parameters Tab" on page 195](#)
- ["Policy Variables Tab" on page 196](#)
- ["Properties Page" on page 197](#)
- ["Schedule Page" on page 198](#)

- "Start, Success, and Failure Event Page" on page 199
- "Task Page" on page 200

Advanced Tab

UI Element	Description
Application	Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM, 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 RTSM, the object attribute is a simple string-type attribute (for example, C:, and /dev/spool).
HPOM Service ID	ID of the service associated with 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.
Enable Agent MSI	<p>The message stream interface (MSI) allows external applications to interact with the internal event flow of HP Operations Agent. The external application can be a read-write application, for example, an event processing program that can read events, modify attributes, and generate new events for retransmission to the server. The application could also read events, or send its own events.</p> <p>Divert events. Divert an event to the MSI instead of to the server when an event is requested by an external application.</p> <p>Copy events. Send the event to the server, and a copy of the event to the MSI.</p>

Custom Attributes Tab

UI Element	Description
	Create New Custom Attribute: Creates a new custom attribute with the default name CA_ <i>n</i> . To rename the custom attribute, double-click the name to select it and type the new name.
	Delete Custom Attribute: Deletes an existing custom attribute.

UI Element Description	
Name	<p>The name of the custom attribute. The name is case-insensitive.</p> <p>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.</p> <p>The following custom attribute names cannot be used because they are reserved for internal use:</p> <p>Description</p> <p>EtiHint</p> <p>HP_OPR_SAAS_CUSTOMER_ID</p> <p>NoDuplicateSuppression</p> <p>RelatedCiHint</p> <p>SourceCiHint</p> <p>SourcedFromExternalId</p> <p>SourcedFromExternalUrl</p> <p>SubCategory</p> <p>SubCiHint</p>
Value	Value of the custom attribute.





Event Attributes Tab

UI Element Description	
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.
Send with closed status	Sets the event's lifecycle status to Closed before sending it to the Event Browser in Operations Management.

Event Correlation Tab

UI Element Description	
Event Key	An identifier used to identify duplicates and for Close Events with Key.



Indicators Tab

UI Element	Description
	<p>Refresh. Loads the configured indicators from the BSM server.</p> <p>Note: Loading indicators from the BSM server may take a few seconds.</p>
<Search ...>	<p>Entered search string is used to search the indicators and highlight only the indicators containing the specified string.</p> <p>To search for indicators with specific text strings in the name, type the string in the <Search ...> field and click the  button. The first matching indicator is selected in the list of rules. Click the  and  buttons to move to the previous and next matching indicator.</p>
<Indicators>	<p>Hierarchy of configuration item types with associated health indicators (HIs) and event type indicators (ETIs). To insert an indicator in a policy, drag and drop the indicator from the Indicators tab to the relevant field in the policy.</p>





Instructions Tab





UI Element	Description
Instructions	<p>Instructions that you want to accompany the event.</p> <p>Events generated by a policy can include instructions that explain what to do when the event is generated. This instruction text can often help an operator to solve a problem when a particular type of event is received. The operator can view the instructions included with an event by viewing the Event Details pane in the Event Browser. You can define default instructions for all rules in a policy. You can also override the default with different instructions for any rule.</p> <p>You can type URLs in the text, and the Event Browser automatically converts them into clickable hyperlinks. For example, you can add URLs of external Web sites, support sites, documentation repositories, troubleshooting information, and similar sites.</p> <p>To add a link, type any URL that begins with one of the following URI scheme names:</p> <ul style="list-style-type: none"> • http:// • https:// • ftp:// • ftps://

Policy Data Page

UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Check Syntax: Validates the syntax of the policy data. If the policy syntax is incorrect, the validation tool reports an error and points to the corresponding line and position of the unexpected token (for example the incorrect keyword).
<policy data>	Policy data in text form. The data uses the HP Operations Agent policy syntax.

Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>

UI Element	Description
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Policy Variables Tab

Variable	Description
<code><\$MSG_NODE></code>	Returns the IP address of the node on which the original event took place. Sample output: 192.168.1.123
<code><\$MSG_NODE_NAME></code>	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-event basis.
<code><\$MSG_TEXT></code>	Returns the full text of the event. Sample output: SU 03/19 16:13 + ttyp7 bill-root
<code><\$NAME></code>	Returns the name of the policy that sent the event. Sample output: cpu_util
<code><\$PROG></code>	Returns the name of the program executed by the scheduled task policy Sample output: check_for_upgrade.bat
<code><\$USER></code>	Returns the name of the user under which the scheduled task was executed. Sample output: administrator



Properties Page


UI Element	Description
Name	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.

¹(globally unique identifier)

UI Element	Description
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

Schedule Page


UI Element	Description
	
	Select All. Selects all units of time.
Scheduling Options	<p>The following options are available:</p> <ul style="list-style-type: none"> • Once. When Once is selected, the command runs on one specific day at the time you indicate. <p>Note: If the selected date or time occurs in the past, the command is not executed, and the Schedule tab shows a warning.</p> <ul style="list-style-type: none"> • Once per interval. When Once per interval is selected, the command runs once each time the interval that you indicate passes. • Advanced. When Advanced is selected, you can indicate specific days and times when the command should be run. You select specific days of the week, specific days of the month, and specific months. This allows you to specify odd schedules such as, "On Monday when it falls on the 2nd of the month." You can also indicate that the command should only be run during a specific year. <p>Note: If you select Advanced but then do not specify a schedule, the command by default runs every minute.</p>
Once	
Set to current time	Selects the current time in the schedule.
Minute of Hour	0 to 59 minutes.

UI Element	Description
Hours of Day	1 to 12 AM and 1 to 12 PM.
Date: <> 	Date when the command should run. Click the calendar icon to open a calendar view for the current month.
Once per interval	
Interval: <> h <> m <> s	Interval in hours, minutes, and seconds.
Advanced (daily execution)	
Minute of Hour	0 to 59 minutes.
Hours of Day	1 to 12 AM and 1 to 12 PM.
Days of Month	1 to 31 days of the month.
Months of Year	Months from January to December.
Days of Week	Days of the week from Sunday to Saturday.
Restrict schedule to the year	Select to schedule the task for the specified year only.

Start, Success, and Failure Event Page

UI Element	Description
Send Start Event	Click to send an event when the command begins to run.
Send Success Event	Click to send an event when the command completes successfully.
Send Failure Event	Click to send an event when the command fails to run or fails to complete successfully.

Task Page

UI Element	Description
	Load. Opens a file selection dialog box for you to select the VB or Perl script to load into the policy.
Task Type	Type of task: <ul style="list-style-type: none"> • Command • VB Script • Perl Script
Command	Complete path and extension of the command that you want to run (for example, %OvDataDir%\bin\instrumentation\cleanup.exe). The file that you specify should exist on the system. By default, the command runs under the same account as the agent is running, which is Local System or root by default.
Username	User name under which the command should be run. The user must exist and have permission to run the command on the system. If you specify a non-existent user, the command fails to run.
Password	Password for the user.
Enable policy parameter in Password field	Enables you to enter a variable in the Password field, for example %%password%%. A corresponding policy parameter should exist in the Policy Parameters tab.
VB Script	Code that defines the VB script. Instead of typing the script into the field, you can upload an existing script. Tip: Use the policy method <code>Rule.Status</code> to specify whether the task is successful. For example, to specify that the task has failed (and trigger a failure event), use <code>Rule.Status=False</code> . Note: HP Operations Agent uses a generic Microsoft scripting engine to run VBScript scripts. You can therefore use standard VBScript objects (for example, the <code>FileSystemObject</code> object) in your scripts. Objects that are specific to <code>wscript</code> or <code>cscript</code> (for example, the <code>WScript</code> object) are not supported.

UI Element	Description
Perl Script	<p>Code that defines the Perl script. Instead of typing the script into the field, you can upload an existing script.</p> <p>Tip: Use the policy method <code>\$Rule->Status</code> to specify whether the task is successful. For example, to specify that the task has failed (and trigger a failure message), use <code>\$Rule->Status (False)</code>.</p> <p>Note: The agent runs as a service that has no standard input, standard output, or standard error. Therefore, the predefined file handles STDIN, STDOUT, and STDERR are not available for Perl scripts in scheduled task policies. It is also not possible to open file handles that use command pipes or capture the standard output from commands within backticks (<code>`</code>).</p>


Configuring Service Auto-Discovery Policies





Service auto-discovery policies enable you to run scripts (or programs) that discover configuration items in your managed environment. The output of a discovery script is used to automatically populate the BSM Run-time Service Model (RTSM). HP Operations Smart Plug-ins (SPIs) supply many service auto-discovery policies. You can also create your own custom service auto-discovery policies.




To access

You can create or edit a service auto-discovery policy using the Discovery Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:




Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.

The Edit Aspect dialog box opens.
 - d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **Service Auto-Discovery Template**, and then click **OK**.




- To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Discovery Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:

Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **Service Auto-Discovery Templates** folder, and then do one of the following:
 - To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New Node Info Policy Editor opens.

- To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit Node Info Policy Editor opens.

Learn More

This section includes:

- ["Service Auto-Discovery Policy Syntax" below](#)
- ["Configuration Item XML Schema Definition \(XSD\)" below](#)
- ["Configuration Item XML Element Description" on page 204](#)

Service Auto-Discovery Policy Syntax

The data part of a service auto-discovery policy is in XML and defines the management module, the service type definition, the discovery command, and the schedule. If you are creating your own custom service auto-discovery policy, choose the `customdiscovery` management module and the `DiscoveredElement` service type definition.

Tip: Because of the complexity of the service auto-discovery policy XML, it is recommended that you copy and paste policy data from an existing discovery policy and modify it.

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>

```

Configuration Item XML Element Description

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

Element	Description
NewInstance	Represents a discovered CI. You must add a <i>ref</i> attribute, which must match the unique CI ID that you specify in the <i>Key</i> element. You can then use this reference in <i>Instance</i> 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 <i>NewInstance</i> in the XML document. Note: You can control how often the discovery script must run before a missing CI is automatically deleted by changing the agent parameter <code>INSTANCE_DELETION_THRESHOLD</code> in the <code>agtrep</code> namespace. However, if you specify this element, the agent deletes the CI immediately and publishes the change to the RTSM ¹ .
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.

¹(Run-time Service Model)

Element	Description
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"> <code>hpom_citype</code> specifies the CI type as stored in the RTSM (for example, <code>nt</code>). <p>The default synchronization package on the BSM server assigns the context <code>IntegrationAdapter</code> to all CIs that have a <code>hpom_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"> <code>hpom_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. 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>).
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.</p> <p>The parent instance that you specify must exist in the RTSM and in the agent repository on the node. 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.</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 (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.

Tasks


How to Create a Service Auto-Discovery Policy

1. In the Properties page, type a **Name** for the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "[Properties Page](#)" on page 208.

2. In the Policy Data page, type the policy data using the HP Operations Agent service auto-discovery policy syntax. If you are creating a new policy, copy and paste template data from an

existing policy template. Alternatively, click the  button to load policy data from a policy template file on your computer.

For details, see "Service Auto-Discovery Policy Syntax" on page 202.

The discovery command that you reference in the policy must output XML that conforms to the XSD described in "Configuration Item XML Schema Definition (XSD)" on page 202.

You can also use policy parameters. For more details, see "Policy Parameters Tab" below.



3. Click **OK** to save the policy template.

UI Reference




This section includes:






- "Policy Data Page" below
- "Policy Parameters Tab" below
- "Properties Page" on the next page

Policy Data Page

UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Service Auto-Discovery policies do not support syntax checking. You can click Check Syntax but the check fails to perform.
<code><policy data></code>	Policy data in text form. The data uses the HP Operations Agent policy syntax. For details, see "Service Auto-Discovery Policy Syntax" on page 202.

Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.
	Delete Parameter: Delete the selected parameter from the list.

UI Element	Description
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Properties Page

UI Element	Description
Name	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.

¹(globally unique identifier)


UI Element	Description
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

Configuring Service/Process Monitoring Policies








Service/process monitoring policies enable you to monitor the status of services (on Windows) and processes (on any operating system that the HP Operations Agent supports). You can configure the policies to create events and launch commands when a change occurs in either the status of a service or the number of running processes.

To access




You can create or edit a service/process monitoring policy using the Service/Process Monitoring Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:
Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.

The Edit Aspect dialog box opens.




- d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **Service/Process Monitoring Template**, and then click **OK**.
 - To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Service/Process Monitoring Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:
Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **Service/Process Monitoring Templates** folder, and then do one of the following:
 - To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw**

Mode) button.

The New Service/Process Monitoring Policy Editor opens.

- To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit Service/Process Monitoring Policy Editor opens.

Learn More

This section includes:

- ["Default and Custom Actions" below](#)
- ["Default Session Object Values" below](#)

Default and Custom Actions

A service/process monitoring policy can run an action when a change occurs in the status of a service or the number of running processes. The following types of action responses are available:

- **Start action.** A start action is triggered when the service is not in the state you specified, or the number of processes, CPU utilization, or memory usage is not as you specified.
- **Continue action.** After the start action runs, continue actions are carried out at each subsequent polling interval if the reset value is not reached.
- **End action.** After the start action runs, end actions are carried out after the service or process returns to the expected state.

You can configure default actions, which apply to all service or process monitors. You can also configure custom actions in policy rules. Custom actions apply to individual service or process monitors. By default, service or process monitors do not have any default actions specified.

Default Session Object Values

You can also use some default session object values in event and command text boxes. The agent automatically sets these values for service/process monitoring policies.

- **Session object values for service monitoring policies.** The agent automatically sets the following values in the session object for service monitor policies:

<\${SESSION (SERVICENAME)} >

Returns the name used to access the Windows service on the node.

<\${SESSION (SERVICEDISPLAYNAME)} >

Returns the display name of the Windows service. This value is retrieved on the specified node and can be displayed in the local language of the node.

<\${SESSION (SERVICEMONITORSTATE)} >

Returns the state of the Windows service to monitor, for example; "running", "stopped", or "disabled". If an agent catalog is available in the local language set on the node, this is the localized text for the monitor state. If no agent catalog is available in the local language of the node, English text is used to display the monitor state.

<\${SESSION (SERVICECURRENTSTATE)} >

Returns the current state of the Windows service being monitored, for example; "running", "stopped", or "disabled". If an agent catalog is available in the local language set on the node, this is the localized text for the monitor state. If no agent catalog is available in the local language of the node, English text is used to display the monitor state.

<\${SESSION (SERVICEACTION)} >

Returns the string used to build the event title. It depends on the monitor mode you define:

- Monitor state "running"
net start /Y <service_name>
 - Monitor state "stopped"
net stop /Y <service_name>
 - Monitor state "disabled"
empty
- **Session object values for process monitoring policies.** The agent automatically sets the following values in the session object for process monitor policies:

<\${SESSION (PROCESSNAME)} >

Returns the name used to access the process on the node.

<\${SESSION (PROCESSPARAMETERS)} >

Returns the parameter pattern used to access the process on the node.

<\${SESSION (PROCESSNBREXPECTED)} >

Returns the number of monitored processes.

<\${SESSION (PROCESSNBRAVAILABLE)} >

Returns the number of available processes matching the process name and parameter pattern.

<\${SESSION (PROCESSCPUUSAGEEXPECTED)} >

Returns the percentage of CPU usage that you expect the process to use.

<\${SESSION (PROCESSCPUUSAGE)} >

Returns the percentage of the current CPU usage of the monitored process.

<\${SESSION (PROCESSMEMUSAGEEXPECTED)} >

Returns the amount of memory (in megabytes) that you expect the process to use.

<\${SESSION (PROCESSMEMUSAGE)} >

Returns the current memory usage of the monitored process.

<\${SESSION (PROCESSMODE)} >

Returns the string used to build the message text. It depends on the monitor you specify, for example:

- MIN
PROCESSMODE is: ">= "
- MAX
PROCESSMODE is: "<= "
- EQUAL
PROCESSMODE is: " " (empty string)

Tasks

How to Create a Service/Process Monitoring Policy

1. In the Service/Process Monitoring Policy Editor, in the Properties page, type a **Name** for the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.


For more details, see "[Properties Page](#)" on page 226.

2. In the Source page, select **Services** or **Processes**, depending on what you want to monitor. Optionally modify the polling interval. The polling interval determines how often the policy checks the source for new information.
3. *Optional.* In the Defaults page, configure start, continue, or end actions for the policy. Default actions apply to all service or process monitors. You can also configure custom actions in policy rules. Custom actions apply to individual service or process monitors. By default, service or process monitors do not have any default actions specified.

For details, see "[Start, Continue, and End Actions \(Defaults\)](#)" on page 227.

In event and command text boxes, you can use policy variables and default session object values. The agent automatically sets these values for service/process monitoring policies.

For details on the each event tab, see "[Event Attributes Tab](#)" on page 222, "[Event Correlation Tab](#)" on page 222, "[Custom Attributes Tab](#)" on page 221, "[UI Element](#)" on page 222, "[Advanced Tab](#)" on page 219, and "[Actions Tab \(Events\)](#)" on page 216.

4. In the Rules page, define one or more policy rules. For each service or process that you want to monitor, add a rule by clicking the  button.

For details, see "[Policy Rules List](#)" on page 224.

5. *Service monitors only.* In the Condition tab, define the service that you want to monitor and the state you expect:
 - a. Type the *real* name of the Windows service you want to monitor.
 - b. *Optional.* Type a **Display Name** of the monitor. The Display Name is used in the policy editor for information purposes only. It is not used to identify the Windows service.
 - c. Select the state that you want to monitor for the selected Windows service. For example, the default monitoring status "Running" checks whether the selected Windows service is running. Other states include "Disabled" and "Stopped". If the policy detects a change in

state for the selected Windows service, it starts the actions defined for the policy.

- d. *Optional.* Click **Send event if service doesn't exist** to ensure that you are informed if the Windows service is not present when you deploy the policy to the node.
6. *Process monitors only.* In the Condition tab, specify the process that you want to monitor:
 - a. Type the name of the process you want to monitor.

For Windows nodes, the string you enter here must match the name of the process as it is known to Windows, including the file extension, for example: "notepad.exe". Duplicates are not allowed.

For UNIX or Linux nodes, specify *only* the name of the executable file for the process that you want to monitor. Do not include the path.
 - b. *Optional.* Define the strings or parameters that you need to match in the **Parameters** field. If you use this option, the parameters you specify are used to identify the running process. Standard pattern matching is used to evaluate the contents of this field, which for Windows managed nodes are not case sensitive. Note that:
 - If the **Parameters** field is empty, the policy editor matches only processes running without parameters.
 - If the **Parameters** field contains a string with no pattern-matching characters, the policy editor matches only processes with the defined string.
 - If the **Parameters** field contains pattern-matching characters, the policy editor matches all process parameters with the string defined (for example, <*> matches *all* parameters, and <*>abc<*> matches all parameters containing the string "abc").
 - c. Use the drop-down list to specify an operator, and the **Number of processes** text box to specify the number of processes that you expect to be running. Use the equals operator (==) to specify an exact value. Alternatively, use less than or equal to (<=), or greater than or equal to (>=) to define a range (for example, >=1).
 - d. *Optional.* Use the drop-down list to specify an operator, and the **CPU utilization** text box to specify the percentage of CPU that you expect the process to use. Use the equals operator (==) to specify an exact value. Alternatively, use less than or equal to (<=), or greater than or equal to (>=) to define a range (for example, <=60).
 - e. *Optional.* Use the drop-down list to specify an operator, and the **Memory usage** text box to specify the amount of memory (in megabytes) that you expect the process to use. Use the equals operator (==) to specify an exact value. Alternatively, use less than or equal to (<=), or greater than or equal to (>=) to define a range (for example, <=200).
 7. *Optional.* Use the Actions tab to define how the policy responds when the status of a monitored service changes, for example from "running" to "stopped", or when the number of processes, CPU utilization, or memory usage changes. Complete the following steps to configure custom actions for a service or process monitor:
 - a. Click **Override default actions**.
 - b. Click **Edit the "Start Actions" event** to open the Start Action tab. A start action is triggered when service is not in the state you specified or when the number of processes, CPU utilization, or memory usage is not as you specified.

Use the event tabs in the Start Action tab to define the details of the event.

For details on the each event tab, see "Event Attributes Tab" on page 222, "Event Correlation Tab" on page 222, "Custom Attributes Tab" on page 221, "UI Element" on page 222, "Advanced Tab" on page 219, and "Actions Tab (Events)" on the next page.

- c. *Optional.* If you want to configure continue actions, click one of the following:
 - **Use the specified "Start Actions"**. This option enables you to send an event that is a duplicate of the start action event. In addition, if the start action has an automatic command, the agent starts this command again.
 - **Define special "Continue Actions"**. This option enables you to configure an event and commands that are different to those in the start action.

To configure the event that the continue action sends, click **Edit the "Continue Action" event** and use the tabs in the Continue Action tab to define the details of the event.

For details on the each event tab, see "Event Attributes Tab" on page 222, "Event Correlation Tab" on page 222, "Custom Attributes Tab" on page 221, "UI Element" on page 222, "Advanced Tab" on page 219, and "Actions Tab (Events)" on the next page.

- d. *Optional.* If you want to configure an end action, click **Start the specified "End Actions"**. Then click **Edit the "End Action" event** and use the tabs in the End Action tab to define the details of the event.

For details on the each event tab, see "Event Attributes Tab" on page 222, "Event Correlation Tab" on page 222, "Custom Attributes Tab" on page 221, "UI Element" on page 222, "Advanced Tab" on page 219, and "Actions Tab (Events)" on the next page.

In event and command text boxes, you can use policy variables and default session object values. The agent automatically sets these values for service/process monitoring policies.

8. Click **OK** to save the policy template.

UI Reference

This section includes:

- "Actions Tab (Events)" on the next page
- "Actions Tab (Rules)" on page 218
- "Advanced Tab" on page 219
- "Condition Tab" on page 219
- "Custom Attributes Tab" on page 221
- "Event Attributes Tab" on page 222
- "Event Correlation Tab" on page 222
- "Instructions Tab" on page 222
- "Policy Data Page" on page 223
- "Policy Parameters Tab" on page 223
- "Policy Rules List" on page 224

- "Policy Variables Tab" on page 225
- "Properties Page" on page 226
- "Source Page" on page 227
- "Start, Continue, and End Actions (Defaults)" on page 227
- "Start, Continue, and End Actions (Rules)" on page 228

Actions Tab (Events)

UI Element	Description
Automatic command	Automatic command that runs when the rule is matched.
Command	Command and parameters to run when the command is started for this event. The command runs on the node you specify in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information on <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.

UI Element	Description
Send event immediately	Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.
Wait until local command completes and then	Options that can help to reduce the amount of unnecessary network traffic to the BSM server. For example, if an automatic command solves the problem that generated the event, you may choose not to inform the BSM server. <ul style="list-style-type: none"> • Send the event • Send the event if the local command fails • Send the event only if the local command is successful
Operator-initiated command	Operator-initiated command that is attached to the event that the rule sends to the Event Browser. This command can be started by the BSM user from the Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.
Command	Command and parameters to run when the command is started for this event. The command runs on the node specified in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information about <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.

UI Element	Description
Close the event when the command is successful	Closes the event automatically if the command is successful.

Actions Tab (Rules)

UI Element	Description
Rule Actions	<p>Use default actions: Applies the action settings configured in the event defaults to this rule.</p> <p>Override default actions: Enables you to configure specific action settings for this rule.</p>
Start Actions	<p>A start action is triggered when the service is not in the state you specified, or the number of processes, CPU utilization, or memory usage is not as you specified.</p> <p>Edit the "Start Actions" event: Opens the Start Action tab, which enables you to define a start action.</p>
Continue Actions	<p>After the start action runs, continue actions are carried out at each subsequent polling interval if the reset value is not reached.</p> <p>Don't start any "Continue Actions": Select this option if you do not want to start any continue actions.</p> <p>Use the specified "Start Actions": This option enables you to send an event that is a duplicate of the start action event. In addition, if the start action has an automatic command, the agent starts this command again.</p> <p>Define special "Continue Actions": This option enables you to configure an event and commands that are different to those in the start action.</p> <p>Edit the "Continue Action" event: Opens the Continue Action tab, which enables you to define a continue action.</p>
End Actions	<p>After the start action runs, end actions are carried out after the service or process returns to the expected state.</p> <p>Start the specified "End Actions": This option enables you to configure an event and commands for the end action.</p> <p>Edit the "End Action" event: Opens the End Action tab, which enables you to define an end action.</p>

Advanced Tab

UI Element	Description
Application	Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM, 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 RTSM, the object attribute is a simple string-type attribute (for example, C:, and /dev/spool).
HPOM Service ID	ID of the service associated with 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.
Enable Agent MSI	<p>The message stream interface (MSI) allows external applications to interact with the internal event flow of HP Operations Agent. The external application can be a read-write application, for example, an event processing program that can read events, modify attributes, and generate new events for retransmission to the server. The application could also read events, or send its own events.</p> <p>Divert events. Divert an event to the MSI instead of to the server when an event is requested by an external application.</p> <p>Copy events. Send the event to the server, and a copy of the event to the MSI.</p> <p>If the agent MSI is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Agent MSI. Applies the agent MSI settings configured in the event defaults to this rule.</p> <p>Override default settings for Agent MSI: Enables you to configure specific agent MSI settings for this policy rule.</p>



Condition Tab

UI Element	Description
Monitoring Services	
Service Name	<p>The <i>real</i> name of the Windows service that you want to monitor.</p> <p>The policy editor does not check whether the Windows service you specify exists (for example, because you have not typed the service name correctly). Select the Send event if service does not exist option to ensure that you are informed if the Windows service you specify here is <i>not</i> present when you deploy the policy to the node.</p>
Display Name	The Display Name is used in the policy editor for information purposes only. It is not used to identify the Windows service.

Monitoring	The state that you want to monitor for the selected Windows service. For example, the default monitoring status "Running" checks whether the selected Windows service is running. Other states include "Disabled" and "Stopped". If the policy detects a change in state for the selected Windows service, it starts the actions defined for the policy.
Send event if service doesn't exist	Sends an event if the service specified in the policy is not present on the node when you deploy the policy.
Monitoring Processes	
Process	<p>The name of the process that you want to monitor.</p> <p>For Windows nodes, the string you enter here must match the name of the process as it is known to Windows, including the file extension, for example: "notepad.exe". Duplicates are not allowed.</p> <p>For UNIX or Linux nodes, specify <i>only</i> the name of the executable file for the process that you want to monitor. Do not include the path.</p> <p>You can monitor multiple instances of a process by using parameters to differentiate between the instances (for example, <code>svchost.exe -k rpcss</code> and <code>svchost.exe -k netsvcs</code>). For more information, see Parameters below.</p>
Parameters	<p>Define the strings or parameters that you need to match. If you use this option, the parameters you specify are used to identify the running process. Standard pattern matching is used to evaluate the contents of this field, which for Windows managed nodes are not case sensitive. Note that:</p> <ul style="list-style-type: none"> • If the Parameters field is empty, the policy editor matches only processes running without parameters. • If the Parameters field contains a string with no pattern-matching characters, the policy editor matches only processes with the defined string. • If the Parameters field contains pattern-matching characters, the policy editor matches all process parameters with the string defined (for example, <code><*></code> matches <i>all</i> parameters, and <code><*>abc<*></code> matches all parameters containing the string "abc").
Number of processes	<p>Use the drop-down list to specify an operator, and the text box to specify the number of processes that you expect to be running. Use the equals operator (<code>==</code>) to specify an exact value. Alternatively, use less than or equal to (<code><=</code>), or greater than or equal to (<code>>=</code>) to define a range (for example, <code>>=1</code>).</p> <p>The value you enter here defines the state which the policy <i>expects</i> to find and considers correct. The policy sends an event only if the state it finds is <i>not</i> the expected one. For example, use <code>>= 1</code> (greater than or equal to one) to check that one or more instances of a process are running. If the policy discovers that 0 (zero) instances of the process are running, it sends an event.</p>

CPU utilization	Use the drop-down list to specify an operator, and the text box to specify the percentage of CPU that you expect the process to use. Use the equals operator (==) to specify an exact value. Alternatively, use less than or equal to (<=), or greater than or equal to (>=) to define a range (for example, <=60).
Memory usage	Use the drop-down list to specify an operator, and the text box to specify the amount of memory (in megabytes) that you expect the process to use. Use the equals operator (==) to specify an exact value. Alternatively, use less than or equal to (<=), or greater than or equal to (>=) to define a range (for example, <=200).

Custom Attributes Tab

UI	
Element	Description
	Create New Custom Attribute: Creates a new custom attribute with the default name CA_n. To rename the custom attribute, double-click the name to select it and type the new name.
	Delete Custom Attribute: Deletes an existing custom attribute.
Name	<p>The name of the custom attribute. The name is case-insensitive.</p> <p>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.</p> <p>The following custom attribute names cannot be used because they are reserved for internal use:</p> <p>Description</p> <p>EtiHint</p> <p>HP_OPR_SAAS_CUSTOMER_ID</p> <p>NoDuplicateSuppression</p> <p>RelatedCiHint</p> <p>SourceCiHint</p> <p>SourcedFromExternalId</p> <p>SourcedFromExternalUrl</p> <p>SubCategory</p> <p>SubCiHint</p>
Value	Value of the custom attribute.

Event Attributes Tab

UI Element	Description
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.
Send with closed status	Sets the event's lifecycle status to Closed before sending it to the Event Browser in Operations Management.



Event Correlation Tab

UI Element	Description
Event Key	An identifier used to identify duplicates and for Close Events with Key.





Instructions Tab





UI Element	Description
Instructions	<p>Instructions that you want to accompany the event.</p> <p>Events generated by a policy can include instructions that explain what to do when the event is generated. This instruction text can often help an operator to solve a problem when a particular type of event is received. The operator can view the instructions included with an event by viewing the Event Details pane in the Event Browser. You can define default instructions for all rules in a policy. You can also override the default with different instructions for any rule.</p> <p>You can type URLs in the text, and the Event Browser automatically converts them into clickable hyperlinks. For example, you can add URLs of external Web sites, support sites, documentation repositories, troubleshooting information, and similar sites.</p> <p>To add a link, type any URL that begins with one of the following URI scheme names:</p> <ul style="list-style-type: none"> • <code>http://</code> • <code>https://</code> • <code>ftp://</code> • <code>ftps://</code>

Policy Data Page








UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Check Syntax: Validates the syntax of the policy data. If the policy syntax is incorrect, the validation tool reports an error and points to the corresponding line and position of the unexpected token (for example the incorrect keyword).
<policy data>	Policy data in text form. The data uses the HP Operations Agent policy syntax.

Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>

UI Element	Description
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Policy Rules List

UI Element	Description
	Create New Rule: Adds a rule to the service/process monitoring policy.
	Copy Rule. Copies the selected rule. You can then rewrite the description of the copied rule and edit the rule.
	Delete Rule. Deletes the selected rule.
<Search rules>	<p>Entered search string is used to search the service or process names and highlight only the rules containing the specified string.</p> <p>To search for rules with specific text strings in the service or process name, type the string in the <Search rules> field and click the  button. The first matching rule is selected in the list of rules. Click the  and  buttons to move the previous and next matching rule.</p>
	Activate/Deactivate Rule Filter. Activates and deactivates the rule filter.
Seq.	Number of the rule in the list.
Rules for service monitors	
Service Name	Name of the Windows service being monitored.

UI Element	Description
Display Name	Display name of the Windows service being monitored.
Monitoring	Expected state of the monitored service: Running, Stopped, Disabled
Rule Actions	Actions configured for the rule: Default or Custom
Rules for process monitors	
Process	Name of the process being monitored.
Parameters	String or pattern to match the parameters of the process.
Operator	equals operator (==) less than or equal to (<=) or greater than or equal to (>=)
Number of Processes	Expected number of running processes.
Rule Actions	Actions configured for the rule: Default or Custom

Policy Variables Tab

You can use the following variables in Windows event log policies. If a variable returns values that contain spaces, surround the variable with quotation marks.

Variable	Description
<\$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-event basis.
<\$MSG_TEXT>	Returns the full text of the event. Sample output: SU 03/19 16:13 + ttyp7 bill-root
<\$NAME>	Returns the name of the policy that sent the event. Sample output: cpu_util

Properties Page

UI Element	Description
Name	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.

¹(globally unique identifier)

UI Element	Description
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

Source Page

UI Element	Description
Monitoring	Choose whether to monitor the status of services (on Windows) or processes (on any operating system that the HP Operations Agent supports).
Polling Interval	<p>Indicate how often the policy should check the source for new information. This period of time is the polling interval.</p> <p>To increase performance, the polling interval should be as large as possible, while still being frequent enough to monitor data at the rate that it is expected to change. A policy begins to evaluate data <i>after</i> the first polling interval passes. A shorter polling interval is better when you are testing a policy.</p>

Start, Continue, and End Actions (Defaults)

Note: The Default Start, Continue, and End Action pages enable you to configure default settings for any actions started by the policy. For details on the each tab, see ["Event Attributes Tab" on page 222](#), ["Event Correlation Tab" on page 222](#), ["Custom Attributes Tab" on page 221](#), ["UI Element" on page 222](#), ["Advanced Tab" on page 219](#), and ["Actions Tab \(Events\)" on page 216](#).

UI Element	Description
Define default start actions	A start action is triggered when the service is not in the state you specified, or the number of processes, CPU utilization, or memory usage is not as you specified.
Define default continue actions	After the start action runs, continue actions are carried out at each subsequent polling interval if the reset value is not reached.
Define default end actions	After the start action runs, end actions are carried out after the service or process returns to the expected state.

Start, Continue, and End Actions (Rules)

UI Element	Description
Event Attributes	Enables you to set the attributes of the start, continue, or end event.
Event Correlation	Enables you to set correlation options for the start, continue, or end event.
Custom Attributes	Enables you to add custom attributes to the start, continue, or end event.
Instructions	Enables you to add instruction information to help operators handle the start, continue, or end event.
Advanced	Enables you to set the advanced attributes of the start, continue, or end event.
Actions	Enables you to add automatic and operator-initiated commands to the start, continue, or end event.






Configuring SNMP Interceptor Policies

SNMP interceptor policies enable you to monitor devices that send SNMP notifications (for example, printers, routers, computers with unsupported operating systems) to the HP Operations Agent. SNMP interceptor policies enable you to filter SNMP notifications through rules. Each rule consists of a condition definition, and optionally an event definition. When an SNMP notification matches your conditions, you can create an event.




To access

You can create or edit an SNMP interceptor policy using the SNMP Trap Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:




Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.
The Edit Aspect dialog box opens.
 - d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy

Template dialog box opens.




- Select the type **SNMP Interceptor Template**, and then click **OK**.
- To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The SNMP Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:

Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **SNMP Interceptor Templates** folder, and then do one of the following:
 - To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New SNMP Trap Policy Editor opens.

- To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit SNMP Trap Policy Editor opens.

Learn More

Receiving SNMP Notifications

SNMP interceptor policies enable you to filter SNMP notifications that other devices send to a node that runs HP Operations Agent. HP Operations Agent has a built-in SNMP interceptor daemon or service (called `opctrapi`), which accepts SNMP notifications on port 162 by default. Therefore, in many cases, you can configure your SNMP devices to send notifications to port 162 on the node that runs HP Operations Agent.

If port 162 is already in use by another process (for example the Microsoft SNMP Trap service or the Linux `snmptrapd` daemon), `opctrapi` cannot start. In this case, you can reconfigure `opctrapi` to use a different port by setting the `SNMP_TRAP_PORT` agent configuration variable (in the `eaagt` namespace). You must also configure your SNMP devices to send notifications to the same port.

Alternatively, for nodes that run a Windows operating system, you can configure `opctrapi` to subscribe to the Microsoft SNMP Trap service. However, this configuration provides only SNMPv1 traps.

To configure `opctrapi` to subscribe to 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 SNMP interceptor:

```
ovc -restart opctrapi
```

For more information about the available SNMP configuration variables and how to set them, see the *HP Operations Agent Reference Guide*.

Tasks

How to Create an SNMP Interceptor Policy

1. In the SNMP Policy Editor, in the Properties page, type a **Name** for the policy.


You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "[Properties Page](#)" on page 247.

2. *Optional.* In the Defaults page, set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

Note: You can set defaults for only a subset of event attributes. You can set the other event attributes within individual rules.

For more details, see "[Event Attributes Tab](#)" on page 238, "[Event Correlation Tab](#)" on page 238, "[Instructions Tab](#)" on page 240, and "[Advanced Tab](#)" on page 234.

3. In the Rules page, define one or more policy rules.
 - a. In the Policy Rules list, click the  button, and then click one of the following options:
 - **Event on matched rule:** Use this option if you want to send an event to BSM when the conditions are met.
 - **Suppress on matched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are met.
 - **Suppress on unmatched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are *not* met.

- b. Click the **Rule Description** and type a brief description of the rule.

For more details, see "[Policy Rules List](#)" on page 243.

4. In Rule Content, use the Condition tab to define values that you want to evaluate against SNMP notifications that arrive at the agent. The attributes that are available in the Condition tab correspond to the attributes that an SNMP notification may contain.

In text boxes, you can use policy variables, policy parameters, and pattern-matching.


For example, to match generic linkDown traps from 192.168.100.123, set the following attributes:

- **Node:** 192.168.100.123
- **SNMPv1 notation** (selected)
- **Generic ID:** linkDown

For more details, see ["Condition Tab" on page 235](#).

5. In the Condition Variable Bindings tab, select the variable bindings you want the policy to evaluate, and write one or more match patterns for each binding. You can use pattern-matching rules when matching variable bindings.

For example, in many SNMP notifications, \$2 contains the hostname of the sender. To match events only from systems in the domain example.com, do the following:

- a. Click the  button.
 - b. In **Variable**, type 2.
 - c. In **Pattern**, type <*>.example.com.
6. *Optional.* If you are creating a rule of the type 'event on matched rule', set attributes for events that you want the policy to send. You can override the default event attributes here. You can also write instructions that help operators handle the associated event and configure actions to solve problems automatically or manually.

In text boxes, you can use indicators, policy variables, and policy parameters.

For more details, see ["Event Attributes Tab" on page 238](#), ["Event Correlation Tab" on page 238](#), ["Custom Attributes Tab" on page 237](#), ["Instructions Tab" on page 240](#), ["Advanced Tab" on page 234](#), and ["Actions Tab" on the next page](#).

7. *Optional.* In the **Options** page, configure options for local event logs, unmatched events, and pattern matching.

For more details, see ["Options Page" on page 240](#).

8. Click **OK** to save the policy template.

UI Reference

This section includes:

- ["Actions Tab" on the next page](#)
- ["Advanced Tab" on page 234](#)
- ["Condition Tab" on page 235](#)
- ["Condition Variable Bindings Tab" on page 236](#)
- ["Custom Attributes Tab" on page 237](#)
- ["Defaults Page" on page 238](#)
- ["Event Attributes Tab" on page 238](#)
- ["Event Correlation Tab" on page 238](#)
- ["Indicators Tab" on page 239](#)

- "Instructions Tab" on page 240
- "Options Page" on page 240
- "Policy Data Page" on page 242
- "Policy Parameters Tab" on page 242
- "Policy Rules List" on page 243
- "Policy Variables Tab" on page 245
- "Properties Page" on page 247
- "Rules Page" on page 248

Actions Tab

UI Element	Description
Automatic command	Automatic command that runs when the rule is matched.
Command	Command and parameters to run when the command is started for this event. The command runs on the node you specify in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information on <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.

UI Element	Description
Close the event when the command is successful	Closes the event automatically if the command is successful.
Send event immediately	Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.
Wait until local command completes and then	Options that can help to reduce the amount of unnecessary network traffic to the BSM server. For example, if an automatic command solves the problem that generated the event, you may choose not to inform the BSM server. <ul style="list-style-type: none"> • Send the event • Send the event if the local command fails • Send the event only if the local command is successful
Operator-initiated command	Operator-initiated command that is attached to the event that the rule sends to the Event Browser. This command can be started by the BSM user from the Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.
Command	Command and parameters to run when the command is started for this event. The command runs on the node specified in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information about <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.

UI Element	Description
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.

Advanced Tab

Note: In the default event attributes, you cannot set the following attributes:

- Event Drilldown URL
- Type

You can set these event attributes within individual rules.

UI Element	Description
Application	Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM, 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 RTSM, the object attribute is a simple string-type attribute (for example, C:, and /dev/spool).
HPOM Service ID	ID of the service associated with 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.

UI Element	Description
Enable Agent MSI	<p>The message stream interface (MSI) allows external applications to interact with the internal event flow of HP Operations Agent. The external application can be a read-write application, for example, an event processing program that can read events, modify attributes, and generate new events for retransmission to the server. The application could also read events, or send its own events.</p> <p>Divert events. Divert an event to the MSI instead of to the server when an event is requested by an external application.</p> <p>Copy events. Send the event to the server, and a copy of the event to the MSI.</p> <p>If the agent MSI is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Agent MSI. Applies the agent MSI settings configured in the event defaults to this rule.</p> <p>Override default settings for Agent MSI: Enables you to configure specific agent MSI settings for this policy rule.</p>

Condition Tab

UI Element	Description
Node	<p>FQDN¹, the primary node name, or the IP address of the configuration item for which you want to forward events.</p> <p>If you only want to match SNMP events from a specific configuration item, type the FQDN², the primary node name, or the IP address. Give multiple entries with the OR operator (for example, <code>celery.example.com broccoli.example.com</code>), or leave blank for all configuration items.</p>
Event Object ID	<p>Complete Event Object Identifier for the SNMP trap that you want to match.</p> <p>For example: <code>.1.3.6.1.4.1.11.2.17.1.0.40000001</code></p>
SNMPv1 notation	<p>If selected, you can specify only part of the identifier rather than the complete event object ID.</p> <p>For example, by specifying only the Enterprise ID, you can match all events with a specific Enterprise ID.</p>




¹(Fully Qualified Domain Name)

²(Fully Qualified Domain Name)

<p>Enterprise ID</p>	<p>Enterprise ID for incoming SNMP traps to be compared with this condition. The enterprise ID is a vendor-specific identifier for the trap. Standard 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:</p> <p>.1.3.6.1.4.1.11.2.17</p> <p>would match:</p> <p>.1.3.6.1.4.1.11.2.17.1</p> <p>.1.3.6.1.4.1.11.2.17.2</p> <p>and so on.</p>
<p>Generic ID</p>	<p>Generic Trap ID. Possible values are:</p> <ul style="list-style-type: none"> • (0) ColdStart • (1) WarmStart • (2) LinkDown • (3) LinkUp • (4) Authentication • (5) EgpNeighborLoss • (6) EnterpriseSpecific • (7) don't care <p>If you select (6) EnterpriseSpecific, you can type in the specific trap ID. Select don't care to intercept any kind of trap.</p>
<p>Specific ID</p>	<p>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.</p>



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

Condition Variable Bindings Tab

UI Element	Description
	<p>Creates a new variable binding.</p>
	<p>Deletes the selected variable binding.</p>
	<p>Opens the Variable Bindings Options page.</p>

UI Element	Description
Variable	Variable binding you want the policy to read. 1 represents the first variable binding in the event, 2 the second variable, and so on. You do not need to prefix the variable with a dollar sign (\$); the editor does this automatically.
Pattern	Match pattern for the binding. Tip: You can click the ► button to open the pattern matching expression toolbox.

Custom Attributes Tab

UI Element	Description
	Create New Custom Attribute: Creates a new custom attribute with the default name CA_ <i>n</i> . To rename the custom attribute, double-click the name to select it and type the new name.
	Delete Custom Attribute: Deletes an existing custom attribute.
Name	<p>The name of the custom attribute. The name is case-insensitive.</p> <p>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.</p> <p>The following custom attribute names cannot be used because they are reserved for internal use:</p> <p>Description</p> <p>EtiHint</p> <p>HP_OPR_SAAS_CUSTOMER_ID</p> <p>NoDuplicateSuppression</p> <p>RelatedCiHint</p> <p>SourceCiHint</p> <p>SourcedFromExternalId</p> <p>SourcedFromExternalUrl</p> <p>SubCategory</p> <p>SubCiHint</p>
Value	Value of the custom attribute.

Defaults Page

The Defaults page enables you to set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

For more details, see ["Event Attributes Tab" below](#), ["Event Correlation Tab" below](#), and ["Advanced Tab" on page 234](#).

Event Attributes Tab

Note: In the default event attributes, you can set only the Severity and Category attributes. You can set the other event attributes within individual rules.

UI Element	Description
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.
Send with closed status	Sets the event's lifecycle status to Closed before sending it to the Event Browser in Operations Management.

Event Correlation Tab






Note: In the default event attributes, you cannot set the following attributes:

- Close Events with Key
- Suppress Deduplication on Server

You can set these event attributes within individual rules.

UI Element	Description
Event Key	An identifier used to identify duplicates and for Close Events with Key.
Enable Event Suppression	<p>Enables event suppression for the events generated by this policy.</p> <p>If event suppression is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Event Suppression. Applies the event suppression settings configured in the event defaults to this rule.</p> <p>Override default settings for Event Suppression: Enables you to configure specific event suppression settings for this policy rule.</p>

Indicators Tab

UI Element	Description
	<p>Refresh. Loads the configured indicators from the BSM server.</p> <p>Note: Loading indicators from the BSM server may take a few seconds.</p>
	<p><i>Event integration policies only:</i> Shows or hides the Select drop target format drop-down panel:</p> <ul style="list-style-type: none"> • Use Indicator States. Click to change the drop target format to indicator states only. • Use Indicator Names and States. Click to change the drop target format to indicator names and states.
<Search ...>	<p>Entered search string is used to search the indicators and highlight only the indicators containing the specified string.</p> <p>To search for indicators with specific text strings in the name, type the string in the <Search ...> field and click the  button. The first matching indicator is selected in the list of rules. Click the  and  buttons to move to the previous and next matching indicator.</p>
<Indicators>	<p>Hierarchy of configuration item types with associated health indicators (HIs) and event type indicators (ETIs). To insert an indicator in a policy, drag and drop the indicator from the Indicators tab to the relevant field in the policy.</p>

Instructions Tab

UI Element	Description
Instructions	<p>Instructions that you want to accompany the event.</p> <p>Events generated by a policy can include instructions that explain what to do when the event is generated. This instruction text can often help an operator to solve a problem when a particular type of event is received. The operator can view the instructions included with an event by viewing the Event Details pane in the Event Browser. You can define default instructions for all rules in a policy. You can also override the default with different instructions for any rule.</p> <p>You can type URLs in the text, and the Event Browser automatically converts them into clickable hyperlinks. For example, you can add URLs of external Web sites, support sites, documentation repositories, troubleshooting information, and similar sites.</p> <p>To add a link, type any URL that begins with one of the following URI scheme names:</p> <ul style="list-style-type: none"> • <code>http://</code> • <code>https://</code> • <code>ftp://</code> • <code>ftps://</code>



Options Page

UI Element	Description
Log Local Events	<p>Defines 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:</p> <p>Windows: <code>%OvDataDir%\log\OpC\opcmsglg</code></p> <p>AIX, HP-UX, Linux, and Solaris: <code>/var/opt/OV/log/OpC/opcmsglg</code></p>
that match a rule and trigger an event	Logs any events in the event source that match the policy rules.
that match a rule and are ignored	Logs any events in the event source that are suppressed. (Suppressed events are not sent to the Event Browser.)
that do not match any rule	Logs any events that do not match any of the rules in the policy.



UI Element	Description
Unmatched Events	<p>Send an event to the 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.</p> <p>Each policy that sends unmatched events to the Event Browser creates an event with the default values of the policy.</p> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p> <p>Note: Nodes create an event about an unmatched event only if the input event is unmatched in all SNMP trap policies on the node. Nodes send only one event for each unmatched input event.</p>
are sent to the Event Browser	Sends unmatched events to the Event Browser.
are sent to the Closed Events Browser	Sends unmatched events to the Closed Events Browser.
are ignored	Ignores unmatched events.
Pattern Matching Options	Defines case sensitivity and field separators for all rules.
Case sensitive check	Defines whether the case (uppercase or lowercase) of a text string is considered when the pattern of a rule is compared with the source data. When switched on, a match only occurs if the use of uppercase and lowercase letters is exactly the same in both the source data and the pattern. This is the default setting.







UI Element	Description
Field Separators	<p>Defines 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:</p> <ul style="list-style-type: none"> • \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 (\) <p>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).</p> <p>If you leave this box empty, the default separators (a blank and the tab character) are used by default.</p> <p>You can set case sensitivity and separator characters for individual rules in a policy by clicking the ▶ button in rule's match condition.</p>
Apply to All	<p>Applies the pattern matching options to all existing rules in a policy. This overwrites any modifications made to the pattern matching options in individual rules.</p> <p>If you change the pattern matching options and do not click Apply to all, they only apply to all new rules in a policy.</p>

Policy Data Page


UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Check Syntax: Validates the syntax of the policy data. If the policy syntax is incorrect, the validation tool reports an error and points to the corresponding line and position of the unexpected token (for example the incorrect keyword).
<policy data>	Policy data in text form. The data uses the HP Operations Agent policy syntax.










Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.

UI Element	Description
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Policy Rules List

UI Element	Description
	<p><i>Event policies:</i> Create New Rule: Provides the following options:</p> <ul style="list-style-type: none"> Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM.

UI Element	Description
	Copy Rule. Copies the selected rule. You can then rewrite the description of the copied rule and edit the rule.
	Delete Rule. Deletes the selected rule.
	Move Up. Moves the selected rule higher in the rule order.
	Move Down. Moves the selected rule lower in the rule order.
<Move to>	Entered number is used to select the rule with that sequence number in the list of rules. To select a specific rule in the rule list, type the rule's sequence number in the <Move to> field and click the  button.
<Search rules>	Entered search string is used to search the rule descriptions and highlight only the rules containing the specified string. To search for rules with specific text strings in the rule description, type the string in the <Search rules> field and click the  button. The first matching rule is selected in the list of rules. Click the  and  buttons to move the previous and next matching rule.
	Activate/Deactivate Rule Filter. Activates and deactivates the rule filter.
Seq.	Sequence number of the rules. Rules are evaluated in a specific order. When one condition is matched, no additional rules are evaluated.
Rule Description	Description of the rule. It is good practice to use a description that helps you remember what the rule does
Rule Type	The three rule types of event policies are: <ul style="list-style-type: none"> • Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. • Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. • Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM. <p>The three rule types of metrics policies are:</p> <p>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.</p>

Policy Variables Tab

Variable	Description
<\$#>	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 <i>time_t</i> 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 <i>n</i> as <i>value</i> 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 <i>n</i> as <i>name:value</i> string. Sample output: .1.2 : asparagus.example.com
<\$+2>	Returns the <i>n</i> th variable binding as <i>name:value</i> . Sample output: .1.2 : artichoke.example.com
<\$\>-n >	Returns all attributes greater than <i>n</i> as [<i>seq</i>] <i>name (type): value</i> strings. Sample output: [2] .1.2 (OctetString): cauliflower.example.com
<\$-2>	Returns the <i>n</i> th variable binding as [<i>seq</i>] <i>name-type:value</i> . 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_ NODE>	Returns the IP address of the node on which the original event took place. Sample output: 192.168.1.123

Variable	Description
<\$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-event basis. For example, if the policy is receiving SNMP traps that originate from other devices, you might want to set this variable to the name of the device where the trap originated.
<\$MSG_ OBJECT>	Returns the name of the object associated with the event. This is set in the Event Defaults section of the policy editor.
<\$MSG_ TEXT>	Returns the full text of the event. Sample output: SU 03/19 16:13 + ttyp7 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
<\$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 an 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

Properties Page

UI Element	Description
Name	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.

¹(globally unique identifier)

UI Element	Description
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

Rules Page

The Rules page enables you to define one or more policy rules.

For more details, see "Policy Rules List" on page 243, "Condition Tab" on page 235, "Condition Variable Bindings Tab" on page 236, "Event Attributes Tab" on page 238, "Event Correlation Tab" on page 238, "Custom Attributes Tab" on page 237, "Advanced Tab" on page 234, and "Actions Tab" on page 232.


Configuring Windows Event Log Policies





Windows event log policies enable you to monitor Windows event logs for entries that match specific rules. You can configure policies to create events and launch commands whenever an event log entry matches one of your rules.




To access

You can create or edit a Windows event log policy using the Windows Event Log Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:




Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.

The Edit Aspect dialog box opens.
 - d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **Windows Event Log Template**, and then click **OK**.




- To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Windows Event Log Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:

Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **Windows Event Log Templates** folder, and then do one of the following:
 - To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New Windows Event Log Policy Editor opens.

- To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit Windows Event Log Policy Editor opens.

Tasks

How to Create a Windows Event Log Policy

1. In the Windows Event Log Policy Editor, in the Properties page, type a **Name** for the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "[Properties Page](#)" on page 263.

2. In the Source page, indicate which event log the policy reads and where the policy should begin to read the event log. You can also choose to receive an event if the event log is missing.


For more details, see "[Source Page](#)" on page 264.

3. *Optional.* In the Defaults page, set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

Note: You can set defaults for only a subset of event attributes. You can set the other event attributes within individual rules.

For more details, see "[Event Attributes Tab](#)" on page 256, "[Event Correlation Tab](#)" on page 257, "[Instructions Tab](#)" on page 258, and "[Advanced Tab](#)" on page 253.

4. In the Rules page, define one or more policy rules.

- a. In the Policy Rules list, click the  button, and then click one of the following options:
 - **Event on matched rule:** Use this option if you want to send an event to BSM when the conditions are met.
 - **Suppress on matched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are met.
 - **Suppress on unmatched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are *not* met.
- b. Click the **Rule Description** and type a brief description of the rule.

For more details, see ["Policy Rules List" on page 261](#).

5. In Rule Content, use the Condition tab to match an entry in the Windows event log that the policy monitors.

In text boxes, you can use policy variables, policy parameters, and pattern-matching.

For example, set these conditions to match an entry in the System event log reporting a problem with the BSM Connector service:

- **Source equals:** `Service Control Manager`
- **Type equals:** `Error / Critical`
- **Event ID equals:** `7016`
- **Description matches:** `<*>BSM Connector service has reported an invalid current state<*>`

For more details, see ["Condition Tab" on page 254](#) and ["Pattern Matching in Policy Rules" on page 357](#).

6. *Optional.* If you are creating a rule of the type 'event on matched rule', set attributes for events that you want the policy to send. You can override the default event attributes here. You can also write instructions that help operators handle the associated event and configure actions to solve problems automatically or manually.

In text boxes, you can use indicators, policy variables, and policy parameters.

For more details, see ["Event Attributes Tab" on page 256](#), ["Event Correlation Tab" on page 257](#), ["Custom Attributes Tab" on page 255](#), ["Instructions Tab" on page 258](#), ["Advanced Tab" on page 253](#), and ["Actions Tab" on the next page](#).

7. *Optional.* In the **Options** page, configure options for local event logs, unmatched events, and pattern matching.

For more details, see ["Options Page" on page 258](#).

8. Click **OK** to save the policy template.

UI Reference

This section includes:

- "Actions Tab" below
- "Advanced Tab" on page 253
- "Condition Tab" on page 254
- "Custom Attributes Tab" on page 255
- "Defaults Page" on page 256
- "Event Attributes Tab" on page 256
- "Event Correlation Tab" on page 257
- "Indicators Tab" on page 257
- "Instructions Tab" on page 258
- "Options Page" on page 258
- "Policy Data Page" on page 260
- "Policy Parameters Tab" on page 260
- "Policy Rules List" on page 261
- "Policy Variables Tab" on page 262
- "Properties Page" on page 263
- "Rules Page" on page 264
- "Source Page" on page 264

Actions Tab

UI Element	Description
Automatic command	Automatic command that runs when the rule is matched.
Command	Command and parameters to run when the command is started for this event. The command runs on the node you specify in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information on <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.

UI Element	Description
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.
Send event immediately	Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.
Wait until local command completes and then	Options that can help to reduce the amount of unnecessary network traffic to the BSM server. For example, if an automatic command solves the problem that generated the event, you may choose not to inform the BSM server. <ul style="list-style-type: none"> • Send the event • Send the event if the local command fails • Send the event only if the local command is successful
Operator-initiated command	Operator-initiated command that is attached to the event that the rule sends to the Event Browser. This command can be started by the BSM user from the Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.
Command	Command and parameters to run when the command is started for this event. The command runs on the node specified in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information about <code>cmd</code> .

UI Element	Description
Non Agent User	<p>By default, the command runs as the agent user (\$AGENT_USER). Alternatively, select Non Agent User and specify a user account and password that exists on the node:</p> <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.

Advanced Tab

Note: In the default event attributes, you cannot set the Event Drilldown URL attribute. You can set this event attribute within individual rules.

UI Element	Description
Application	Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM, 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 RTSM, the object attribute is a simple string-type attribute (for example, C:, and /dev/spool).
HPOM Service ID	ID of the service associated with 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.



UI Element	Description
Enable Agent MSI	<p>The message stream interface (MSI) allows external applications to interact with the internal event flow of HP Operations Agent. The external application can be a read-write application, for example, an event processing program that can read events, modify attributes, and generate new events for retransmission to the server. The application could also read events, or send its own events.</p> <p>Divert events. Divert an event to the MSI instead of to the server when an event is requested by an external application.</p> <p>Copy events. Send the event to the server, and a copy of the event to the MSI.</p> <p>If the agent MSI is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Agent MSI. Applies the agent MSI settings configured in the event defaults to this rule.</p> <p>Override default settings for Agent MSI: Enables you to configure specific agent MSI settings for this policy rule.</p>

Condition Tab

UI Element	Description
Computer equals	<p>The name of the computer where the event occurred. Type a value in this field to match the event log entry from a specific node.</p> <p>Separate multiple entries with the OR operator () or leave blank to match all nodes.</p> <p>Example: celery.example.com broccoli.example.com</p>
Source equals	<p>The source of the event, for example Application, Security, or System.</p> <p>Tip: You can use pattern matching in the Source field, but you must first enable this on the nodes that you want to use it on. To enable pattern matching in the Source field, set the agent parameter <code>OPC_COND_EVT_LOG_SRC_PAT</code> in the <code>eaagt</code> namespace to <code>TRUE</code>.</p>
Category equals	A classification of the event by the event source.

UI Element	Description
Type equals	<p>The type of event:</p> <ul style="list-style-type: none"> • Application, System, and other event logs: <ul style="list-style-type: none"> ▪ Information / Success Audit ▪ Warning / Failure Audit ▪ Error / Critical • Security event log: <ul style="list-style-type: none"> ▪ Failure Audit ▪ Success Audit
Event ID equals	<p>An event number that identifies the event type.</p> <p>Format: decimal, hexadecimal</p>
Description matches	<p>The description of the event.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p>Note: The match pattern may not contain newline characters. If you need to match a multi-line pattern, use the special character <*> to match any carriage return/linefeed characters.</p> </div> <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p>Tip: You can use standard HP Operations Agent pattern-matching rules when matching values. Click ▶ to open the pattern matching expression toolbox. The toolbox displays the following:</p> <ul style="list-style-type: none"> • Pattern Matching Expressions. Click an expression to insert it in the pattern. • Variable Bindings Options. Variable bindings options include 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. </div>

Custom Attributes Tab

UI Element	Description
	Create New Custom Attribute: Creates a new custom attribute with the default name CA_n. To rename the custom attribute, double-click the name to select it and type the new name.
	Delete Custom Attribute: Deletes an existing custom attribute.

UI	
Element	Description
Name	<p>The name of the custom attribute. The name is case-insensitive.</p> <p>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.</p> <p>The following custom attribute names cannot be used because they are reserved for internal use:</p> <p>Description</p> <p>EtiHint</p> <p>HP_OPR_SAAS_CUSTOMER_ID</p> <p>NoDuplicateSuppression</p> <p>RelatedCiHint</p> <p>SourceCiHint</p> <p>SourcedFromExternalId</p> <p>SourcedFromExternalUrl</p> <p>SubCategory</p> <p>SubCiHint</p>
Value	Value of the custom attribute.

Defaults Page

The Defaults page enables you to set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

For more details, see ["Event Attributes Tab"](#) below, ["Event Correlation Tab"](#) on the next page, ["Instructions Tab"](#) on page 258, and ["Advanced Tab"](#) on page 253.

Event Attributes Tab

Note: In the default event attributes, you can set only the Severity, Category, and Node attributes. You can set the other event attributes within individual rules.

UI	
Element	Description
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.

UI Element	Description
Send with closed status	Sets the event's lifecycle status to Closed before sending it to the Event Browser in Operations Management.

Event Correlation Tab



Note: In the default event attributes, you cannot set the following attributes:




- Close Events with Key
- Suppress Deduplication on Server

You can set these event attributes within individual rules.

UI Element	Description
Event Key	An identifier used to identify duplicates and for Close Events with Key.
Enable Event Suppression	<p>Enables event suppression for the events generated by this policy.</p> <p>If event suppression is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Event Suppression. Applies the event suppression settings configured in the event defaults to this rule.</p> <p>Override default settings for Event Suppression: Enables you to configure specific event suppression settings for this policy rule.</p>

Indicators Tab

UI Element	Description
	<p>Refresh. Loads the configured indicators from the BSM server.</p> <p>Note: Loading indicators from the BSM server may take a few seconds.</p>
	<p>Shows or hides the Select drop target format drop-down panel:</p> <ul style="list-style-type: none"> • Use Indicator States. Click to change the drop target format to indicator states only. • Use Indicator Names and States. Click to change the drop target format to indicator names and states.

UI Element	Description
<Search ...>	<p>Entered search string is used to search the indicators and highlight only the indicators containing the specified string.</p> <p>To search for indicators with specific text strings in the name, type the string in the <Search ...> field and click the  button. The first matching indicator is selected in the list of rules. Click the  and  buttons to move to the previous and next matching indicator.</p>
<Indicators>	<p>Hierarchy of configuration item types with associated health indicators (HIs) and event type indicators (ETIs). To insert an indicator in a policy, drag and drop the indicator from the Indicators tab to the relevant field in the policy.</p>

Instructions Tab

UI Element	Description
Instructions	<p>Instructions that you want to accompany the event.</p> <p>Events generated by a policy can include instructions that explain what to do when the event is generated. This instruction text can often help an operator to solve a problem when a particular type of event is received. The operator can view the instructions included with an event by viewing the Event Details pane in the Event Browser. You can define default instructions for all rules in a policy. You can also override the default with different instructions for any rule.</p> <p>You can type URLs in the text, and the Event Browser automatically converts them into clickable hyperlinks. For example, you can add URLs of external Web sites, support sites, documentation repositories, troubleshooting information, and similar sites.</p> <p>To add a link, type any URL that begins with one of the following URI scheme names:</p> <ul style="list-style-type: none"> • http:// • https:// • ftp:// • ftps://



Options Page

UI Element	Description
Log Local Events	<p>Defines 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:</p> <p>Windows: %OvDataDir%\log\OpC\opcmsglg</p> <p>AIX, HP-UX, Linux, and Solaris: /var/opt/OV/log/OpC/opcmsglg</p>



UI Element	Description
that match a rule and trigger an event	Logs any events in the event source that match the policy rules.
that match a rule and are ignored	Logs any events in the event source that are suppressed. (Suppressed events are not sent to the Event Browser.)
that do not match any rule	Logs any events that do not match any of the rules in the policy.
Unmatched Events	<p>Send an event to the 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.</p> <p>Each policy that sends unmatched events to the Event Browser creates an event with the default values of the policy.</p> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p>
are sent to the Event Browser	Sends unmatched events to the Event Browser.
are sent to the Closed Events Browser	Sends unmatched events to the Closed Events Browser.
are ignored	Ignores unmatched events.
Pattern Matching Options	Defines case sensitivity and field separators for all rules.
Case sensitive check	Defines whether the case (uppercase or lowercase) of a text string is considered when the pattern of a rule is compared with the source data. When switched on, a match only occurs if the use of uppercase and lowercase letters is exactly the same in both the source data and the pattern. This is the default setting.







UI Element	Description
Field Separators	<p>Defines 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:</p> <ul style="list-style-type: none"> • \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 (\) <p>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).</p> <p>If you leave this box empty, the default separators (a blank and the tab character) are used by default.</p> <p>You can set case sensitivity and separator characters for individual rules in a policy by clicking the ▶ button in rule's match condition.</p>
