

HP Business Service Management

For the Windows[®] and Linux operating systems

Software Version: 9.23

Monitoring Automation for HP Operations Manager i Administrator Guide

Document Release Date: December 2013

Software Release Date: December 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/hpsupport>

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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **<http://h20230.www2.hp.com/sc/solutions/index.jsp>**

Contents

Contents	4
Chapter 1: Monitoring	7
Chapter 2: Management Templates and Aspects	9
Configuration Folders	23
Configuring Management Templates	27
Configuring Aspects	58
Viewing Details	92
Chapter 3: Policy Templates	94
Configuring HP ArcSight Logger Policies	108
Configuring ConfigFile Policies	118
Configuring Flexible Management Policies	125
Configuring Log File Entry Policies	139
Configuring Measurement Threshold Policies	163
Configuring Node Info Policies	203
Configuring Open Message Interface Policies	209
Configuring Scheduled Task Policies	229
Configuring Service Auto-Discovery Policies	242
Configuring Service/Process Monitoring Policies	251
Configuring SNMP Interceptor Policies	272
Configuring Windows Event Log Policies	293
Configuring Windows Management Interface Policies	314
Configuring XML File Policies	336
Importing HP SiteScope Templates	364
Developing Instrumentation	375
Policy Objects for Scripts	383
Pattern Matching in Policy Rules	405
Pattern-Matching Details	405
User-Defined Variables in Patterns	409
Pattern Matching for Variables	411

Examples of Pattern Matching in Rule Conditions	412
Chapter 4: Assignments and Tuning	415
Learn More	415
Chapter 5: Automatic Assignment Rules	438
Chapter 6: Deployment Jobs	457
Chapter 7: Settings for Monitoring Automation	460
Infrastructure Settings for Monitoring Automation	460
License Settings for Monitoring Automation	461
Logging and Tracing for Monitoring Automation	462
Chapter 8: Migrating Configuration Data	464
Copying Configurations Between Servers	464
Importing Configuration Data from HP Operations Manager	465
Chapter 9: Connecting HP Operations Agents to HP Operations Manager i	474
Connecting a New HP Operations Agent Installation	474
Connecting an Existing HP Operations Agent Installation	476
Chapter 10: Tools	486
ConfigExchange Command-Line Interface	486
ConfigWsTool Command-Line Interface	497
ConfigExchangeSIS Command-Line Interface	503
HP Operations Manager i and HP Operations Agent Command-Line Interfaces	506
Chapter 11: Monitored Nodes	508
We appreciate your feedback!	521

Chapter 1: Monitoring

This section describes the BSM Monitoring Automation (MA) features.

Tip: User Permissions

The Monitoring Automation user interface resides in the Operations Management administration area, and special user permissions are needed to be able to use each individual view used in the administration manager screens. Make sure you have sufficient permissions to use all views needed to complete your intended task.

Some examples:

- To be able to create a management template, you need permission to use both the Management Template & Aspect and System views.
- To be able to use the Assignment & Tuning manager you need permission to use both the Assignment & Tuning and System views.

If in doubt, or if you experience problems, contact your BSM administrator.

Note: Monitoring Automation Licenses

Monitoring Automation is licensed on 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 415](#).

This part of the guide contains the following chapters:

- **"Configuration Folders" on page 23**

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 and aspects. A management template provides a complete solution for managing 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 94**

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 415**

This chapter describes how to assign management templates, aspects, and policy templates, and tune the default values of the parameters contained in them.

- **"Automatic Assignment Rules" on page 438**

This chapter describes how to configure rules for automatically assigning management templates and aspects.

- **"Deployment Jobs" on page 457**

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 460**

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

- **"Migrating Configuration Data" on page 464**

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 23](#).

- **Management Templates & Aspects Pane**

The *Management Templates & Aspects* 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 27](#). For detailed information about creating and using aspects, see ["Configuring Aspects" on page 58](#).

- **Details Pane**

The *Details* pane (right pane) contains details about the management template or aspect selected in the *Management Templates & Aspects* pane (middle pane). If no management template or aspect is selected, the *Details* 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 92](#).

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 Inventory 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 Assignment 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 & Tuning* screen.


UI Reference
















Assign and Deploy Wizard —Configuration Item

UI Element	Description
	<p>Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none">• Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in.• The search is not case-sensitive.• If a filter is active, click  No Filter to remove the filter and show all items in the list.
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 or aspect:</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.

UI Element	Description
	<ul style="list-style-type: none"> Any CIs of the aspect's assigned CI types that have not been discovered but are flagged as Node Compatible.
Type	The type of configuration item.
Also Show CIs of Type Node (Only Visible for Node-Compatible Items)	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 .





—Required Parameters
















UI Element	Description
Required Parameters List	<p>This step lists all mandatory parameters in the management template that do not yet have a value. As they are mandatory, however, all listed parameters <i>must</i> be given a value before the management template can be deployed.</p> <p>If all required values are specified, you can choose one of the following actions:</p> <ul style="list-style-type: none"> Click Finish to assign the configuration object to the selected CI and close the wizard or dialog. Click Next to go to <i>All Parameters</i>, where you can override the default value of any parameter, including those that are not required. <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: To access step <i>Configure Options</i>, click Next in this step, and Next again in step <i>All Parameters</i>.</p> </div> <p>The toolbar provides the following controls:</p> <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="margin-right: 10px;">  </div> <div> <p>Edit: Specify the value of the selected parameter.</p> <ul style="list-style-type: none"> For standard parameters, the <i>Edit Parameter</i> dialog opens. For instance parameters, the <i>Edit Instance Parameter</i> dialog opens. <p>For details on using the dialogs, see the relevant <i>UI Reference</i> section.</p> </div> </div> <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p>

UI Element	Description												
	<p>The parameter list has the following columns:</p> <table> <tr> <td>Target (Visible Only for Assignments of Management Templates)</td><td>The CI type of the item using the parameter.</td></tr> <tr> <td>Defined In (Visible Only for Assignments of Management Templates)</td><td>The management template, aspect or policy template in which the parameter is defined.</td></tr> <tr> <td>Instance Parameter (Visible Only for Assignments with Instance Parameters)</td><td>The instance parameter the parameter depends on.</td></tr> <tr> <td>Instance (Visible Only for Assignments with Instance Parameters)</td><td>The instance of the parameter.</td></tr> <tr> <td>Name</td><td>The name of the parameter.</td></tr> <tr> <td>Value</td><td> <p>The parameter value for this assignment.</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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value. </td></tr> </table>	Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.	Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.	Instance Parameter (Visible Only for Assignments with Instance Parameters)	The instance parameter the parameter depends on.	Instance (Visible Only for Assignments with Instance Parameters)	The instance of the parameter.	Name	The name of the parameter.	Value	<p>The parameter value for this assignment.</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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.												
Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.												
Instance Parameter (Visible Only for Assignments with Instance Parameters)	The instance parameter the parameter depends on.												
Instance (Visible Only for Assignments with Instance Parameters)	The instance of the parameter.												
Name	The name of the parameter.												
Value	<p>The parameter value for this assignment.</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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value. 												

UI Element	Description
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.

—All Parameters





UI Element	Description
Parameter List	<p>Lists all parameters in the management template, aspect or policy template you are assigning to the configuration item.</p> <p>The toolbar provides the following controls:</p> <div>  <p>Edit: Specify the value of the selected parameter.</p> <ul style="list-style-type: none"> For standard parameters, the <i>Edit Parameter</i> dialog opens. For instance parameters, the <i>Edit Instance Parameter</i> dialog opens. <p>For details on using the dialogs, see the relevant <i>UI Reference</i> section.</p> </div> <div>  <p>Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p> </div> <div>  <p>Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. </div>









UI Element	Description								
	<p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p> <table> <tr> <td>Target (Visible Only for Assignments of Management Templates)</td><td>The CI type of the item using the parameter.</td></tr> <tr> <td>Defined In (Visible Only for Assignments of Management Templates)</td><td>The management template, aspect or policy template in which the parameter is defined.</td></tr> <tr> <td>Name</td><td>The name of the parameter.</td></tr> <tr> <td>Value</td><td> <p>The parameter value for this assignment.</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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value. </td></tr> </table>	Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.	Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.	Name	The name of the parameter.	Value	<p>The parameter value for this assignment.</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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.								
Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.								
Name	The name of the parameter.								
Value	<p>The parameter value for this assignment.</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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value. 								
Back	Moves back to the previous step.								
Next	Moves on to the next step.								
Finish	Accepts the values in all steps and creates the item.								
Cancel	Closes the wizard without creating the item.								
Help	Opens the relevant help in a new browser window.								




—Configure Options






UI Element	Description
Enable Assigned Objects	If you do not want to enable the assignments immediately, clear the Enable Assigned Objects check box. To enable assignments after closing the wizard, use the <i>Assignments & Tuning</i> screen.
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.

Assignments Dialog







UI Element	Description
Assignments Pane	<p>Lists all current assignments of the selected management template, aspect, or policy template.</p> <p>The toolbar provides the following controls:</p> <div>  Refresh: Reloads the list of assignments. </div> <div>  New Assignment: Opens the <i>Assign and Deploy</i> wizard to create a new assignment of the selected item. </div> <div> <p>Note: If a particular management template version or aspect version is selected, the selected version is assigned; otherwise the latest version of the selected item is assigned.</p> </div> <div>  Tune Assignment: Opens the <i>Tune Assignment</i> dialog to set parameter values defined for the selected management template or aspect to a deployment-level value, which overrides any management template-level, aspect-level and policy template-level values. </div> <div>  Delete Assignment: Deletes the selected assignment and removes the monitoring configuration from the relevant HP Operations Agents. </div>





UI Element	Description
	Enable Assignment: Starts or resumes monitoring the target CI.
	Disable Assignment: Pauses monitoring the target CI.
	<p>Note: In contrast to deleting an assignment by using  Delete Assignment, using  Disable Assignment does not result in the monitoring configuration being removed from the relevant HP Operations Agents, allowing you to restart monitoring by simply clicking  Enable Assignment.</p>
	Re-deploy Selected Assignment(s): Redeploys the selected assignments.
	Generate Assignment Report: Shows all CIs to which the item used to create the assignment is currently assigned.
	Get Help: Opens the relevant help in a new browser window.
	The list has the following columns:
D	✓ indicates that the aspect or policy template is assigned directly to the selected CI. — indicates it is assigned indirectly through the assignment of a management template or aspect that contains this aspect or policy template.
Target CI	The name of the CI to which the management template, aspect, or policy template is assigned.
Version	The version of the management template, aspect, or policy template that was used to create the assignment.
Assigned By	The user name of the user who made the assignment.

UI Element	Description				
	<p>Enabled ✓ indicates that the assignment is enabled, — indicates it is disabled.</p> <p>Note: When an assignment is disabled, monitoring is paused.</p>				
Assignment Details Pane	<p>Lists the parameters contained in the assigned item.</p> <p>Note: Only parameters that can be resolved for the target CI are listed.</p> <p>The toolbar provides the following controls:</p> <div>  <p>Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p> </div> <div>  <p>Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. </div> <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p> <table> <tr> <td>Name</td><td>The name of the parameter.</td></tr> <tr> <td>Value</td><td>The parameter value for this assignment.</td></tr> </table> <p>An icon represents the type of parameter value, which can be one of the following:</p>	Name	The name of the parameter.	Value	The parameter value for this assignment.
Name	The name of the parameter.				
Value	The parameter value for this assignment.				








UI Element	Description
	<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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
Close	Closes the dialog.









Configuration Folders Pane

UI Element	Description
	Refresh: Reloads the tree of configuration folders.
	Create Configuration Folder: Opens the <i>Create Folder Dialog</i> to create a new configuration folder, which will be created as a subfolder of the selected folder.
	Edit Item: Opens the <i>Edit Folder Dialog</i> to edit the selected configuration folder.
	Delete Item: Deletes the selected configuration folder. A message box will prompt you to Confirm or Cancel deletion.
	Show Item Properties: Shows the name, description and ID of the selected configuration folder in a message box. Click OK to close the message.
	Search: Opens the <i>Search Dialog</i> to search for folders or items contained in them.

UI Element	Description
	<p>Cut Item: Copies the selected configuration folder and its content to the clipboard.</p> <ul style="list-style-type: none"> The item you 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.
	<p>Paste Item: Pastes the last configuration folder that was cut to the clipboard and its contents as a subfolder to the selected folder.</p>
Drag-and-Drop	You can move configuration folders to a different location in the hierarchy using drag-and-drop.
	<p>Generate Inventory Report: Generates an inventory showing 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. Select a template to show the inventory report.</p>
	<p>Get Help: Opens the relevant help in a new browser window.</p>



Management Templates & Aspects Pane

UI Element	Description
	<p>Refresh: Reloads all management templates and aspects and refreshes the list.</p>
	<p>New: Provides the following options:</p> <ul style="list-style-type: none">  Management Template: Opens the <i>Create/Edit Management Template</i> wizard to create a new management template.  Aspect: Opens the <i>Create/Edit Aspect</i> wizard to create a new aspect.
	<p>Edit Item: Opens the <i>Create/Edit Management Template</i> or <i>Create/Edit Aspect</i> dialog to edit the selected management template or aspect.</p>
	<p>Delete Item: Deletes 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.

UI Element	Description
	<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>
	Update to Latest: Updates the selected management template or aspect and all aspects contained in it to their latest version.
	Copy Item: Copies the selected management template or aspect to the clipboard.
	Cut Item: Cuts the selected management template or aspect to the clipboard.
	Paste Item: Pastes a management template or aspect from the clipboard to the selected configuration folder. When pasting the item, you are prompted to define a name for the item to be pasted; if required, change the suggested name, which is the name of the copied item followed by - Copy. Click OK to accept the name and paste the item.
	<p>Show Assignments List for Selected Item: Opens the <i>Assignments</i> dialog, which shows all assignments of the selected management template or aspect, and allows you to create, edit, delete, activate or deactivate and tune them.</p> <p>Note: If a management template or aspect is selected, the assignments for all versions are listed. If a management template version or an aspect version is selected, only the assignments of the selected version are listed.</p>
	Assign and Deploy Item: Opens the <i>Assign and Deploy</i> wizard, which enables you to assign the selected management template or aspect to a configuration item, and then deploy it.
	Generate Assignment Report: Displays a report listing the CIs to which the selected management template or aspect is assigned in a new browser window.
	Get Help: Opens the relevant help in a new browser window.



Details Pane

—Attributes

UI Element	Description
Attribute Categories	<p>The attributes are organized in the following categories:</p> <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.





—Parameters

The *Details* pane is for information only; you cannot change the default value of the parameters here. To change the default value, edit the management template or aspect the parameter is defined in, and go to **Parameters**. For more information, see ["Configuring Management Templates" on page 27](#) and ["Configuring Aspects" on page 58](#).

UI Element	Description
Target (Management Template only)	The target CI for the parameter.
Defined In (Management Template only)	<p>Indicates in which management template or aspect the parameter is defined. The type of configuration object is indicated by the icon preceding the element name:</p> <div>  Indicates the name is the name of a management template. </div> <div>  Indicates the name is the name of an aspect. </div>
Name	The name of the parameter.
Instance Parameter	The instance parameter the parameter depends on (if any). The name of the instance parameter is followed by the management template or aspect the instance parameter is defined in, enclosed in parentheses.

UI Element	Description
Default Value	The default value of the parameter, as it will be applied to the target CI. This corresponds to the default value at the highest level of override. For more information about the levels at which parameter default values can be set, see "Configuring Management Templates" on page 27 , under <i>Learn More, Parameterization</i> .

—Structure

UI Element	Description
	Expand: Expands 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
	Expands this branch only.
	Collapse: Collapses the entire structure tree.
	Collapses this branch only.