Apply to All	<p>Applies the pattern matching options to all existing rules in a policy. This overwrites any modifications made to the pattern matching options in individual rules.</p> <p>If you change the pattern matching options and do not click Apply to all, they only apply to all new rules in a policy.</p>

Policy Data Page


UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Check Syntax: Validates the syntax of the policy data. If the policy syntax is incorrect, the validation tool reports an error and points to the corresponding line and position of the unexpected token (for example the incorrect keyword).
<policy data>	Policy data in text form. The data uses the HP Operations Agent policy syntax.










Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.

UI Element	Description
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Policy Rules List

UI Element	Description
	<p>Create New Rule: Provides the following options:</p> <ul style="list-style-type: none"> Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM.

UI Element	Description
	Copy Rule. Copies the selected rule. You can then rewrite the description of the copied rule and edit the rule.
	Delete Rule. Deletes the selected rule.
	Move Up. Moves the selected rule higher in the rule order.
	Move Down. Moves the selected rule lower in the rule order.
<Move to>	Entered number is used to select the rule with that sequence number in the list of rules. To select a specific rule in the rule list, type the rule's sequence number in the <Move to> field and click the  button.
<Search rules>	Entered search string is used to search the rule descriptions and highlight only the rules containing the specified string. To search for rules with specific text strings in the rule description, type the string in the <Search rules> field and click the  button. The first matching rule is selected in the list of rules. Click the  and  buttons to move the previous and next matching rule.
	Activate/Deactivate Rule Filter. Activates and deactivates the rule filter.
Seq.	Sequence number of the rules. Rules are evaluated in a specific order. When one condition is matched, no additional rules are evaluated.
Rule Description	Description of the rule. It is good practice to use a description that helps you remember what the rule does
Rule Type	<ul style="list-style-type: none"> • Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. • Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. • Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM. <p>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.</p>

Policy Variables Tab

You can use the following variables in Windows event log policies. If a variable returns values that contain spaces, surround the variable with quotation marks.

Variable	Description
<\$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-event basis.
<\$MSG_TEXT>	Returns the full text of the event. For the Windows Event Log this value is the event ID and description. Sample output: SU 03/19 16:13 + ttyp7 bill-root

Properties Page

UI Element	Description
Name	Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed. The name is set when the policy is created and cannot be changed in new versions of a policy.
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.
Version	The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy. Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.
Change Log	Text that describes what is new or modified in this version of the policy.

¹(globally unique identifier)

UI Element	Description
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

Rules Page

The Rules page enables you to define one or more policy rules.

For more details, see ["Policy Rules List" on page 261](#), ["Condition Tab" on page 254](#), ["Event Attributes Tab" on page 256](#), ["Event Correlation Tab" on page 257](#), ["Custom Attributes Tab" on page 255](#), ["Advanced Tab" on page 253](#), and ["Actions Tab" on page 251](#).

Source Page

UI Element	Description
Event log name	Windows produces several event logs. You can choose which event log you want a policy to monitor. If you want to monitor more than one event log, you need more than one policy.

Send event if log file does not exist	The agent sends an event if for some reason the event log is missing. Default value: not selected
--	--


<p>Read Mode</p>	<p>The read mode of an event log policy indicates whether the policy processes the entire event log or only new entries.</p>	
	<p>Read from last position. The policy reads only new—appended—entries written in the Event Log while the policy is enabled on the managed node. If the Event Log decreases in size between readings, then the entire Event Log is read. Event Log entries that are added to the Event Log when the policy is disabled are not processed by the policy. If the agent stops, all entries written to the monitored Event Log while the agent is not running will be processed after the agent restarts.</p> <p>Choose this option if you are concerned only with Event Log entries that occur when the policy is enabled.</p>	<p>Advantage: No chance of reading the same entry twice. (Unless the Event Log decreases in size because some entries were deleted.)</p> <p>Disadvantage: Entries written to the Event Log while the policy is disabled will not be processed by the policy.</p>
	<p>Read from beginning (first time). The policy reads the complete event log each time the policy is enabled or the agent restarts. This ensures that all entries in the file are compared with the rules in the policy. Each successive time that the policy reads the file, only new (appended) entries in the file are processed.</p> <p>Choose this option if you want to ensure that every existing and future entry in the file is processed by the policy while it is enabled.</p>	<p>Advantage: Every existing and future entry in the file will be processed by the policy.</p> <p>Disadvantage: Duplicate entries can occur if an enabled policy is disabled and re-enabled, or if the agent stops and restarts.</p>
<p>Note: Every policy reads the same event log independently from any other policies. This means, for example, that if "Policy 1" with read mode Read from beginning (first time) is enabled and "Policy 2" with the same read mode already exists, "Policy 1" still reads the entire file after it has been enabled.</p> <p>Default value: Read from last position</p>		

Configuring Windows Management Interface Policies








Windows Management Interface (WMI) policies enable you to monitor the properties of WMI classes and instances. You can configure policies to create events and launch commands whenever a WMI property matches a value you specify, or when a WMI instance you specify is created, modified, or deleted.

To access

You can create or edit a Window Management Interface policy using the Window Management Interface Policy Editor, which you can open in the following ways.




- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:
Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.

The Edit Aspect dialog box opens.




- d. Click the **Policy Templates** tab, and then do one of the following:
 - To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **Windows Management Interface Templates**, and then click **OK**.
 - To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Windows Management Interface Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:
Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **Windows Management Interface Templates** folder, and then do one of the following:

- To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New Windows Management Interface Policy Editor opens.

- To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit Windows Management Interface Policy Editor opens.

Learn More

This section includes:

- ["Information in WMI" below](#)
- ["WMI Instances and Events" below](#)

Information in WMI

WMI contains a very large amount of information about the configuration of Windows, and about the configuration of other programs that write information to WMI namespaces. In order to write a useful WMI policy, you need to gain an understanding of the kinds of information that are available in WMI.

The information provided by WMI is divided into namespaces. The default namespaces provided by WMI are `Root`, `Root\Default`, `Root\Security` and `Root\CimV2`. Other applications may add other namespaces.

Namespace `Root\CimV2` is one of the most interesting namespaces, as it contains a large amount of information about the Windows operating system, and about hardware installed on the computer. The classes that are most useful are prefixed with `Win32_`, for example, `Win32_Service`, `Win32_Desktop`, `Win32_Share`, `Win32_PhysicalDisk` and so on. A good way to become acquainted with the information is to use a tool like `wbemtest` to examine the contents of the classes.

WMI Instances and Events

An instance is static information that is written to the WMI repository. This information remains in the repository until it is changed or deleted.

WMI events contain information that briefly appears in the WMI repository. This information is transitory, and never remains in the repository. Some events are defined by WMI by default, and are known as **intrinsic events**. Intrinsic events include the creation, modification, or deletion of an instance, class, or namespace. Other events, known as **extrinsic events**, are only available to a WMI policy if the namespace designer has defined them. In both cases, the event is only available to the WMI policy if the namespace designer has written a provider for the event, although intrinsic events can be simulated by the WMI policy by using a polling interval.

Tasks

How to Create a Windows Management Interface Policy

1. In the Windows Management Interface Policy Editor, in the Properties page, type a **Name** for

the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "[Properties Page](#)" on page 283.

2. In the Source page, choose the instance or event that you want the WMI policy to monitor:
 - a. *Optional.* Type the **Node** that hosts the WMI database that you want to monitor. If you do not specify a node, the policy monitors the WMI database of the node that has this policy deployed.
 - b. Type the **WMI namespace** that contains the data that you want to manage, for example `Root\CimV2`.
 - c. As **Object type**, choose **Event** or **Instance**.
 - d. Type the **Event/Instance class name** that contains the event that you want to monitor, for example `Win32_Service`.
 - e. *Optional.* If you want to access the WMI database using an account other than the default agent account, click **Non Agent User** and provide the user name and password of a user with local administrator privileges.
 - f. Define how the policy queries the event or instance:
 - If you are monitoring an event for which a provider is defined, you do not need to enter any information in **Type of query**.
 - If you are monitoring an intrinsic event for which no provider is defined, then you need to specify a polling interval in **Type of query**.
 - Select **Query instances of class** if you want to match specific values contained within the class. You must indicate the polling interval to indicate the frequency with which the WMI policy checks the instances you selected.
 - Alternatively, select **Query the intrinsic event for these instances** if you want to check for the creation, modification or deletion of the instance, the class that contains the instance, or the namespace that contains the instance. If there is no provider for the event, you must also set the **Polling interval** to indicate the frequency with which the Windows Management Interface policy will check the object you selected. (This results a Wbem Query Language **within** clause.)
 - g. *Optional.* Click **Use global WQL filter** to define a global filter that is applied to the instance or event before the policy begins to evaluate it. Events or instances that do not get through the filter are not evaluated by the policy.

Use the syntax *PROPERTY OPERATOR VALUE*; for example, `StartMode = "Auto"` filters all instances that have the property `StartMode` set to `Auto`.

If the global filter filters intrinsic events, the syntax is one of the following:


- `TargetInstance.PROPERTY OPERATOR VALUE`
- `TargetClass.PROPERTY OPERATOR VALUE`
- `TargetNamespace.PROPERTY OPERATOR VALUE`

For example, `TargetInstance ISA "ds_domaindns"`

3. *Optional.* In the Defaults page, set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

Note: You can set defaults for only a subset of event attributes. You can set the other event attributes within individual rules.

For more details, see ["Event Attributes Tab" on page 276](#), ["Event Correlation Tab" on page 277](#), ["Instructions Tab" on page 278](#), and ["Advanced Tab" on page 273](#).

4. In the Rules page, define one or more policy rules.
 - a. In the Policy Rules list, click the  button, and then click one of the following options:
 - o **Event on matched rule:** Use this option if you want to send an event to BSM when the conditions are met.
 - o **Suppress on matched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are met.
 - o **Suppress on unmatched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are *not* met.
 - b. Click the **Rule Description** and type a brief description of the rule.

For more details, see ["Policy Rules List" on page 281](#).

5. In Rule Content, use the Condition tab to specify conditions for a WMI policy rule. Conditions are sets of WMI instance or event properties, along with values that these properties must have in order for a match to be successful.

In text boxes, you can use policy variables, policy parameters, and pattern-matching.

For example, the following condition checks whether a service (an instance of the class `Win32_Service` in the namespace `Root\CimV2`) is in the state "Stopped":

- **Property name:** `State`
- **Operator:** `equals`
- **Operand:** `Stopped`

For more details, see ["Condition Tab" on page 274](#) and ["Pattern Matching in Policy Rules" on page 357](#).

6. *Optional.* If you are creating a rule of the type 'event on matched rule', set attributes for events that you want the policy to send. You can override the default event attributes here. You can also write instructions that help operators handle the associated event and configure actions to solve problems automatically or manually.

In text boxes, you can use indicators, policy variables, and policy parameters.

For more details, see ["Event Attributes Tab" on page 276](#), ["Event Correlation Tab" on page 277](#), ["Custom Attributes Tab" on page 275](#), ["Instructions Tab" on page 278](#), ["Advanced Tab" on page 273](#), and ["Actions Tab" on the next page](#).

7. *Optional.* In the **Options** page, configure options for local event logs, unmatched events, and pattern matching.

For more details, see ["Options Page" on page 278](#).

8. Click **OK** to save the policy template.

UI Reference

This section includes:

- "Actions Tab" below
- "Advanced Tab" on page 273
- "Condition Tab" on page 274
- "Custom Attributes Tab" on page 275
- "Defaults Page" on page 276
- "Event Attributes Tab" on page 276
- "Event Correlation Tab" on page 277
- "Indicators Tab" on page 277
- "Instructions Tab" on page 278
- "Options Page" on page 278
- "Policy Data Page" on page 280
- "Policy Parameters Tab" on page 280
- "Policy Rules List" on page 281
- "Policy Variables Tab" on page 282
- "Properties Page" on page 283
- "Rules Page" on page 284
- "Source Page" on page 284

Actions Tab

UI Element	Description
Automatic command	Automatic command that runs when the rule is matched.
Command	Command and parameters to run when the command is started for this event. The command runs on the node you specify in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information on <code>cmd</code> .

UI Element	Description
Non Agent User	<p>By default, the command runs as the agent user (\$AGENT_USER). Alternatively, select Non Agent User and specify a user account and password that exists on the node:</p> <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.
Send event immediately	Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.
Wait until local command completes and then	<p>Options that can help to reduce the amount of unnecessary network traffic to the BSM server. For example, if an automatic command solves the problem that generated the event, you may choose not to inform the BSM server.</p> <ul style="list-style-type: none"> • Send the event • Send the event if the local command fails • Send the event only if the local command is successful
Operator-initiated command	Operator-initiated command that is attached to the event that the rule sends to the Event Browser. This command can be started by the BSM user from the Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.









UI Element	Description
Command	Command and parameters to run when the command is started for this event. The command runs on the node specified in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information about <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.

Advanced Tab

UI Element	Description
Application	Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM, 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 RTSM, the object attribute is a simple string-type attribute (for example, C:, and /dev/spool).



UI Element	Description
HPOM Service ID	ID of the service associated with 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.
Enable Agent MSI	<p>The message stream interface (MSI) allows external applications to interact with the internal event flow of HP Operations Agent. The external application can be a read-write application, for example, an event processing program that can read events, modify attributes, and generate new events for retransmission to the server. The application could also read events, or send its own events.</p> <p>Divert events. Divert an event to the MSI instead of to the server when an event is requested by an external application.</p> <p>Copy events. Send the event to the server, and a copy of the event to the MSI.</p> <p>If the agent MSI is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Agent MSI. Applies the agent MSI settings configured in the event defaults to this rule.</p> <p>Override default settings for Agent MSI: Enables you to configure specific agent MSI settings for this policy rule.</p>

Condition Tab

UI Element	Description
	New Item. Creates a new condition with the default operator equals.
	Delete Item. Deletes the selected condition.
	Move Up. Moves the selected condition higher in the condition order.
	Move Down. Moves the selected condition lower in the condition order.
	Expand. Expands the list of conditions to display all details.
	Collapse. Collapses the list of conditions to display only the names and hide the details.
	Click to expand the details of a condition.
	Click to hide the details of a condition.
Property	The name of the property that you want the rule to inspect. Properties must begin with a letter.

UI Element	Description
Operator	<p>The following operators are available:</p> <ul style="list-style-type: none"> • equals • not equals • less than • greater than • less or equal • greater or equal • matches (Enables you to enter a pattern in the Operand field.)
Operand	<p>The value (or property) that you want to compare. This is the value or property that will be compared—using the comparison operator you selected—against the property specified in Property. Properties must begin with a letter.</p> <p>Tip: You can use standard HP Operations Agent pattern-matching rules when matching values. Select the matches operator and click ► in the Operand field to open the pattern matching expression toolbox. The toolbox displays the following:</p> <ul style="list-style-type: none"> • Pattern Matching Expressions. Click an expression to insert it in the Operand field. • Variable Bindings Options. Variable bindings options include 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.

Custom Attributes Tab

UI Element	Description
	Create New Custom Attribute: Creates a new custom attribute with the default name CA_ <i>n</i> . To rename the custom attribute, double-click the name to select it and type the new name.
	Delete Custom Attribute: Deletes an existing custom attribute.

UI	
Element	Description
Name	<p>The name of the custom attribute. The name is case-insensitive.</p> <p>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.</p> <p>The following custom attribute names cannot be used because they are reserved for internal use:</p> <p>Description</p> <p>EtiHint</p> <p>HP_OPR_SAAS_CUSTOMER_ID</p> <p>NoDuplicateSuppression</p> <p>RelatedCiHint</p> <p>SourceCiHint</p> <p>SourcedFromExternalId</p> <p>SourcedFromExternalUrl</p> <p>SubCategory</p> <p>SubCiHint</p>
Value	Value of the custom attribute.

Defaults Page

The Defaults page enables you to set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

For more details, see ["Event Attributes Tab"](#) below, ["Event Correlation Tab"](#) on the next page, ["Instructions Tab"](#) on page 278, and ["Advanced Tab"](#) on page 273.






Event Attributes Tab

UI	
Element	Description
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.
Send with closed status	Sets the event's lifecycle status to Closed before sending it to the Event Browser in Operations Management.

Event Correlation Tab

UI Element	Description
Event Key	An identifier used to identify duplicates and for Close Events with Key.
Enable Event Suppression	<p>Enables event suppression for the events generated by this policy.</p> <p>If event suppression is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Event Suppression. Applies the event suppression settings configured in the event defaults to this rule.</p> <p>Override default settings for Event Suppression: Enables you to configure specific event suppression settings for this policy rule.</p>

Indicators Tab

UI Element	Description
	<p>Refresh. Loads the configured indicators from the BSM server.</p> <p>Note: Loading indicators from the BSM server may take a few seconds.</p>
	<p>Shows or hides the Select drop target format drop-down panel:</p> <ul style="list-style-type: none"> • Use Indicator States. Click to change the drop target format to indicator states only. • Use Indicator Names and States. Click to change the drop target format to indicator names and states.
<Search ...>	<p>Entered search string is used to search the indicators and highlight only the indicators containing the specified string.</p> <p>To search for indicators with specific text strings in the name, type the string in the <Search ...> field and click the  button. The first matching indicator is selected in the list of rules. Click the  and  buttons to move to the previous and next matching indicator.</p>
<Indicators>	<p>Hierarchy of configuration item types with associated health indicators (HIs) and event type indicators (ETIs). To insert an indicator in a policy, drag and drop the indicator from the Indicators tab to the relevant field in the policy.</p>

Instructions Tab

UI Element	Description
Instructions	<p>Instructions that you want to accompany the event.</p> <p>Events generated by a policy can include instructions that explain what to do when the event is generated. This instruction text can often help an operator to solve a problem when a particular type of event is received. The operator can view the instructions included with an event by viewing the Event Details pane in the Event Browser. You can define default instructions for all rules in a policy. You can also override the default with different instructions for any rule.</p> <p>You can type URLs in the text, and the Event Browser automatically converts them into clickable hyperlinks. For example, you can add URLs of external Web sites, support sites, documentation repositories, troubleshooting information, and similar sites.</p> <p>To add a link, type any URL that begins with one of the following URI scheme names:</p> <ul style="list-style-type: none"> • <code>http://</code> • <code>https://</code> • <code>ftp://</code> • <code>ftps://</code>



Options Page

UI Element	Description
Log Local Events	<p>Defines 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:</p> <p>Windows: <code>%OvDataDir%\log\OpC\opcmsglg</code></p> <p>AIX, HP-UX, Linux, and Solaris: <code>/var/opt/OV/log/OpC/opcmsglg</code></p>
that match a rule and trigger an event	Logs any events in the event source that match the policy rules.
that match a rule and are ignored	Logs any events in the event source that are suppressed. (Suppressed events are not sent to the Event Browser.)
that do not match any rule	Logs any events that do not match any of the rules in the policy.



UI Element	Description
Unmatched Events	<p>Send an event to the 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.</p> <p>Each policy that sends unmatched events to the Event Browser creates an event with the default values of the policy.</p> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p>
are sent to the Event Browser	Sends unmatched events to the Event Browser.
are sent to the Closed Events Browser	Sends unmatched events to the Closed Events Browser.
are ignored	Ignores unmatched events.
Pattern Matching Options	Defines case sensitivity and field separators for all rules.
Case sensitive check	Defines whether the case (uppercase or lowercase) of a text string is considered when the pattern of a rule is compared with the source data. When switched on, a match only occurs if the use of uppercase and lowercase letters is exactly the same in both the source data and the pattern. This is the default setting.







UI Element	Description
Field Separators	<p>Defines 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:</p> <ul style="list-style-type: none"> • \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 (\) <p>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).</p> <p>If you leave this box empty, the default separators (a blank and the tab character) are used by default.</p> <p>You can set case sensitivity and separator characters for individual rules in a policy by clicking the ▶ button in rule's match condition.</p>
Apply to All	<p>Applies the pattern matching options to all existing rules in a policy. This overwrites any modifications made to the pattern matching options in individual rules.</p> <p>If you change the pattern matching options and do not click Apply to all, they only apply to all new rules in a policy.</p>

Policy Data Page


UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Check Syntax: Validates the syntax of the policy data. If the policy syntax is incorrect, the validation tool reports an error and points to the corresponding line and position of the unexpected token (for example the incorrect keyword).
<policy data>	Policy data in text form.










Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.

UI Element	Description
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Policy Rules List

UI Element	Description
	<p>Create New Rule: Provides the following options:</p> <ul style="list-style-type: none"> Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM.

UI Element	Description
	Copy Rule. Copies the selected rule. You can then rewrite the description of the copied rule and edit the rule.
	Delete Rule. Deletes the selected rule.
	Move Up. Moves the selected rule higher in the rule order.
	Move Down. Moves the selected rule lower in the rule order.
<Move to>	Entered number is used to select the rule with that sequence number in the list of rules. To select a specific rule in the rule list, type the rule's sequence number in the <Move to> field and click the  button.
<Search rules>	Entered search string is used to search the rule descriptions and highlight only the rules containing the specified string. To search for rules with specific text strings in the rule description, type the string in the <Search rules> field and click the  button. The first matching rule is selected in the list of rules. Click the  and  buttons to move the previous and next matching rule.
	Activate/Deactivate Rule Filter. Activates and deactivates the rule filter.
Seq.	Sequence number of the rules. Rules are evaluated in a specific order. When one condition is matched, no additional rules are evaluated.
Rule Description	Description of the rule. It is good practice to use a description that helps you remember what the rule does
Rule Type	<ul style="list-style-type: none"> • Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. • Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. • Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM. <p>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.</p>

Policy Variables Tab

You can use the following variables in Windows event log policies. If a variable returns values that contain spaces, surround the variable with quotation marks.

Variable	Description
<\$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-event basis.
<\$MSG_TEXT>	Returns the full text of the event. Sample output: SU 03/19 16:13 + ttyp7 bill-root
<\$WBEM:WMI class property>	Returns the value of the WMI property specified in the variable (for example, <\$WBEM:TimeCreated>). Sample output: 19991130105330.000000+060)

Properties Page

UI Element	Description
Name	Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed. The name is set when the policy is created and cannot be changed in new versions of a policy.
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.
Version	The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy. Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.
Change Log	Text that describes what is new or modified in this version of the policy.

¹(globally unique identifier)

UI Element	Description
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

Rules Page

The Rules page enables you to define one or more policy rules.

For more details, see ["Policy Rules List" on page 281](#), ["Condition Tab" on page 274](#), ["Event Attributes Tab" on page 276](#), ["Event Correlation Tab" on page 277](#), ["Custom Attributes Tab" on page 275](#), ["Advanced Tab" on page 273](#), and ["Actions Tab" on page 271](#).

Source Page

UI Element	Description
Node	The node that hosts the WMI database that you want to monitor. This can be an agentless node. If you do not specify a node, the policy monitors the WMI database of the node that has this policy deployed.
WMI Namespace	The namespace that contains the data that you want to manage.

Object type	<p>Choose one of the following:</p> <ul style="list-style-type: none"> • Instance. Static information written to the WMI repository. This information remains in the repository until it is changed or deleted. • Event. Information that briefly appears in the WMI repository. This information is transitory, and never remains in the repository. Some events are defined by WMI by default, and are known as intrinsic events. Intrinsic events include the creation, modification, or deletion of an instance, class, or namespace. Other events, known as extrinsic events, are only available to a WMI policy if the namespace designer has defined them. In both cases, the event is only available to the WMI policy if the namespace designer has written a provider for the event, although intrinsic events can be simulated by the WMI policy by using a polling interval.
Event or Instance class name	<p>The class that contains the event or instance that you want to monitor. (A class is a collection of data properties that is defined for information that will be stored in the WMI repository.)</p>
Non Agent User	<p>If selected, the agent accesses the node's WMI database using the following account information. This account must exist on the agentless node and must have local administrator privileges. If not selected, the agent account is used.</p> <ul style="list-style-type: none"> • Username. User name of the account that the agent will use to connect to the WMI database. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Type of query	<p>The type of query depends on the object type that you are monitoring: Event or Instance.</p>
Query event	<p>If you are monitoring an event for which a provider is defined, then you do not need to enter any information here. If you are monitoring an intrinsic event for which no provider is defined, then you need to specify a polling interval.</p>
Query instance of class	<p>Select Query instances of class if you want to match specific values contained within the class. You must indicate the polling interval to indicate the frequency with which the WMI policy checks the instances you selected.</p>
Query the intrinsic event for these instances	<p>Select Query the intrinsic event for these instances if you want to check for the creation, modification or deletion of the instance, the class that contains the instance, or the namespace that contains the instance. If there is no provider for the event, you must also set the Polling interval to indicate the frequency with which the Windows Management Interface policy will check the object you selected. (This results a WBEM Query Language within clause.)</p>

<p>Use global WQL filter</p>	<p>A global filter can be described as a rule. It is a test that is applied to the instance or event before the policy begins to evaluate it. A global filter can improve performance, because events or instances that do not get through the filter are not evaluated by the policy. (The global filter is a WBEM Query Language where clause.)</p> <p>Sample global filters</p> <p>The syntax of a global filter has three parts:</p> <p><i>PROPERTY OPERATOR VALUE</i></p> <p>for example: <code>_PATH = "C:/program files"</code></p> <p>If the global filter filters intrinsic events, the syntax is somewhat different:</p> <p><code>TargetInstance.PROPERTY OPERATOR VALUE</code> or <code>TargetClass.PROPERTY OPERATOR VALUE</code> or <code>TargetNamespace.PROPERTY OPERATOR VALUE</code></p> <p>for example,</p> <pre>TargetInstance.InteractWithDeskTop = 1 TargetNamespace.name = "CIMV2"</pre>
-------------------------------------	--


Configuring XML File Policies








XML file policies enable you to monitor XML files for elements and attributes that match specific rules. Each rule consists of a condition definition, and optionally an event definition. When the XML file contains elements or attributes that match your conditions, you can create an event.

To access

You can create or edit an XML file policy using the XML File Policy Editor, which you can open in the following ways.




- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:

Admin > Operations Management > Monitoring > Management Templates & Aspects
 - b. In the Configuration Folders pane, expand the configuration folders.
 - c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.
The Edit Aspect dialog box opens.
 - d. Click the **Policy Templates** tab, and then do one of the following:




- To add a new policy template:
 - Click the  button. The Add Policy Template to Aspect dialog box opens.
 - Click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button. The Select Type for New Policy Template dialog box opens.
 - Select the type **XML File Template**, and then click **OK**.
- To edit an existing policy template, click the policy template in the list, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The XML Policy Editor opens.

- To open the editor from the Policy Templates manager:
 - a. Open the Policy Templates manager:

Admin > Operations Management > Monitoring > Policy Templates
 - b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.
 - c. Click the **XML File Templates** folder, and then do one of the following:
 - To add a new policy template, in the Policy Templates pane, click the  button, and then click the  **Add New Policy Template** or the  **Add New Policy Template (Raw Mode)** button.

The New XML File Policy Editor opens.

- To edit an existing policy template, click the policy template in the Policy Templates pane, click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit XML File Policy Editor opens.

Learn More

This section includes:

- ["Requirements for XML source files" below](#)
- ["Mappings overview" on the next page](#)

Requirements for XML source files

XML files must meet the following criteria so that they can be processed correctly by XML file 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 file policies, only those events are processed by XML file policies.

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

Mappings overview

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 HP Operations Agent 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.

Default Value Mapping

* ✖		* ✖	
Map Name	Input Data Property	Source Value	Target Value
mapSeverity	<\$DATA:/PerformanceAlert/Severity>	serious	critical
		not so serious	warning

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 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.

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, the editor 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.

Tasks



How to Create an XML File Policy

1. In the XM File Policy Editor, in the Properties page, type a **Name** for the policy.

You can also type a **Description** of the policy, select the **Instrumentation** that will be deployed with the policy, and select the **OS Types** with which this policy is compatible.