Update to Latest Wizard

—Options

UI Element	Description
Radio buttons to choose a versioning alternative	<p>Update to the Latest Major and Minor Version: Allow the system to update both major and minor version numbers to the latest version.</p> <p>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.</p>
Radio buttons to choose the scope of the update	<p>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.</p> <p>Update This Object and All Containing Objects, Recursively: Update all objects in the entire tree.</p>

UI Element	Description
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.

—Preview

UI Element	Description
	Expand: Expand the structure element to show the entire tree of contained elements.
	Collapse: 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	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.

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  **Create 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  **Cut** and  **Paste**.
3. Create the aspects you need to manage your cloud. To create an aspect, select an appropriate folder, click  **New** in the *Management Templates & Aspects* pane, and select  **Create Aspect**. For details about how to create aspects, see ["Configuring Aspects" on page 58](#).
4. Create the management template(s) you need to manage your cloud. To create a management template, select an appropriate folder, click  **New** in the *Management Templates & Aspects* pane, and select  **Create Management Template**. 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 27](#).

Note: You assign a version number to any new items you create manually. To view all versions of an item, click 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 & Aspects* pane (middle pane).
2. Select an element in the *Management Templates & 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 27](#), and for aspects see ["Configuring Aspects" on page 58](#).

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

Click  **Search** to open the *Search* dialog, used to search for any subfolders and elements with a particular search string in their name or description.


To use the dialog:

1. Specified a search string in the **Search for** field. Observe the following principles when entering a search string:

- 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.
 - The search is not case-sensitive.
 - Use the character * as a wildcard; to find all elements in the tree, specify * as the search string
 - 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. Search string Oracle* Server returns both; when preceded by * the space is ignored.
2. Click **Search** to perform the search. All elements conforming to the search criteria are listed.
 3. 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.
 - b. Click  **Edit Item** to open an edit dialog for the selected element. (At the same time the search dialog 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.
 4. Click **Close** to close the dialog.

For more information see the UI reference section on *Search Dialog*.

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 Configuration Folder Dialog






UI Element	Description
Name	Provide a name for the new folder.
Description	Provide a description for the new folder.

UI Element	Description
ID (read-only)	Left blank until the folder is created.
OK	Create the folder, assign an ID and close the dialog.
Cancel	Close the dialog without creating a folder.

Edit Folder Dialog



UI Element	Description
Name	The name of the folder.
Description	The description of the folder.
ID (read-only)	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.
Cancel	Close the dialog without changing the folder.

Reports Screen

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

Search Dialog

UI Element	Description
Search for	<p>Search string.</p> <ul style="list-style-type: none"> Search returns all elements (configuration folders, management templates, aspects, and policy templates) with the search string in their name or description. The search is not case-sensitive. Spaces are interpreted literally. Use * as a wildcard.

UI Element	Description
Search	<p>List all elements conforming to the specified search criteria.</p> <p>Note: If you specify a search string for Name only, the search returns only the last version of an aspect or management template. If you specify a Description, all versions are returned, whether a Name is specified or not.</p>
Search Results Table	<div>  <p>Show Item: Selects the selected item in the main window. The relevant details are displayed in the <i>Details</i> pane in the background.</p> </div> <div>  <p>Edit Item: Opens the edit dialog for the selected item:</p> <ul style="list-style-type: none"> • If a management template is selected, the <i>Edit Management Template Dialog</i> opens. For details, see Configuring Management Templates. • If an aspect is selected, the <i>Edit Aspect Dialog</i> opens. For details, see Configuring Aspects. </div> <div> <p>Name The name of the item.</p> <p>Version The elements for which the search criteria are true.</p> <p>Configuration 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> </div>
Close	Close the dialog.

Configuring Management Templates

A management template provides a complete solution for managing 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.

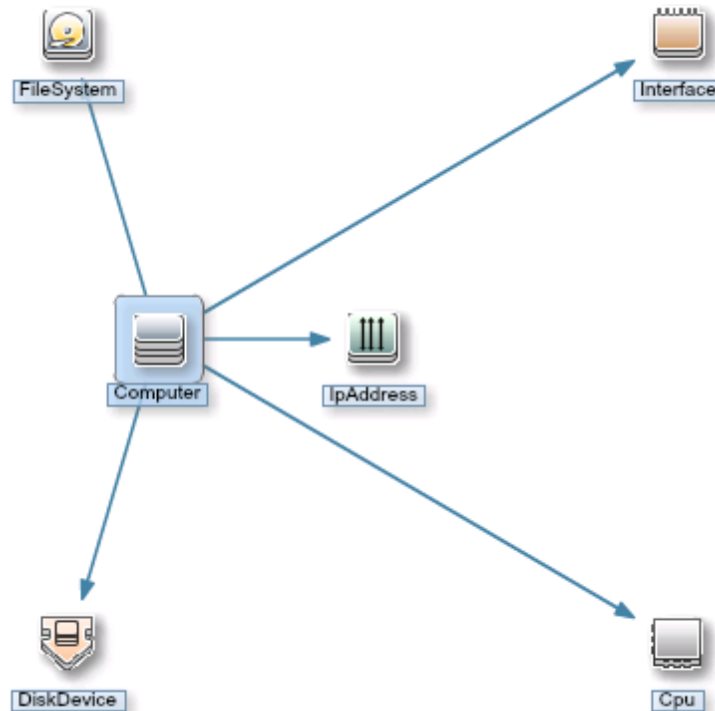
Learn More

Topology Views for Management Templates

The 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). Entities in RTSM are represented as configuration items (CIs), of which there are many different types (for example, Computer, CPU, DiskDevice, WebServer, Oracle).

The RTSM supports data flow probes and connections to external data providers such as HP Operations Manager and HP BSM Integration Adapter), thereby enabling automatic population of the database.

You can use views to find a specific CI among the numerous CIs in the database by its CI type and its relation to other CIs. The figure below shows the Systems_Infrastructure view, which is one of the default views provided with BSM.

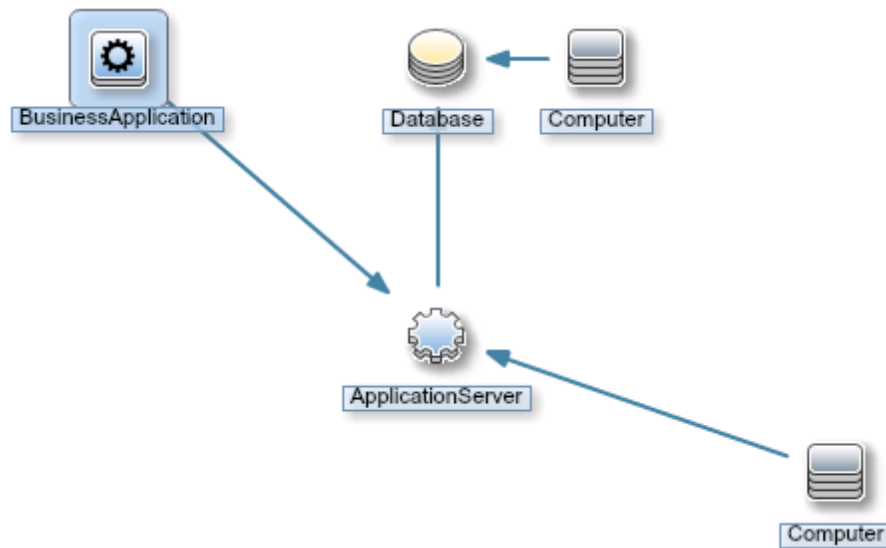


The Systems_Infrastructure view selects CIs of the type Computer, and related CIs of the types Cpu, IPAddress, DiskDevice, Interface, and FileSystem.

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 can create a management template you need a view selecting the CI types to be monitored. If necessary, you can create a new view using the Modeling Studio.

Version Numbers

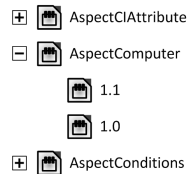
All the items in a management template are versioned. Note the following with respect to version numbers:

- 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 parameter contained in a policy template or an aspect:

- *CI type*

Policy templates must be deployed to 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.

- *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 the MySQL DBMS, 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 attribute*

You can configure a policy template to be deployed only when a CI attribute has a specific value, enabling Operations Management to automatically change the policy template for a CI when an attribute reaches a certain 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.

Tasks

How to Create or Edit Management Templates

1. In the *Configuration Folders* pane, select or create the configuration folder in which you want to create a new management template. For details about creating and managing configuration folders, see "[Configuration Folders](#)" on page 23.
2. To edit an existing management template, select it in the list of management templates in the *Management Templates & Aspects* pane and click  **Edit Item**. The *Edit Management Template* dialog opens on the *General* tab.

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

Note: Do not use  **New** to create a new *version* of an existing management template. To create a new version of an existing management template, use  **Edit Item**, specify a new version number in the *General* tab, make any required changes, and click **OK**.

3. The *General* tab 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.

- 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 **Next** to accept the values, generate an ID and go to the *Topology View* tab.
4. The *Topology View* tab 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 define the root CI type:

- a. Select a view containing the items you want to manage using one of the following methods:
 - Select a view in the **Topology View** list.
 - If you need more choices, click the **Browse Views** button ... to the right of the drop-down arrow to the right of the list. The *Browse Views* dialog opens. Browse the views on the system or, if a suitable view does not exist, click  **Go to Modeling Studio** to start the Modeling Studio and create a new view.
- b. Select a convenient layout from the drop-down list associated with the **Layout** field. You can zoom in or out using the zoom buttons  and  and scroll the graphic.
- c. In the topology view, click the CI type to which you want to be able to assign the management template. The CI type of the selected CI is selected in the **CI Type** field and the selected CI is shown with a blue background in the topology view. The selected CI type is now the root CI type of the management template.

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. If inconsistencies are possible, make sure you select a CI type that occurs only once in the selected view before continuing.




Instead of clicking the view, you can select a CI type from the drop-down list associated with the **CI Type** field.

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

5. The *Aspects* tab is used to add aspects to the management template. Grouping all relevant aspects together in a single management template generates a complete monitoring solution for a particular application.
 - a. 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.
 - b. Select the aspects to be added to the management template and click . The selected aspects are added to the list of selected aspects, at the bottom of the pane.

- **Target** is automatically set to the CI type of the node that is selected 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 aspects from the template, select them in the list of selected aspects and click .
 - Click **Next** to accept the values and go to the *Parameters* tab.
- The *Parameters* tab lists all parameters contained in the aspects you added in the *Aspects* tab.
 - To set parameter values at management template level, select a single parameter and click  **Edit**.
 - 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  **Combine**.

The *Edit/Combine* dialog opens, allowing you to set the value of the selected or combined parameter. Set the desired value and click **OK** to accept the new value.

- Click **OK** or **Finish** to save the management template and close the dialog or wizard.

How to Start Monitoring Using a Management Template

Tip: You may want to consider some special methods when using SiteScope (SiS) templates for monitoring. For recommendations, see ["Importing HP SiteScope Templates" on page 364](#).


There are several ways to start the monitoring process:

- You can assign the template to a CI from the *Assignments & Tuning* screen at **Admin > Operations Management > Monitoring > Assignments & Tuning**

Use this location to deploy a finished solutions to a node in your cloud. The *Assignments & Tuning* screen also allows you to tune the solution before deployment by overriding the default values configured in the management template. For detailed information, see ["Assignments and Tuning" on page 415](#).
- A template can be automatically assigned if it is included in an auto-assignment rule configured for a certain view in the *Automatic Assignment Rules* screen. For detailed information, see ["Automatic Assignment Rules" on page 438](#).
- You can assign and deploy a management template directly from the *Management Templates & Aspects* pane described in this section.

Use this location to try out a monitoring solution while developing or configuring it.

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


- a. 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.
- b. In step *Configuration Item*, click the configuration item(s) to which you want to assign the management template. You can select multiple items by holding down the **Ctrl** or **Shift** key while selecting them. Click **Next** to accept the CIs and go to *Required Parameters*.
- c. Step *Required Parameters* lists all mandatory parameters in the management template that do not yet have a value.

This step lists all mandatory parameters in the management template that do not yet have a value. As they are mandatory, however, all listed parameters *must* be given a value before the management template can be deployed.

If all required values are specified, you can choose one of the following actions:

- Click **Finish** to assign the configuration object to the selected CI and close the wizard or dialog.
- Click **Next** to go to *All Parameters*, where you can override the default value of any parameter, including those that are not required.

Note: To access step *Configure Options*, click **Next** in this step, and **Next** again in step *All Parameters*.

To change a parameter, double-click it, or select it in the list and click  **Edit**.

- For standard parameters, the *Edit Parameter* dialog opens.


Click **Value**, specify the value, and then click **OK**.


- For instance parameters, the *Edit Instance Parameter* dialog 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**.

When finished, click **Next** to go to **All Parameters**.

- d. In step **All Parameters**, you can specify a value for each parameter on management template level. This value overrides any value defined on a lower level. If no parameters are available, a message informs you of this.

By default, parameters defines as expert parameters are not shown. To show expert parameters, click  **Hide/Unhide Expert Parameters**.

To change a parameter, double-click it, or select it in the list and click  **Edit**.

- For standard parameters, the *Edit Parameter* dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the *Edit Instance Parameter* dialog 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**.

When finished, click **Next** to go to *Configuration Options*, or click **Finish** to deploy the management template and close the wizard.

- e. *Optional*. In step *Configuration Options*, 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* screen 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 exclude them as follows:

- 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 and Aspects

1. Go to the *Automatic Assignment Rules* screen (**Monitoring > Automatic Assignment Rules**). The screen consists of the *Auto-Assignment Rules* pane at the top, and a parameter list at the bottom.
2. Click  **New Assignment** in the toolbar of the *Auto-Assignment Rules* pane and select the appropriate option. The *Create Auto-Assignment Rule* wizard is shown, at step *Select Target View*.
3. Select a view containing the CIs for which you want to create an automatic assignment, and click **Next** to go to *Select Item to Assign*.
4. In step *Select Item to Assign*, click the management template or aspect that you want to automatically assign to all CIs with a CI type appearing in the selected view.

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.

The latest version of the management template or aspect that you want to assign is selected by default. If required, select a different version in column **Version**.


Click **Next** to go to *Required Parameters*.

5. This step lists all mandatory parameters in the management template that do not yet have a value. As they are mandatory, however, all listed parameters *must* be given a value before the management template can be deployed.

If all required values are specified, you can choose one of the following actions:

- Click **Finish** to assign the configuration object to the selected CI and close the wizard or dialog.
- Click **Next** to go to *All Parameters*, where you can override the default value of any parameter, including those that are not required.

Note: To access step *Configure Options*, click **Next** in this step, and **Next** again in step *All Parameters*.

To change a parameter, double-click it, or select it in the list and click  **Edit**.


- For standard parameters, the *Edit Parameter* dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the *Edit Instance Parameter* dialog 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**.

6. *Optional*. In step *All Parameters*, specify a value for each parameter that needs to be monitored against a different value than the default value.

To change a parameter, double-click it, or select it in the list and click  **Edit**.

- For standard parameters, the *Edit Parameter* dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the *Edit Instance Parameter* dialog 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 go to the *Configure Options* tab, or **Finish** to save the assignment and close the wizard.

7. *Optional*. In step *Configuration Options*, clear the **Enable Assigned Objects** check box if you do not want to activate the assignment rule immediately. (You can activate automatic assignment rules later using the *Automatic Assignment Rules* screen at **Admin > Operations Management > Monitoring > Automatic Assignment Rules**.)
8. Click **Finish** to save the changes and close the wizard. The assignment rule is added to the list of auto-assignment rules.