For more details, see "Properties Page" on page 305.

2. In the Source page, define the XML file that the policy reads (for example, the path and name of the XML file).

- a. In **Log File Path / Name**, type the full path to the XML file on nodes.
- b. Click **Logfile Character Set** and select the character set of the XML file that you want to monitor.
- c. *Optional.* Click  to load a sample XML file from your system.
- d. Click  to create one or more XML event tags. You can create a tag manually by typing the XML element. If you are working with sample data, you can create a tag by double-clicking the XML element in the list.


The XML event tag creates a shortcut to the XML element that you want the policy to process. 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 process both types, define both elements as event tags.

For more details, see "[Source Page](#)" on page 307.

3. In the Mappings page, configure the default mappings of XML elements and attributes to custom variables.


- a. Create one or more custom variables.

If you are working with sample data, drag the XML elements or attributes from the XML Properties list to the Map Name column. The editor automatically adds the default prefix `map` to the map name and inserts the correct path to the XML property.

Alternatively, click  above the Map Name column and type the variable name in the map name field. 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.

- b. Add one or more source and target value pairs to each custom variable.

- o If you are working with sample data, drag the group value from the Values list to the Source Value column, and type the target value in the corresponding field.

Alternatively, click  above the Source Value column and type the source and target values in the corresponding fields.

- o Optionally, use the Indicators tab to add indicators to the source or target value fields. After loading the indicators from the BSM server, the Indicators tab shows a hierarchy of configuration item types with the associated health indicators (HIs) and event type indicators (ETIs).


To insert an indicator in a source or target value field, drag the indicator from the Indicators tab. When dropping an indicator state, you can choose between inserting the state only (for example, `Normal`) or the indicator name and state (for example, `HTTPServer:Normal`).

For more details, see "[Mappings Page](#)" on page 299 and "[Indicators Tab](#)" on page 298.



4. *Optional.* In the Defaults page, set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

Note: You can set defaults for only a subset of event attributes. You can set the other event attributes within individual rules.

For more details, see ["Event Attributes Tab" on page 298](#), ["Event Correlation Tab" on page 298](#), ["Custom Attributes Tab" on page 297](#), ["Instructions Tab" on page 299](#), and ["Advanced Tab" on page 295](#).

5. In the Rules page, define one or more policy rules.
 - a. In the Policy Rules list, click the  button, and then click one of the following options:
 - **Event on matched rule:** Use this option if you want to send an event to BSM when the conditions are met.
 - **Suppress on matched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are met.
 - **Suppress on unmatched rule:** Use this option if you want to stop processing the policy when the conditions that you specify are *not* met.
 - b. Click **Rule Description** and type a brief description of the rule.


For more details, see ["Policy Rules List" on page 304](#).

6. In Rule Content, use the Condition tab to define values that you want to evaluate against elements and attributes in the XML file.
 - a. Click  to create a new condition. New conditions by default use the equals operator.
 - b. Click  to expand the new condition.
 - c. In the **Property** field, specify the XML element or attribute that the policy searches for. You must specify the XML path from the XML event tag to the property, separated by slash marks (/) (for example, `/PerformanceAlert/Severity`).

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.

 - d. Select the pattern operator.

If you select the matches operator, you can type a pattern in the Operand field.
 - e. In the **Operand** field, type the value or pattern that you want the policy to compare with the XML property. If you are working with sample data, you can drag the value from the Values list and drop it in the Operand field.

Tip: You can use standard HP Operations Agent pattern-matching rules when matching values. Select the matches operator and click  in the Operand field to open the pattern matching expression toolbox. The toolbox displays the following:

- **Pattern Matching Expressions.** Click an expression to insert it in the Operand field.
- **Variable Bindings Options.** Variable bindings options include 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.

For more details, see ["Condition Tab" on page 295](#).

7. *Optional.* If you are creating a rule of the type 'event on matched rule', set attributes for events that you want the policy to send. You can override the default event attributes here. You can also write instructions that help operators handle the associated event and configure actions to solve problems automatically or manually.

In text boxes, you can use sample data, mappings, pattern-matching variables, indicators, policy variables, and policy parameters.

For more details, see ["Event Attributes Tab" on page 298](#), ["Event Correlation Tab" on page 298](#), ["Custom Attributes Tab" on page 297](#), ["Instructions Tab" on page 299](#), ["Advanced Tab" on page 295](#), and ["Actions Tab" on the next page](#).

8. *Optional.* In the **Options** page, configure options for local event logs, unmatched events, and pattern matching.

For more details, see ["Options Page" on page 300](#).

9. Click **OK** to save the policy template.

UI Reference

This section includes:

- ["Actions Tab" on the next page](#)
- ["Advanced Tab" on page 295](#)
- ["Condition Tab" on page 295](#)
- ["Custom Attributes Tab" on page 297](#)
- ["Defaults Page" on page 297](#)
- ["Event Attributes Tab" on page 298](#)
- ["Event Correlation Tab" on page 298](#)
- ["Indicators Tab" on page 298](#)
- ["Instructions Tab" on page 299](#)
- ["Mappings Page" on page 299](#)
- ["Mappings Tab" on page 300](#)
- ["Options Page" on page 300](#)
- ["Pattern Matching Variables Tab" on page 302](#)
- ["Policy Data Page" on page 302](#)
- ["Policy Parameters Tab" on page 303](#)
- ["Policy Rules List" on page 304](#)

- "Policy Variables Tab" on page 305
- "Properties Page" on page 305
- "Rules Page" on page 306
- "Sample Data Tab" on page 307
- "Source Page" on page 307

Actions Tab

UI Element	Description
Automatic command	Automatic command that runs when the rule is matched.
Command	Command and parameters to run when the command is started for this event. The command runs on the node you specify in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information on <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.
Close the event when the command is successful	Closes the event automatically if the command is successful.

UI Element	Description
Send event immediately	Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.
Wait until local command completes and then	Options that can help to reduce the amount of unnecessary network traffic to the BSM server. For example, if an automatic command solves the problem that generated the event, you may choose not to inform the BSM server. <ul style="list-style-type: none"> • Send the event • Send the event if the local command fails • Send the event only if the local command is successful
Operator-initiated command	Operator-initiated command that is attached to the event that the rule sends to the Event Browser. This command can be started by the BSM user from the Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.
Command	Command and parameters to run when the command is started for this event. The command runs on the node specified in the Node field. If the command contains spaces, enclose it in quotation marks. Commands that are internal to the Windows command shell (for example <code>echo</code> or <code>move</code>), must be preceded by <code>cmd /c</code> . See the Windows help for more information about <code>cmd</code> .
Non Agent User	By default, the command runs as the agent user (<code>\$AGENT_USER</code>). Alternatively, select Non Agent User and specify a user account and password that exists on the node: <ul style="list-style-type: none"> • Username. Runs the command under the specified user account. The account must exist on the node. • Password. Password of the specified user account. • Enable policy parameter in Password field. Enables you to enter a variable in the Password field, for example <code>%%password%%</code>. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	Name of the node on which the command will be started. You can also use the variable <code><\$MSG_NODE_NAME></code> to configure reusable policies for replicated sites.
Append output of command as annotation to the event	Adds an annotation to the event when the command completes. The annotation contains the start time, output, exit value, and finish time of the command. If a command fails, an annotation is provided even if this item is not selected.









UI Element	Description
Close the event when the command is successful	Closes the event automatically if the command is successful.

Advanced Tab



UI Element	Description
Application	Application that caused the event to occur. Unlike the Related CI attribute, which is a direct relationship to a CI in the RTSM, 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 RTSM, the object attribute is a simple string-type attribute (for example, C:, and /dev/spool).
HPOM Service ID	ID of the service associated with 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.
Enable Agent MSI	<p>The message stream interface (MSI) allows external applications to interact with the internal event flow of HP Operations Agent. The external application can be a read-write application, for example, an event processing program that can read events, modify attributes, and generate new events for retransmission to the server. The application could also read events, or send its own events.</p> <p>Divert events. Divert an event to the MSI instead of to the server when an event is requested by an external application.</p> <p>Copy events. Send the event to the server, and a copy of the event to the MSI.</p> <p>If the agent MSI is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Agent MSI. Applies the agent MSI settings configured in the event defaults to this rule.</p> <p>Override default settings for Agent MSI: Enables you to configure specific agent MSI settings for this policy rule.</p>

Condition Tab

UI Element	Description
	New Item. Creates a new condition with the default operator equals.

UI Element	Description
	Delete Item. Deletes the selected condition.
	Move Up. Moves the selected condition higher in the condition order.
	Move Down. Moves the selected condition lower in the condition order.
	Expand. Expands the list of conditions to display all details.
	Collapse. Collapses the list of conditions to display only the names and hide the details.
	Click to expand the details of a condition.
	Click to hide the details of a condition.
Property	XML property that the policy searches for. You must specify the XML path from the XML event tag to the property, separated by slash marks (/) (for example, /PerformanceAlert/Severity).
Operator	The following operators are available: <ul style="list-style-type: none"> • equals • not equals • less than • greater than • less or equal • greater or equal • matches (Enables you to enter a pattern in the Operand field.)
Operand	Value or pattern that you want the policy to compare with the XML property. If you are working with sample data, you can drag the value from the XML Values list and drop it in the Operand field. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Tip: You can use standard HP Operations Agent pattern-matching rules when matching values. Select the matches operator and click  in the Operand field to open the pattern matching expression toolbox. The toolbox displays the following:</p> <ul style="list-style-type: none"> • Pattern Matching Expressions. Click an expression to insert it in the Operand field. • Variable Bindings Options. Variable bindings options include 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. </div>

Custom Attributes Tab

UI	
Element	Description
	Create New Custom Attribute: Creates a new custom attribute with the default name CA_ <i>n</i> . To rename the custom attribute, double-click the name to select it and type the new name.
	Delete Custom Attribute: Deletes an existing custom attribute.
Name	<p>The name of the custom attribute. The name is case-insensitive.</p> <p>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.</p> <p>The following custom attribute names cannot be used because they are reserved for internal use:</p> <p>Description</p> <p>EtiHint</p> <p>HP_OPR_SAAS_CUSTOMER_ID</p> <p>NoDuplicateSuppression</p> <p>RelatedCiHint</p> <p>SourceCiHint</p> <p>SourcedFromExternalId</p> <p>SourcedFromExternalUrl</p> <p>SubCategory</p> <p>SubCiHint</p>
Value	Value of the custom attribute.

Defaults Page

The Defaults page enables you to set default attributes for all events that a policy sends. The event defaults only affect new rules. You can override the defaults for individual rules.

For more details, see ["Event Attributes Tab"](#) on the next page, ["Event Correlation Tab"](#) on the next page, ["Custom Attributes Tab"](#) above, ["Instructions Tab"](#) on page 299, and ["Advanced Tab"](#) on page 295.






Event Attributes Tab

UI Element		Description
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.

Event Correlation Tab

UI Element		Description
Event Key		An identifier used to identify duplicates and for Close Events with Key.
Enable Event Suppression		<p>Enables event suppression for the events generated by this policy.</p> <p>If event suppression is enabled in the event defaults, you can choose to apply them to or override them for this rule:</p> <p>Use default settings for Event Suppression. Applies the event suppression settings configured in the event defaults to this rule.</p> <p>Override default settings for Event Suppression: Enables you to configure specific event suppression settings for this policy rule.</p>






Indicators Tab






UI Element		Description
		<p>Refresh. Loads the configured indicators from the BSM server.</p> <p>Note: Loading indicators from the BSM server may take a few seconds.</p>
		<p>Shows or hides the Select drop target format drop-down panel:</p> <ul style="list-style-type: none"> • Use Indicator States. Click to change the drop target format to indicator states only. • Use Indicator Names and States. Click to change the drop target format to indicator names and states.
<Search ...>		<p>Entered search string is used to search the indicators and highlight only the indicators containing the specified string.</p> <p>To search for indicators with specific text strings in the name, type the string in the <Search ...> field and click the  button. The first matching indicator is selected in the list of rules. Click the  and  buttons to move to the previous and next matching indicator.</p>
<Indicators>		<p>Hierarchy of configuration item types with associated health indicators (HIs) and event type indicators (ETIs). To insert an indicator in a policy, drag and drop the indicator from the Indicators tab to the relevant field in the policy.</p>

Instructions Tab

UI Element	Description
Instructions	<p>Instructions that you want to accompany the event.</p> <p>Events generated by a policy can include instructions that explain what to do when the event is generated. This instruction text can often help an operator to solve a problem when a particular type of event is received. The operator can view the instructions included with an event by viewing the Event Details pane in the Event Browser. You can define default instructions for all rules in a policy. You can also override the default with different instructions for any rule.</p> <p>You can type URLs in the text, and the Event Browser automatically converts them into clickable hyperlinks. For example, you can add URLs of external Web sites, support sites, documentation repositories, troubleshooting information, and similar sites.</p> <p>To add a link, type any URL that begins with one of the following URI scheme names:</p> <ul style="list-style-type: none"> • <code>http://</code> • <code>https://</code> • <code>ftp://</code> • <code>ftps://</code>

Mappings Page

UI Element	Description
	Create new mapping definition. Adds a new mapping definition to the list of mappings.
	Delete mapping definition. Deletes the selected mapping definition.
	Copy Mapping Definition. Creates a copy of the selected mapping definition.
	Move Up. Moves the selected mapping definition up to a higher position.
	Move Down. Moves the selected mapping definition down to a lower position.
Map Name	Name of the custom variable. The editor automatically adds the default prefix <code>map</code> to the map name if the variable has been created from sample data.

Data Input Property	<p>XML element or attribute assigned to the custom variable.</p> <p>XML properties use the following syntax: <\$DATA:/<XML_property>></p> <p><XML_property> is the XML path, separated by slash marks (/), from the XML event tag to the XML element or attribute.</p> <p>The agent 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.</p>
	Create new mapping. Adds a new pair of source and target values to the mapping definition.
	Delete mapping. Deletes the selected source and target value pair.
	Copy Value Mapping. Creates a copy of the selected value mapping.
	Move Up. Moves the selected value mapping up to a higher position.
	Move Down. Moves the selected value mapping down to a lower position.
Source Value	Original value of the XML element or attribute.
Target Value	New value of the XML element or attribute.

Mappings Tab

UI Element	Description
<Mappings>	Displays the mapping definitions configured for the policy.

Options Page

UI Element	Description
Log Local Events	<p>Defines 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:</p> <p>Windows: %OvDataDir%\log\OpC\opcmsglg</p> <p>AIX, HP-UX, Linux, and Solaris: /var/opt/OV/log/OpC/opcmsglg</p>
that match a rule and trigger an event	Logs any events in the event source that match the policy rules.
that match a rule and are ignored	Logs any events in the event source that are suppressed. (Suppressed events are not sent to the Event Browser.)



UI Element	Description
that do not match any rule	Logs any events that do not match any of the rules in the policy.
Unmatched Events	<p>Send an event to the 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.</p> <p>Each policy that sends unmatched events to the Event Browser creates an event with the default values of the policy.</p> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p> <p>Note: If several XML file policies forward unmatched events to BSM, you could receive multiple events about a single input event.</p>
are sent to the Event Browser	Sends unmatched events to the Event Browser.
are sent to the Closed Events Browser	Sends unmatched events to the Closed Events Browser.
are ignored	Ignores unmatched events.
Pattern Matching Options	Defines case sensitivity and field separators for all rules.
Case sensitive check	Defines whether the case (uppercase or lowercase) of a text string is considered when the pattern of a rule is compared with the source data. When switched on, a match only occurs if the use of uppercase and lowercase letters is exactly the same in both the source data and the pattern. This is the default setting.

UI Element	Description
Field Separators	<p>Defines 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:</p> <ul style="list-style-type: none"> • \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 (\) <p>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).</p> <p>If you leave this box empty, the default separators (a blank and the tab character) are used by default.</p> <p>You can set case sensitivity and separator characters for individual rules in a policy by clicking the ► button in rule's match condition.</p>
Apply to All	<p>Applies the pattern matching options to all existing rules in a policy. This overwrites any modifications made to the pattern matching options in individual rules.</p> <p>If you change the pattern matching options and do not click Apply to all, they only apply to all new rules in a policy.</p>









Pattern Matching Variables Tab

UI Element	Description
<variables>	Displays the user-defined variables configured in the Condition tab.











Policy Data Page

UI Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	Check Syntax: Validates the syntax of the policy data. If the policy syntax is incorrect, the validation tool reports an error and points to the corresponding line and position of the unexpected token (for example the incorrect keyword).
<policy data>	Policy data in text form. The data uses the HP Operations Agent policy syntax.

Policy Parameters Tab

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String

Policy Rules List

UI Element	Description
	<p>Create New Rule: Provides the following options:</p> <ul style="list-style-type: none"> • Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. • Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. • Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM.
	<p>Copy Rule. Copies the selected rule. You can then rewrite the description of the copied rule and edit the rule.</p>
	<p>Delete Rule. Deletes the selected rule.</p>
	<p>Move Up. Moves the selected rule higher in the rule order.</p>
	<p>Move Down. Moves the selected rule lower in the rule order.</p>
<Move to>	<p>Entered number is used to select the rule with that sequence number in the list of rules.</p> <p>To select a specific rule in the rule list, type the rule's sequence number in the <Move to> field and click the  button.</p>
<Search rules>	<p>Entered search string is used to search the rule descriptions and highlight only the rules containing the specified string.</p> <p>To search for rules with specific text strings in the rule description, type the string in the <Search rules> field and click the  button. The first matching rule is selected in the list of rules. Click the  and  buttons to move the previous and next matching rule.</p>
	<p>Activate/Deactivate Rule Filter. Activates and deactivates the rule filter.</p>
Seq.	<p>Sequence number of the rules. Rules are evaluated in a specific order. When one condition is matched, no additional rules are evaluated.</p>
Rule Description	<p>Description of the rule. It is good practice to use a description that helps you remember what the rule does</p>

UI Element	Description
Rule Type	<ul style="list-style-type: none"> • Event on matched rule. If matched, the agent sends an event to BSM. The event uses the settings defined for the rule. If you do not configure these settings, the default settings are used. • Suppress on matched rule. If matched, the agent stops processing and does not send an event to BSM. • Suppress on unmatched rule. If not matched, the agent stops processing and does not send an event to BSM. <p>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.</p>

Policy Variables Tab

Variable	Description
<\$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-event basis.
<\$MSG_TEXT>	Returns the full text of the event. Sample output: SU 03/19 16:13 + tty7 bill-root

Properties Page

UI Element	Description
Name	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.

¹(globally unique identifier)








UI Element	Description
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

Rules Page

The Rules page enables you to define one or more policy rules.

For more details, see ["Policy Rules List" on page 304](#), ["Condition Tab" on page 295](#), ["Event Attributes Tab" on page 298](#), ["Event Correlation Tab" on page 298](#), ["Custom Attributes Tab" on page 297](#), ["Advanced Tab" on page 295](#), and ["Actions Tab" on page 293](#).

Sample Data Tab

UI Element	Description
<Search Properties>  	<p>Entered search string is used to find an XML property or value. The list changes as you type; only matching items appear.</p> <p>To clear the search results, click .</p>
	<p>Toggle Short/Full Path Notation. Shows or hides the full path to the XML property or value. The full path begins with the XML event tag specified in the Source tab. The XML Properties section by default shows the short path to the XML property or value.</p>
	<p>Find Matching Events. 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.</p>
	<p>Toggle Deduplication. Shows or hides duplicate values.</p>
XML Properties	<p>Shows all XML elements and attributes that match an XML event tag. (You can identify attributes based on the preceding at sign (@).)</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>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.</p> </div>
Values for <...>	<p>Displays the values of the XML property selected in the XML Properties section.</p>





Source Page

UI Element	Description
------------	-------------

Log File Path / Name	<p>Path and name of the XML file that the policy reads. Type the drive letter and the full path for the location of this file on the node.</p> <p>Tip:</p> <ul style="list-style-type: none"> You can use Windows environment variables (for example <code>winnt</code> or <code>clusterlog</code>) to make your policies more flexible. The proper syntax for these variables is <code><\$variablename></code>, for example <code><\$winnt></code>. You can also call a script or command that returns the path and name of the log file you want to access. For example, type <pre><`command`></pre> <p>where <code>command</code> is the name of a script that returns the path and name of the log file you want the policy to read. The command can also return more than one log file path separated by spaces. The HP Operations Agent processes 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 process multiple instances of a log file.</p> <p>Note: The agent cannot process log files that are larger than 2 GB.</p>
Polling Interval	<p>Determines how often the policy reads the XML 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 <i>after</i> the first polling interval passes. A shorter polling interval is better when you are testing a policy.</p> <p>To modify the time, click the ▼ button and use the drop-down lists to specify increments of hours, minutes, or seconds.</p> <p>To insert a parameter in a time field, type the parameter in the format <code>%%<variable_name>%%</code> or drag and drop the parameter from the Policy Parameters tab.</p> <p>Default value: 5 minutes</p>
Logfile Character Set	<p>Name of the character set used by the XML file that the policy reads.</p> <p>Note: 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 XML file, pattern matching may not work, and the event details can have incorrect characters or be truncated in BSM. If you are unsure of which character set is used by the XML file that the policy reads, consult the documentation of the program that writes the file.</p> <p>Default value: UTF-8</p>

<p>Send event if log file does not exist</p>	<p>The agent sends an event if the specified XML file does not exist.</p> <p>Default value: not selected</p>
<p>Close after reading</p>	<p>The policy keeps the XML file open (and retains its file handle) after reading it. Do not use a polling interval of less than one minute when this option is selected.</p> <p>If you do not select this option and the name of the XML file changes, the policy continues to read the original XML file instead of processing any new XML file with the specified name. Consider the following example: a policy reads the log file <code>syslog.log</code>. Mondays at 23:59, the file is renamed to <code>syslog.monday</code>, and a new version of <code>syslog.log</code> is created for the Tuesday log. Without Close after reading being selected, the policy continues to read <code>syslog.monday</code> because the file handle refers to the original, renamed file.</p> <p>Default value: not selected</p>

<p>Read Mode</p>	<p>The read mode of an XML file policy indicates whether the policy processes the entire file or only new entries.</p>	
	<p>Read from last position. The policy reads only new—appended—entries written in the XML file while the policy is activated. If the file decreases in size between readings, then the entire file is read. Entries that are added to the file when the policy is disabled are not processed by the policy.</p> <p>Choose this option if you are concerned only with entries that occur when the policy is enabled.</p>	<p>Advantage: No chance of reading the same entry twice. (Unless the file decreases in size because some entries were deleted.)</p> <p>Disadvantage: Entries written to file while the policy is disabled or the agent is not running are not processed by the policy.</p>
	<p>Read from beginning (first time). The policy reads the complete XML file each time the policy is activated or the agent restarts. This ensures that all entries in the file are compared with the rules in the policy. Each successive time that the policy reads the file, only new (appended) entries in the file are processed.</p> <p>Choose this option if you want to ensure that every existing and future entry in the file is processed by the policy while it is activated.</p>	<p>Advantage: Every existing and future entry in the file will be processed by the policy.</p> <p>Disadvantage: Duplicate entries can occur if an activated policy is deactivated and reactivated, or if the agent stops and restarts.</p>
	<p>Read from beginning (always). The policy reads the complete XML file every time it detects that the file has changed. The policy scans the file at the specified polling interval. If no change is detected, the file is not processed. Any 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 the policy reads a file that is overwritten, rather than appended.</p>	<p>Advantage: Ensures that files that are overwritten are correctly processed.</p> <p>Disadvantage: Only valid for files that are overwritten, rather than appended.</p>
<p>Note: Every policy reads the same XML files independently from any other policies. This means, for example, that if "Policy 1" with read mode Read from beginning (first time) is activated and "Policy 2" with the same read mode</p>		

	<p>already exists, "Policy 1" still reads the entire file after it has been activated.</p> <p>Default value: Read from last position</p>
Sample Data	<p>Enables you to upload an XML sample file. The editor makes the XML elements and values of the sample file available to you in the Event and Rules pages so that you can insert them by dragging and dropping.</p>
	<p>Load sample data from local file system. Loads an XML sample file from the system where the Web browser runs.</p> <p>Note: The editor can only load a maximum of 50 MB of sample data.</p>
	<p>Opens the XML Sample Data dialog box. This dialog box displays the contents of the uploaded XML sample file.</p>
XML Event Tag	<p>Enables you to specify one or more XML event tags. The XML event tag creates a shortcut to the XML element that you want to process. An event tag typically identifies an event record in an XML file. You can define more than one event tag.</p>
	<p>Create new XML event tag manually. Enables you to type an XML element in the provided box.</p> <p>Create new XML event tag from XML sample data. Opens the XML Sample Data Outline dialog box. This dialog box displays the XML elements and attributes contained in the uploaded XML sample data.</p>
	<p>Deletes the selected XML event tag.</p> <p>Caution: Deleting an event tag that is referenced in a policy corrupts the policy and renders it unusable.</p>


Importing HP SiteScope Templates

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

To access

You can edit the properties of a SiteScope policy using the SiteScope Policy Editor, which you can open in the following ways.

- To open the editor from the Edit Aspect dialog box:
 - a. Open the Management Templates & Aspects manager:
 - Admin > Operations Management > Monitoring > Management Templates & Aspects**

- b. In the Configuration Folders pane, expand the configuration folders.
- c. In the Management Templates & Aspects pane, click an aspect, and then click the  button.

The Edit Aspect dialog box opens.

- d. Click the **Policy Templates** tab, and then click the SiteScope policy template in the list.

Click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The SiteScope Policy Editor opens.

- To open the editor from the Policy Templates manager:

- a. Open the Policy Templates manager:

Admin > Operations Management > Monitoring > Policy Templates

- b. In the Policy Template Groups pane, expand **Policy Template Group > Templates grouped by type**.

- c. Click the **SiteScope Templates** folder, and then click the SiteScope policy template in the Policy Templates pane.

Click the  button, and then click the  **Edit Policy Template** or the  **Edit Policy Template (Raw Mode)** button.

The Edit SiteScope Policy Editor opens.

Learn More

This section includes:

- ["Monitors" below](#)
- ["Templates" on the next page](#)
- ["Prerequisite for Importing SiteScope Templates" on the next page](#)
- ["Assigning and Deploying SiteScope Policy Templates" on the next page](#)
- ["ConfigExchangeSIS" on the next page](#)

Monitors

In SiteScope, *monitors* are tools that can retrieve specific availability and performance data from remote servers. Different types of monitors are available for monitoring different types of systems. When you want to use a particular type of monitor, you create a new instance of it. For each new instance of a monitor, you must specify the remote server that you want to monitor and values for any other settings that configure the monitor.

For example, SiteScope provides a monitor called CPU, which can monitor the level of CPU usage on a remote server. When you create an instance of the CPU monitor, you must specify the remote server that you want to monitor. You can also specify the frequency that you want to check the CPU usage on that server, and thresholds at which you want the monitor to report an error or warning.

Templates

You can use *templates* in SiteScope to create sets of monitors that you want to deploy together. When you add a monitor to a template, you can specify fixed values for the monitor's settings. In addition, you can add variables to a template so that you can set the values of some settings when you deploy the template.

For example, you could have a template that contains the monitors called CPU and Memory. You could configure some fixed settings that you always want to use for those monitors, but add variables called Remote Host and Monitoring Interval, for settings that you want to specify each time you deploy the template.

When you import templates from SiteScope, Operations Management converts the variables to parameters in the resulting policy templates.

Prerequisite for Importing SiteScope Templates

SiteScope templates contain information about the remote servers that they monitor. This information is usually stored in a variable that is replaced by the list of remote servers when the template is deployed.

When importing a SiteScope template, the import tool must be able to identify the variable that contains the host information in order to create a corresponding instance parameter in the resulting policy template. The import tool choose one the following SiteScope variable, in the order described below, to create the host instance parameter:

1. The variable with the display order number 0 in the SiteScope template.
2. The variable named "host" in the SiteScope template.

Note: If the variable "host" exists in a SiteScope template but does not have a value, the value will be set to "%HOST%" during the template import.

3. The variable with the value "%HOST%" in the SiteScope template.

If none of the above variables exist, the SiteScope template cannot be imported and an error is reported.

Assigning and Deploying SiteScope Policy Templates

You assign SiteScope policy templates to the remote servers that you want to monitor with SiteScope. Before deploying the policy template, Operations Management replaces the parameter with the value %HOST% with the list of remote servers to which the policy template is assigned. Based on the connected server configuration, Operations Management then selects the SiteScope server that qualifies for monitoring the remote servers and deploys the policy template to that server. The SiteScope server finally creates the corresponding monitors and starts monitoring the remote servers.

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

ConfigExchangeSIS

Operations Management provides the following script for importing templates from a SiteScope

server:

- On Windows:

```
<HP BSM root directory>\opr\bin\ConfigExchangeSIS.bat
```

- On Linux:

```
/opt/HP/BSM/opr/bin/ConfigExchangeSIS.sh
```

The command accepts the following parameters:

`-sis_group_container`

The name of a template container on the SiteScope server. The command imports all the templates from that container, and any subcontainers.

`-sis_hostname`

The hostname of the SiteScope server. Instead of the default `localhost`, type the fully qualified domain name of the SiteScope server, for example `sitescope1.example.com`.

`-sis_user`

Optional. The user name of a SiteScope user with permission to read the templates (default: `admin`).

`-sis_passwd`

Optional. The password of the SiteScope user (default: `admin`).

`-sis_port`

Optional. The port of the SiteScope server (default: `8080`).

`-sis_ssl`

Optional. Opens an HTTPS connection to the SiteScope server (default: `HTTP`).

`-bsm_hostname`

The hostname of the BSM server. Instead of the default `localhost`, type the fully qualified domain name of the BSM server, for example `bsm1.example.com`.

`-bsm_user`

Optional. The user name of a BSM user with permission to create policy templates (default: `admin`).

`-bsm_passwd`

Optional. The password of the BSM user (default: `admin`).

`-bsm_port`

Optional. The port of the BSM server (default: `80`).

`-bsm_root_dir`

Optional. The base path of the BSM server (default `c:\HPBSM\`).

-bsm_ssl

Optional. Opens an HTTPS connection to the BSM server (default: HTTP).

-verbose

Optional. Displays verbose information (default: false).

Example

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

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

Tasks

This section includes:

- ["Prerequisite Tasks" below](#)
- ["How to Configure the Agent on the SiteScope System" on the next page](#)

Prerequisite Tasks

Before you can monitor a configuration item (CI) with SiteScope, you must complete the following steps:

- Install and configure the agent on the SiteScope system:
 - Install the HP Operations Agent on the SiteScope system. For details, see the HP SiteScope Deployment Guide.
 - Connect the agent to BSM (in SiteScope, navigate to **Preferences > Integration Preferences > New Integration > HP Operations Manager Integration**). To establish the connection, the agent sends a certificate request to BSM, which must be granted in BSM. For details, see the SiteScope Help.
- Prepare the agent on the SiteScope system for deployment:
 - Configure the agent with the SiteScope user credentials. The SiteScope user credentials are required for the deployment of SiteScope policy templates.
 - Configure the agent on the SiteScope system to accept the BSM server as authorized manager.

For details, see ["How to Configure the Agent on the SiteScope System" on the next page](#).

- Set up the SiteScope system as a connected server in Operations Management.
For details, see "Connected Servers" in the BSM Application Administration Guide.
- Verify that a node CI has been created for the SiteScope system, access:
Admin > Operations Management > Setup > Monitored Nodes

- Make sure the systems that SiteScope monitors are represented as node CIs in the RTSM, access:

Admin > Operations Management > Setup > Monitored Nodes

- Configure templates in SiteScope and import them. For details, see "[Prerequisite for Importing SiteScope Templates](#)" on page 313 and "[ConfigExchangeSIS](#)" on page 313.

Note:

- You cannot create SiteScope policy templates in Operations Management.
- After the import, you can edit only the general properties of SiteScope policy templates; the data part is read only.

How to Configure the Agent on the SiteScope System

1. Configure the agent with the SiteScope user credentials:

- a. On the SiteScope system, run the following command-line tool:

Windows: %OvInstallDir%\lbin\sisconfig\sisSetCredentials.bat

UNIX or Linux: /opt/OV/lbin/sisconfig/sisSetCredentials.sh

- b. The tool prompts you for the following information:

SiteScope login: The user name of an SiteScope user (default: admin).

SiteScope password: The password of the SiteScope user (default: admin).

SiteScope port: The port of the SiteScope server (default: 8080).

- c. *Optional.* After the tool has completed, verify the credentials by typing:

```
ovconfget opr.sisconfig
```

2. Configure the MANAGER_ID on the SiteScope system. The MANAGER_ID defines who is allowed to access the agent from outside.

- a. On the BSM Gateway Server system, type the following command to find out the core ID:

```
ovcoreid -ovrg server
```

- b. On the SiteScope system, set the MANAGER_ID to the core ID of the BSM Gateway Server:

```
ovconfchg -ns sec.core.auth -set MANAGER_ID <core ID of BSM Gateway Server>
```

- c. Restart the agent processes, type:

```
ovc -restart
```

- d. *Optional.* Verify the MANAGER_ID by typing:

```
ovconfget sec.core.auth
```



UI Reference

This section includes:

- "Policy Data Page" below
- "Policy Parameters Tab" below
- "Properties Page" on the next page





Policy Data Page

Note: In HP SiteScope templates, the Policy Data page is read only.

UI	
Element	Description
	Load From Local File System: Click to open the Select file to upload dialog box. Use the dialog box to upload a policy file. These files are data files and end in <code>_data</code> .
	HP SiteScope policies do not support syntax checking. You can click Check Syntax but the check fails to perform.
<code><policy data></code>	Policy data in text form.

Policy Parameters Tab

Note: In HP SiteScope templates, the Policy Parameters tab is read only.

UI Element	Description
	Create Parameter: Open the Create Parameter dialog box.
	Edit Parameter: Open the Edit Parameter dialog box.
	Delete Parameter: Delete the selected parameter from the list.
	<p>Synchronize Parameters: Check the policy template to make sure that variables in the format <code>%%<variable_name>%%</code> have corresponding parameters. Each variable should have one corresponding parameter.</p> <p>Also checks for unused parameters, for which no corresponding variable exists in the policy template.</p> <p>If any missing or unused parameters exist, the Synchronize Parameters dialog box opens. Read the summary, and then click Change or Ignore. If you click Change, the missing parameters are automatically created, and unused parameters are automatically deleted.</p>

UI Element	Description
<Parameters>	<p>List of parameters configured for this policy template.</p> <p>Parameters enable you to create policy templates that other users can easily customize. Each parameter corresponds to a variable in a policy template. A parameter gives consumers of a policy template the opportunity to specify the value of a variable, without having to modify the policy template themselves.</p> <p>To insert a parameter, drag the parameter from the Policy Parameters tab to any text field within a condition or an event definition in a policy template. Alternatively, type the parameter in the text box using the format <code>%%<variable_name>%%</code> (for example <code>%%CriticalThreshold%%</code>).</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none"> Enumeration (of several options) Number Password String

Properties Page

UI Element	Description
Name	<p>Name of the policy. You can use spaces in the name. The equal sign (=) is not allowed.</p> <p>The name is set when the policy is created and cannot be changed in new versions of a policy.</p>
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Policy ID	GUID ¹ assigned to the policy when it is first created.

¹(globally unique identifier)

UI Element	Description
Version	<p>The current version of the policy. If you modify an existing policy, you create a new version of the policy in the database with a unique version number. By default, the minor version number increases by one automatically after you modify the policy and save it. If you want to save the policy with a specific version number, you can select the major or minor version number that you want. It is not possible to replace an existing version of a policy. However, you can delete a specific version of a policy.</p> <p>Note: If you modify a policy template that is part of an HP Operations Smart Plug-in (SPI), increase the minor version number only. The next version of the SPI normally uses the next major version number.</p>
Change Log	Text that describes what is new or modified in this version of the policy.
Last Modification	<p>The date and time that the policy was saved.</p> <p>The date and time displays using the current time zone of the computer on which the Web browser 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 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.</p>
Last Modified by	The name of the user active when the policy was saved.
Instrumentation	Instrumentation selected for this policy. Instrumentation consists of one or more programs (for example scripts or executables) that some policies may require to complete a configuration or monitoring task. Instrumentation is deployed to nodes that have HP Operations Agent installed when the policy is deployed.
OS Types	<p>Types of operating system with which this policy is compatible.</p> <p>To enable platform neutrality, you can create several platform specific variations of the same policy, and include them all in one aspect. Operations Management ensures that a policy is deployed only to host nodes that have the operating systems that you specify.</p> <p>If you leave all the OS type check boxes clear, the policy can be deployed to host nodes with any operating system.</p>

Importing HP Operations Manager Policies and Instrumentation

HP Operations Manager (HPOM) is a server and agent-based monitoring solution that enables you to monitor the availability and performance of your IT infrastructure and services. With HPOM, you can configure the HP Operations Agent on the nodes that you want to manage by deploying policies to those agents. HP BSM Operations Management provides a script that enables you to import policies from HPOM so that you can include them in aspects, and also deploy them directly from HP BSM Operations Management.

Learn More

Template Groups

In HPOM, policy groups are sets of policies that share some common attribute or logical connection. Policy groups enable you to more easily work with multiple policies simultaneously. For example, you can deploy all the policies in a group to managed nodes together.

You can export policy groups from HP Operations Manager and import them into Operations Management. The policy groups appear under Template Groups in the Policy Templates manager.

Instrumentation

Instrumentation consists of one or more programs, which are deployed with policies to nodes that have the HP Operations Agent. The programs are scripts or executables that can be used by policies.

Instrumentation is grouped into categories. Policies can be associated with instrumentation categories to ensure that HP Operations Manager automatically deploys the instrumentation when it deploys the policy.

When you export policy configuration data from HPOM, you can choose to include any associated instrumentation categories. If you import this configuration data, the instrumentation categories will be available in Operations Management. You can deploy the instrumentation categories with individual policies, and you can add the instrumentation to aspects.

Script Parameters

In HPOM, you can create measurement threshold policies that contain VB Script or Perl scripts. The scripts can do complicated calculations, evaluate thresholds, or add functionality. Script parameters enable you to change the values of variables in the script without the need to edit the script itself.

When you import measurement threshold policies from HPOM, any script parameters are converted to Operations Management policy template parameters.

Automatic and Operator-initiated Commands

HPOM policies can create events (called messages in HPOM) that include automatic and operator-initiated commands:

- Automatic commands can run locally on a managed node when the HP Operations Agent detects the event. HPOM can also run automatic commands on the management server or a

remote node when the event arrives on the management server. Operators can restart automatic commands manually from the HPOM message browser.

- HPOM operators can start operator-initiated commands manually from the HPOM message browser, after evaluating the details of the event.

If you import policies from HPOM into Operations Management, any automatic and operator-initiated commands are included. After you deploy policy templates using Operations Management, any automatic commands can run locally on a managed node. However, Operations Management does not run automatic-commands on the BSM server, or remote nodes. You cannot restart automatic commands from Operations Management, and you cannot start operator-initiated commands either.

If you have connected your HPOM management servers to Operations Management, and you are forwarding events from Operations Management to HPOM, you can start any commands that exist in those events using the HPOM message browser.

Export of Policies from HPOM

You can export policies, policy groups, and instrumentation from HPOM using the following tools on the HPOM management server:

- HPOM for Windows:

```
ovpmutil cfg pol dnl <folder> /p <identifier> [/instrum]
```

- Replace *<folder>* with the path of a folder into which you want to download the policy configuration data.
- Replace *<identifier>* with the path to a policy group from which to download policies. The path must contain the path to the policy, as shown in the console tree, starting under Policy groups. Start the policy group path with a backslash (\), and separate sub-groups with a backslash (\) too. If the name of a policy group contains spaces, enclose the entire path in quotation marks.
- Add */instrum* if you want to export any associated instrumentation categories.

Example:

The following command downloads policies and instrumentation from the policy group 'Samples' to the folder `c:\test`:

```
ovpmutil cfg pol dnl c:\test /p \Samples /instrum
```

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

- HPOM on UNIX or HPOM on Linux:

You can use the shopping cart functionality to export policies, policy groups, and instrumentation:

- a. In the Administration UI, click **Browse > All Policy Groups**.
- b. Select policy groups in the list, and then click **Choose an action > Add to Shopping Cart**.
- c. *Optional.* Click **Browse > All Categories**. Select any categories of instrumentation that the policies require, and then click **Choose an action > Add to Shopping Cart**.

- d. Click **Browse > Shopping Cart** and then click **Choose an action > Download Shopping Cart**. Type a comment, and then click **OK**.
- e. The data is then available in a new sub-folder under **Browse > Downloads** and in the following folder on the management server:

```
/opt/OV/OMU/adminUI/data/clipboard/
```

Alternatively, you can use the `opccfgdwn` command. For more information, see the `opccfgdwn man` page.

Copy to output folder from the HPOM server to the BSM server.

UI Reference

ConfigExchange

Operations Management provides the following script for importing policies, policy groups, and instrumentation from HP Operations Manager:

- On Windows:

```
<HP BSM root directory>\opr\bin\ConfigExchange.bat
```

- On Linux:

```
/opt/HP/BSM/opr/bin/ConfigExchange.sh
```

The command requires the following parameters (in the following order):

`-uploadOM -input <folder>`

The path to a folder that contains the policy data and instrumentation. The folder must be the output of `ovpmutil` (HPOM for Windows) or `opccfgdwn` (HPOM on UNIX or HPOM on Linux).

`-server <gateway server> [-port <port>] [-ssl]`

The hostname of the BSM gateway server.

By default, the command attempts to connect to port 80 for HTTP connections, or port 443 for HTTPS connections. Specify `-port` if the BSM gateway server uses a different port.

Specify `-ssl` to connect to the BSM gateway server using HTTPS.

`-username`

The user name of a BSM user with permission to create policy templates.

`-password`

The password of the BSM user.

`-verbose`

Optional. Print verbose output.

`-force`

Optional. Continue the upload even if an error occurs.

Example:

The following command uploads policies, policy groups, and instrumentation from a folder called 'example_policy_group':

```
c:\HPBSM\opr\bin\ConfigExchange.bat -uploadOM -input  
c:\Users\Administrator\Desktop\example_policy_group -server  
bsm1.example.com -port 8080 -username admin -password password
```

Instrumentation Development

Instrumentation includes scripts and executables executed by the HP Operations Agent as defined in policies for managed nodes that have the agent installed on them.

SPI developers and users wanting to develop their own monitoring packages must follow these guidelines while developing, testing, and updating instrumentation. Instrumentation is developed outside of BSM. You use the "[ConfigExchange Command-Line Tool](#)" on page 332 to upload your instrumentation into the RTSM. Production-ready instrumentation can be distributed to other BSM instances using content packs.

Note: For more information about instrumentation, see the HP Operations Manager for Windows and HP Operations Agent documentation.

Note: Only base packages can be assigned to templates or aspects. If you try to assign a patch or hotfix, an error is displayed.

To access:

The **ConfigExchange** command-line interface is located in:

```
<BSM_Root_Directory>/opr/bin
```

Learn More

Development of Instrumentation

The instrumentation development utility is designed to help you to develop instrumentation. It is used to:

- Create instrumentation directory structures
- Upload and download instrumentation directory structures
- Upload and download instrumentation directory structures as a patch
- Upload and download instrumentation directory structures as a hotfix

After completing instrumentation development, the instrumentation components must be included in a content pack for distribution to the BSM servers.

Deployment of Instrumentation Packages

Instrumentation packages (including patch and hotfixes) must be deployed to managed nodes.

Conventions for Naming of Instrumentation Packages

There are 3 instrumentation artifacts:

- Instrumentation package (also referred as base package)
- Instrumentation package patch
- Instrumentation package hotfix

Artifact types are defined using the following naming convention:

- Instrumentation package names should only include alphanumeric characters and the underscore character (`_`) (similar to category names in HPOM).
- Patch names should only include alphanumeric characters, the underscore character (`_`), and include the following suffix: `__PATCH__<num>`.
- c) Hotfix names should only include alphanumeric characters, the underscore character (`_`), and include the following suffix: `__PATCH__<num>__HOTFIX__<name>`.

Patching and Hotfix Strategy

The following outlines the strategy you should follow for creating instrumentation patches and hotfixes:

• Base Package Definition

The base package definition is a zipped directory structure for a category.

Removal of the base package also removes any hotfixes and patches.

Re-upload of a base package can be achieved using the `-force` option.

• Instrumentation Patch Definition

Patch naming convention: `<base_pkg_name>__PATCH__<num>`

Instrumentation patch definitions are deployed to the associated base package and will overwrite files of the base package. The directory structure must be the same as the base package. The file set is usually a subset of the base package files.

Multiple patches can exist for a base package and they are ordered by version number.

Version number syntax: `<major>.<minor>` where `<major>` or `<minor>` is an integer ≥ 1 .

Rollback of a patch removes the patch and any associated hotfixes from the database. Other patches associated with the same base package remain unchanged.

Re-upload of a patch can be achieved using the `-force` option.

• Hotfix Definition

Hotfix naming convention: `<categoryname>[__PATCH__<num>]__HOTFIX__<hotfixname>`

Hotfix definitions are deployed in alphabetical order to the associated base package and will overwrite files with identical names of the base package and any preceding patches. The

directory structure must be the same as the base package. The file set is usually a subset of the base package files.

Multiple Hotfixes can exist for a base package or a patch and they are ordered by version number.

Version number syntax: *<major>.<minor>* where *<major>* or *<minor>* is an integer ≥ 1 .

Rollback of a hotfix removes the hotfix only from the database.

Note: No check is made to ascertain whether two hotfixes have conflicting files, but deployment order is defined (alphabetical).

Re-upload of a hotfix can be achieved using the `-force` option.

- **Deployment Strategy for Patches and Hotfixes**

Patches with higher version numbers supercede patches with lower version numbers.

An agent node always gets the base package merged with the latest available patch, and with any available hotfixes of the latest patch. If no patch is present, any available hotfixes for the base package are merged.

Note:

- If a patch or hotfix exists, it is deployed with the base package.
- If a hotfix exists, the related base package or patch cannot be deployed independently.
- A patch which does not have the highest version number cannot be deployed.

For example, the following two patches are available for the mySPI: `mySpi__PATCH__1` and `mySpi__PATCH__2`. It is not possible to deploy `mySpi__PATCH__1`. `mySpi__PATCH__2` will always be selected.

- **Branching of Instrumentation Packages**

If you need several variants of an instrumentation package which shall branch off from the same base package then this must be solved by instrumentation package naming. Just duplicate the base package to a new name.

Instrumentation Commands of the ConfigExchange CLI

The ConfigExchange command line interface includes the following options dedicated to instrumentation.

For detailed information, see "[ConfigExchange Command-Line Tool](#)" on page 332.

UI Element	Description
-createinstrumdir -output <categoryname>	<p>Creates the required directory structure in the file system, complete with the sub-directories for the Windows and Unix, operating system types. The availability of the complete directory structure makes it clear where the various instrumentation components should be located. It is essential to follow the prescribed structure.</p> <p>Note: Operating system version names are hard-coded, and taken from the HP Operations Agent, version 11.10.</p>
-description <descr>	Description text for a base package, patch or hotfix. Set to "" if the option is omitted.
-force	If the <code>-force</code> option is specified, the database item is replaced. If not set, the database upload fails if the instrumentation package (or patch, or hotfix) already exists in the database.
-hotfix <hotfix_name> -forpatch <num>	Specifies the hotfix name and the related patch number. <code><num> = 0</code> indicates the base package.
-instrumname <categoryname>	Instrumentation name.
-label <label>	<p>Label for base package, patch or hotfix. If omitted, the category name is used as follows:</p> <p>Patches: <code>__PATCH__ <num></code></p> <p>Hotfixes: <code>__HOTFIX__ <hotfixname></code></p> <p>For example: <code>ISSPI__HOTFIX__cpu_fix</code>" or <code>ISPI__PATCH__1__HOTFIX__cpu_fix</code></p>
-list -instrumname <categoryname>	<p>Lists the actual status (name and label of base package, patches, and hotfixes) of a package in the database.</p> <p><code>-instrumname ALL</code> lists all instrumentation packages available in the database.</p>
-merge -output <targetdir> -instrumname <categoryname>	<p>Downloads merged instrumentation directory structure to file system using the layout as applied to agent nodes. This option is useful for instrumentation development and testing.</p> <p>Note: You can use this option on the development BSM server to simulate which instrumentation artifacts would be deployed to the agent node.</p> <p>You can also merge a base package, patches, and hotfixes into a new base package.</p>

UI Element	Description
-patch <num>	Upload instrumentation directory structure as a patch. Prerequisites: base package must be available in the database with name <categoryname>__PATCH__<num>.
-remove -instrumname <categoryname> [(-patch <num>) (-hotfix <hotfixname> -forpatch <num>)]	Rollback functionality for patches and hotfixes. Can also be used to remove a complete instrumentation package.

Usage Examples for the ConfigExchange CLI

The following lists some usage examples for the ConfigExchange CLI:

- ConfigExchange.sh -upload -input <upload_dir> -instrumname <categoryname>**

Uploads <upload_dir> to database under the name <categoryname>. Fails if package <categoryname> already exists in the database.
- ConfigExchange.sh -upload -input <upload_dir> -instrumname <categoryname> -force**

Uploads <upload_dir> to database under the names <categoryname>. Overwrites the package <categoryname> if it already exists in the database.
- ConfigExchange.sh -upload -input <upload_dir> -instrumname <categoryname> -patch 3 -label <label>**

Uploads <upload_dir> and stores it as patch 3 for package <categoryname> in the database. Also applies label <label> to Patch 3.
- ConfigExchange.sh -upload -input <upload_dir> -instrumname <categoryname> -hotfix <hotfix_name> -forpatch 0 -description <descr>**

Uploads <upload_dir> and stores it as hotfix <hotfixname> for base package <categoryname> in the database. Also applies description <descr> to the hotfix <hotfixname>.
- ConfigExchange.sh -upload -input mySPI -instrumname mySPI -hotfix hf_CPUfix -forpatch 3 -force -description "mySPI hotfix for patch 3; fix CPU issue"**

Uploads from directory ./mySPI and stores the data as hotfix hf_CPUfix for mySPI's patch 3 to the database, using the description mySPI__PATCH__3__HOTFIX__hf_CPUfix.

-force ensures that the package is re-uploaded if the hotfix package is already in the database.
- ConfigExchange.sh -download -output <download_dir> -instrumname <categoryname>**

Download instrumentation package with name `<categoryname>` from the database and unzips it to the directory `<download_dir>`.

Note: Patch and hotfixes are not downloaded.

- `ConfigExchange.sh -download -output <download_dir> -instrumname <categoryname> -patch 1`

Downloads `patch 1` for instrumentation package `<categoryname>` from the database and unzips to the directory `<download_dir>`.

Note: Base package and hotfixes are not downloaded.

- `ConfigExchange.sh -download -output <download_dir> -instrumname <categoryname> -hotfix <hotfix_name> -forpatch 1`

Downloads hotfix `<hotfix_name>` of `patch 1` for instrumentation package `<categoryname>` from the database and unzips it to the directory `<download_dir>`.

Note: Base package and `patch 1` are not downloaded.

- `ConfigExchange.sh -merge -instrumname <categoryname> -output <download_dir>`

Downloads instrumentation package `<categoryname>`, associated patches, and hotfixes from the database and unzips them to the directory `<download_dir>` in the following order (as they would be deployed to the agent node):

- Base package
- Highest patch
- Hotfixes for the highest patch in alphabetical order

- `ConfigExchange.sh -remove -instrumname <categoryname> -hotfix hf1 -forpatch 0`

Rolls back hotfix `hf1` of the base instrumentation package `<categoryname>`.

- `ConfigExchange.sh -remove -instrumname <categoryname> -patch 1`

Rolls back `patch 1` and its hotfixes.

Note: Patches with higher version numbers than `patch 1` are not downloaded.

- `ConfigExchange.sh -createinstrumdir -output <categoryname>`

Generates an empty directory structure under `<categoryname>` which can be used to contain instrumentation files.

- `ConfigExchange.sh -list -instrumname <categoryname>`

lists all patches and hotfixes for instrumentation package `<categoryname>`.

Workflows

Deploying Instrumentation to Agent Nodes

When deploying instrumentation to agent nodes, you must consider the following:

- Deployment order:
 - Base package
 - Highest patch
 - Hotfixes for the highest patch or of base package in alphabetical order
- If one of the following modifications is made:
 - New patch or hotfix is uploaded to the database
 - Base package is modified
 - Patches or hotfix is modified

the next deployment of instrumentation to a system where the base package is already deployed, automatically deploys the new instrumentation to the agent node.

The merge of base package, patches, and hotfixes is performed on the Gateway Server, eliminating superfluous network traffic when deploying to agent nodes.

Including Instrumentation Patches and Hotfixes Into Content Packs

1. Instrumentation patches and hotfixes are artifacts, and can be handled in the same way as instrumentation base packages. They are individually identifiable and can be specified for export and import using the Content Manager.

Note: Ignore a patch or hotfix package at upload time if no base package is available in the database, and ignore a hotfix for a patch if the patch not yet in the database.

2. When selecting and exporting a base package using the Content Manager UI, its patches and hotfixes are automatically selected and exported. If a patch is selected, all associated hotfixes are downloaded.

SPI Workflow for Developing Instrumentation Base Package

The following workflow outlines how to develop a new mySPI instrumentation package:

1. Create the directory structure for the mySPI instrumentation package:

```
ConfigExchange.sh -createinstrumdir -output mySPI
```

2. Copy any mySPI files to the newly created directory structure.

3. Import to database for testing:

```
ConfigExchange.sh -upload -input mySPI -instrumname mySPI
```

4. Continue development and fix bugs. Export package to the database:

```
ConfigExchange.sh -upload -input mySPI -instrumname mySPI -force
```

5. Create a content pack and add the instrumentation package mySPI to the other mySPI artifacts in the Content Pack. Export the content pack.
6. Publish the mySPI content pack for production use.

SPI Workflow for Developing Instrumentation Patches or Hotfixes

The following workflow outlines how to develop a new patch or hotfix for the mySPI instrumentation package:

1. Download the mySPI instrumentation package to the file system for editing:

```
ConfigExchange.sh -download -output . -instrumname mySPI
```

2. Edit, enhance, and add the files you need for the patch or hotfix.

3. Upload new content as a patch or hotfix:

```
ConfigExchange.sh -upload -input mySPI -instrumname mySPI -patch 1
```

or when hotfixing the base package:

```
ConfigExchange.sh -upload -input mySPI -instrumname mySPI -hotfix hf1 forpatch 0
```

or if you want a hotfix for patch 1:

```
ConfigExchange.sh -upload -input mySPI -instrumname mySPI -hotfix hf1 forpatch 1
```

Note: alternatively create a new directory structure and only add the files you need for patch or hotfix.

4. Test new content and rework if required. Upload with the `-force` option to replace the previous updates in the database:

```
ConfigExchange.sh -upload -input mySPI -instrumname mySPI -patch 1 -force
```

or

```
ConfigExchange.sh -upload -input mySPI -instrumname mySPI -hotfix hf1 -forpatch 0 -force
```

5. Create a content pack. You can consider whether the mySPI base package should also be included in the content pack.
6. Publish mySPI patch or hotfix content pack for production use.

Validating HP Operations Manager Policies

This chapter describes how to check and validate whether HP Operations Manager (HPOM) policies are compatible with Monitoring Automation.

To access:

Run the `configexchange` command line tool from the following location:

```
<BSM_Root_Directory>/opr/bin/configexchange -check -policyfile <file_or_dir> -logfile <logfile>
```

For details, see the "ConfigExchange Command-Line Tool" on page 332 section.

How to Create a Compatibility Report for an HPOM Policy or Set of Policies

1. Run the command:

```
<BSM_Root_Directory>/opr/bin/configexchange -check -policyfile
<file_or_dir> -logfile <logfile>
```

A Policy Parser Report is generated for the file or all files in the directory specified in *<file_or_dir>* and written to the file specified in *<logfile>*.

2. Open the newly generated Policy Parser Report. It contained the following information:

- Summary of the number and types of problems and incompatibilities
- Policies without problems
- Policy files containing ECS
- Policy File problem details

Example:

Policies without problems: 4 of 11 (36.36%)

Potential policy problems:

ECS-Policies:	Error	1 of 10
Patterns:	Error	9 of 10

Actions:

Server Var:	Error	10 of 36
Server Exe:	Error	9 of 36
Var in Action String:	Error	0 of 36
Pwd encryption:	Error	0 of 36

Forwarding rules (MPI_SV...):

In # of conditions:	Warning	0
---------------------	---------	---

Server functionality (TroubleTicket, Notification, INSTRUCTION_TEXT_INTERFACE):

In # of conditions:	Warning	10
---------------------	---------	----

Suspicious instructions:

In # of conditions:	Warning	1
---------------------	---------	---

Policies without problems

[OK] /data/Work/Unified-Config/Policies_for_test/cd56be9e-fee3-71e0-1bf0-1039249e0000_data

[OK] /data/Work/Unified-Config/Policies_for_test/dfa1c17a-fee3-71e0-1bf0-1039249e0000_data

[OK] /data/Work/Unified-Config/Policies_for_test/e1f3301e-9837-

```
4f28-a103-4ec3b09dbc09_data
[OK] /data/Work/Unified-Config/Policies_for_test/f5969ab4-fee3-
71e0-1bf0-1039249e0000_data
```

```
Policy files containing ECS
-----
```

```
[ECS] /data/Work/Unified-Config/Policies_for_test/f7df32d6-fee3-
71e0-1bf0-1039249e0000_data
```

```
Problem details of problematic policies
-----
```

```
Policy File: /data/Work/Unified-Config/Policies_for_test/f4d5252c-
4600-4c2e-99a2-67dbf002f333_data
```

```
Condition ID: b0c51b22-ece3-71d9-09fb-0f8878050000
Condition: "Verify opcmona flag files - not found at all"
  Problem: ACTION_SERVER_VAR [ERROR]
    Action: "opcragt -start <$MSG_NODE_NAME>"
    Action Node: ACTIONNODE IP 0.0.0.0 "<$OPC_MGMTSV>"
    Password:
```

```
Condition ID: 258941c8-ece3-71d9-09fb-0f8878050000
Condition:
  Problem: ACTION_SERVER_VAR [ERROR]
    Action: "opcragt -start <$MSG_NODE_NAME>"
    Action Node: ACTIONNODE IP 0.0.0.0 "<$OPC_MGMTSV>"
    Password:
```

```
...
```

Note: Some policy settings can be global to the policy in addition to being part of a condition. As a result, the Condition ID is null if it was found outside a condition, and the following is logged:

```
Policy Default Settings:
  Problem: SERVER_FUNCTION [ERROR]
  Server Function: INSTRUCTION_TEXT_INTERFACE
```

3. For each policy file with reported errors, using the policy editor, modify the policy to suit your requirements.

ConfigExchange Command-Line Tool

This section describes the options and parameters available in the **ConfigExchange** command-line tool.

The **ConfigExchange** command-line tool is located in:

```
<BSM_Root_Directory>/opr/bin
```

The **ConfigExchange** command requires the following usage syntax:

ConfigExchange <Operation> <Connection> <UserCredentials> <Option>

Operation: Requires one of the following options:

```
-upload -input <input file or directory>
-uploadOM -input <input file or directory>
-remove <InstrumOpts>
-merge -output <output file or directory> <InstrumOpts>
-list <InstrumOpts>
-createinstrumdir -output <output file or directory>
-version
-help
-check -policyfile <fileordir> -logfile <logfile>
```

Instrumentation Options: Requires one of the following options:

```
-instrumname <name> [ ( -patch <patchnum> ) | (-hotfix <hotfixname> -
forpatch <patchnum> ) ] [ -label <label> ] [ -description <descr> ] [ -
force ]
```

(-list and -merge offer only the -instrumname suboption; -list -instrumname ALL lists all instrumentation packages; -label, -description and -force is only supported by -upload).

Connection: Requires one of the following options:

```
-url <URL>
-server <gateway server> [-port <port>] [-ssl]
```

User Credentials:

```
-username <login name> [-password <password>]
```

Option: Any of the following:

```
-verbose
-force
-policyname
```

The following table gives more information about the arguments recognized by the **ConfigExchange** command:

Option	Description
-c, -check	Check policies exported from HPOM for incompatibilities.
-cin, -createinstrumdir	Creates the directory layout in the file system for an instrumentation package.

Option	Description
-de, -description <description>	Description text for an instrumentation package, patch or hotfix.
-dl, -download	Downloads Operations Management instrumentation.
-f, -force	Continues the upload and download of data even when an error occurs.
-fp, -forpatch <patch number>	Patch number to which an instrumentation hotfix refers. "0" means a hotfix for the base package.
-h, -help	Displays a summary of the command options and exits.
-hf, -hotfix <hotfix name>	Hotfix name. Hotfix is for either the base package or for one of its patches.
-i, -input <input file or directory>	Input file or directory.
-inn, -instrumname <instrum name>	Instrumentation package name as used in the database.
-l, -list	Lists an instrumentation package with its patches and hotfixes.
-label, -label <label>	Label for an instrumentation package, patch or hotfix.
-lf, -logfile <log file>	Log file to which the parsing results are written.
-m, -merge	Downloads an instrumentation package with its patches and hotfixes to the file system. Data is merged in the following order: <ul style="list-style-type: none"> • Base package • Highest patch version • Hotfixes in alphabetic order for highest patch or for base package (if no patch exists)
-o, -output <output file or directory>	Output file or directory.
-p, -port <port>	Sets the port number. Default port is 80 for HTTP and 443 for HTTPS. This option cannot be specified in conjunction with the option: <code>url</code> .
-password <password>	Password for the specified user.
-patch, -patch <patch number>	Number for an instrumentation package patch. Must be an integer ≥ 1 .

Option	Description
-rm, -remove	Removes one of the following from the database: <ul style="list-style-type: none"> • Instrumentation package (including patches and hotfixes) • A patch (with hotfixes) from the specified instrumentation package • A hotfixes from the specified instrumentation package
-server <gatewayserver>	Sets target Gateway Server. The value can be a hostname or IP address of a Gateway Server. Default is: {0}. This option cannot be specified in conjunction with the option: <code>url</code> .
-ssl	Sets the protocol to HTTPS. Default is to use HTTP. This option cannot be specified in conjunction with the option: <code>url</code> .
-u, -url <URL>	URL of the Gateway Server. Default is: <code>http://<BSM gateway FQDN>:80/opr-config-server/rest</code> This option cannot be specified in conjunction with the options: <code>ssl</code> , <code>server</code> , or <code>port</code> .
-ul , -upload	Uploads Operations Management instrumentation.
-uom, -uploadOM	Uploads HPOM data: policies, policy groups, and instrumentation.
-username <login name>	Login name of the user required for authentication.
-v, -verbose	Prints verbose output.
-version	Prints the version information and exits.

The **ConfigExchange** command displays the following values to indicate the exit status of the requested operation:

Exit Status	Description
0	Successful completion
1	Failure of requested operation
300-399	HTTP Redirection (300-399)
400-499	HTTP Client Error (400-499)
500-599	HTTP Internal Server Error (500-599)

The exit status numbers (300-599) reflect a standard HTTP-status category (and number), for example: `Redirection` (300-399). For more information about a specific HTTP error status, for example: 307, which signifies a temporary HTTP re-direct, see the publicly available HTTP documentation.

Policy Objects for Scripts

The objects listed here are available for each policy and can be manipulated with Visual Basic Scripting Edition or with Perl. These policy objects can only be used in scripts that run within a policy. They cannot be used in standalone scripts that are executed from the command line.

Caution: Policy scripts provide administrators with a powerful tool to evaluate and manipulate data. If, however, a script is incorrectly written, it could cause the agent to fail. Hewlett-Packard Company is not responsible for agent failures resulting from incorrectly written scripts.

This section includes:

- "Policy Object" below
- "Source Object" on page 343
- "Session Object" on page 348
- "Rule Object" on page 349
- "ConsoleMessage Object" on page 350
- "ExecuteCommand Object" on page 354

Policy Object

This object is used to access the attributes of a policy.

Policy Method:	Source
Parameter:	<i>name</i> (The Short name indicated in the policy's source properties.)
Return Type:	VB Script: IDispatch object of type "Source" (This is the default method for the Policy object.) Perl: <code>source</code> object
VB Script Syntax:	<code>Policy.Source ("name")</code>
Perl Syntax:	<code>\$Policy->Source ("name") ;</code>
Description:	Returns the <code>source</code> object for the defined source and metric. Measurement type sources must use a separate source for each metric. Note: To improve performance, assign the <code>source</code> object to a variable instead of using the <code>Source</code> method every time it is needed.

Policy Method: Name	
Parameter:	void
Return Type:	VB Script: BSTR, Perl: string
VB Script Syntax:	Policy.Name()
Perl Syntax:	\$Policy->Name();
Description:	Returns the name of the policy that started the script.

Policy Method: CreateObject	
Parameter:	<i>progID</i> (string of format: [Vendor.]Component[.Version])
Return Type:	VB Script: IDispatch Perl: not applicable
VB Script Syntax:	Policy.CreateObject (" <i>progID</i> ")
Perl Syntax:	not applicable
Description:	Creates a component instance of a COM object. Note that this method is valid only on Windows nodes, and cannot be used in a Perl script.

Policy Method: SourceEx	
Parameter:	<i>expression</i> (See Description, below, for valid expressions.)
Return Type:	VB Script: IDispatch object of type "Source" Perl: source object
VB Script Syntax:	Policy.SourceEx (" <i>expression</i> ")
Perl Syntax:	\$Policy->SourceEx (" <i>expression</i> ");

Policy Method:	SourceEx
Description:	<p>Returns the source object instance of the source defined by the expression. This source object is identical to the object returned by the Policy.Source method, but because it does not have to be configured in the policy, it can be used for scheduled tasks, as well as for measurement threshold policies. The expression can have the following format depending on which component the performance metric will be collected from:</p> <ul style="list-style-type: none"> • <code>NTPERFMON\ObjectName\Counter\Instance</code> <p>Access a perflib metric (not supported on UNIX nodes). Object, Counter, and Instance are strings as specified in the current monitor configuration for NT performance monitors.</p> <p>Example: <code>NTPERFMON\Process\Elapsed Time*</code></p> • <code>SNMP\object id[\hostname]</code> <p>Perform an SNMP get on the specified object id (OID). By default, the collection will be done on the managed node but can be elsewhere if the optional hostname is given. For SNMP, the method will have to wait until the value is returned which might take some time</p> <p>Example: <code>SNMP\1.3.6.1.2.1.1.7.0\onion.veg.com</code></p> • <code>PROGRAM\command[\monname]</code> <p>Run the specified command or script for gathering the monitored value. The command or script must at some point run the <code>opcmon</code> command to return the value associated with the monitor. If no monitor name is specified, then the default <code>DynPROGRAM</code> must be used. For example, to specify the monitor <code>mymonname</code>: <code>opcmon mymonname=value</code>; to specify the default, <code>opcmon DynPROGRAM=value</code>.</p> <p>Examples: <code>PROGRAM\opcmon DynPROGRAM=12</code> <code>PROGRAM\opcmon testmon=25\testmon</code></p> • <code>EXTERNAL[\monname]</code> <p>Wait for a value returned by the execution of the <code>opcmon</code> command. This is similar to the <code>PROGRAM</code> expression but a command is not directly carried out. An external command previously triggered by the <code>ExecuteCommand</code> object must provide the monitor value. The default value is <code>DynEXTERNAL (opcmon DynExternal=10)</code></p> <p>Examples: <code>EXTERNAL</code> <code>EXTERNAL\testmon</code></p> • <code>WBEM\namespace\class name\property name</code> <p>WMI interface (not supported on UNIX nodes). Get access to WBEM values. Namespace, class name and property name are strings as specified in the current monitor configuration for WBEM.</p>

Policy Method:	SourceEx
	<p>Example: Wbem\ROOT\CIMV2\Win32_PerfRawData_PerfDisk_LogicalDisk\DiskReadBytesPersec</p> <ul style="list-style-type: none"> • CODA\data source\collection\metric name <p>Query a metric from the embedded performance component. Data source, collection and metric name are strings as specified in the monitor configuration for the embedded performance component. Currently if the data source is empty, the string Coda will be used.</p> <p>Example: CODA\CPU\BYCPU_CPU_TOTAL_UTIL</p> <p>You can view a list of available metrics in the <i>HP Performance Agent Dictionary of Operating System Performance Metrics</i> which is available at HP Software Product Manuals. (Select the product Performance Agent, the required version, OS, and language.)</p> <div style="border: 1px solid gray; padding: 5px; background-color: #f0f0f0;"> <p>Note: In Perl, the backslash character '\' is an escape code. A backslash is only introduced in a string when preceded by another backslash. Because of this, tokens in expressions need to be separated by quadruple backslashes '\\\\'. Example for Perl: my \$TestSource = \$Policy->SourceEx ("PROGRAM\\\\/tmp/script.sh\\\\testmon");</p> </div>

Policy Method	SourceExTimeout
Parameter:	<i>seconds</i> (integer)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	Policy.SourceExTimeout = <i>seconds</i>
Perl Syntax:	\$Policy->SourceExTimeout (<i>seconds</i>);
Description:	Specifies the maximum amount of time, in seconds, the SourceEx and SourceCollection methods will wait before a value is returned. Default is 30 seconds.

Policy Method:	Execute
Parameter:	<i>command</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	Policy.Execute (" <i>command</i> ")
Perl Syntax:	\$Policy->Execute (" <i>command</i> ");

Policy Method: Execute	
Description:	Run the specified command asynchronously. The command is executed in the context of agent security, so could be run as Local System or any other user-selected user to run the agent. The method will return immediately. See the ExecuteCommand method Command for more information about how to indicate commands.

Policy Method: Output	
Parameter:	<i>string</i>
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>Policy.Output ("string")</code>
Perl Syntax:	<code>\$Policy->Output ("string");</code>
Description:	Appends the string to the annotation field of the event sent to the Event Browser in response to the success or failure of a scheduled task. This method is valid only for scheduled task policies.

Policy Method: ExecuteEx	
Parameter:	<i>command</i> (string)
Return Type:	VB Script: BSTR Perl: string
VB Script Syntax:	<code>Policy.ExecuteEx ("command")</code>
Perl Syntax:	<code>\$Policy->ExecuteEx ("command");</code>

Policy Method: <code>ExecuteEx</code>	
Description:	<p>Run the specified command synchronously and wait for it to complete before returning the output of the command.</p> <ul style="list-style-type: none"> • Security. The command is executed in the context of agent security, so could be run as Local System or any other user-selected user to run the agent. • Return values. If the command is successful, STDOUT is returned. If the command is not successful (return value non-zero), the string "ERROR:\n" followed by STDERR will be returned. <p>To handle non-zero return values, run ExecuteEx in an eval function and then check the result, for example for the string ERROR.</p> <p>Perl script example:</p> <pre>eval '\$ReturnText = \$ExecuteCommand->ExecuteEx()'; \$returnText = \$? if \$?;</pre> <ul style="list-style-type: none"> • Paths. You must use complete paths or ensure that any needed path is included in the PATH variable. <p>Example: <code>dir_con = Policy.ExecuteEx ("cmd /c dir c:\")</code></p>

Policy Method: <code>StoreCollection</code>	
Parameters:	<ul style="list-style-type: none"> • <i>expression</i>: (An embedded performance component metric in the format: <code>CODA\data source\collection\metric name [category]</code>) • <i>sourceobj</i>: (Any valid source object)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>Policy.StoreCollection("expression", sourceobj)</code>
Perl Syntax:	<code>\$Policy->StoreCollection("expression", sourceobj);</code>

Policy Method: StoreCollection	
Category Type:	<p>Describes available category types.</p> <ul style="list-style-type: none"> • UNDEFINED: Ignored • NOTAPPLICABLE: Ignored • ATTRIBUTE: Static definitions or values, such as the OS name, version, release, physical memory, and CPU clock speed. • DELTA: Show the activity during the last interval, such as intervalized counts, rates, and utilizations. • GAUGE: Numeric value that shows the current use or value at the time of the observation, such as the run queue, number of users, and files system space utilization. • COUNTER: Cumulative counts of activity, such as CPU times, physical IOs, paging, network packet counts, and interrupts.
Description:	<p>Stores the source object into the embedded performance component data source identified by the expression. Example:</p> <pre>Policy.StoreCollection "CODA\\DBSPI\\TABLE\\SPACE", Source</pre>

Policy Method: SourceCollection	
Parameters:	<ul style="list-style-type: none"> • <i>expression</i>: An embedded performance component metric in the format: <code>CODA\\data source\\collection\\metric name</code>. • <i>rangeofseconds</i>: The number of seconds for which metrics should be returned. • <i>endtime</i>: End time for <i>rangeofseconds</i>. The format of time is of type DATE for VB Script or a string (format DD/MM/YYYY HH:MM:SS) for Perl. The date is optional.
Return Type:	VB Script: IDispatch object of type "Source" Perl: source object
VB Script Syntax:	<code>Policy.SourceCollection ("expression", rangeofseconds, endtime)</code>
Perl Syntax:	<code>\$Policy->SourceCollection ("expression", rangeofseconds, endtime);</code>
Description:	<p>Returns the source object containing all values collected by the specified embedded performance component metric. For each instance, all metrics collected between the expression "<i>endtime - rangeofseconds</i>" and "<i>rangeofseconds</i>" will be returned. If <i>endtime</i> is 0 (NULL for Perl) it is evaluated with the current time. Example: <code>Policy.SourceCollection ("CODA\\CPU\\BYCPU_CPU_TOTAL_UTIL", 300, 0)</code> The number of seconds specified should usually be less than 3600 (one hour), since retrieving a large number of values takes time and consumes resources.</p>

Source Object

The source object is used to access the current values of the metrics. The source object instances can be created by any method that returns the `source` object.

Source Method: Value	
Parameter:	void
Return Type:	VB Script: variant (This is the default method for the Source object.) Perl: string
VB Script Syntax:	<code>Sourceobj.Value ()</code>
Perl Syntax:	<code>\$Sourceobj->Value () ;</code>
Description:	Current instance value if the option <i>Process each instance separately</i> is selected in the policy's processing options.

Source Method: Name	
Parameter:	void
Return Type:	VB Script: BSTR Perl: string
VB Script Syntax:	<code>Sourceobj.Name ()</code>
Perl Syntax:	<code>\$Sourceobj->Name () ;</code>
Description:	Returns the name of the current instance if option <i>Process each instance separately</i> is selected in the processing options of the measurement threshold policy.

Source Method: InstanceCount	
Parameter:	void
Return Type:	VB Script: Int, Perl: integer
VB Script Syntax:	<code>Sourceobj.InstanceCount ()</code>
Perl Syntax:	<code>\$Sourceobj->InstanceCount () ;</code>
Description:	Returns the number of instances that the source has.

Source Method: Count	
Parameter:	void
Return Type:	VB Script: Int Perl: integer

Source Method: Count	
VB Script Syntax:	<code>Sourceobj.Count ()</code>
Perl Syntax:	<code>\$Sourceobj->Count () ;</code>
Description:	Same as InstanceCount. This parameter exists to provide backwards compatibility.

Source Method: Item	
Parameter:	<i>index</i>
Return Type:	VB Script: IDispatch object of type "Source" Perl: source object
VB Script Syntax:	<code>Sourceobj.Item (index)</code>
Perl Syntax:	<code>\$Sourceobj->Item (index) ;</code>
Description:	Access to the instance defined by the index. The index is a number from 0 to InstanceCount - 1. The returned source object can be extracted using the Value and Name methods. This parameter exists to provide backwards compatibility.

Source Method: ValueOf	
Parameter:	<i>index</i> (integer)
Return Type:	VB Script: variant Perl: string
VB Script Syntax:	<code>Sourceobj.ValueOf (index)</code>
Perl Syntax:	<code>\$Sourceobj->ValueOf (index) ;</code>
Description:	Direct access to the value of the instance defined by the index. This method is useful for looping over all instances, if the option <i>Process all instances once</i> is defined. The index is a number from 0 to InstanceCount - 1.

Source Method: NameOf	
Parameter:	<i>index</i> (integer)
Return Type:	VB Script: BSTR Perl: string
VB Script Syntax:	<code>Sourceobj.NameOf (index)</code>
Perl Syntax:	<code>\$Sourceobj->NameOf (index) ;</code>
Description:	Direct access to the name of the instance defined by the index. The index is a number from 0 to InstanceCount - 1. This method is useful for looping over all instances, if the option <i>Process all instances once</i> is selected in the policy's processing options.

Source Method: Top	
Parameter:	<i>number</i>
Return Type:	VB Script: IDispatch object of type "Source" Perl: source object
VB Script Syntax:	<code>Sourceobj.Top(<i>number</i>)</code>
Perl Syntax:	<code>\$Sourceobj->Top(<i>number</i>);</code>
Description:	Returns a new source object instance that contains only the instances with the <number> highest values. For example, if these three instances exist: c: = 90%; d = 80%; e = 40% then Sourceobj.Top(2) returns c: and d:.

Source Method: Bottom	
Parameter:	<i>number</i>
Return Type:	VB Script: IDispatch object of type "Source" Perl: source object
VB Script Syntax:	<code>Sourceobj.Bottom(<i>number</i>)</code>
Perl Syntax:	<code>\$Sourceobj->Bottom(<i>number</i>);</code>
Description:	Returns a new source object instance that contains only the instances with the <number> lowest values. For example, if these three instances exist: c: = 90%; d = 80%; e = 40% then Sourceobj.Bottom(2) will return d: and e:.

Source Method: Exclude	
Parameter:	<i>namepattern, valuepattern</i>
Return Type:	VB Script: IDispatch object of type "Source" Perl: source object
VB Script Syntax:	<code>Sourceobj.Exclude("namepattern", "valuepattern")</code>
Perl Syntax:	<code>\$Sourceobj->Exclude("namepattern", "valuepattern");</code>
Description:	Returns a new source object instance excluding values specified by the patterns. You can specify two parameters, one for the name of the variable (type, object, and instance) and one for the value. Specify NULL if no matching is required for one argument. Patterns should be valid HP Operations Agent pattern-matching expressions.

Source Method: Include	
Parameter:	<i>namepattern, valuepattern</i>

Source Method: Include	
Return Type:	VB Script: IDispatch object of type "Source" Perl: source object
VB Script Syntax:	<code>Sourceobj.Include ("namepattern", "valuepattern")</code>
Perl Syntax:	<code>\$Sourceobj->Include ("namepattern", "valuepattern");</code>
Description:	Returns a new source object instance including only values specified by the patterns. You can specify two parameters, one for the name of the variable (type, object, and instance) and one for the value. Specify NULL if no matching is required for one argument. Patterns should be valid HP Operations Agent pattern-matching expressions.

Source Method: Time	
Parameter:	void
Return Type:	VB Script: DATE Perl: string (format: DD/MM/YYYY HH:MM:SS)
VB Script Syntax:	<code>Sourceobj.Time ()</code>
Perl Syntax:	<code>\$Sourceobj->Time ();</code>
Description:	Returns the time when the expression was evaluated.

Source Method: TimeOf	
Parameter:	index (integer)
Return Type:	VB Script: DATE Perl: string (format: DD/MM/YYYY HH:MM:SS)
VB Script Syntax:	<code>Source.TimeOf (index)</code>
Perl Syntax:	<code>\$Sourceobj->TimeOf (index);</code>
Description:	Returns the time when the expression was evaluated for a specific instance. The index is a number from 0 to InstanceCount - 1.

Source Method: Add	
Parameter:	<i>instancename, value</i>
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>Sourceobj.Add "instancename:", value</code>
Perl Syntax:	<code>\$Sourceobj->Add ("instancename:", value);</code>

Source Method: Add	
Category Type:	<p>Describes available category types.</p> <ul style="list-style-type: none"> • UNDEFINED: Ignored • NOTAPPLICABLE: Ignored • ATTRIBUTE: Static definitions or values, such as the OS name, version, release, physical memory, and CPU clock speed. • DELTA: Show the activity during the last interval, such as intervalized counts, rates, and utilizations. • GAUGE: Numeric value that shows the current use or value at the time of the observation, such as the run queue, number of users, and files system space utilization. • COUNTER: Cumulative counts of activity, such as CPU times, physical IOs, paging, network packet counts, and interrupts.
Description:	<p>Adds the instance name to the source object and sets the value. If this instance is already part of the source object, the new instance will not be added and the value will be replaced. This method can be used on a newly created object or an object retrieved from any method returning a source object. This method is used to store data into the embedded performance component.</p> <p>VB Script example:</p> <pre>set Sourceobj = Policy.CreateObject ("Ito.OvEpScriptMetric") Sourceobj.Add "a:",10 Sourceobj.Add "b:",25 Policy.StoreCollection "CODA\\floppy \\disk\\space\\\\"gauge", Sourceobj</pre> <p>Perl example:</p> <pre>my \$Sourceobj = new Source; \$Sourceobj->Add("a:",10); \$Sourceobj->Add("b:",25); \$Policy->StoreCollection("CODA\\\\"floppy \\\\"disk\\\\"space\\\\"gauge",\$Sourceobj);</pre>

Source Method: DataAvailable	
Parameter:	void
Return Type:	VB Script: Boolean Perl: integer
VB Script Syntax:	Sourceobj.DataAvailable
Perl Syntax:	\$Sourceobj->Sourceobj.DataAvailable;

Source Method: <code>DataAvailable</code>	
Description:	Returns TRUE if the <code>source</code> object contains any value, otherwise, returns FALSE.

Source Method: <code>ValueOfInstance</code>	
Parameter:	<code>instancename</code>
Return Type:	VB Script: variant Perl: string
VB Script Syntax:	<code>Sourceobj.ValueOfInstance ("instancename")</code>
Perl Syntax:	<code>\$_Sourceobj->ValueOfInstance ("instancename");</code>
Description:	Direct access to the value of the instance defined by the instance name.

Session Object

The Session object can be used to store data and to access it later within the script running at a different interval. The session object can also be used to transfer data from the script to the policy actions using the action variable `<$SESSION(KEY)>`. The Session object is unique for each policy.

Session Method: <code>IsPresent</code>	
Parameter:	<code>key</code>
Return Type:	VB Script: Boolean Perl: integer
VB Script Syntax:	<code>Session.IsPresent ("key")</code>
Perl Syntax:	<code>\$_Session->IsPresent ("key");</code>
Description:	Returns TRUE if a value for <code>key</code> exists. Returns FALSE if no value for <code>key</code> exists. Keys are set with the <code>Session.Value</code> method.

Session Method: <code>Remove</code>	
Parameter:	<code>key</code>
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>Session.Remove ("key")</code>
Perl Syntax:	<code>\$_Session->Remove ("key");</code>
Description:	Removes the key specified from the session object.

Session Method: RemoveAll	
Parameter:	void
Return Type:	VB Script: void Perl: void
VB Script Syntax:	Session.RemoveAll()
Perl Syntax:	\$Session->RemoveAll();
Description:	Removes all keys from the session object.

Session Method: Value	
Parameter:	<i>key</i> <i>value</i> (for Perl only)
Return Type:	VB Script: variant (This is the default method for the Session object.) Perl: string
VB Script Syntax:	for put: Session.Value("key")=value for get: value=Session.Value("key")
Perl Syntax:	for put: \$Session->Value("key", "value"); for get: Value = \$Session->Value("key");
Description:	Gets or puts a value for the defined key.

Rule Object

The Rule object is used to indicate to the policy whether a threshold has been crossed or not. TRUE = threshold crossed, FALSE = threshold not crossed.

In scheduled task policies, the Rule object is used to indicate whether the command has succeeded or failed. TRUE = command succeeded, FALSE = command failed.

Rule Method: Status	
Parameter:	void
Return Type:	VB Script: Boolean Perl: integer
VB Script Syntax:	for put: Rule.Status = <i>boolvalue</i> for get: <i>boolvalue</i> = Rule.Status
Perl Syntax:	for put: \$Rule.Status(<i>boolvalue</i>); for get: <i>boolvalue</i> = \$Rule.Status();
Description:	For measurement threshold policies, puts or gets the value for threshold status. For scheduled task policies, FALSE indicates that the scheduled task failed.

ConsoleMessage Object

The ConsoleMessage object provides a method for sending events directly to the Event Browser. Events sent in this way will not be intercepted by an open message interface policy, but instead will be sent directly to the server (event will go to MSI, if configured). The specified event will be sent to the HP Operations message agent. Multiple uses of the Send method are supported. The same script can then send multiple events to BSM depending on which problem it detects.

Note: You cannot use action variables with the ConsoleMessage object.

ConsoleMessage Method: Application	
Parameter:	<i>application</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.Application = "application"</code>
Perl Syntax:	<code>\$ConsoleMessage->Application("application");</code>
Description:	This optional method sets the content of Application in the event properties of the event sent to the Event Browser.

ConsoleMessage Method: Object	
Parameter:	<i>object</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.Object = "object"</code>
Perl Syntax:	<code>\$ConsoleMessage->Object("object");</code>
Description:	This optional method sets the content of Object in the event properties of the event sent to the Event Browser.

ConsoleMessage Method: MsgText	
Parameter:	<i>msgtext</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.MsgText = "msgtext"</code>
Perl Syntax:	<code>\$ConsoleMessage->MsgText("msgtext");</code>
Description:	This method sets the message text for the event that is sent to the Event Browser.

ConsoleMessage Method: <i>Severity</i>	
Parameter:	<i>severity</i> (valid strings are: Unknown Normal Warning Minor Major Critical)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.Severity = "severity"</code>
Perl Syntax:	<code>\$ConsoleMessage->Severity("severity");</code>
Description:	Sets the severity of the event that is sent. If not specifically set with this method, the default is Normal. If an invalid string is supplied, severity Unknown will be used.

ConsoleMessage Method: <i>MsgGrp</i>	
Parameter:	<i>messagegroup</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.MsgGrp = "messagegroup"</code>
Perl Syntax:	<code>\$ConsoleMessage->MsgGrp("messagegroup");</code>
Description:	Sets the value for the Message Group in event properties of the event sent to the Event Browser. If this method does not supply a value, Misc is used.

ConsoleMessage Method: <i>Node</i>	
Parameter:	<i>nodename</i> (IP address or fully qualified hostname)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.Node = "nodename"</code>
Perl Syntax:	<code>\$ConsoleMessage->Node("nodename");</code>
Description:	Sets the value for Primary Node Name that will be displayed in the event properties of the event sent to the Event Browser. IP addresses and fully qualified hostnames are valid. If this method does not supply a value, the hostname of the system is used by default.

ConsoleMessage Method: <i>ServiceId</i>	
Parameter:	<i>serviceid</i> (string)
Return Type:	VB Script: void Perl: void

ConsoleMessage Method: ServiceId	
VB Script Syntax:	<code>ConsoleMessage.ServiceId = "serviceid"</code>
Perl Syntax:	<code>\$ConsoleMessage->ServiceId("serviceid");</code>
Description:	This optional method sets the Service ID for the event.

ConsoleMessage Method: MessageType	
Parameter:	<i>messagetype</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.MessageType = "messagetype"</code>
Perl Syntax:	<code>\$ConsoleMessage->MessageType("messagetype");</code>
Description:	This optional method sets the value for the message type field of the event properties of the event sent to the Event Browser.

ConsoleMessage Method: MessageKey	
Parameter:	<i>messagekey</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.MessageKey = "messagekey"</code>
Perl Syntax:	<code>\$ConsoleMessage->MessageKey("messagekey");</code>
Description:	This optional methods sets a key for event correlation.

ConsoleMessage Method: AcknowledgeMessageKey	
Parameter:	<i>messagekey</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.AcknowledgeMessageKey = "messagekey"</code>
Perl Syntax:	<code>\$ConsoleMessage->AcknowledgeMessageKey("messagekey");</code>
Description:	This optional method sets the message key to indicate which events are automatically closed in the Event Browser.

ConsoleMessage Method: TroubleTicket	
Parameter:	<i>Booleanvalue</i>
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.TroubleTicket = <i>Booleanvalue</i></code>
Perl Syntax:	<code>\$ConsoleMessage->TroubleTicket (<i>Booleanvalue</i>);</code>
Description:	This optional method specifies if the event is to be sent to a trouble ticket interface. Default is FALSE.

ConsoleMessage Method: Notification	
Parameter:	<i>Booleanvalue</i>
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.Notification = <i>Booleanvalue</i></code>
Perl Syntax:	<code>\$ConsoleMessage->Notification (<i>Booleanvalue</i>);</code>
Description:	This optional method specifies if the event is sent to the notification mechanism. Default is FALSE.

ConsoleMessage Method: AgentMSI	
Parameter:	<i>type</i> (valid strings are: copy divert none)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.AgentMSI = "<i>type</i>"</code>
Perl Syntax:	<code>\$ConsoleMessage->AgentMSI ("<i>type</i>");</code>
Description:	This optional method specifies if the event is to be sent through the message stream interface on the agent. Default (or if string misspelled) is none.

ConsoleMessage Method: ServerMSI	
Parameter:	<i>type</i> (valid strings are: copy divert none)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.ServerMSI = "<i>type</i>"</code>
Perl Syntax:	<code>\$ConsoleMessage->ServerMSI ("<i>type</i>");</code>
Description:	This optional method specifies if event is sent through the event stream interface on the server. Default (or if string misspelled) is none.

ConsoleMessage Method: <i>Send</i>	
Parameter:	void
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ConsoleMessage.Send()</code>
Perl Syntax:	<code>\$ConsoleMessage->Send();</code>
Description:	This method sends the event to the BSM server. The <code>MsgText</code> method must set the message text before using this method. Multiple uses of the <code>Send</code> method are supported. Policy variables will not be expanded.

ExecuteCommand Object

Object used for requesting a command to be run. It starts a command to be run by the HP Operations Agent.

ExecuteCommand Method: <i>Command</i>	
Parameter:	<i>command</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ExecuteCommand.Command = "command"</code>
Perl Syntax:	<code>\$ExecuteCommand->Command("command");</code>
Description:	This mandatory method is the name of the command to run with all necessary parameters. <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Note: For scripts that will run on Windows systems, internal commands such as <code>Copy</code>, <code>Rename</code>, and <code>DIR</code> use a command interpreter that must be started before the command can be run. For commands of this type, the command must be preceded with <code>cmd /k</code>, followed by any other parameters required.</p> </div>

ExecuteCommand Method: <i>KillonTimeout</i>	
Parameter:	<i>seconds</i> (integer)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ExecuteCommand.KillonTimeout = seconds;</code>
Perl Syntax:	<code>\$ExecuteCommand->KillonTimeout(seconds);</code>

ExecuteCommand Method: <i>KillonTimeout</i>	
Description:	This method sets the maximum time, in seconds, that the command will run. The default is unlimited. Valid only with the StartEx method.

ExecuteCommand Method: <i>UserName</i>	
Parameter:	username (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ExecuteCommand.UserName = "username"</code>
Perl Syntax:	<code>\$ExecuteCommand->UserName ("username") ;</code>
Description:	User name under which the command should be run. Optional, default is \$AGENT_USER.

ExecuteCommand Method: <i>Password</i>	
Parameter:	password (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ExecuteCommand.Password = "password"</code>
Perl Syntax:	<code>\$ExecuteCommand->Password ("password") ;</code>

ExecuteCommand Method: Password	
Description:	<p>Password for accessing the specified user account. To prevent the password from being visible in the script, use the following instructions:</p> <ol style="list-style-type: none"> 1. Open a command prompt. 2. Change directory to the agent install directory: <code><install_dir>/bin/<arch>/OpC/install</code> 3. Encrypt your password with the command: <code>opcpwcrpt <yourpassword></code> 4. Use the output string as the password in your script. <p>In some cases it is better not to supply a password.</p> <p>Should I provide the password or not?</p> <p>Executing the command without the password is the easier of the two methods, but it has some restrictions that make it unsuitable in some situations. The lists below show the restrictions and advantages of both methods.</p> <p>Without a password:</p> <ul style="list-style-type: none"> • For Windows systems, resources accessed through the network are not available. • For Windows systems, if a domain user is specified, the agent must be installed on the domain controller that authenticates the user. • For all systems, changed passwords do not invalidate the policy. <p>With a password:</p> <ul style="list-style-type: none"> • For all systems, resources accessed through the network are available. • For all systems, the encrypted password is sent over the network. • For all systems, if the password changes, the policy must be updated and redeployed.

ExecuteCommand Method: Start	
Parameter:	void
Return Type:	VB Script: void Perl: void

ExecuteCommand Method: Start	
VB Script Syntax:	<code>ExecuteCommand.Start()</code>
Perl Syntax:	<code>\$ExecuteCommand->Start();</code>
Description:	Run the command specified by <code>ExecuteCommand.Command</code> and return immediately the control to the script so the next lines can be processed right away.

ExecuteCommand Method: StartEx	
Parameter:	void
Return Type:	VB Script: BSTR Perl: String
VB Script Syntax:	<code>ExecuteCommand.StartEx</code>
Perl Syntax:	<code>\$ExecuteCommand->StartEx();</code>
Description:	<p>Run the command <code>ExecuteCommand.Command</code> and wait until it finishes. Commands can be run synchronously or asynchronously, as needed. Multiple uses of the Start method are supported. This way, the same script can trigger multiple external commands.</p> <p>If the command is successful, STDOUT is returned. If the command is not successful (return value non-zero), the string "ERROR:\n" followed by STDERR will be returned.</p> <p>To handle non-zero return values, run StartEx in an eval function and then check the result, for example for the string ERROR.</p> <p>Perl script example:</p> <pre>eval '\$ReturnText = \$ExecuteCommand->StartEx()'; \$returnText = \$@ if \$@;</pre>


Pattern Matching in Policy Rules

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

HP Operations Agent 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.

Note: In text boxes where pattern-matching expressions are allowed you can click  for a shortcut menu with pattern-matching expressions that can be selected and inserted into the text box.

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
- `<S>` matches one or more white space characters: space, tab and new line characters (" ", \t, \n, \r)
- `<nS>` matches exactly *n* white space characters

Note: On Windows operating systems, a new line consists of two white space characters (\n\r).

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

HP Operations Agent 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	<[<i>pattern</i> ¹] -lt <i>n</i> ² >	<[<#>] -lt 5> matches every number less than 5
Less than or equal to	<[<i>pattern</i>] -le <i>n</i> >	<[<#>] -le 5> matches 5 and every number less than 5
Greater than	<[<i>pattern</i>] -gt <i>n</i> >	<[<#>] -gt 5> matches every number greater than 5
Greater than or equal to	<[<i>pattern</i>] -ge <i>n</i> >	<[<#>] -ge 5> matches 5 and every number greater than 5
Equal to	<[<i>pattern</i>] -eq <i>n</i> >	<[<#>] -eq 5> matches 5 or 5.0
Not equal to	<[<i>pattern</i>] -ne <i>n</i> >	<[<#>] -ne 5> 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	< <i>n</i> -lt [<i>pattern</i>] -lt <i>n</i> >	<5 -lt [<#>] -lt 10> matches every number between 5 and 10 (but not 5 or 10)

¹This is a match pattern you provide that returns the number to be compared

²This is the value against which you want to test the number returned by the match pattern

Matches numbers that belong to the interval, including the limits	<code>< n -le [pattern] -le n ></code>	<code><5 -le [<#>] -le 10></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>< n -gt [pattern] -gt n ></code>	<code><10 -gt [<#>] -gt 5></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>< n -ge [pattern] -ge n ></code>	<code><10 -ge [<#>] -ge 5></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 HP Operations Agent 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, the word "Error", the error number, and the text are assigned to **complete**.

The second example requires the dollar sign (`$`) at the end to anchor the expression. As mentioned above, patterns without expression anchoring can match any substring within the input line. Therefore, the pattern:

```
<[Error[<#.n><*.msg>]].complete>
```

would be treated as:

```
<*><[Error[<#.n><*.msg>]].complete><*>
```

Patterns are evaluated from left to right, and `<*>` expressions are assigned as few characters as possible. Therefore, without a dollar sign (`$`) to anchor the end of the expression, the `<*.msg>` expression always matches zero characters, and the remainder of the line is matched with the implicit `<*>` expression at the end.

Pattern Matching for Variables

You can 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 a policy variable (for example `<$LOGPATH>`).

`pattern`

Specify a pattern, using HP Operations Agent 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 a policy 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 a policy 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
- Category
- Application
- Object
- Title

Note: You can use `$MATCH` only once in each message attribute. You cannot use `$MATCH` recursively.

Example

A policy can read a number of log files. The name of the path of the log file is available in the policy 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.

Chapter 4

Assignments and Tuning

A management template provides a complete management solution for an application or service. To start monitoring an application or service, you must assign and deploy the appropriate management template to instances of the CIs comprising the application or service. Users who have not purchased the HP Monitoring Automation for Composite Applications add-on license cannot create management templates, but should use the same process and assign all required aspects individually to the CIs to be monitored and deploy these instead. Management templates, aspects and policy templates are called configuration objects (COs).

Tip: It is also possible to directly assign policy templates, but to obtain a more flexible monitoring solution that is easier to maintain HP recommends using management templates or aspects.

Assignment identifies which instance of a CI is to be monitored against the values defined for the corresponding CI type referenced in a management template or aspect.

Note: If you are using the auto-assignment feature, management templates or aspects may already be assigned automatically to some of the CI instances.

Before starting the monitoring process, you may want to tune the values against which the CIs are monitored.

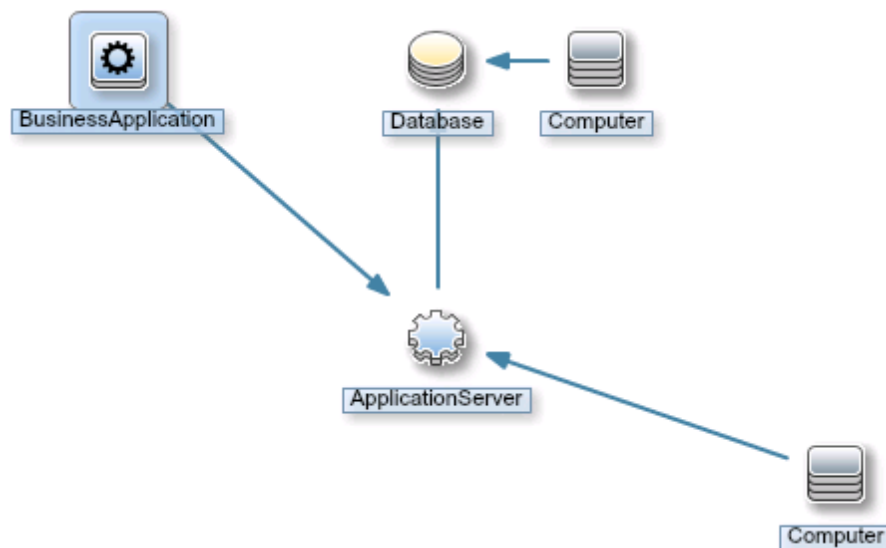
While the monitoring process is active, you can manage deployment jobs in the Deployment Jobs screen. For more information, see "[Deployment Jobs](#)" on page 383.

Learn More

Manual Assignments

Each management template is designed using a topology view, which selects all the CIs for a particular application or service from the BSM Run-time Service Model (RTSM). A topology view selects the CIs based on their CI type and their relations with other CIs of other types. One CI type in the topology view is the management template's root CI type. A management template can only be assigned to CIs of a CI type corresponding to its root CI type or a subtype thereof.

For example, the following graphic shows a topology view that selects CIs of the type Business Application, and related CIs of the types Application Server, Database, and Computer. A management template with the root CI type Business Application can only be assigned to CIs of the type Business Application (or a subtype), but would also monitor other CIs in the view.



Depending on the configuration of a management template, you may be able to define values for various parameters when you assign the management template to a CI. Parameters may give you the opportunity to customize monitoring behavior (for example, to define the monitoring interval), or to provide values that are required to enable monitoring (for example, user names and passwords).

When you assign and deploy a management template to a CI, Operations Management identifies the CI instance you want to monitor with the management template or aspect, and deploys the monitoring configuration to the relevant HP Operations Agents.

After Operations Management deploys the monitoring configuration, you can change the parameter values for that assignment to tune the monitoring behavior. When you tune parameter values, Operations Management sends just the new parameter values to the relevant HP Operations Agents.

You can disable assignments if it is necessary to stop monitoring the CI temporarily. Alternatively, if you no longer want to monitor a CI with a particular management template, you can delete the assignment. When you delete an assignment, Operations Management removes the monitoring configuration from the relevant HP Operations Agents.

Automatic Assignments

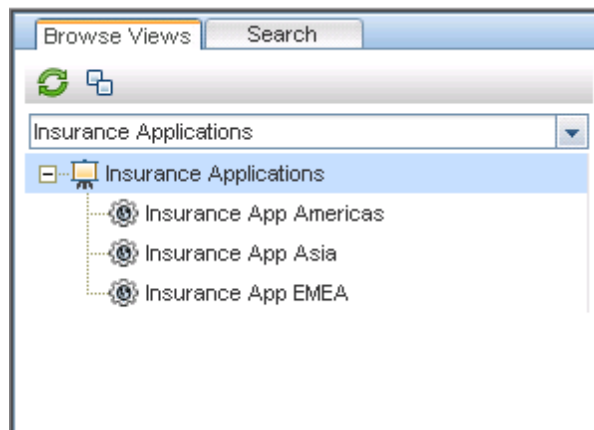
A view is a query that selects the CIs based on their CI type and their relations with other CIs. When you create a management template, you identify a view and root CI for auto-assignment. Whenever a CI corresponding to the root CI type is discovered, the auto-assignment process dynamically assigns the management template to that CI.

For example, you could create a view that selects a CI of a type called Insurance Application and identify it in a number of management templates. Operations Management automatically assigns those management templates to all new Insurance Application CIs when they appear in that view.

If the management template is designed to monitor related CIs, Operations Management will assign the monitoring configuration to those CIs as well, even if those CIs are not visible in the auto-assignment view, and even if they are added to RTSM after the initial automatic assignment took place.

For example:



- You have a management template called 'Monitor Business Applications'.
- You have a view called 'Insurance Applications', which selects some Business Application CIs from RTSM according to specific criteria.






- The management template 'Monitor Business Applications' is configured with the view 'Insurance Applications' and the root CI type 'Business Application' for auto-assignment, and also includes monitoring configuration for related CIs of the types Application Server, Database, and Computer.
- A new CI called 'Insurance App Asia 2' is added to RTSM. The CI matches the criteria of the 'Insurance Applications' view, and so Operations Management assigns the 'Monitor Business Applications' management template to the new CI.
- Later new CIs of the type Application Server, Database, and Computer are added to RTSM, and are related to 'Insurance App Asia 2'. Operations Management assigns the monitoring configuration from the 'Monitor Business Applications' management template to these new CIs.
- Later 'Insurance App EMEA' is removed from the RTSM, and so the 'Monitor Business Applications' management template is unassigned from 'Insurance App EMEA'.

Tasks

How to Monitor CIs Using a Management Template

1. In the **Browse Views** tab of the View Browser (left pane), select a view that contains the CIs that you want to monitor. The discovered COs matching the CIs in the view are listed in the View Browser. Alternatively, use the Search tab to find a CO.
2. In the list of COs, click the CO that you want to monitor. The Assignments pane shows details of any existing assignments for that CO.
3. If the assignments suit your needs, you can use **Re-Deploy**  to redeploy all or some selected assignments. If you need to create new assignments, click **New Assignment...**  and select the item you want to assign. The Assign and Deploy wizard opens on the Select Configuration Object screen. The screen consists of a list of items that can be assigned to the CI type of the selected CO.
4. In the Select Configuration Object page, click the **Name** of the management template that you want to assign, and, If necessary, Select the **Version** of the management template that you

want to assign.


5. Click **Next** to move to the Parameter page.
6. In the Parameter page, specify a value for each parameter:
 - a. *Optional.* By default, the list shows only mandatory parameters. To see all parameters, click the  button. You can also click the  button to see expert parameters.
 - b. Select a parameter in the list, and then click the  button.
 - For standard parameters, the Edit Parameter dialog box opens.
Click **Value**, specify the value, and then click **OK**.
 - For instance parameters, the Edit Instance Parameter dialog box opens.
Add instance values, and then for each instance value, specify dependent parameter values. After you specify the instances and dependent parameter values, click **OK**.

Click **Next** to move to the Configure Options screen.

7. *Optional.* In the Configure Options page, if you do not want to enable the assignment immediately, clear the **Enable Assigned Objects** check box. You can then enable the assignment later using the Assignments & Tuning manager.
8. Click **Finish**. If **Enable Assigned Objects** was checked, the aspects in the management template are assigned to and deployed on the selected CI, as notified by the system. Click **OK** to close the notification.


Operations Management creates deployment jobs to transfer the monitoring configuration to the nodes. After a policy template has been deployed, the BSM server specified in the **Default Virtual Gateway Server for Data Collectors URL** infrastructure setting becomes the owner of the policy on the node.

How to Automatically Assign Management Templates or Aspects

1. Go to the Assignments & Tuning screen.
2. In the drop-down list at the top of the **Browse Views** tab of the View Browser (left pane), select the view for which you want to configure auto-assignment. The view and the first level of assigned COs are shown in the View Browser.
3. Select the view itself, which is the top level item labeled  <view name>. The list of assignments (at the top of the right-hand pane) now shows the auto-assignments for the view, as indicated by the header **Auto-Assignments**.

Note: Make sure that the view you selected for auto-assignment contains the root CI type of the management template or, in case an aspect is auto-assigned, the CI type of the aspect.

It is not necessary for the view to contain all CI types of the aspects contained in a management template to be auto-assigned.

4. Click **New Assignment...**  in the toolbar of the list of auto-assignments and select the appropriate option. The Assign and Deploy Wizard is shown.



5. In the Select Configuration Object page, click the **Name** of the management template or aspect that you want to automatically assign.

The list shows only the management templates that have a root CI type that appears in the view that you selected or, in case an aspect is auto-assigned, compatible aspects.

6. Select the **Version** of the management template or aspect that you want to assign.

Click **Next**.

7. In the Parameter page, specify a value for each parameter:

- a. *Optional.* By default, the list shows only mandatory parameters. To see all parameters, click the  button. You can also click the  button to see expert parameters.

- b. Select a parameter in the list, and then click the  button.

- For standard parameters, the Edit Parameter dialog box opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the Edit Instance Parameter dialog box opens.

Add instance values, and then for each instance value, specify dependent parameter values. After you specify the instances and dependent parameter values, click **OK**.




In the Parameter page, click **Next**.

8. *Optional.* In the Configure Options page, if you do not want to enable the assignment immediately, clear the **Enable Assigned Objects** check box. You can then enable the assignment later.

9. Click **Finish**. The management template or aspect is added to the list of auto-assignments.


Operations Management creates deployment jobs to transfer the monitoring configuration to the nodes. After a policy template has been deployed, the BSM server specified in the **Default Virtual Gateway Server for Data Collectors URL** infrastructure setting becomes the owner of the policy on the node.

How to Tune Parameter Values for Existing Assignments




1. In the Browse Views tab, select a view that contains the CI for which you want to tune parameters. Alternatively, use the Search tab to find a CI.
2. In the list of CIs, click a CI. The Assignments pane shows details of any existing direct or indirect assignments for that CI.
3. Click the assignment for which you want to tune parameters. The Details of Assignment pane shows the current parameter values.
4. In the Assignments pane, click the  button. The Tune Assignment dialog box opens.
5. Change the parameters:
 - a. *Optional.* By default, the list shows only mandatory parameters. To see all parameters, click the  button.
 - b. Select a parameter in the list, and then click the  button.

- For standard parameters, the Edit Parameter dialog box opens.
Click **Value**, specify the value, and then click **OK**.
 - For instance parameters, the Edit Instance Parameter dialog box opens.
Change the instance values if necessary, and then for each instance value, change dependent parameter values. After you change the instances and dependent parameter values, click **OK**.
6. In the Details of Assignment dialog box, click **OK**. Operations Management sends the new parameter values to the relevant HP Operations Agents.

How to Display a Report for a CI

1. Select a CI and choose one of the available reports from the  menu. The following CI-related reports are available:
 - **CI Configuration Report:** Describes how the selected CI is monitored.
 - **CI Configuration Report for all CIs in view:** Describes how all the CIs in the selected view are monitored.
 - **Comparison Report:** Compares the monitoring configuration of a selected CI with the monitoring configuration of all CIs (from same type) in a view.
 - **Assignment Report:** Shows to which Management Template or Aspect the selected CI is assigned. The preconfigured report for the selected CI is displayed. An Assignment Report is only available when a Management Template or Aspect assignment is selected in the Assignments (right) pane.

The preconfigured report for the selected CI is displayed.

You can use the **Expand** () and **Collapse** () buttons to expand or collapse the assigned CI information. The **Show** () button toggles between displaying all values or only the customized values.


UI Reference









Assign and Deploy Wizard

—Select Configuration Object Screen

UI Element	Description
List of Configuration Objects	<p>List of configuration objects (COs) that can be assigned to the selected CI instances. COs are management templates, aspects, and policy templates.</p> <p>The List of Configuration Objects has the following columns:</p> <p>Name The name of the CO.</p> <p>Version The version of the CO. By default, the latest version is listed. To assign a different version, select the desired version from the drop-down list before leaving the screen.</p> <p>Description A description of the CO.</p>
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.

—Parameter Screen

UI Element	Description
Parameter List	<p>Lists all parameters in the management template, aspect or policy template you are assigning to the configuration object.</p> <p>The toolbar provides the following controls:</p> <p> Edit: Open a dialog box that enables you to specify the value of the selected parameter for this assignment.</p> <ul style="list-style-type: none"> • For standard parameters, the Edit Parameter dialog box opens. <ul style="list-style-type: none"> ▪ If you select Value you must specify or select a value in the range that is valid for the parameter. The value you specify overrides any default values defined in the policy template, aspect, or management template. ▪ Select Use Default Value if you want to use the default value defined in the policy template, aspect, or management template.

UI Element	Description								
	<p>Click OK to apply the values and close the Edit Parameter dialog box, or Cancel to close the dialog box without making changes.</p> <ul style="list-style-type: none"> For instance parameters, the Edit Instance Parameter dialog box opens. For details, see the UI Reference section for the Edit Instance Parameter dialog box. <p> Show Only Mandatory Parameters: Show or hide optional parameters in the table of parameters.</p> <p> Show Expert Parameters: Show or hide expert parameters in the table of parameters.</p> <p> Sort According to UI Order: Sort the list of parameters according to their UI order values (lowest to highest).</p> <p>The parameter list has the following columns:</p> <table border="0"> <tr> <td data-bbox="573 932 743 1031">Target (Management Template only)</td> <td data-bbox="773 932 1295 959">The CI type of the aspect using the parameter.</td> </tr> <tr> <td data-bbox="573 1056 743 1155">Defined In (Management Template only)</td> <td data-bbox="773 1056 1268 1119">The management template, aspect or policy template in which the parameter is defined.</td> </tr> <tr> <td data-bbox="573 1180 646 1207">Name</td> <td data-bbox="773 1180 1081 1207">The name of the parameter.</td> </tr> <tr> <td data-bbox="573 1232 646 1260">Value</td> <td data-bbox="773 1232 1333 1295">The value for this parameter in this assignment. If the value is dimmed, it is the default value.</td> </tr> </table> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String <p>If the icon is dimmed, the value is read-only.</p> <p>If the invalid icon appears () , the parameter is mandatory, and you need to specify a value.</p> <p>Description A description of the parameter.</p>	Target (Management Template only)	The CI type of the aspect using the parameter.	Defined In (Management Template only)	The management template, aspect or policy template in which the parameter is defined.	Name	The name of the parameter.	Value	The value for this parameter in this assignment. If the value is dimmed, it is the default value.
Target (Management Template only)	The CI type of the aspect using the parameter.								
Defined In (Management Template only)	The management template, aspect or policy template in which the parameter is defined.								
Name	The name of the parameter.								
Value	The value for this parameter in this assignment. If the value is dimmed, it is the default value.								








UI Element	Description
Back	Move back to the previous screen.
Next	Move on to the next screen.
Finish	Accept the values in all screens and creates the item.
Cancel	Close the wizard/dialog box without creating/updating the item.
Help	Open the relevant help in a new browser window.













—Configure Options Screen






UI Element	Description						
List of Objects	<p>Lists the management templates, aspects, or policy templates that you are assigning to the selected configuration object.</p> <p>The list of objects has the following columns:</p> <table border="0"> <tr> <td style="padding-right: 20px;">Name</td> <td>Name of the management template, aspect, or policy template.</td> </tr> <tr> <td>Enable Assigned Objects</td> <td>If the checkbox is checked, the assignment is carried out immediately at deployment.</td> </tr> <tr> <td></td> <td>If you prefer to carry out the assignment manually after deployment, uncheck the checkbox.</td> </tr> </table>	Name	Name of the management template, aspect, or policy template.	Enable Assigned Objects	If the checkbox is checked, the assignment is carried out immediately at deployment.		If you prefer to carry out the assignment manually after deployment, uncheck the checkbox.
Name	Name of the management template, aspect, or policy template.						
Enable Assigned Objects	If the checkbox is checked, the assignment is carried out immediately at deployment.						
	If you prefer to carry out the assignment manually after deployment, uncheck the checkbox.						
Back	Move back to the previous screen.						
Next	Move on to the next screen.						
Finish	Accept the values in all screens and creates the item.						
Cancel	Close the wizard/dialog box without creating/updating the item.						
Help	Open the relevant help in a new browser window.						






Assignments/Auto-Assignments/Parent Direct Assignments Panes

UI Element	Description
List of Assignments	<p>Lists all management templates and aspects assigned to the item selected in the View Browser pane:</p> <p>If you select a CI in the View Browser, the list of assignments shows the management templates and aspects assigned to it. Note the following:</p> <ul style="list-style-type: none"> • The list of assignments itself has no header. • If you select an assigned management template or aspect in the list of assignments, the list of assigned parameters, which is


UI Element	Description
	<p>documented below, appears underneath the assignment list.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p>Note: Only parameters that can be resolved for the discovered topology are listed.</p> </div> <ul style="list-style-type: none"> • If you select an aspect that is not at the top level the structure that contains it, you cannot change its assignments unless you remove all assignments from the top level down to the aspect level. The assignments to the top level of the structure in which the selected aspect is contained are listed underneath the list of parameters with the header Parent Direct Assignments. • <i>Advanced license only:</i> If you have an advanced license and select the view in the View Browser, the list of assignments shows its auto-assignments, as indicated by the header Auto-Assignments. • If you have a standard license and select the view in the View Browser, the list of assignments is empty. <p>The toolbar of the list of assignments provides the following controls:</p> <ul style="list-style-type: none">  Refresh: Reload the list of assignments for the selected CI.  New Assignment...: Provides the following options: <ul style="list-style-type: none"> •  Assign Management Template: Opens the Assign and Deploy wizard to assign a management template to the selected CI. •  Assign Aspect: Opens the Assign and Deploy wizard to assign an aspect to the selected CI. •  Assign Policy Template: Opens the Assign and Deploy wizard to assign a policy template to the selected CI.  Edit Assignment: Opens the Tune Assignment Dialog Box to set parameter values assigned to the management template or aspect to a deployment-level value, which overrides any management template-level, aspect-level and policy template-level values.  Delete Assignment: Deletes the assignment of a management template, aspect, or policy template.









UI Element	Description
	<p>Operations Management removes the monitoring configuration from the relevant HP Operations Agents.</p> <p> Enable Assignment: Starts or resumes monitoring the selected CI with the management template, aspect, or policy template.</p> <p> Disable Assignment: Pauses monitoring the selected CI with the specified management template, aspect, or policy template. You can restart monitoring by simply clicking Enable Assignment , as Operations Management does not remove the monitoring configuration from the relevant HP Operations Agents.</p> <p> (If CI is selected in View Browser only)</p> <p>Re-deploy... Provides the following options:</p> <ul style="list-style-type: none">  Re-Deploy All: Redeploy all listed assignments for the CI selected in the View Browser, independent of which assignments are selected.  Re-deploy Selected Assignment(s): Redeploy the selected assignments only for the CI selected in the View Browser. <p> Show/Hide Template Assignments: Switches between showing and hiding template assignments for the selected CI.</p> <p> Show/Hide Only Assignments to This Node: Switches between showing and hiding assignments to the selected CI on the related node.</p> <p> Generate Report: Report menu for the available CI-related reports:</p> <ul style="list-style-type: none">  Generate CI Configuration Report: Describes how the selected CI is monitored.  Generate CI Configuration Report for all CIs in view: Describes how all the CIs in the selected view are monitored.  Generate Comparison Report: Compares the monitoring configuration of a selected CI with the monitoring configuration of all CIs (from same type) in a view.






UI Element	Description
	<ul style="list-style-type: none">  Generate Assignment Report: Shows to which CIs a selected Management Template or Aspect is assigned. The preconfigured report for the selected CI is displayed. An Assignment Report is only available when a Management Template or Aspect assignment is selected in the Assignments (right) pane. <p>  Help: Open the relevant help in a new browser window. </p> <p>The list of assignments has the following columns:</p> <p>D <input checked="" type="checkbox"/> indicates that the aspect or policy template is assigned directly to the selected CI. <input type="checkbox"/> indicates it is assigned indirectly through an aspect in a management template assigned to the CI.</p> <p>Name The name of the assigned management template, aspect, or policy template.</p> <p>Description A description of the assigned management template, aspect, or policy template.</p> <p>Version The version of the management template, aspect, or policy template that is currently assigned to the CI.</p> <p>Enabled <input checked="" type="checkbox"/> indicates that the assignment is enabled, <input type="checkbox"/> indicates it is disabled.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: When an assignment is disabled, monitoring is paused.</p> </div>
List of Assigned Parameters	<p>Appears when a management template or aspect is selected in the list of assignments.</p> <p>The toolbar provides the following controls:</p> <p>  Show Only Mandatory Parameters: Shows or hides optional parameters in the table of parameters. </p> <p>  Show Expert Parameters: Shows or hides expert parameters in the table of parameters. </p> <p>  Sort According to UI Order: Sorts the list of parameters according to their UI order values (lowest to highest). </p>

UI Element	Description
	<p>The list has the following columns:</p> <p>Name The name of the parameter.</p> <p>Value Parameter value.</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none"> •  Enumeration (of several options) •  Number •  Password •  String <p>Note the following:</p> <ul style="list-style-type: none"> • If the value is dimmed, the listed value is the default value. • If the icon is dimmed, the value is read-only. • If the invalid icon appears () , the parameter is mandatory but has no value. You must specify a value before continuing. <p>Description A description of the parameter.</p>
<p>List of Parent Direct Assignments</p> <p>(Only if an indirect assignment is selected in the list of assignments)</p>	<p>The assignments to the top level of the structure in which the selected aspect is contained are listed underneath the list of parameters with the header Parent Direct Assignments.</p> <p>If you select an aspect that is not at the top level the structure that contains it, you cannot change its assignments unless you remove all assignments from the top level down to the aspect level.</p>

Edit Instance Parameter Dialog

UI Element	
<p>Instance Values List</p>	<p>The toolbar provides the following controls:</p> <p> Create Instance Parameter: Open the Edit Parameter Dialog Box. To create a new value, select Value and specify a value in the text box. Click OK to close the dialog box and add the new value to the Instance Values list, or click Cancel to close the dialog box without making changes.</p>



UI Element									
	<div style="display: flex; flex-direction: column; gap: 10px;"> <div style="display: flex; align-items: flex-start;">  <div> <p>Edit Instance Parameter: Open the Edit Parameter Dialog Box. To change the instance value, edit the value in the text box. Click OK to close the dialog box and replace the value in the Instance Value list with the new value, or click Cancel to close the dialog box without making changes.</p> </div> </div> <div style="display: flex; align-items: flex-start;">  <div> <p>Delete Instance Parameter: Delete the selected instance value.</p> </div> </div> <div style="display: flex; align-items: flex-start;">  <div> <p>Move Up: Move the selected instance value up in the list.</p> </div> </div> <div style="display: flex; align-items: flex-start;">  <div> <p>Move Down: Move the selected instance value down in the list.</p> </div> </div> </div>								
<p>Dependent Values List</p>	<p>The Dependent Value list lists the dependent values for the instance value selected in the Instance Values list.</p> <p>The toolbar provides the following controls:</p> <div style="display: flex; flex-direction: column; gap: 10px;"> <div style="display: flex; align-items: flex-start;">  <div> <p>Edit... Show the Edit Parameter Dialog Box to specify a value for the parameter.</p> </div> </div> <div style="display: flex; align-items: flex-start;">  <div> <p>Show Only Mandatory Parameters: Show or hide optional parameters.</p> </div> </div> <div style="display: flex; align-items: flex-start;">  <div> <p>Show/Hide Expert Parameters: Show or hide expert parameters.</p> </div> </div> <div style="display: flex; align-items: flex-start;">  <div> <p>Sort According to UI Order: Sort the list of dependent values according to the order as shown in the Operations Management console.</p> </div> </div> </div> <p>The list has the following columns:</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Defined In</td> <td>Policy template containing the definition of the value.</td> </tr> <tr> <td>Target CI Type</td> <td>Name of the CI type to which this value applies..</td> </tr> <tr> <td>Name</td> <td>The name of the dependent value.</td> </tr> <tr> <td>Value</td> <td>The value of the dependent value.</td> </tr> </table> <p>If the value is dimmed, it is the default value.</p> <p>An icon represents the type of parameter value, which can be one of the following:</p>	Defined In	Policy template containing the definition of the value.	Target CI Type	Name of the CI type to which this value applies..	Name	The name of the dependent value.	Value	The value of the dependent value.
Defined In	Policy template containing the definition of the value.								
Target CI Type	Name of the CI type to which this value applies..								
Name	The name of the dependent value.								
Value	The value of the dependent value.								








UI Element	
	<ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String <p>If the icon is dimmed, the value is read-only.</p> <p>If the invalid icon appears () when you select the value, the value is mandatory needs to be specified.</p> <p>Description A description of the dependent value.</p>
OK	<p>Add all selected aspects as nested aspects and close the dialog box.</p> <p>You can select multiple items by holding down the Ctrl or Shift key while selecting them.</p>
Cancel	<p>Close the dialog box without making changes.</p>

Edit Parameter Dialog Box

UI Element	Description
Value	Enables you to set a specific default value for the parameter in this assignment.
Use Default Value	Enables you to use the default value of the parameter. The default value can be defined in a policy template, aspect, or management template.
OK	Accept the changes and close the dialog box.
Cancel	Close the dialog box without making changes.



Tune Assignment dialog box

UI Element	Description
List of Parameters	<p>Lists the parameters for this assignment.</p> <p>The toolbar provides the following controls:</p> <ul style="list-style-type: none">  Edit... Show the Edit Parameter Dialog Box to specify a value for the parameter.  Show Only Mandatory Parameters: Show or hide optional parameters.

UI Element	Description
	<p> Show/Hide Expert Parameters: Show or hide expert parameters.</p> <p> Sort According to UI Order: Sort the list of dependent values according to the order as shown in the Operations Management console.</p> <p>The list of parameters has the following columns:</p> <p>Defined In Policy template containing the definition of the value.</p> <p>Target CI Type Name of the CI type to which this value applies..</p> <p>Name The name of the dependent value.</p> <p>Value The value of the dependent value.</p> <p>If the value is dimmed, it is the default value.</p> <p>An icon represents the type of parameter value, which can be one of the following:</p> <ul style="list-style-type: none">  Enumeration (of several options)  Number  Password  String <p>If the icon is dimmed, the value is read-only.</p> <p>If the invalid icon appears () when you select the value, the value is mandatory needs to be specified.</p> <p>Description A description of the dependent value.</p>
OK	Accept the changes and close the dialog box.
Cancel	Close the dialog box without making changes.

View Browser

UI Element	Description
Browse Views Tab	<p>Select a view in the drop-down list. The view and the CIs with CI types occurring in the selected view are listed as a browser in the area below the list.</p> <p>You can use the browser to take the following actions:</p> <ul style="list-style-type: none"> Select the view to list the auto-assignments for the view in the

UI Element	Description				
	<p>Assignments pane.</p> <ul style="list-style-type: none"> • Select a CI to list the management templates and aspects assigned to the CI in the Assignments pane. Hover the mouse over a CI to see the name of the CI followed by its CI type in parentheses. • Expand a CI to see the values of the CI attributes available for the CI. Hover the mouse over a CI attribute to see the value of the CI attribute followed by its attribute type in parentheses. • Select a CI attribute to list the management templates and aspects assigned to the CI attribute in the Assignments pane. • Right-click a CI or CI attribute to get a menu of actions for the CI. <p>The toolbar provides the following controls:</p> <p> Refresh: Refresh the view browser.</p> <p> Clear All: Unselect any selection in the view browser.</p>				
Search Tab	<p>Specify a string in the Name box, and click Search to search for a View, CI, or CI attribute value with the specified string in its name.</p> <p>The search results table has the following columns:</p> <table border="0"> <tr> <td data-bbox="573 1073 649 1104">Name</td> <td data-bbox="773 1073 1352 1136">The name of the View, CI, or CI attribute value with the specified string in its name.</td> </tr> <tr> <td data-bbox="573 1163 638 1194">Type</td> <td data-bbox="773 1163 1338 1226">The CI Type of a found CI or the attribute type of a found CI attribute.</td> </tr> </table>	Name	The name of the View, CI, or CI attribute value with the specified string in its name.	Type	The CI Type of a found CI or the attribute type of a found CI attribute.
Name	The name of the View, CI, or CI attribute value with the specified string in its name.				
Type	The CI Type of a found CI or the attribute type of a found CI attribute.				




Chapter 5

Deployment Jobs

Deployment refers to the process of transferring policies, aspects, management templates, and other software from the management server to one or more managed nodes.

Operations Management automatically creates a deployment job whenever you deploy or remove instrumentation, policies or policy groups for a managed node. Use the Deployment Jobs screen to manage pending deployment jobs.

Use the Deployment Jobs screen to ensure if the monitoring process is running as configured. Some examples of tasks:

- Investigate and repair jobs with status  FAILED.
- Investigate and repair jobs job remaining in state  PENDING longer than expected..
- Manually restart jobs with status  SUSPENDED after repairs or other updates.

After correcting problems, you can restart the affected jobs from the Deployment Jobs screen.

Note: The Deployment Jobs screen only lists pending deployment jobs. As soon as a deployment job is completed successfully, it is deleted from the list of pending jobs.


Tasks

How to Restart Deployment Jobs

Select the jobs you want to restart and click **Restart Deployment Jobs** . The state of the selected jobs changes to  RUNNING,  PENDING or  FAILED.

You can select multiple items by holding down the **Ctrl** or **Shift** key while selecting them.

How to Suspend Deployment Jobs

Select the jobs you want to suspend and click **Suspend Deployment Jobs** . The state of the selected jobs changes to  SUSPENDED.

You can select multiple items by holding down the **Ctrl** or **Shift** key while selecting them.


How to Delete Deployment Jobs

Select the jobs you want to delete and click **Delete Deployment Jobs** . The selected deployment jobs are removed from the list.

You can select multiple items by holding down the **Ctrl** or **Shift** key while selecting them.

How to Start Jobs for Delayed Assignments










It is possible to configure delayed deployment of jobs by clearing the **Enable Assigned Objects** checkbox in the Assign and Deploy wizard. To manually start these jobs from the Deployment Jobs

screen, select the delayed jobs you want to start and click **Start Jobs for Undeployed Deployments** . Delayed jobs are started and added to the list of deployment jobs automatically.

You can select multiple items by holding down the **Ctrl** or **Shift** key while selecting them.

UI Reference

Deployment Jobs Screen

UI Element	Description
	Refresh: Reload the list of policy templates.
	Restart Deployment Jobs: Start deployment of the selected deployment jobs.
	Suspend Deployment Jobs: Suspend deployment of the selected deployment jobs.
	Delete Deployment Jobs: Delete the selected deployment jobs.
	Start Jobs for Undeployed Deployments: Start jobs for assignments that have not yet been deployed.
State	Indicates state of the associated deployment job. The possible states are: <ul style="list-style-type: none">  RUNNING  PENDING  SUSPENDED  FAILED
Node	Target system for the deployment job.
Scope	Describes the artifacts included in the deployment job.
Time Created	Time of creation of the deployment job.
Description	Overview of the deployment job. If a deployment job has failed, the description column shows the details of the error or exception.

Chapter 6

Settings for Monitoring Automation

This chapter provides an overview of the settings required for Monitoring Automation including information that helps to configure the Monitoring Automation settings.

The following settings are covered:

- "Infrastructure Settings for Monitoring Automation" below
- "License Settings for Monitoring Automation" on the next page
- "Logging and Tracing for Monitoring Automation" on page 387


Infrastructure Settings for Monitoring Automation

The Infrastructure Settings Manager page for Monitoring Automation page enables you to view and modify the default configuration for Monitoring Automation. The settings displayed on this page determine how Monitoring Automation behaves and performs. Changing settings can affect the performance of both the application itself and the underlying platform. Only users with both the required background knowledge and access permission should attempt to change these settings.

Note: Modified values are displayed in **bold** text. In some cases, the changes you make are not effective immediately. You might have to restart the browser session or a server process.

To Access

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**
2. Select **Applications** and use the list to set the administration context to **Monitoring Automation**

Note: To change an existing or default setting, click the  button behind the setting.

This sections includes:

- "The Auto Assignment Settings contains the available configurations used to customize how Auto Assignment is controlled." below
- "The Proxy Deployment Scripts Settings contains the available configurations used to specify the scripts used to select deployment servers." on the next page
- "The Template Syntax Check Settings contains the available configurations used to control syntax checking of templates." on the next page

Auto Assignment

The Auto Assignment Settings contains the available configurations used to customize how Auto

Assignment is controlled.

The following elements are included in the Auto Assignment Settings pane.

UI Element (A-Z)	Description
Allow automatic deletion of assignments	Allows the deletion of existing assignments if the corresponding CI was deleted.
Enable Auto Assignment	Globally enables or disables Auto Assignment.
Time interval to scan for changed topology	Time interval in minutes to scan for changed topology and perform automatic assignment.
Update existing assignments	Automatically update existing assignments when new CIs are added.

Proxy Deployment Scripts

The Proxy Deployment Scripts Settings contains the available configurations used to specify the scripts used to select deployment servers.

The following elements are included in the Proxy Deployment Scripts Settings pane.

UI Element (A-Z)	Description
Arcsight Script	Groovy script to determine Arcsight Servers for deployment.
Sitescope Script	Groovy script to determine Sitescope Servers for deployment.

Template Syntax Check

The Template Syntax Check Settings contains the available configurations used to control syntax checking of templates.

The following elements are included in the Template Syntax Check Settings pane.

UI Element (A-Z)	Description
Disable template syntax check	Disables syntax check of template contents on save.

License Settings for Monitoring Automation

The License Manager page enables you to add a license from a file.

To Access


Select **Admin > Platform > Setup and Maintenance > License Management**.

Tasks

How to Add a Monitoring Automation for Composite Applications License





1. Find the `Operations Management` licenses folder in the License Management pane. If

necessary, click  to expand the folder or click **Expand All** .

2. If there is an entry called *Monitoring Automation for Composite Applications*, you already have the license installed and you can close the license manager. If there is no such entry, purchase a license from your HP Sales Office to obtain a license file.
3. Place the license file you receive in a location accessible on the server hosting BSM.
4. Click **Add License From File** . The Add License dialog box is displayed, allowing you to browse for the license file in the file system. When the license file is selected, click **Add License**. The license is added to the list of licenses as *Monitoring Automation for Composite Applications*, under *Operations Management*.

UI Reference

License Management Pane

UI Element	Description
	Add License From File: Open the Add License file browser allowing you to select the license file to add.
	Expand all multi-level list entries.
	Collapse all multi-level list entries.
	Open the Choose Columns to Display dialog box. For each column, the dialog contains a checkbox. <ul style="list-style-type: none"> • To be able to see a column, make sure its checkbox is checked. • To hide a column, make sure the checkbox is unchecked.

Logging and Tracing for Monitoring Automation

Logging and Tracing for Monitoring Automation use the same mechanisms as Operations Management, but have specific configuration and log files.

Tasks

How to Enable Logging from the Operations Management Console

To enable logging, log on to BSM and go to the relevant logging configuration application:

1. To enable logging for monitoring automation, go to `http://<hostname>/opr-config-server/logging/logging.html`
2. To enable logging for policy editors, go to `http://<hostname>/opr-pm/logging/logging.html`

How to Configure Logging and Tracing for Monitoring Automation

Monitoring automation is defined in the following logfile configuration files:

```
<HPBSM root directory>\conf\core\Tools\log4j\EJB\opr-webapp.properties  
<HPBSM root directory>\conf\core\Tools\log4j\EJB\opr-config.properties
```

For more information about how to configure and use logging and tracing, see the BSM User Guide, under *Application Administration > Operations Management > Additional Configuration*.

Where to Find the Monitoring Automation Log Files

Monitoring automation logs to the following log files:

```
<HPBSM root directory>\log\EJBContainer\opr-webapp.log  
<HPBSM root directory>\log\EJBContainer\opr-configserver.log
```

Chapter 7

Exporting Configuration Data

You can export configuration data from one system and import it to other systems using the Content manager. The following artifacts must be selected in the Content manager interface:

- **All Configuration Folders**

All aspects, management templates, and their respective versions are automatically included.

- **All Template Versions**

All templates which are not already included in an aspect or management template that is part of the content pack definition are automatically included.

- **All Instrumentation**

All instrumentation not used by a template or aspect are automatically included.

- **All Template Groups**

Note: Exporting and importing assignment information (the aspects, management templates, policy templates on each CI) is not supported.

Chapter 8

Monitored Nodes

Use the Monitored Nodes screen to organize and manage monitored nodes, which are devices in your IT Infrastructure that are monitored by an OM Agent or SiteScope.

The Monitored Nodes screen consists of the following panes:

- **Node Views browser** (left pane)

Each root folder in the browser corresponds to one of the filtering methods mentioned above.

The type of filter created when clicking **New Item** * depends on which root folder is selected when the icon is clicked (see also section *Tasks*).

- **List of monitored nodes** (middle pane)

The list of monitored nodes, filtered according to the filter selected in the Node Views browser.

The following filtering methods can be applied:

- Predefined filters.
- Custom filters, which you can configure to suit your needs.
- Node Collections, which are containers for nodes available in the RTSM. You can configure and use Node Collections to organize your nodes to suit your needs.

Note: Node Collections are modeled in the RTSM as CIs of type `CI Collection`, where the attribute `monitored_by` is set to `OM`.

- **Node details** (right pane)

Details for the node selected in the list of monitored nodes.

To access:

Select **Admin > Operations Management > Setup > Monitored Nodes**.


Tasks

How to Create Custom Filters

1. Select root folder `Custom Node Filter` or one of its subfolders in the Node Views browser.
2. Click the * button. The Create New Custom Node Filter dialog box opens.
3. Enter a unique **Display Name** for the new filter. Optionally, you can enter a description for the filter.
4. Enable the filter criteria entries that you want to apply and enter appropriate values for each selected criteria.
5. Click **OK**. The dialog box is closed and the new node is added to the list of nodes in the Nodes

pane.

How to Create Node Collections

1. Select root folder `Node Collection` or one of its subfolders in the Node Views browser.
2. Click the  button. The Create New Node Collection dialog box opens.
3. Enter the name of the new node collection and a description, if required.
4. If you want the new node collection to be contained within an existing node collection, select the parent collection from within the **Parent Collection** pane.
5. Click **OK**. The dialog box is closed and the new node collection is added to the `Node Collection` folder.

How to Create a New Monitored Node

1. In the **Nodes** pane, click the  button and select the type of node that you want to add to the RTSM, for example, **Generic Node**, **Computer**, **Net Device**, and so on.


The Create New Monitored Node dialog box opens.

2. Define the node by entering appropriate values in the required fields.


Note: You must enter a primary DNS name and an IP address for the new node.

3. Click **OK**. The dialog box is closed and the new node is created and added to the list of nodes.

How to Add a Node to a Node Collection

1. In the Nodes pane, select one or more nodes and click the  button. The Add Node to a Node Collection dialog box opens.
2. Select the node collection to which you want to add the selected nodes as the **Parent Collection**.
3. Click **OK**. The dialog box is closed and the selected nodes are added to the node collection. If you click the node collection in the Node Views browser, the added node is listed in the Nodes pane.




How to Delete a Node from a Node Collection

In the Nodes pane, select one or more nodes and click the  button.

How to Display a Report for a Node





In the Nodes pane, select one node and click the  button.

The preconfigured report for the selected node is displayed. It compares the monitoring configuration of a selected node to the actual state. The report includes detailed information about the related aspects and templates, such as version, and state.






You can use the **Expand** () and **Collapse** () buttons to expand or collapse the aspects and templates information. The **Show** () button toggles between displaying all values or only the customized values.






UI Reference

Node Views Browser



UI Element	Description
	Refresh: Reloads the content of the Node Views browser.
	New Custom Node Filter: <ul style="list-style-type: none"> If the <code>Custom Node Filter</code> root folder or an item in it is selected, this button opens the Create New Custom Node Filter dialog box to create a new custom node filter. If the <code>Node Collection</code> root folder or an item in it is selected, this button opens the Create New Node Collection dialog box to create a new node collection.
	Edit Item: <ul style="list-style-type: none"> If the <code>Custom Node Filter</code> root folder or an item in it is selected, this button opens the Edit Custom Node Filter dialog box to edit the selected custom node filter. If the <code>Node Collection</code> root folder or an item in it is selected, this button opens the Edit Node Collection dialog box to edit the selected node collection.
	Delete Item: Deletes the selected filter or collection.

List of Monitored Nodes

UI Element	Description
	Refresh: Reloads the Nodes list.
	New Node: Opens the Create New Monitored Node dialog box to enable you to create a new node. Types of commonly found nodes are available from the selections in the dropdown menu, for example, <code>Computer - Unix</code> , or <code>Net Device -Router</code> . If no suitable predefined node type is available, select Generic Node .
	Edit Item: Opens a dialog box to edit the selected node.
	Delete Item: Opens a confirmation dialog box asking you whether you are sure you want to delete the selected object. Click Yes to deletes the selected nodes from the RTSM, or No to cancel deletion.
	Add to Node Collection: Opens the Add Node to Node Collection dialog box and enables you to add the selected nodes to a node collection.



UI Element	Description
	Remove from Node Collection: Deletes the selected nodes from the active node collection.
	<p>Open Node Report: Opens the predefined report for the selected node.</p> <p>You can use the Expand () and Collapse () buttons to expand or collapse the aspects and templates information. The Show () button toggles between displaying all values or only the customized values.</p> <p>The preconfigured report for the selected node is displayed. It compares the monitoring configuration of a selected node to the actual state. The report includes detailed information about the related aspects and templates, such as version, and state.</p>
Primary DNS Name	Fully-qualified DNS name of the selected node.
Monitored by	Displays the system type that is currently responsible for monitoring the selected node.
Node Type	Describes the type of node, for example, Window or Unix. When creating a node, select the node type that most accurately describes the node from the options available.
Operating System	Describes the operating system installed on the selected node, for example, Windows Server 2008 (6.1) or LINUX Red Hat EL 5.x (2.6).

Node Details

UI Element	Description
	Collapse the category.
	Expand the category.
Category General	Displays general information about the node selected in the list of monitored nodes.
Category Additional Information	Displays the system type that is currently responsible for monitoring the selected node and the CI type of node.

Create/Edit Monitored Node Dialog Box

UI Element	Description
ID	The system-assigned ID of the node.
Node Type	The CI Type of the node.

UI Element	Description
Primary DNS Name	Fully qualified DNS hostname of the node, which also determines the name of the node as shown in topology views.
List of IP Addresses	<p>All IP addresses of the node.</p> <p>The toolbar provides the following controls:</p> <ul style="list-style-type: none">  New Item: Open the Create New IP Address dialog box used to specify a new IP address and add it to the list.  Delete Item: Remove the selected IP addresses from the list. <p>The list has the following columns:</p> <ul style="list-style-type: none"> IP Address The IP address. DHCP <input checked="" type="checkbox"/> if the IP addresses was assigned by a DHCP server, or empty if it was not. Routing Domain The routing domain for the IP address, or \$(DefaultDomain) if the default domain is used.
Operating System	The operating system of the node.
Processor Architecture	The processor architecture of the node.
Description	A description for the node.
OK	Accept all changes and close the dialog box.
Cancel	Close the dialog box without making any changes.
Help	Open the relevant help in a new browser window.