As soon as the automatic assignment rule evaluates to true for a newly discovered CI, Operations Management creates an actual assignment for the CI, and starts the deployment jobs required 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.

An assignment may trigger an event to be sent to BSM if one of the following situations applies:

- A deployment job fails.
- An auto-assignment fails.
- An auto-assignment succeeds. This behavior can be configured in the Infrastructure Settings.


You can check if the automatic assignment rule successfully created the expected assignments as follows:

- Go the *Assignments and Tuning* screen (**Monitoring > Assignments and Tuning**).
- In the *Views* browser, select the view you identified when creating your automatic assignment rule.
- Expand the view, and select a node that corresponds to the root CI type of the assigned item. Assignments created as a result of Automatic Assignment Rules are shown in the list of assignments at the top of the right pane, and have the value AutoAssignment in the column **Assigned By**.

You can consider the following options for tuning the assignment:

- Use the *Automatic Assignment Rules* screen to tune the parameter values for all assignments triggered by the automatic assignment rule.
- Use the *Assignments and Tuning* screen to tune, redeploy, delete, and enable or disable individual assignments.

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 display additional types of reports from the ["Assignments and Tuning" on page 415](#) screen.


UI Reference





Create Management Template Wizard/Edit Management Template Dialog —General

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.

UI Element	Description
Version	<p>The current version of the management template. The version is formatted as follows:</p> <p><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	Text that describes what is new or modified in this version of the management template.
Back (Visible Only in a Wizard)	Moves back to the previous screen.
Next (Visible Only in a Wizard)	Moves on to the next screen.
Finish (Visible Only in a Wizard)	Accepts the values in all screens and creates the item.
OK (Visible Only in a Dialog)	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard or dialog without creating or updating the item.
Help	Opens the relevant help in a new browser window.






—Topology View







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 <i>Browse Views</i> dialog. If a suitable view does not exist, you can click the  button to go to the Modeling Studio and create a suitable view.</p>

UI Element	Description
Topology Map	<p>A graphical representation of the selected topology view.</p> <p>The toolbar provides the following controls:</p> <div>  Refresh: Refresh the topology map. </div> <div>  Zoom In: Enlarge the topology map. </div> <div>  Zoom Out: Show a larger part of the topology map. </div> <div>  Display Edge Labels: Switch the label associated with the arrows connecting the topology elements on and off. </div> <div> Layout </div> <div> Change the format of the topology view. </div>
CI Type	<p>The root CI type for assignment. To set the root CI type, click the node to which Operations Management you want to be able to the management template in the topology view, or select it from the CI Type drop-down list. The selected root CI type is shown in the topology view with a blue background.</p> <div> <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>ow to Automatically Assign Management Templates or Aspects</i>.</p> <div> <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 tab.</p> </div>

UI Element	Description
Back (Visible Only in a Wizard)	Moves back to the previous screen.
Next (Visible Only in a Wizard)	Moves on to the next screen.
Finish (Visible Only in a Wizard)	Accepts the values in all screens and creates the item.
OK (Visible Only in a Dialog)	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard or dialog without creating or updating the item.
Help	Opens the relevant help in a new browser window.

—Aspects










UI Element	Description
Topology View	<p>Shows the topology view for the management template.</p> <p>The toolbar provides the following controls:</p> <div>  Refresh: Refresh the topology map. </div> <div>  Zoom In: Enlarge the topology map. </div> <div>  Zoom Out: Show a larger part of the topology map. </div> <div>  Display Edge Labels: Switch the label associated with the arrows connecting the topology elements on and off. </div> <div> Layout Change the format of the topology view. </div> <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



UI Element	Description
	<p>aspects (lower list on the right).</p> <p>The toolbar provides the following controls:</p> <p>Information bar above toolbar States 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> <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 Aspects (lower list on the right)	<p>Lists all aspects contained in the management template.</p> <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 <i>Edit Aspect</i> dialog for the selected aspect.</p> <p>The list has the following columns:</p> <p>Name The name of the selected aspect.</p>







UI Element	Description
	<p>Version The version of the selected aspect used with the management template.</p> <p>To change to a different version, select the desired version from the drop-down list.</p> <div> <p>Note: Operations Management does not automatically update configuration objects. If a new version of an object is available, either use the Update to Latest for the parent object, or update the version manually. See also "Configuring Management Templates" on page 27, task <i>How to Update a Management Template</i>.</p> </div> <p>Target The CI type the aspect can be assigned to.</p>
Back (Visible Only in a Wizard)	Moves back to the previous screen.
Next (Visible Only in a Wizard)	Moves on to the next screen.
Finish (Visible Only in a Wizard)	Accepts the values in all screens and creates the item.
OK (Visible Only in a Dialog)	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard or dialog without creating or updating the item.
Help	Opens the relevant help in a new browser window.

—Parameters

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>

UI Element	Description
	<div data-bbox="573 317 605 348"></div> <p>Edit: Opens the <i>Edit/Combine Parameters</i> dialog, where you can edit parameter settings for an individual parameter.  Edit is only active if a single parameter is selected.</p> <div data-bbox="792 478 1339 611"> <p>Note: Changes made here are applied at aspect or management template level. They overrule the definitions in the policy template, but do not change the policy template itself.</p> </div> <div data-bbox="573 657 605 688"></div> <p>Undo Edit: Undoes all changes that have been made to the selected parameters.</p> <div data-bbox="792 768 1307 867"> <p>Note:  Undo Edit is only active for uncombined parameters. To undo changes to combined parameters, use  Combine.</p> </div> <div data-bbox="573 919 605 951"></div> <p>Combine Opens the <i>Edit/Combine Parameters</i> dialog, where you can define the parameter settings for the new parameter resulting from combining the selected parameters.</p> <p>To combine parameters:</p> <ol style="list-style-type: none"> Click the first parameter to be combined. The following happens: <ol style="list-style-type: none"> The parameter is selected. All parameters that cannot be combined with the selected parameter are dimmed. Only parameters of a compatible type remain selectable.  Combine remains inactive. <p>To access the full list of parameters again, click  Refresh.</p> Holding down the Ctrl or Shift key, select one or more parameters to be combined with the first.  Combine is activated.

UI Element	Description
	<div data-bbox="829 331 1357 848" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <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>You can manipulate the set of selected parameters as follows:</p> <ol style="list-style-type: none"> a. Click an already selected parameter to remove all other parameters from the selection. Only the clicked parameter remains selected and  Combine is deactivated. b. Click an unselected parameter that is not dimmed while holding down the Ctrl key to add it to the selection. c. Click an already selected parameter while holding down the Ctrl key to remove it from the selection. d. Click a parameter while holding down the Shift key to select the range of parameters between the clicked parameter and the parameters last clicked before. Any selected parameters outside the range are deselected. e. To clear the entire selection and activate the full list of parameters again, click  Refresh.

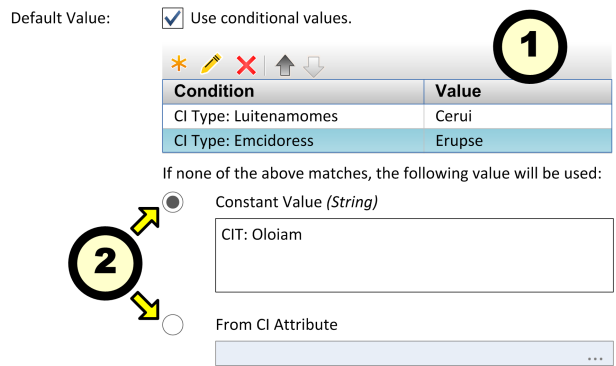
UI Element	Description
	<div data-bbox="781 310 1341 516"> <p>3. Click  Combine. The <i>Edit/Combine Parameters</i> dialog opens.</p> <p>4. Specify the parameter settings for the new parameter to represent the combination of the selected parameters.</p> </div> <div data-bbox="573 537 605 573">  </div> <div data-bbox="773 537 1365 737"> <p>Uncombine/Undo Changes: Undoes any changes that were made to the selected parameters, and restores the single parameters making up any selected combined parameters changes as well as undoing any changes made before the parameters were combined.</p> </div> <div data-bbox="573 762 605 798">  </div> <div data-bbox="773 762 1349 863"> <p>Show Parameter Details: Expand the table of parameters to show the extra columns Defined In, Description, Type and Instance Parameter.</p> </div> <div data-bbox="573 888 605 924">  </div> <div data-bbox="773 888 1216 919"> <p>Refresh: Reload the list of parameters.</p> </div> <div data-bbox="573 945 646 980">  </div> <div data-bbox="773 945 1359 1339"> <p>Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. </div> <div data-bbox="792 1398 1286 1463" style="background-color: #f0f0f0; padding: 10px;"> <p>Note: Specifying a search string clears any parameter selection you made.</p> </div> <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The list has the following columns:</p>






UI Element	Description
I	Instance Parameter: ✓ indicates that the parameter is an instance parameter, — indicates it is not.
C	Combined Parameter: ✓ indicates that the parameter is a combined parameter or that the parameter is changed, — indicates it is not.
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 (Visible Only in a Wizard)	Moves back to the previous screen.
Next (Visible Only in a Wizard)	Moves on to the next screen.
Finish (Visible Only in a Wizard)	Accepts the values in all screens and creates the item.
OK (Visible Only in a Dialog)	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard or dialog without creating or updating the item.
Help	Opens 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	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 checkbox 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.

UI Element	Description		
	<ul style="list-style-type: none"> • Hidden: Select this checkbox 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	<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>  <p>1. Any conditions in the conditional value list ① are evaluated in the order in which they appear, and the value corresponding to the first condition evaluating to true is used as default value.</p> <p>2. It is possible that none of the conditions evaluates to true. If this happens, however, the system still requires a default value, and you must use the radio buttons ② to define which value should be used. You can either have the system use a constant string value (top radio button) or the value of an attribute of the CI to which the aspect is assigned (bottom radio button).</p> <p>The following table describes how to use the controls in the default value group:</p> <table> <tr> <td>Use Conditional</td><td>After checking this checkbox the conditional</td></tr> </table>	Use Conditional	After checking this checkbox the conditional
Use Conditional	After checking this checkbox the conditional		

UI Element	Description
	<p>Values</p> <p>value list 1 is shown, with the following UI elements:</p> <div>  <p>New Item: Open the <i>Edit Conditional Value</i> dialog, which is used to define a new condition.</p> </div> <div>  <p>Edit Item: Open the <i>Edit Conditional Value</i> dialog, which is used to edit the selected condition.</p> </div> <div>  <p>Delete Item: Delete the selected condition.</p> </div> <div>  <p>Move Up: Increase the priority of the condition.</p> </div> <div>  <p>Move Down: Decrease the priority of the condition.</p> </div> <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> <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>








UI Element	Description
	<p>Constant Value (String)</p> <p>Select this radio button to use the constant string value specified in the text box as the default value in case no conditional values are defined, or if none of the conditions evaluates to true.</p> <p>If the parameter type is Password, two text boxes are provided displaying input as a number of asterisks. The values entered in the box Password and Verify Password must be identical to be accepted.</p> <p>From CI Attribute</p> <p>Select this radio button to use an attribute value as the default value in case no conditional values are defined, or if none of the conditions evaluates to true.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: The value evaluates to the attribute value resulting from resolving the aspect for the CI the aspect is assigned to, even if it is overwritten on management template level.</p> </div> <p>To create a default value from a CI attribute:</p> <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 <i>Available Attributes</i> dialog box is shown. 3. Select a CI Type from the list of CI types for the current aspect to list its Attributes. Select the desired attribute and click Insert to use the attribute value as the default value if no conditions match.
OK	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard/dialog without creating/updating the item.
Help	Opens the relevant help in a new browser window.






Edit Conditional Value Dialog

UI Element	Description								
Condition	Specify the condition to evaluated. The conditional value is used if all checked choices match the selected options.								
	You can create a condition based on the following choices:								
	<table><tr><td>OS Type</td><td>The condition applies if the aspect is assigned to a system running on the specified OS or OSs (check all that apply).</td></tr><tr><td>CI Type</td><td>The condition applies if the aspect is assigned to a CI of the selected type.</td></tr><tr><td>CI Attribute</td><td><p>The condition applies if the value of the selected CI attribute meets the specified condition.</p><p>To specify a condition:</p><ol style="list-style-type: none">1. Click the ... button to the right of the input field. The <i>Available Attributes</i> dialog is shown.2. Select a CI Type and the desired attribute. Click Insert. The selected attribute is entered in the CI Attribute field.3. Select an operator from the drop-down list in the middle. Choose Equals to have the attribute compared with a constant value, or MatchesRegexp to have the result of a regular expression compared with a constant value.4. Specify the constant value or the expression to match the attribute value with in the text box labeled Value.</td></tr><tr><td></td><td></td></tr></table>	OS Type	The condition applies if the aspect is assigned to a system running on the specified OS or OSs (check all that apply).	CI Type	The condition applies if the aspect is assigned to a CI of the selected type.	CI Attribute	<p>The condition applies if the value of the selected CI attribute meets the specified condition.</p> <p>To specify a condition:</p> <ol style="list-style-type: none">1. Click the ... button to the right of the input field. The <i>Available Attributes</i> dialog is shown.2. Select a CI Type and the desired attribute. Click Insert. The selected attribute is entered in the CI Attribute field.3. Select an operator from the drop-down list in the middle. Choose Equals to have the attribute compared with a constant value, or MatchesRegexp to have the result of a regular expression compared with a constant value.4. Specify the constant value or the expression to match the attribute value with in the text box labeled Value.		
	OS Type	The condition applies if the aspect is assigned to a system running on the specified OS or OSs (check all that apply).							
CI Type	The condition applies if the aspect is assigned to a CI of the selected type.								
CI Attribute	<p>The condition applies if the value of the selected CI attribute meets the specified condition.</p> <p>To specify a condition:</p> <ol style="list-style-type: none">1. Click the ... button to the right of the input field. The <i>Available Attributes</i> dialog is shown.2. Select a CI Type and the desired attribute. Click Insert. The selected attribute is entered in the CI Attribute field.3. Select an operator from the drop-down list in the middle. Choose Equals to have the attribute compared with a constant value, or MatchesRegexp to have the result of a regular expression compared with a constant value.4. Specify the constant value or the expression to match the attribute value with in the text box labeled Value.								

UI Element	Description
Value	<p>Specify the value to be used if the condition is the first condition that is met.</p> <p>Select one of the radio buttons to choose from the following types of values:</p> <div> <div> <p>Constant Value (String)</p> <p>Select this radio button to use the constant string value specified in the text box as the default value in case no conditional values are defined, or if none of the conditions evaluates to true.</p> <p>If the parameter type is Password, two text boxes are provided displaying input as a number of asterisks. The values entered in the box Password and Verify Password must be identical to be accepted.</p> </div> <div> <p>From CI Attribute</p> <p>Select this radio button to use an attribute value as the default value in case no conditional values are defined, or if none of the conditions evaluates to true.</p> <div> <p>Note: The value evaluates to the attribute value resulting from resolving the aspect for the CI the aspect is assigned to, even if it is overwritten on management template level.</p> </div> <p>To create a default value from a CI attribute:</p> <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 <i>Available Attributes</i> dialog box is shown. 3. Select a CI Type from the list of CI types for the current aspect to list its Attributes. Select the desired attribute and click Insert to use the attribute value as the default value if no conditions match. </div> </div>

Edit Instance Parameter Dialog

UI Element					
Instance Values	<p>The toolbar provides the following controls:</p> <div>  <p>Create Instance Parameter: Open the <i>Edit Parameter</i> dialog. To create a new value, select Value and specify a value in the text box. Click OK to close the dialog and add the new value to the Instance Values list, or click Cancel to close the dialog without making changes.</p> </div> <div>  <p>Edit Instance Parameter: Open the <i>Edit Parameter</i> dialog. To change the instance value, edit the value in the text box. Click OK to close the dialog and replace the value in the Instance Value list with the new value, or click Cancel to close the dialog without making changes.</p> </div> <div>  <p>Delete Instance Parameter: Delete the selected instance value.</p> </div> <div>  <p>Move Up: Move the selected instance value up in the list.</p> </div> <div>  <p>Move Down: Move the selected instance value down in the list.</p> </div>				
Dependent Values	<p>Lists the dependent values for the instance value selected in the Instance Values list.</p> <p>The toolbar provides the following controls:</p> <div>  <p>Edit Show the <i>Edit Parameter Dialog</i> to specify a value for the parameter.</p> </div> <div>  <p>Hide/Unhide Expert Parameters: Show or hide expert parameters.</p> </div> <p>The list has the following columns:</p> <table> <tr> <td>Name</td><td>The name of the dependent value.</td></tr> <tr> <td>Value</td><td> <p>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> </td></tr> </table>	Name	The name of the dependent value.	Value	<p>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>
Name	The name of the dependent value.				
Value	<p>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>				




UI Element	
	<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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
OK	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.

Edit Parameter Dialog (During Deployment)

UI Element	Description
Value	Select Value if you want to set a specific default value for the parameter in this assignment. 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.
Use Default Value	The other choice offered is Use Default Value . Select this option if you want to use the default value defined in the policy template, aspect, or management template.
OK	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.

Reports Window

UI Element	Description
	Expand all CIs: Expand all CIs.
	Collapse all CIs: Collapse all CIs.

UI Element	Description
	Toggle between Show Customized Values Only and Show All Values .
	Expand the category to show the attributes contained in it.
	Collapse the category to hide the attributes contained in it.

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 parameter contained in a policy template or an aspect:

- *CI type*

Policy templates must be deployed to 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.

- *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 the MySQL DBMS, 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 attribute*

You can configure a policy template to be deployed only when a CI attribute has a specific value, enabling Operations Management to automatically change the policy template for a CI when an attribute reaches a certain 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.


Tasks

How to Create Aspects

Perform the following steps to create an aspect:

1. In the *Configuration Folders* pane, select the configuration folder to create a new aspect in, or create a new folder. For details about creating and managing configuration folders, see ["Configuration Folders" on page 23](#).
2. To create a new aspect, click  **New** in the *Management Templates & Aspects* pane and select  **Create Aspect**. The *Edit Aspect* wizard opens on the *General* tab.

Note: Do not use  **New** to create a new *version* of an existing aspect. To create a new version of an existing aspect, use  **Edit Item**, specify a new version number in the *General* tab, make any required changes, and click **OK**.


Tip: To edit an existing aspect, select it in the list of aspects in the *Management Templates & Aspects* pane and click  **Edit Item**. The *Edit Aspect* dialog opens on the *General* tab. The *Edit Aspect* dialog takes the same inputs as the *Create Aspect* wizard, but lets you move freely between tabs.


3. In step *General* you 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.


- 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 **Next** to accept the values, generate an ID and go to *CI Type*.

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* step, select the **Available CI Type(s)** to which you need to be able to assign the aspect, and click . 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 a node independent of its CI type, check **Node Compatible**.

After adding a CI type to the list and selecting it, you can specify a deployment condition for the aspect based on the value of an attribute of the CI instance to which the aspect is assigned. The system will only assign the aspect if the condition is enabled and evaluates to true at deployment time. To specify a deployment condition, click  **Edit Condition** and use the *Edit CI Type Condition* dialog to select an attribute and specify a value for the condition.

Click **Next** to accept the values and go to *Instrumentation*.

5. In the *Instrumentation* step, click  **Add Instrumentation** to add instrumentation to the aspect. The *Add Instrumentation* dialog 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 **Next** to accept the values and go to the *Aspects* step.





Optional. The *Aspects* step allows you to include existing aspects as nested aspects.

To include an aspect, click  **Add Aspect**. The *Add Existing Aspect* dialog opens. To add an

aspect as a nested aspect:

1. Select the aspect(s) 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.

Note: To include a new aspect from scratch, you must create it first. To do this:




- a. Click **Cancel** to close the *Add Existing Aspect* dialog.
- b. Click **Finish** to save the aspect you are working on.
- c. Click  **New** >  **Create Aspect** in the *Management Templates & Aspects* pane and create the new aspect to be nested.
- d. Select the aspect to contain the new aspect again, and click  **Edit** > **Aspects** >  **Add Existing Aspect**. The new aspect is now available for nesting.

2. Click **OK** to accept the aspects and close the *Add Existing Aspect* dialog.

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

1. In step *Policy Templates* you can assign policy templates defining the parameters and instrumentation needed to monitor the configured CI types.

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

- To include policy templates created earlier, 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. Click **OK** to accept the values and return to the *Policy Templates* tab.
- To create a new policy template from scratch, click  **New**, then  **Add New Policy Template** to create a new policy template using a wizard, or  **Add New Policy Template (Raw)** to create a new policy template in raw mode. The *Create New Policy Template* wizard opens. Create a new policy template as described in ["Policy Templates" on page 94](#). After clicking **Finish** at the end of the process, the *Add Policy to Template to Aspect* wizard closes and the new policy template is added to the aspect.

Click **Next** to accept the values and go to *Parameters*.

2. In step *Parameters* you can override the default value of the parameters defined in the policy templates you added in the *Add Policy Templates* tab.

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 and the *Learn More* section on *Aspect Parameterization*.

3. Click **Finish** to save the values in all screens and close the wizard. The new aspect is shown in the *Management Templates & Aspects* pane.

How to Edit and Combine Parameters


You can edit parameters in several places, typically a parameter-related tab of a wizard or dialog. This task describes in detail what options can be used and in which situation they are useful.

Editing a Parameter


To edit a parameter, select a *single* parameter to be edited and click  **Edit**. The *Edit/Combine Parameters* dialog box opens, allowing you to specify the following information for the existing or combined parameter.

Combining Parameters

To combine parameters:

1. Click the first parameter to be combined. The following happens:
 - a. The parameter is selected.
 - b. All parameters that cannot be combined with the selected parameter are dimmed. Only parameters of a compatible type remain selectable.
 - c.  **Combine** remains inactive.




To access the full list of parameters again, click  **Refresh**.

2. Holding down the **Ctrl** or **Shift** key, select one or more parameters to be combined with the first.  **Combine** is activated.

Note: You can combine parameters only if they meet the following criteria:


- 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.

You can manipulate the set of selected parameters as follows:

- a. Click an already selected parameter to remove all other parameters from the selection. Only the clicked parameter remains selected and  **Combine** is deactivated.
 - b. Click an unselected parameter that is not dimmed while holding down the **Ctrl** key to add it to the selection.
 - c. Click an already selected parameter while holding down the **Ctrl** key to remove it from the selection.
 - d. Click a parameter while holding down the **Shift** key to select the range of parameters between the clicked parameter and the parameters last clicked before. Any selected parameters outside the range are deselected.
 - e. To clear the entire selection and activate the full list of parameters again, click  **Refresh**.
3. Click  **Combine**. The *Edit/Combine Parameters* dialog opens.
 4. Specify the parameter settings for the new parameter to represent the combination of the selected parameters.

Using the Edit/Combine Parameters Dialog

In the *Edit/Combine Parameters* dialog you can specify the following information:

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  **New** to open the *Edit Conditional Value* dialog box and specify a conditional value.
 - 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 apply the changes 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 27](#), 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 27](#), UI Reference section *Assign and Deploy Dialog*, but omitted from the UI reference section in this topic. You can also deploy aspects as described in ["Assignments and Tuning" on page 415](#).

How to Display an Assignment Report

To create a report:


1. Select the aspect you want to create the report for.
2. Click  **Generate Assignment Report** 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  **Collapse All CIs** and  **Expand All CIs** to collapse or expand the list of assigned CIs.
 - Click  **Show All Values** to switch between all values and only customized values 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 exclude them as follows:

- 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 and Aspects

1. Go to the *Automatic Assignment Rules* screen (**Monitoring > Automatic Assignment Rules**). The screen consists of the *Auto-Assignment Rules* pane at the top, and a parameter list at the bottom.
2. Click  **New Assignment** in the toolbar of the *Auto-Assignment Rules* pane and select the appropriate option. The *Create Auto-Assignment Rule* wizard is shown, at step *Select Target View*.
3. Select a view containing the CIs for which you want to create an automatic assignment, and click **Next** to go to *Select Item to Assign*.
4. In step *Select Item to Assign*, click the management template or aspect that you want to automatically assign to all CIs with a CI type appearing in the selected view.

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.

The latest version of the management template or aspect that you want to assign is selected by default. If required, select a different version in column **Version**.


Click **Next** to go to *Required Parameters*.

5. This step lists all mandatory parameters in the management template that do not yet have a value. As they are mandatory, however, all listed parameters *must* be given a value before the management template can be deployed.

If all required values are specified, you can choose one of the following actions:

- Click **Finish** to assign the configuration object to the selected CI and close the wizard or dialog.
- Click **Next** to go to *All Parameters*, where you can override the default value of any parameter, including those that are not required.

Note: To access step *Configure Options*, click **Next** in this step, and **Next** again in step *All Parameters*.

To change a parameter, double-click it, or select it in the list and click  **Edit**.


- For standard parameters, the *Edit Parameter* dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the *Edit Instance Parameter* dialog 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**.

6. *Optional*. In step *All Parameters*, specify a value for each parameter that needs to be monitored against a different value than the default value.

To change a parameter, double-click it, or select it in the list and click  **Edit**.

- For standard parameters, the *Edit Parameter* dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the *Edit Instance Parameter* dialog 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 go to the *Configure Options* tab, or **Finish** to save the assignment and close the wizard.

7. *Optional*. In step *Configuration Options*, clear the **Enable Assigned Objects** check box if you do not want to activate the assignment rule immediately. (You can activate automatic assignment rules later using the *Automatic Assignment Rules* screen at **Admin > Operations Management > Monitoring > Automatic Assignment Rules**.)

8. Click **Finish** to save the changes and close the wizard. The assignment rule is added to the list of auto-assignment rules.

As soon as the automatic assignment rule evaluates to true for a newly discovered CI, Operations Management creates an actual assignment for the CI, and starts the deployment jobs required 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.

An assignment may trigger an event to be sent to BSM if one of the following situations applies:

- A deployment job fails.
- An auto-assignment fails.

- An auto-assignment succeeds. This behavior can be configured in the Infrastructure Settings.

You can check if the automatic assignment rule successfully created the expected assignments as follows:



- Go the *Assignments and Tuning* screen (**Monitoring > Assignments and Tuning**).
- In the *Views* browser, select the view you identified when creating your automatic assignment rule.
- Expand the view, and select a node that corresponds to the root CI type of the assigned item. Assignments created as a result of Automatic Assignment Rules are shown in the list of assignments at the top of the right pane, and have the value AutoAssignment in the column **Assigned By**.

You can consider the following options for tuning the assignment:

- Use the *Automatic Assignment Rules* screen to tune the parameter values for all assignments triggered by the automatic assignment rule.
- Use the *Assignments and Tuning* screen to tune, redeploy, delete, and enable or disable individual assignments.

UI Reference





Add Existing Aspect Dialog




UI Element	
	Refresh: Reload the list of aspects that are available to nest within this aspect.
	Search: Specifying a string restricts the list to items having the string in their name and, if available, their description and value.
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. You can select multiple items by holding down the Ctrl or Shift key while selecting them.
Cancel	Close the dialog without adding aspects.
Help	Get Help: Opens the relevant help in a new browser window.

Add Instrumentation Dialog

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	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.

Add Policy Template to Aspect Dialog

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 <i>Select Type for New Policy Template</i> dialog, 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 <i>Select Type for New Policy Template</i> dialog, 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> <ul style="list-style-type: none"> Arcsight Logger ConfigFile Flexible Management Logfile Entry Measurement Threshold Node Info Open Message Interface

UI Element	Description
	<ul style="list-style-type: none"> • Scheduled Task • Service Auto-Discovery • Service/Process Monitoring • SiteScope • SNMP Interceptor • Windows Event Log • Windows Management Interface • XML File
 	<p>Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> • Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. • The search is not case-sensitive. • If a filter is active, click  No Filter to remove the filter and show all items in the list.
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	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard/dialog without creating/updating the item.
Help	Opens the relevant help in a new browser window.


Create Aspect Wizard/Edit Aspect Dialog



—General

UI Element	Description
Name	The name of the aspect.



UI Element	Description
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.
Back (Visible Only in a Wizard)	Moves back to the previous screen.
Next (Visible Only in a Wizard)	Moves on to the next screen.
Finish (Visible Only in a Wizard)	Accepts the values in all screens and creates the item.
OK (Visible Only in a Dialog)	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard or dialog without creating or updating the item.
Help	Opens the relevant help in a new browser window.

—CI Type

UI Element	Description
Node Compatible	<p>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.</p> <p>To enable an aspect to be assigned to nodes, check Node Compatible.</p>
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.
	Edit Condition: Open the <i>Edit CI Type Condition</i> dialog to specify a deployment condition for the aspect based on the value of an attribute of the CI instance to which the aspect is being assigned.





UI Element	Description
	Add the selected CI type(s), from the list of available CI types to the list of assigned CI types.
	Remove the selected CI types from the list of assigned CI types.
Back (Visible Only in a Wizard)	Moves back to the previous screen.
Next (Visible Only in a Wizard)	Moves on to the next screen.
Finish (Visible Only in a Wizard)	Accepts the values in all screens and creates the item.
OK (Visible Only in a Dialog)	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard or dialog without creating or updating the item.
Help	Opens the relevant help in a new browser window.

—Instrumentation

UI Element	Description
List of Instrumentation Categories	<div>  <p>Add Instrumentation: Opens the <i>Add Instrumentation</i> dialog, 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 installed on them.</p> </div> <div>  <p>Delete Instrumentation: Removes 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> </div> <div> <p>Name The name of an instrumentation category that is included in this aspect.</p> </div> <div> <p>Description A description of the instrumentation category.</p> </div>



UI Element	Description
Back (Visible Only in a Wizard)	Moves back to the previous screen.
Next (Visible Only in a Wizard)	Moves on to the next screen.
Finish (Visible Only in a Wizard)	Accepts the values in all screens and creates the item.
OK (Visible Only in a Dialog)	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard or dialog without creating or updating the item.
Help	Opens the relevant help in a new browser window.






—Aspects



UI Element	Description
List of Aspects	<p>Lists the nested aspects.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: You cannot add any of the following types of aspects:</p> <ul style="list-style-type: none"> Aspects containing the aspect itself 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. </div> <p>The toolbar provides the following controls:</p> <div style="display: flex; align-items: center; margin-bottom: 10px;">  <div style="margin-left: 10px;">Refresh: Reload the list of aspects.</div> </div> <div style="display: flex; align-items: center; margin-bottom: 10px;">  <div style="margin-left: 10px;">Add Existing Aspect: Opens the <i>Add Existing Aspect</i> dialog to add an existing aspect.</div> </div> <div style="display: flex; align-items: center; margin-bottom: 10px;">  <div style="margin-left: 10px;">Edit Aspect: Open the <i>Edit Aspect</i> dialog for the selected aspect.</div> </div> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;">Delete Aspect: Deletes the selected nested aspect (s) from the aspect.</div> </div> <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 <i>Details</i> 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="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Note: Operations Management does not automatically update configuration objects. If a new version of an object is available, either use the Update to Latest for the parent object, or update the version manually. See also "Configuring Management Templates" on page 27, task <i>How to Update a Management Template</i>.</p> </div> <p>Description A description of the nested aspect.</p>
Back (Visible Only in a Wizard)	Moves back to the previous screen.
Next (Visible Only in a Wizard)	Moves on to the next screen.
Finish (Visible Only in a Wizard)	Accepts the values in all screens and creates the item.
OK (Visible Only in a Dialog)	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard or dialog without creating or updating the item.
Help	Opens the relevant help in a new browser window.

—Policy Templates

UI Element	Description
List of Policy Templates	<div>  Refresh: Reload the list of policy templates in this aspect. </div> <div>  Add Policy Template: Open the Add Policy Template to Aspect dialog, which enables you to either add an </div>




UI Element	Description
	<p>existing policy template or create a new policy templates.</p> <div> <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 policy template to be added. • The aspect is a nested aspect, and its parent aspect uses the policy template to be added. </div> <p> Edit Item: Provides the following options:</p> <ul 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> Edit Deployment Condition: Open the Edit Deployment Condition Dialog, which enables you to specify deployment conditions for the selected policy template.</p> <p> Delete Policy Template: Remove the selected policy template(s) 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 a policy template.</p>







UI Element	Description
	<p>Version The version of the policy template.</p> <p>To change to a different version, select the desired version from the drop-down list.</p> <div> <p>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 27, task <i>How to Update a Management Template After a Management Pack Update</i>.</p> </div> <p>Deployment Condition The deployment conditions for the policy template. To specify deployment conditions for a policy template, select it, click  Edit Item and select the  Edit Deployment Condition option to open the Edit Deployment Condition Dialog.</p> <p>Type The type of the policy template.</p>
Type	The type of the policy template.
Back (Visible Only in a Wizard)	Moves back to the previous screen.
Next (Visible Only in a Wizard)	Moves on to the next screen.
Finish (Visible Only in a Wizard)	Accepts the values in all screens and creates the item.
OK (Visible Only in a Dialog)	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard or dialog without creating or updating the item.
Help	Opens the relevant help in a new browser window.

—Parameters

UI Element	Description
List of	Lists all parameters defined in the policy templates assigned to the

UI Element	Description
Parameters	<p>aspects contained in the management template or aspect.</p> <p>The toolbar provides the following controls:</p> <div data-bbox="573 422 605 453"></div> <p>Edit: Opens the <i>Edit/Combine Parameters</i> dialog, where you can edit parameter settings for an individual parameter. Edit is only active if a single parameter is selected.</p> <div data-bbox="792 583 1339 716" style="background-color: #f0f0f0; padding: 5px;"> <p>Note: Changes made here are applied at aspect or management template level. They overrule the definitions in the policy template, but do not change the policy template itself.</p> </div> <div data-bbox="573 762 605 793"></div> <p>Undo Edit: Undoes all changes that have been made to the selected parameters.</p> <div data-bbox="792 873 1307 974" style="background-color: #f0f0f0; padding: 5px;"> <p>Note: Undo Edit is only active for uncombined parameters. To undo changes to combined parameters, use Uncombine.</p> </div> <div data-bbox="573 1026 605 1058"></div> <p>Combine Opens the <i>Edit/Combine Parameters</i> dialog, where you can define the parameter settings for the new parameter resulting from combining the selected parameters.</p> <p>To combine parameters:</p> <ol style="list-style-type: none"> Click the first parameter to be combined. The following happens: <ol style="list-style-type: none"> The parameter is selected. All parameters that cannot be combined with the selected parameter are dimmed. Only parameters of a compatible type remain selectable. Combine remains inactive. <p>To access the full list of parameters again, click Refresh.</p> Holding down the Ctrl or Shift key, select one

UI Element	Description
	<p data-bbox="824 310 1114 346"> Combine is activated.</p> <div data-bbox="824 384 1359 917" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p data-bbox="841 405 1328 472">Note: You can combine parameters only if they meet the following criteria:</p> <ul style="list-style-type: none"> <li data-bbox="841 504 1317 571">■ Parameters to be combined must be of the same type. <li data-bbox="841 602 1295 669">■ Parameters to be combined must not have conditional values. <li data-bbox="841 701 1317 800">■ The range of allowed values of numeric parameters to be combined must overlap. <li data-bbox="841 831 1338 898">■ Enumeration parameters to be combined must have at least one common value. </div> <p data-bbox="824 947 1265 1014">You can manipulate the set of selected parameters as follows:</p> <ol style="list-style-type: none"> <li data-bbox="824 1045 1359 1215">a. Click an already selected parameter to remove all other parameters from the selection. Only the clicked parameter remains selected and  Combine is deactivated. <li data-bbox="824 1247 1352 1346">b. Click an unselected parameter that is not dimmed while holding down the Ctrl key to add it to the selection. <li data-bbox="824 1377 1359 1476">c. Click an already selected parameter while holding down the Ctrl key to remove it from the selection. <li data-bbox="824 1507 1352 1709">d. Click a parameter while holding down the Shift key to select the range of parameters between the clicked parameter and the parameters last clicked before. Any selected parameters outside the range are deselected. <li data-bbox="824 1740 1370 1808">e. To clear the entire selection and activate the full list of parameters again, click .

UI Element	Description
	<p>Refresh.</p> <ol style="list-style-type: none"> Click  Combine. The <i>Edit/Combine Parameters</i> dialog opens. Specify the parameter settings for the new parameter to represent the combination of the selected parameters. <p> Uncombine/Undo Changes: Undoes any changes that were made to the selected parameters, and restores the single parameters making up any selected combined parameters changes as well as undoing any changes made before the parameters were combined.</p> <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/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. <div data-bbox="776 1444 1360 1549" style="background-color: #f0f0f0; padding: 5px;"> <p>Note: Specifying a search string clears any parameter selection you made.</p> </div> <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The list has the following columns:</p>

UI Element	Description
I	Instance Parameter: ✓ indicates that the parameter is an instance parameter, — indicates it is not.
C	Combined Parameter: ✓ indicates that the parameter is a combined parameter or that the parameter is changed, — indicates it is not.
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 (Visible Only in a Wizard)	Moves back to the previous screen.
Next (Visible Only in a Wizard)	Moves on to the next screen.
Finish (Visible Only in a Wizard)	Accepts the values in all screens and creates the item.
OK (Visible Only in a Dialog)	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard or dialog without creating or updating the item.
Help	Opens the relevant help in a new browser window.



Edit CI Type Condition Dialog

UI Element	Description
Condition	<p>Specify a deployment condition for the aspect based on the value of an attribute of the CI instance to which the aspect is assigned. The system will only assign the aspect if the condition is enabled and evaluates to true at deployment time.</p> <p>If the checkbox is checked, the condition is enabled; if it is unchecked it is disabled.</p> <p>To specify a condition:</p> <ol style="list-style-type: none"> 1. Click the ... button to the right of the input field. The <i>Available Attributes</i> dialog is shown. 2. Select a CI Type and the desired attribute. Click Insert. The selected attribute is entered in the CI Attribute field. 3. Select an operator from the drop-down list in the middle. Choose Equals to have the attribute compared with a constant value, or MatchesRegexp to have the result of a regular expression compared with a constant value. 4. Specify the constant value or the expression to match the attribute value with in the text box labeled Value.
OK	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.

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 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 checkbox 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 checkbox 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	<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>

UI Element	Description								
	<p>Default Value: <input checked="" type="checkbox"/> Use conditional values. 1</p> <div>      </div> <table border="1"> <thead> <tr> <th>Condition</th><th>Value</th></tr> </thead> <tbody> <tr> <td>CI Type: Luitenamomes</td><td>Cerui</td></tr> <tr> <td>CI Type: Emcidoress</td><td>Erupse</td></tr> </tbody> </table> <p>If none of the above matches, the following value will be used:</p> <div> 2 <input checked="" type="radio"/> Constant Value (<i>String</i>) <div> CIT: Oloiam </div> </div> <div> <input type="radio"/> From CI Attribute <div> ... </div> </div> <p>1. Any conditions in the conditional value list 1 are evaluated in the order in which they appear, and the value corresponding to the first condition evaluating to true is used as default value.</p> <p>2. It is possible that none of the conditions evaluates to true. If this happens, however, the system still requires a default value, and you must use the radio buttons 2 to define which value should be used. You can either have the system use a constant string value (top radio button) or the value of an attribute of the CI to which the aspect is assigned (bottom radio button).</p> <p>The following table describes how to use the controls in the default value group:</p> <table> <tr> <td>Use Conditional Values</td><td> <p>After checking this checkbox the conditional value list 1 is shown, with the following UI elements:</p> <div>  <p>New Item: Open the <i>Edit Conditional Value</i> dialog, which is used to define a new condition.</p> </div> <div>  <p>Edit Item: Open the <i>Edit Conditional Value</i> dialog, which is used to edit the selected condition.</p> </div> <div>  <p>Delete Item: Delete the selected condition.</p> </div> </td></tr> </table>	Condition	Value	CI Type: Luitenamomes	Cerui	CI Type: Emcidoress	Erupse	Use Conditional Values	<p>After checking this checkbox the conditional value list 1 is shown, with the following UI elements:</p> <div>  <p>New Item: Open the <i>Edit Conditional Value</i> dialog, which is used to define a new condition.</p> </div> <div>  <p>Edit Item: Open the <i>Edit Conditional Value</i> dialog, which is used to edit the selected condition.</p> </div> <div>  <p>Delete Item: Delete the selected condition.</p> </div>
Condition	Value								
CI Type: Luitenamomes	Cerui								
CI Type: Emcidoress	Erupse								
Use Conditional Values	<p>After checking this checkbox the conditional value list 1 is shown, with the following UI elements:</p> <div>  <p>New Item: Open the <i>Edit Conditional Value</i> dialog, which is used to define a new condition.</p> </div> <div>  <p>Edit Item: Open the <i>Edit Conditional Value</i> dialog, which is used to edit the selected condition.</p> </div> <div>  <p>Delete Item: Delete the selected condition.</p> </div>								

UI Element	Description
	<div>  Move Up: Increase the priority of the condition. </div> <div>  Move Down: Decrease the priority of the condition. </div> <div> Condition A semicolon-separated string listing all expressions used in the condition. </div> <div> Value The value used as default when the condition is the first to evaluate to true. </div> <div> Note: At management template level you cannot add, remove, or rearrange conditions, but you can change the values used to evaluate them. </div>
Constant Value (String)	<p>Select this radio button to use the constant string value specified in the text box as the default value in case no conditional values are defined, or if none of the conditions evaluates to true.</p> <p>If the parameter type is Password, two text boxes are provided displaying input as a number of asterisks. The values entered in the box Password and Verify Password must be identical to be accepted.</p>
From CI Attribute	<p>Select this radio button to use an attribute value as the default value in case no conditional values are defined, or if none of the conditions evaluates to true.</p> <div> Note: The value evaluates to the attribute value resulting from resolving the aspect for the CI the aspect is assigned to, even if it is overwritten on management template level. </div> <p>To create 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 <i>Available Attributes</i> dialog box is shown.3. Select a CI Type from the list of CI types for the current aspect to list its AttributesSelect the desired attribute and click Insert to use the attribute value as the default value if no conditions match.
OK	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard/dialog without creating/updating the item.
Help	Opens the relevant help in a new browser window.

Edit Conditional Value Dialog


UI Element	Description						
Condition	<p>Specify the condition to evaluated. The conditional value is used if all checked choices match the selected options.</p> <p>You can create a condition based on the following choices:</p> <table border="1" data-bbox="565 447 1383 1503"> <tr> <td data-bbox="573 457 841 573">OS Type</td><td data-bbox="849 457 1375 573">The condition applies if the aspect is assigned to a system running on the specified OS or OSs (check all that apply).</td></tr> <tr> <td data-bbox="573 583 841 667">CI Type</td><td data-bbox="849 583 1375 667">The condition applies if the aspect is assigned to a CI of the selected type.</td></tr> <tr> <td data-bbox="573 678 841 1493">CI Attribute</td><td data-bbox="849 678 1375 1493"> <p>The condition applies if the value of the selected CI attribute meets the specified condition.</p> <p>To specify a condition:</p> <ol style="list-style-type: none"> 1. Click the ... button to the right of the input field. The <i>Available Attributes</i> dialog is shown. 2. Select a CI Type and the desired attribute. Click Insert. The selected attribute is entered in the CI Attribute field. 3. Select an operator from the drop-down list in the middle. Choose Equals to have the attribute compared with a constant value, or MatchesRegexp to have the result of a regular expression compared with a constant value. 4. Specify the constant value or the expression to match the attribute value with in the text box labeled Value. </td></tr> </table>	OS Type	The condition applies if the aspect is assigned to a system running on the specified OS or OSs (check all that apply).	CI Type	The condition applies if the aspect is assigned to a CI of the selected type.	CI Attribute	<p>The condition applies if the value of the selected CI attribute meets the specified condition.</p> <p>To specify a condition:</p> <ol style="list-style-type: none"> 1. Click the ... button to the right of the input field. The <i>Available Attributes</i> dialog is shown. 2. Select a CI Type and the desired attribute. Click Insert. The selected attribute is entered in the CI Attribute field. 3. Select an operator from the drop-down list in the middle. Choose Equals to have the attribute compared with a constant value, or MatchesRegexp to have the result of a regular expression compared with a constant value. 4. Specify the constant value or the expression to match the attribute value with in the text box labeled Value.
OS Type	The condition applies if the aspect is assigned to a system running on the specified OS or OSs (check all that apply).						
CI Type	The condition applies if the aspect is assigned to a CI of the selected type.						
CI Attribute	<p>The condition applies if the value of the selected CI attribute meets the specified condition.</p> <p>To specify a condition:</p> <ol style="list-style-type: none"> 1. Click the ... button to the right of the input field. The <i>Available Attributes</i> dialog is shown. 2. Select a CI Type and the desired attribute. Click Insert. The selected attribute is entered in the CI Attribute field. 3. Select an operator from the drop-down list in the middle. Choose Equals to have the attribute compared with a constant value, or MatchesRegexp to have the result of a regular expression compared with a constant value. 4. Specify the constant value or the expression to match the attribute value with in the text box labeled Value. 						





UI Element	Description
Value	<p>Specify the value to be used if the condition is the first condition that is met.</p> <p>Select one of the radio buttons to choose from the following types of values:</p> <div> <div> <p>Constant Value (String)</p> <p>Select this radio button to use the constant string value specified in the text box as the default value in case no conditional values are defined, or if none of the conditions evaluates to true.</p> <p>If the parameter type is Password, two text boxes are provided displaying input as a number of asterisks. The values entered in the box Password and Verify Password must be identical to be accepted.</p> </div> <div> <p>From CI Attribute</p> <p>Select this radio button to use an attribute value as the default value in case no conditional values are defined, or if none of the conditions evaluates to true.</p> <div> <p>Note: The value evaluates to the attribute value resulting from resolving the aspect for the CI the aspect is assigned to, even if it is overwritten on management template level.</p> </div> <p>To create a default value from a CI attribute:</p> <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 <i>Available Attributes</i> dialog box is shown. 3. Select a CI Type from the list of CI types for the current aspect to list its Attributes. Select the desired attribute and click Insert to use the attribute value as the default value if no conditions match. </div> </div>


Edit Deployment Condition Dialog

UI Element	Description
OS Type	The condition applies if the aspect is assigned to a system running on the specified OS or OSs (check all that apply).
CI Type	The condition applies if the aspect is assigned to a CI of the selected type.
CI Attribute	<p>The condition applies if the value of the selected CI attribute meets the specified condition.</p> <p>To specify a condition:</p> <ol style="list-style-type: none"> 1. Click the ... button to the right of the input field. The <i>Available Attributes</i> dialog is shown. 2. Select a CI Type and the desired attribute. Click Insert. The selected attribute is entered in the CI Attribute field. 3. Select an operator from the drop-down list in the middle. Choose Equals to have the attribute compared with a constant value, or MatchesRegexp to have the result of a regular expression compared with a constant value. 4. Specify the constant value or the expression to match the attribute value with in the text box labeled Value.
OK	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.

Edit Instance Parameter Dialog

UI Element	
Instance Values	<p>The toolbar provides the following controls:</p> <div>  <p>Create Instance Parameter: Open the <i>Edit Parameter</i> dialog. To create a new value, select Value and specify a value in the text box. Click OK to close the dialog and add the new value to the Instance Values list, or click Cancel to close the dialog without making changes.</p> </div>






UI Element					
	<div data-bbox="573 317 607 348"></div> <p>Edit Instance Parameter: Open the <i>Edit Parameter</i> dialog. To change the instance value, edit the value in the text box. Click OK to close the dialog and replace the value in the Instance Value list with the new value, or click Cancel to close the dialog without making changes.</p> <div data-bbox="573 541 607 573"></div> <p>Delete Instance Parameter: Delete the selected instance value.</p> <div data-bbox="573 632 607 663"></div> <p>Move Up: Move the selected instance value up in the list.</p> <div data-bbox="573 722 607 753"></div> <p>Move Down: Move the selected instance value down in the list.</p>				
<p>Dependent Values</p>	<p>Lists the dependent values for the instance value selected in the Instance Values list.</p> <p>The toolbar provides the following controls:</p> <div data-bbox="573 978 607 1010"></div> <p>Edit Show the <i>Edit Parameter Dialog</i> to specify a value for the parameter.</p> <div data-bbox="573 1068 607 1100"></div> <p>Hide/Unhide Expert Parameters: Show or hide expert parameters.</p> <p>The list has the following columns:</p> <table data-bbox="573 1230 1156 1318"> <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 <p>Note the following:</p>	Name	The name of the dependent value.	Value	The value of the dependent value.
Name	The name of the dependent value.				
Value	The value of the dependent value.				

UI Element	
	<ul style="list-style-type: none"> • If the value is dimmed, it is the default value. • If the icon is dimmed, the value is read-only. • If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
OK	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.

Edit Parameter Dialog (During Deployment)

UI Element	Description
Value	Select Value if you want to set a specific default value for the parameter in this assignment. 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.
Use Default Value	The other choice offered is Use Default Value . Select this option if you want to use the default value defined in the policy template, aspect, or management template.
OK	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.

Reports Screen

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

Viewing Details



Management templates and aspects have a number of properties, parameters, 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 shown for management templates or aspects only are marked accordingly.

UI Reference



Details Pane

—Attributes





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.

—Parameters

The *Details* pane is for information only; you cannot change the default value of the parameters here. To change the default value, edit the management template or aspect the parameter is defined in, and go to **Parameters**. For more information, see ["Configuring Management Templates" on page 27](#) and ["Configuring Aspects" on page 58](#).

UI Element	Description
Target (Management Template only)	The target CI for the parameter.
Defined In (Management Template only)	<p>Indicates in which management template or aspect the parameter is defined. The type of configuration object is indicated by the icon preceding the element name:</p> <div>  Indicates the name is the name of a management template. </div> <div>  Indicates the name is the name of an aspect. </div>
Name	The name of the parameter.
Instance Parameter	The instance parameter the parameter depends on (if any). The name of the instance parameter is followed by the management template or aspect the instance parameter is defined in, enclosed in parentheses.
Default Value	The default value of the parameter, as it will be applied to the target CI. This corresponds to the default value at the highest level of override. For more information about the levels at which parameter default values can be set, see "Configuring Management Templates" on page 27 , under <i>Learn More, Parameterization</i> .

—Structure

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

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 96](#)

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 98](#)
- ["How to Display an Inventory Report" on page 98](#)

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:

To change a parameter, double-click it, or select it in the list and click  **Edit**.

- For standard parameters, the *Edit Parameter* dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the *Edit Instance Parameter* dialog 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**.



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 the **Search for** field.

You can type one or more characters and combine them with asterisks (*) to match zero or more characters. Spaces are taken literally. The search is case-insensitive.

4. Click **Search**. The search results are displayed in the lower half of the dialog box.
5. *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.

How to Display an Inventory Report

Click  **Generate Inventory Report** in the Policy Template Groups pane.

A new browser window opens and displays the preconfigured inventory report. The report lists all management templates, aspects, and policy templates that are available on a server.

Related Tasks

- ["How to Assign SiteScope Policy Templates to Remote Servers" on page 372](#)

UI Reference


This section includes:




- ["Assign and Deploy—Configuration Item" below](#)
- ["Assign and Deploy—Parameters" below](#)
- ["Assign and Deploy—Configure Options" on page 101](#)
- ["Policy Parameters Dialog Box" on page 102](#)
- ["Policy Template Details Pane" on page 105](#)
- ["Policy Template Groups Pane" on page 105](#)
- ["Policy Templates Pane" on page 106](#)
- ["Search Dialog Box" on page 107](#)
- ["Template Group Dialog Box" on page 107](#)






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>Lists all parameters in the management template, aspect or policy template you are assigning to the configuration item.</p> <p>The toolbar provides the following controls:</p> <div> Edit: Specify the value of the selected parameter.</div> <ul style="list-style-type: none">• For standard parameters, the <i>Edit Parameter</i> dialog opens.• For instance parameters, the <i>Edit Instance</i>

UI Element	Description								
	<p><i>Parameter</i> dialog opens.</p> <p>For details on using the dialogs, see the relevant <i>UI Reference</i> section.</p> <p> Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p> <p> Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p> <table> <tr> <td>Target (Visible Only for Assignments of Management Templates)</td><td>The CI type of the item using the parameter.</td></tr> <tr> <td>Defined In (Visible Only for Assignments of Management Templates)</td><td>The management template, aspect or policy template in which the parameter is defined.</td></tr> <tr> <td>Name</td><td>The name of the parameter.</td></tr> <tr> <td>Value</td><td>The parameter value for this assignment.</td></tr> </table> <p>An icon represents the type of parameter value, which can be one of the following:</p>	Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.	Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.	Name	The name of the parameter.	Value	The parameter value for this assignment.
Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.								
Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.								
Name	The name of the parameter.								
Value	The parameter value for this assignment.								

UI Element	Description
	<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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens 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 the assignments immediately, clear the Enable Assigned Objects check box. To enable assignments after closing the wizard, use the <i>Assignments & Tuning</i> screen.
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.

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 OBJECT 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 DISK, 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

UI Element	Description
	<ul style="list-style-type: none"> • Service Auto-Discovery • 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 only include ASCII characters. The user interface displays asterisks (*) instead of 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).










UI Element	Description
Default Value	<p>Defines the default value of the parameter.</p> <p>To specify enumeration values, click  Edit Enumeration Values and configure the values using the Edit Enumeration Values dialog box. You can also change the order of the values in this dialog box.</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.

UI Element	Description
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.
	Generate Inventory Report: Generates an inventory showing which management templates, aspects and policy templates are available on a server. When you click this icon, a new browser window opens displaying the report.

Policy Templates Pane

UI Element	Description
	Refresh: Reloads the list of policy templates.
	New: Provides the following options: <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.
	Edit Item: Provides the following options: <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.

UI Element	Description
	<p>Show Assignments List for Selected Item: Opens the <i>Assignments</i> dialog, which shows all assignments of the selected policy template, and allows you to create, edit, delete, activate or deactivate and tune them.</p> <p>Note: If a policy template is selected, the assignments for all versions are listed. If a policy template version is selected, only the assignments of the selected version are listed.</p>

Search Dialog Box

UI Element	Description
Search for	<p>Search string. The search returns all policy templates with the search string in their name or description.</p> <p>The search is case-insensitive. Spaces are interpreted literally. Use * as a wildcard.</p>
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.

UI Element	Description
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

- 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 **ArcSight Logger Template**, and then click **OK**.
 - To edit an existing policy template, click the policy template in the list, click the 

¹(globally unique identifier)




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:
 - 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.

- 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" below](#)
- ["Example ArcSight Logger Receiver Configuration Policy" on page 113](#)
- ["Assigning and Deploying ArcSight Logger Policy Templates" on page 113](#)

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 template name determines the name of the receiver in ArcSight Logger. 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 template does not contain the parameters `_logger_receiver_type` and `_logger_receiver_state`, the policy template by default creates a receiver of the type File Receiver. The state of the receiver in ArcSight Logger depends on the state of the deployed policy (that is, enabled or disabled). If the parameters exist in the policy template but have empty values, a receiver of the type File Receiver will be created in ArcSight Logger but will be disabled by default.

Parameter Name	Parameter Type	Parameter Value	
_logger_receiver_type	Enumeration	Defines the receiver type. Supported values are:	
		udp	Creates a receiver for UDP messages (for example, SYSLOG).
		tcp	Creates a receiver for TCP messages (for example, SYSLOG, which can also be sent with TCP).
		localfile	Creates a receiver to read logs from a local or remote file system (for example, NFS, CIFS, or SAN).
		filetransfer	Creates a receiver to read remote logs using scp, sftp or ftp.
		smartmsg	Creates a receiver for encrypted SmartMessage messages sent by SmartConnectors.
		cefudp	Creates a receiver for CEF (Common Event Format) messages sent through UDP.
		ceftcp	Creates a receiver for CEF (Common Event Format) messages sent through TCP.

Parameter Name	Parameter Type	Parameter Value
_logger_receiver_state	String	Defines the receiver state. Supported values are: true Sets the receiver state to enabled in ArcSight Logger. false Sets the receiver state to disabled in ArcSight Logger.

- **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
ip	IP/Host
PORT	Port
Encoding	Encoding

File Receiver parameters

Parameter Name	Receiver Property
rfsname	RFS Names
folder	Folder
sourcetype	Source Type
wildcard	Wildcard (regex)

Parameter Name	Receiver Property
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
datetimelocale	Date/time locale
datetimezone	Date/time zone
datetimelocregex	Date/time loc regex

Parameter Name	Receiver Property
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" on the next page](#)

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 page 117](#).

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 109](#) and ["Policy Parameters Tab" on the next page](#).

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 111](#).


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" on the next page](#)
- ["Properties Page" on page 117](#)

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> .

UI Element	Description
	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 109 .

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

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).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.

¹(globally unique identifier)

²(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 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" on the next page](#)
- ["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 124](#).

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 120](#) and ["ConfigFile Data" on the previous page](#).

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 124](#)

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.
<policy data>	Policy data in text form. For details, see "ConfigFile Definition" on page 120 and "ConfigFile Data" 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.
	<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	<p>Description of what the policy does. You might also add other notes (for example, data sources that are used).</p>
Template ID	<p>GUID¹ assigned to the policy template when it is first created.</p>
Version ID	<p>GUID² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.</p>
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> <div>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.</div>
Change Log	<p>Text that describes what is new or modified in this version of the policy.</p>
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	<p>The name of the user active when the policy was saved.</p>

¹(globally unique identifier)

²(globally unique identifier)

UI Element	Description
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

By default, HP Operations Agents send events to the BSM Operations Management server to which they are connected. This server is called the primary server. 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.


If you want to switch the primary server after you connect the agent, you can change the OPC_PRIMARY_MGR parameter in the agent configuration. After you do this, the agents send their events to the new primary server. For example, you may want to switch primary servers when migrating an agent from a BSM Operations Management server to another.

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" on the next page](#)
- ["Flexible Management Policy Syntax and Keywords" on the next page](#)
- ["Time Templates" on page 133](#)

- ["Event Target Rules" on page 133](#)
- ["Action-Allowed and Secondary Servers" on page 134](#)

Flexible Management Policies

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

- You can configure agents to communicate with multiple BSM Operations Management servers:
 - Configure agents to send events to different BSM Operations Management servers based on the time of day or based on criteria in the event. (See ["Time Templates" on page 133](#) and ["Event Target Rules" on page 133](#).)
 - Configure agents to allow actions from several BSM Operations Management servers. (See ["Action-Allowed and Secondary Servers" on page 134](#).)
 - Switch the primary server function to another server to manage an expanding network environment, and reduce primary server bottlenecks. (See ["Configuring Flexible Management Policies" on page 125](#).)
- You can deploy policies to any agent from any server, if the servers are configured to be the agent's primary or secondary server.

Even though some policies are specific to a particular BSM Operations Management server, the events that result from the policies can be sent to any 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, NODE IP 0.0.0.0 hpbbn). If the node is defined using the format IP <ipaddress> or IP <ipaddress> <string>, 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: SERVICE_NAME "Service<*> [A B]" 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"  
    ID "e77b4992-5d78-753f-1387-c01230fe2648"  
  ACTIONALLOWMANAGER NODE IP 0.0.0.0 "manager2.example.com"  
    ID "68f01602-8bfa-7557-0403-8467ba97477a"  
  ACTIONALLOWMANAGER NODE IP 192.168.1.3  
    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 server with the 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 137](#).

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 127](#).

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> .
	Flexible Management 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 "Flexible Management Policy Syntax and Keywords" on page 127 .

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	<p>Description of what the policy does. You might also add other notes (for example, data sources that are used).</p>

UI Element	Description
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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)

²(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 156](#).

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 158](#).

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.

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

For more details, see ["Event Attributes Tab" on page 148](#), ["Event Correlation Tab" on page 149](#), ["Instructions Tab" on page 151](#), and ["Advanced Tab" on page 145](#).

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 155](#).

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 enter pattern matching expressions and policy parameters in the 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 146](#) and ["Pattern Matching in Policy Rules" on page 405](#).

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 148](#), ["Event Correlation Tab" on page 149](#), ["Custom Attributes Tab" on page 147](#), ["Instructions Tab" on page 151](#), ["Advanced Tab" on page 145](#), 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 151](#).

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

UI Reference

This section includes:

- ["Actions Tab" below](#)
- ["Advanced Tab" on page 145](#)
- ["Condition Tab" on page 146](#)
- ["Custom Attributes Tab" on page 147](#)
- ["Defaults Page" on page 148](#)
- ["Event Attributes Tab" on page 148](#)
- ["Event Correlation Tab" on page 149](#)
- ["Indicators Tab" on page 149](#)
- ["Instructions Tab" on page 151](#)
- ["Options Page" on page 151](#)
- ["Policy Data Page" on page 153](#)
- ["Policy Parameters Tab" on page 154](#)
- ["Policy Rules List" on page 155](#)
- ["Policy Variables Tab" on page 156](#)
- ["Properties Page" on page 156](#)
- ["Rules Page" on page 158](#)
- ["Source Page" on page 158](#)

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 echo or move), must be preceded by cmd /c. See the Windows help for more information on cmd.

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 %%password%%. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	<p>Name of the node on which the command will be started. You can also use the variable <\$MSG_NODE_NAME> to configure reusable policies for replicated sites.</p>
Append output of command as annotation to the event	<p>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.</p>
Close the event when the command is successful	<p>Closes the event automatically if the command is successful.</p>
Send event immediately	<p>Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.</p>
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	<p>Operator-initiated command that is attached to the event that the rule sends to BSM. This command can be started by the BSM user from the Operations Management Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.</p>

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 echo or move), must be preceded by cmd /c. See the Windows help for more information about cmd.
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 %%password%%. 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 <\$MSG_NODE_NAME> 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: celery.example.com broccoli.example.com</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 151](#), and ["Advanced Tab" on page 145](#).

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.
Send with closed status	Sets the event's lifecycle status to Closed before sending it to BSM.


Event Correlation Tab





Note: The following event correlation attributes are only available in individual rules, not in the event defaults:

- Close Events with Key
- Suppress Deduplication on Server

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

UI Element	Description
	<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 Operations Management 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 Operations Management 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	<p>Logs any events in the event source that match the policy rules.</p>
that match a rule and are ignored	<p>Logs any events in the event source that are suppressed. (Suppressed events are not sent to BSM.)</p>









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 BSM when the input 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 BSM creates an event with the default values of the policy.</p> <div> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p> </div> <div> <p>Note:</p> <p>Windows event log, log file, measurement threshold, WMI and XML file policies: If several policies forward unmatched events to BSM, you could receive multiple events about a single input event.</p> </div>
are forwarded to BSM Server	Sends unmatched events to BSM.
are forwarded to BSM Server with state 'closed'	Sets the unmatched event's lifecycle status to Closed before sending it to BSM.
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 _data.
	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><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.
	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>	<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>
	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

UI Element	Description
Rule Type	<p>The three rule types of event policies are:</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>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

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	<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).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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)

²(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 155](#), ["Condition Tab" on page 146](#), ["Event Attributes Tab" on page 148](#), ["Event Correlation Tab" on page 149](#), ["Custom Attributes Tab" on page 147](#), ["Advanced Tab" on page 145](#), and ["Actions Tab" on page 143](#).

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>You can use the following configurations to make your policy more flexible:</p> <ul style="list-style-type: none"> • Windows environment variables (for example, winnt or clusterlog). The syntax for these variables is <code><\$variablename></code>, for example <code><\$winnt></code>. • Script or command that returns the path and name of the log file you want to access. For example, type <code><`command`></code> 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. <p>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> <ul style="list-style-type: none"> • Pattern matching. The pattern-matching language enables you to very accurately specify the file names that you want the policy to match. For example, you can use the pattern <code><path>/events<*>.xml</code> to match XML source file names such as <code>events.1.xml</code> and <code>events.2.xml</code>. <p>For more information on pattern matching, see "Pattern-Matching Details" on page 405.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <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> </div>
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. When dropping a numeric parameter in a time field, the policy editor appends an s to the parameter to indicate that the parameter specifies the time in seconds (for example, <code>%%interval%%s</code>).</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 style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <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 syslog.log. Mondays at 23:59, the file is renamed to syslog.monday, and a new version of syslog.log is created for the Tuesday log. Without Close after reading being selected, the policy continues to read syslog.monday because the file handle refers to the original, renamed file.</p> <p>Default value: not selected</p>
----------------------------	--

Read Mode	<p>The read mode of an log file policy indicates whether the policy processes the entire file or only new entries.</p> <table border="1"> <tr> <td data-bbox="492 338 1125 884"> <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> </td><td data-bbox="1125 338 1375 884"> <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> </td></tr> <tr> <td data-bbox="492 884 1125 1367"> <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> </td><td data-bbox="1125 884 1375 1367"> <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> </td></tr> <tr> <td data-bbox="492 1367 1125 1745"> <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> </td><td data-bbox="1125 1367 1375 1745"> <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> </td></tr> </table> <p>Note: Every policy reads the same log files independently from any other</p>	<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>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>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 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:

- Open the Management Templates & Aspects manager:








Admin > Operations Management > Monitoring > Management Templates & Aspects

- In the Configuration Folders pane, expand the configuration folders.




- In the Management Templates & Aspects pane, click an aspect, and then click the  button.

The Edit Aspect dialog box opens.




- 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" on the next page](#)
- ["opcmon Command" on the next page](#)
- ["Java API" on the next page](#)
- ["C API" on page 166](#)

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 (libopcagtap, 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 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 190](#).

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 optionally a **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 192](#).
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 178](#), ["Instructions Tab" on page 184](#), and ["Advanced Tab" on page 176](#).

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:

- **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.

- 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.

- d. *Optional.* Click **Show only newest event in event browser** to ensure that only the most current status of a threshold is shown in the Operations Management Event Browser.

This option automatically inserts values in the Event Key and Close Events with Keys fields, which cause a threshold event to close all events that were created by the same policy and that have the same node and instance.

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

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 199](#).

- 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"**.


- 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 202](#).

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:
 - **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.

For more details, see ["Instance Rules—Overview" on page 180](#).

- 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:

- 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.

- 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 181](#).

- 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:

- 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.
- 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 199](#).

- 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 202](#).

- 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 184](#).

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

UI Reference

This section includes:

- ["Actions Tab" on the next page](#)
- ["Advanced Tab" on page 176](#)
- ["Custom Attributes Tab" on page 177](#)
- ["Defaults Page" on page 178](#)
- ["Event Attributes Tab" on page 178](#)
- ["Event Correlation Tab" on page 179](#)
- ["Indicators Tab" on page 179](#)
- ["Instance Rules—Overview" on page 180](#)
- ["Instance Rules—Definition" on page 181](#)
- ["Instance Rules—Thresholds" on page 182](#)
- ["Instructions Tab" on page 184](#)
- ["Options Page" on page 184](#)
- ["Policy Data Page" on page 186](#)
- ["Policy Parameters Tab" on page 187](#)
- ["Policy Variables Tab" on page 187](#)
- ["Processing Page" on page 188](#)
- ["Properties Page" on page 190](#)
- ["Rules Page" on page 191](#)

- ["Script API Tab" on page 192](#)
- ["Source Objects Tab" on page 192](#)
- ["Source Page" on page 192](#)
- ["Threshold Rules—Overview" on page 198](#)
- ["Threshold Rules—Definition Tab" on page 199](#)
- ["Threshold Rules—Actions Tab" on page 202](#)
- ["Threshold Rules—Start Actions Tab" on page 202](#)
- ["Threshold Rules—Continue Actions Tab" on page 202](#)
- ["Threshold Rules—End Actions Tab" on page 203](#)

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 echo or move), must be preceded by cmd /c. See the Windows help for more information on cmd.
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 %%password%%. 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 <\$MSG_NODE_NAME> 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 BSM. This command can be started by the BSM user from the Operations Management 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 echo or move), must be preceded by cmd /c. See the Windows help for more information about cmd.

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 %%password%%. 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 <\$MSG_NODE_NAME> 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).

UI Element	Description
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>

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 176](#).

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 BSM.

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.
Event Suppression	





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>

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.
	<p>Copy Rule: Copies the selected instance rule. You can then rewrite the description of the copied rule and edit the rule.</p>
	<p>Delete Item: Deletes the selected instance rule.</p>
	<p>Move Up. Moves the selected instance rule higher in the rule order.</p>
	<p>Move Down. Moves the selected instance rule lower in the rule order.</p>
<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>






UI Element	Description
<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.
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.

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. <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 Rule.Status = True if the object instance matches the condition. Otherwise set Rule.Status = False.</p> <p>For a Perl Script threshold, set \$Rule->Status(TRUE); if the object instance matches the condition. Otherwise set \$Rule->Status(FALSE);.</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.

UI Element	Description
<Move to>	<p>Entered number is used to select the threshold rule with that sequence number in the list of rules.</p> <p>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.</p>
<Search Thresholds>	<p>Entered search string is used to search the threshold rule descriptions and highlight only the rules containing the specified string.</p> <p>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.</p>
	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 Operations Management 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 Operations Management 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>
that match a rule and trigger an event	<p>Logs any events in the event source that match the policy rules.</p>
that match a rule and are ignored	<p>Logs any events in the event source that are suppressed. (Suppressed events are not sent to BSM.)</p>









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 BSM when the input 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 BSM creates an event with the default values of the policy.</p> <div> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p> </div> <div> <p>Note:</p> <p>Windows event log, log file, measurement threshold, WMI and XML file policies: If several policies forward unmatched events to BSM, you could receive multiple events about a single input event.</p> </div>
are forwarded to BSM Server	Sends unmatched events to BSM.
are forwarded to BSM Server with state 'closed'	Sets the unmatched event's lifecycle status to Closed before sending it to BSM.
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) • \r Carriage return (CR) • \t Horizontal tab (HT) • \f Form feed (FF) • \v Vertical tab (VT) • \a Alert (BEL) • \b Backspace (BS) • \\ 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 _data.
	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 Variables Tab

Variable	Description
<code><\$INSTANCE></code>	Returns the name of the current instance Sample output: C;

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_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 + tty7 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, VBScriptSample 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</p>

	<p>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.• 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>
Instance Filter	<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>

Processing Options	<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.)
Event Correlation Settings	<p>You may want to ensure that only the most current status of a threshold is shown in the Operations Management Event Browser. The values that measurement threshold policies monitor can change rapidly. A condition that produces an error event might only exist for a short time. To prevent the Event Browser from filling up with threshold events that might not be current, you can use Show only newest event in event browser.</p> <p>This option automatically inserts values in the Event Key and Close Events with Keys fields, which cause a threshold event to close all events that were created by the same policy and that have the same node and instance.</p>

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).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.

¹(globally unique identifier)

²(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 instance or threshold rules.

For more details on instance rules, see ["Threshold Rules—Overview" on page 198](#), ["Threshold Rules—Definition Tab" on page 199](#), ["Threshold Rules—Actions Tab" on page 202](#), ["Threshold](#)

[Rules—Start Actions Tab](#) on page 202, ["Threshold Rules—Continue Actions Tab"](#) on page 202, and ["Threshold Rules—End Actions Tab"](#) on page 203.

For more details on threshold rules, see ["Instance Rules—Overview"](#) on page 180, ["Instance Rules—Definition"](#) on page 181, ["Instance Rules—Thresholds"](#) on page 182, ["Threshold Rules—Definition Tab"](#) on page 199, ["Threshold Rules—Actions Tab"](#) on page 202, ["Threshold Rules—Start Actions Tab"](#) on page 202, ["Threshold Rules—Continue Actions Tab"](#) on page 202, and ["Threshold Rules—End Actions Tab"](#) on page 203.


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 383.

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	 Add Source: Provides the following options: <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 information in the WMI database as the source for the threshold alarm.

	<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 optionally a 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 at 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 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 opcmn). 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>







<p>Management Information Base</p>	<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 uses the default community public 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> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Note: Instance filters are not available for threshold policies based on the source MIB.</p> </div>
<p>Program</p>	<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, <code>%OvDataDir%\bin\instrumentation\collector.exe</code>). 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: <code>example_policy_name-example_source_name</code></p> <p><\$NAME></p> <p>Returns the name of the policy, which you specify when you save the policy. Sample output: <code>example_policy_name</code></p> <p><\$SRCNAME></p> <p>Returns the name of the source, which you specify in Short Name. Sample output: <code>example_source_name</code></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>
Real Time Performance Measurement	<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 used as a wildcard to match any parent instance. For example: ?/C: matches 0/C and 1/C <p>Examples</p> <ul style="list-style-type: none"> • The percentage of free disk space on a C drive on SCSI port 0: <ul style="list-style-type: none"> Object: LogicalDisk Counter: % Free Space Instance: 0/C: • The number of free megabytes on any C: drive: <ul style="list-style-type: none"> Object: LogicalDisk Counter: Free Megabytes Instance: ?/C: • The available bytes of RAM: <ul style="list-style-type: none"> Object: Memory Counter: Available Bytes Instance: <i>empty</i>

	<ul style="list-style-type: none"> The amount of CPU time used by a specific process: Object:Process Counter:% Processor Time Instance: <i>process name</i> The paging file utilization: Object: Paging File Counter: % Usage Instance: /DosDevices/C:/pagefile.sys
Windows Management Instrumentation	<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 %%password%%. A corresponding policy parameter should exist in the Policy Parameters tab.

Polling Interval	<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. When dropping a numeric parameter in a time field, the policy editor appends an s to the parameter to indicate that the parameter specifies the time in seconds (for example, <code>%%interval%%s</code>).</p> <p>Default value: 5 minutes</p>
-------------------------	---

Threshold Rules—Overview

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>	<p>Entered number is used to select the threshold rule with that sequence number in the list of rules.</p> <p>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.</p>
<Search Thresholds>	<p>Entered search string is used to search the threshold rule descriptions and highlight only the rules containing the specified string.</p> <p>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.</p>
	Activate/Deactivate Threshold Filter. Activates and deactivates the threshold rule filter.

UI Element	Description
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)	<p>Minimum thresholds: <= (less than or equal to): Set the value that triggers an event if the monitored value is equal or lower.</p> <p>Maximum thresholds: >= (greater than or equal to): Set the value that triggers an event if the monitored value is equal or higher.</p> <p>Use the following syntax guidelines when specifying the minimum or maximum threshold:</p> <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</p> <p>One or more decimal digits. For example: 25.88e4</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <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 cpu load with a threshold level called condition critical that you want to override with the limit 75 and the reset value 70, set a parameter with the following value:</p> </div>

UI Element	Description
	<p>cpu load/condition critical/75:70</p> <p>The following limitations apply:</p> <ul style="list-style-type: none"> Specify <i><policy_name></i> and <i><threshold_level_description></i> exactly as they appear in the policy editor. The first and last slash marks (/) delimit the <i><threshold_level_description></i>, which can itself contain slash marks. <i><reset_value></i> is required, even if it is the same as <i><limit></i>. <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 <i><parameter_name></i> can be any alphanumeric string that is unique within the eaagt.thresholds namespace. Adding (thresholds) after <i><parameter_name></i> 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_value></pre> <p>The <i><parameter_name></i> can be any alphanumeric string that is unique within the eaagt.thresholds namespace.</p>
Threshold Limit (Perl or VB Script)	<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

UI Element	Description
	<p>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>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. When dropping a numeric parameter in a time field, the policy editor appends an s to the parameter to indicate that the parameter specifies the time in seconds (for example, <code>%%interval%%s</code>).</p>
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.
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.

UI Element	Description
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](#).

2. 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](#).



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> .
	Node Info 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 "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.

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>

UI Element	Description
Description	Description of what the policy does. You might also add other notes (for example, data sources that are used).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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)

²(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 Open Message Interface Policies

The HP Operations Agent provides a command (called `opcmsg`), 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" on the next page](#)
- ["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>]
```

opcmsg is available in one of the following locations.

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

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 (jopcagtbases.jar and jopcagtmessages.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 (libopcagtcapi, 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 227](#).

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.

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

For more details, see ["Event Attributes Tab" on page 219](#), ["Event Correlation Tab" on page 220](#), ["Instructions Tab" on page 222](#), and ["Advanced Tab" on page 217](#)

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 226](#).

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.

You can enter pattern matching expressions and policy parameters in the text boxes.

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:

```
opcmmsg application="Insurance Application" object="Server Process" msg_  
text="FATAL ERROR: The server process failed to start."
```

For more details, see ["Condition Tab" on page 218](#).

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 219](#), ["Event Correlation Tab" on page 220](#), ["Custom Attributes Tab" on page 219](#), ["Instructions Tab" on page 222](#), ["Advanced Tab" on page 217](#), 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 222](#).

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

UI Reference

This section includes:

- ["Actions Tab" below](#)
- ["Advanced Tab" on page 217](#)
- ["Condition Tab" on page 218](#)
- ["Custom Attributes Tab" on page 219](#)
- ["Defaults Page" on page 219](#)
- ["Event Attributes Tab" on page 219](#)
- ["Event Correlation Tab" on page 220](#)
- ["Indicators Tab" on page 220](#)
- ["Instructions Tab" on page 222](#)
- ["Options Page" on page 222](#)
- ["Policy Data Page" on page 224](#)
- ["Policy Parameters Tab" on page 225](#)
- ["Policy Rules List" on page 226](#)
- ["Policy Variables Tab" on page 227](#)
- ["Properties Page" on page 227](#)
- ["Rules Page" on page 229](#)

Actions Tab

UI Element	Description
Automatic command	Automatic command that runs when the rule is matched.

UI Element	Description
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 echo or move), must be preceded by cmd /c. See the Windows help for more information on cmd.
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 %%password%%. 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 <\$MSG_NODE_NAME> 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 BSM. This command can be started by the BSM user from the Operations Management 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 echo or move), must be preceded by cmd /c. See the Windows help for more information about cmd.
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 %%password%%. 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 <\$MSG_NODE_NAME> 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

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.
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 node option of the opcmmsg 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 msg_grp option of the opcmmsg 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 application option of the opcmmsg command.</p>
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 object option of the opcmmsg command.</p> <div> <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> </div>
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 severity option of the opcmmsg 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 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> <ul style="list-style-type: none"> Description EtiHint HP_OPR_SAAS_CUSTOMER_ID NoDuplicateSuppression RelatedCiHint SourceCiHint SourcedFromExternalId SourcedFromExternalUrl SubCategory SubCiHint
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 217](#).

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.
Send with closed status	Sets the event's lifecycle status to Closed before sending it to BSM.

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.
Event Suppression	
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>

UI Element	Description
	<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 Operations Management 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 Operations Management 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>
that match a rule and trigger an event	<p>Logs any events in the event source that match the policy rules.</p>
that match a rule and are ignored	<p>Logs any events in the event source that are suppressed. (Suppressed events are not sent to BSM.)</p>









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 BSM when the input 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 BSM creates an event with the default values of the policy.</p> <div> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p> </div> <div> <p>Note:</p> <p>Open message interface and SNMP trap policies: The agent creates an event for an unmatched event only if the input event is unmatched in all policies on the node. The agent sends only one event for each unmatched input event.</p> </div>
are forwarded to BSM Server	Sends unmatched events to BSM.
are forwarded to BSM Server with state 'closed'	Sets the unmatched event's lifecycle status to Closed before sending it to BSM.
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) • \r Carriage return (CR) • \t Horizontal tab (HT) • \f Form feed (FF) • \v Vertical tab (VT) • \a Alert (BEL) • \b Backspace (BS) • \\ 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 _data.
	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>Event policies: 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.
	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>	<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>
	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

UI Element	Description
Rule Type	<p>The three rule types of event policies are:</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>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 msg_text parameter submitted by the opcmsg command. Sample output: SU 03/19 16:13 + ttyp7 bill-root
<\$OPTION(N)>	Returns the value of an optional variable that is set by opcmsg (for example, <\$OPTION(A)>, <\$OPTION(B)>, and so on.).

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
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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)

²(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 226](#), ["Condition Tab" on page 218](#), ["Event Attributes Tab" on page 219](#), ["Event Correlation Tab" on page 220](#), ["Custom Attributes Tab" on page 219](#), ["Advanced Tab" on page 217](#), and ["Actions Tab" on page 214](#).

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:
 - 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 **Scheduled Task 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 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:
 - 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.

- 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 237.

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 240](#).

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 238](#).

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 indicators, policy variables, and policy parameters.

For more details, see ["Event Attributes Tab" on page 233](#), ["Event Correlation Tab" on page 234](#), ["Custom Attributes Tab" on the next page](#), ["Instructions Tab" on page 235](#), 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 233](#)
- ["Event Correlation Tab" on page 234](#)
- ["Indicators Tab" on page 234](#)
- ["Instructions Tab" on page 235](#)


- ["Policy Data Page" on page 235](#)
- ["Policy Parameters Tab" on page 235](#)
- ["Policy Variables Tab" on page 236](#)
- ["Properties Page" on page 237](#)
- ["Schedule Page" on page 238](#)
- ["Start, Success, and Failure Event Page" on page 240](#)
- ["Task Page" on page 240](#)

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_n. To rename the custom attribute, double-click the name to select it and type the new name.

UI Element	Description
	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 BSM.

Event Correlation Tab

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



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 Operations Management 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 Operations Management 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.

UI Element	Description
	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 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

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.
<\$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
<\$PROG>	Returns the name of the program executed by the scheduled task policy Sample output: check_for_upgrade.bat
<\$USER>	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).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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> <div> <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> </div>


¹(globally unique identifier)

²(globally unique identifier)

UI Element	Description
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>

Schedule Page

UI Element	Description
	
	Select All. Selects all units of time.


UI Element	Description
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.
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)	

UI Element	Description
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

UI Element	Description
Command	<p>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.</p> <p>By default, the command runs under the same account as the agent is running, which is Local System or root by default.</p>
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	<p>Code that defines the VB script. Instead of typing the script into the field, you can upload an existing script.</p> <div> <p>Tip: Use the policy method Rule.Status to specify whether the task is successful. For example, to specify that the task has failed (and trigger a failure event), use Rule.Status=False.</p> </div> <div> <p>Note: 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.</p> </div>

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" on the next page](#)
- ["Configuration Item XML Schema Definition \(XSD\)" on the next page](#)
- ["Configuration Item XML Element Description" on page 246](#)

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>
    </xs:schema>
```

```
</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>
```

```

        </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 <code>ref</code> 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	<p>Represents a CI that you want to delete immediately.</p> <p>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.</p> <div> <p>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 RTSM¹.</p> </div>
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.

¹(Run-time Service Model)

Element	Description
Key	Contains the full CI ID for this CI, which must be unique. You must include this element in all <i>NewInstance</i> and <i>DeleteInstance</i> elements. You must not specify a <i>NewInstance</i> and <i>DeleteInstance</i> with the same key in the same XML document.
Attributes	Contains <i>Attribute</i> elements.
Attribute	<p>Has a name attribute and a value attribute.</p> <p>Attributes with the following names have a special meaning:</p> <ul style="list-style-type: none"> • <i>hpom_citype</i> specifies the CI type as stored in the RTSM (for example, nt). <p>The default synchronization package on the BSM server assigns the context <i>IntegrationAdapter</i> to all CIs that have a <i>hpom_citype</i> 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"> • <i>hpom_rootcontainer</i> specifies the full ID of the CI that contains or hosts this CI. Maps to the CI attribute <i>Container</i>. Creates a composition relationship. • Attribute names with the prefix <i>ucmdb_map</i> directly to CI attributes (for example, <i>ucmdb_primary_dns_name</i> maps to the CI attribute <i>Primary DNS Name</i>).
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 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 <i>ref</i> 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 <i>type</i> attribute that refers to the type of relation as stored in the RTSM (for example, <i>usage</i>). 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 250](#).

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 244](#).

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 244](#).

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 250](#)

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.

UI Element	Description
<policy data>	Policy data in text form. The data uses the HP Operations Agent policy syntax. For details, see "Service Auto-Discovery Policy Syntax" on page 244.

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).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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.

¹(globally unique identifier)

²(globally unique identifier)

UI Element	Description
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" on the next page](#)

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 269](#).

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 271](#).

In text boxes, you can use indicators, policy variables, and policy parameters. You can also use 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 265](#), ["Event Correlation Tab" on page 266](#), ["Custom Attributes Tab" on page 264](#), ["UI Element" on page 266](#), ["Advanced Tab" on page 262](#), and ["Actions Tab \(Events\)" on page 258](#).

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 267](#).

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).

You can insert policy parameters in the text boxes of the Condition tab.

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 265](#), ["Event Correlation Tab" on page 266](#), ["Custom Attributes Tab" on page 264](#), ["UI Element" on page 266](#), ["Advanced Tab" on page 262](#), 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 265](#), ["Event Correlation Tab" on page 266](#), ["Custom Attributes Tab" on page 264](#), ["UI Element" on page 266](#), ["Advanced Tab" on page 262](#), 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 265](#), ["Event Correlation Tab" on page 266](#), ["Custom Attributes Tab" on page 264](#), ["UI Element" on page 266](#), ["Advanced Tab" on page 262](#), and ["Actions Tab \(Events\)" on the next page](#).

In text boxes, you can use indicators, policy variables, and policy parameters. You can also use 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 \(Events\)" below](#)
- ["Actions Tab \(Rules\)" on page 261](#)
- ["Advanced Tab" on page 262](#)
- ["Condition Tab" on page 262](#)
- ["Custom Attributes Tab" on page 264](#)
- ["Event Attributes Tab" on page 265](#)
- ["Event Correlation Tab" on page 266](#)
- ["Instructions Tab" on page 266](#)
- ["Policy Data Page" on page 266](#)
- ["Policy Parameters Tab" on page 267](#)
- ["Policy Rules List" on page 267](#)
- ["Policy Variables Tab" on page 268](#)
- ["Properties Page" on page 269](#)
- ["Source Page" on page 270](#)
- ["Start, Continue, and End Actions \(Defaults\)" on page 271](#)
- ["Start, Continue, and End Actions \(Rules\)" on page 271](#)

Actions Tab (Events)

UI Element	Description
Automatic command	Automatic command that runs when the rule is matched.

UI Element	Description
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 echo or move), must be preceded by cmd /c. See the Windows help for more information on cmd.
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 %%password%%. 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 <\$MSG_NODE_NAME> 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 BSM. This command can be started by the BSM user from the Operations Management 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 echo or move), must be preceded by cmd /c. See the Windows help for more information about cmd.
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 %%password%%. 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 <\$MSG_NODE_NAME> 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, svchost.exe -k rpcss and svchost.exe -k netsvcs). 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, <*> matches <i>all</i> parameters, and <*>abc<*> 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 (==) 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).</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 >= 1 (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	<p>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).</p>
Memory usage	<p>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).</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 BSM.



Event Correlation Tab

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









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 Operations Management 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 Operations Management 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 _data.
	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
	Create New Rule: Adds a rule to the service/process monitoring policy.

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.
<Search rules>	Entered search string is used to search the service or process names and highlight only the rules containing the specified string. 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.
	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.
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).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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> <div> <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> </div>
Change Log	Text that describes what is new or modified in this version of the policy.

¹(globally unique identifier)

²(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>

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> <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. When dropping a numeric parameter in a time field, the policy editor appends an s to the parameter to indicate that the parameter specifies the time in seconds (for example, <code>%%interval%%s</code>).</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 265](#), ["Event Correlation Tab" on page 266](#), ["Custom Attributes Tab" on page 264](#), ["UI Element" on page 266](#), ["Advanced Tab" on page 262](#), and ["Actions Tab \(Events\)" on page 258](#).

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.

UI Element	Description
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 292](#).

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.

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

For more details, see ["Event Attributes Tab" on page 282](#), ["Event Correlation Tab" on page 283](#), ["Instructions Tab" on page 285](#), and ["Advanced Tab" on page 278](#).

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 289](#).

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.

You can enter pattern matching expressions and policy parameters in the text boxes.


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 279](#).

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 and policy parameters 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 282](#), ["Event Correlation Tab" on page 283](#), ["Custom Attributes Tab" on page 281](#), ["Instructions Tab" on page 285](#), ["Advanced Tab" on page 278](#), 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 285](#).

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

UI Reference

This section includes:

- ["Actions Tab" below](#)
- ["Advanced Tab" on page 278](#)
- ["Condition Tab" on page 279](#)
- ["Condition Variable Bindings Tab" on page 281](#)
- ["Custom Attributes Tab" on page 281](#)
- ["Defaults Page" on page 282](#)
- ["Event Attributes Tab" on page 282](#)
- ["Event Correlation Tab" on page 283](#)
- ["Indicators Tab" on page 283](#)
- ["Instructions Tab" on page 285](#)
- ["Options Page" on page 285](#)
- ["Policy Data Page" on page 287](#)
- ["Policy Parameters Tab" on page 288](#)
- ["Policy Rules List" on page 289](#)
- ["Policy Variables Tab" on page 290](#)
- ["Properties Page" on page 292](#)
- ["Rules Page" on page 293](#)

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 echo or move), must be preceded by cmd /c. See the Windows help for more information on cmd.

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 %%password%%. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	<p>Name of the node on which the command will be started. You can also use the variable <\$MSG_NODE_NAME> to configure reusable policies for replicated sites.</p>
Append output of command as annotation to the event	<p>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.</p>
Close the event when the command is successful	<p>Closes the event automatically if the command is successful.</p>
Send event immediately	<p>Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.</p>
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	<p>Operator-initiated command that is attached to the event that the rule sends to BSM. This command can be started by the BSM user from the Operations Management Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.</p>

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 echo or move), must be preceded by cmd /c. See the Windows help for more information about cmd.
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 %%password%%. 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 <\$MSG_NODE_NAME> 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.
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, celery.example.com broccoli.example.com), or leave blank for all configuration items.</p>





¹(Fully Qualified Domain Name)

²(Fully Qualified Domain Name)



Event Object ID	Complete Event Object Identifier for the SNMP trap that you want to match. For example: .1.3.6.1.4.1.11.2.17.1.0.40000001
SNMPv1 notation	If selected, you can specify only part of the identifier rather than the complete event object ID. For example, by specifying only the Enterprise ID, you can match all events with a specific Enterprise ID.
Enterprise ID	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: .1.3.6.1.4.1.11.2.17 would match: .1.3.6.1.4.1.11.2.17.1 .1.3.6.1.4.1.11.2.17.2 and so on.
Generic ID	Generic Trap ID. Possible values are: <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>
Specific ID	Type in the specific trap ID if you have selected (6) EnterpriseSpecific in Generic Trap. Enterprise-specific SNMP traps can be implemented by vendors on their specific network devices. The specific trap ID is used to identify the source of the trap.

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

Condition Variable Bindings Tab

UI Element	Description
	Creates a new variable binding.
	Deletes the selected variable binding.
	Opens the Variable Bindings Options page.
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.

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 278](#).

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 BSM.

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.
Event Suppression	
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>

UI Element	Description
	<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 Operations Management 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 Operations Management 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	<p>Logs any events in the event source that match the policy rules.</p>
that match a rule and are ignored	<p>Logs any events in the event source that are suppressed. (Suppressed events are not sent to BSM.)</p>









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 BSM when the input 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 BSM creates an event with the default values of the policy.</p> <div> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p> </div> <div> <p>Note:</p> <p>Open message interface and SNMP trap policies: The agent creates an event for an unmatched event only if the input event is unmatched in all policies on the node. The agent sends only one event for each unmatched input event.</p> </div>
are forwarded to BSM Server	Sends unmatched events to BSM.
are forwarded to BSM Server with state 'closed'	Sets the unmatched event's lifecycle status to Closed before sending it to BSM.
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) • \r Carriage return (CR) • \t Horizontal tab (HT) • \f Form feed (FF) • \v Vertical tab (VT) • \a Alert (BEL) • \b Backspace (BS) • \\ 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 _data.
	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><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.
	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>	<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>
	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

UI Element	Description
Rule Type	<p>The three rule types of event policies are:</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>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>nth</i> 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>nth</i> variable binding as [<i>seq</i>] <i>name-type:value</i> . Sample output: [2] .1.2 (OctetString): brusselsprouts.example.com

Variable	Description
<\$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
<\$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

Variable	Description
<\$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).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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> <div> <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> </div>
Change Log	Text that describes what is new or modified in this version of the policy.

¹(globally unique identifier)

²(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	<p>The name of the user active when the policy was saved.</p>
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 289](#), ["Condition Tab" on page 279](#), ["Condition Variable Bindings Tab" on page 281](#), ["Event Attributes Tab" on page 282](#), ["Event Correlation Tab" on page 283](#), ["Custom Attributes Tab" on page 281](#), ["Advanced Tab" on page 278](#), and ["Actions Tab" on page 276](#).

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 310](#).

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 312](#).

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.

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

For more details, see ["Event Attributes Tab" on page 303](#), ["Event Correlation Tab" on page 303](#), ["Instructions Tab" on page 305](#), and ["Advanced Tab" on page 299](#).

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 309](#).

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 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 300](#) and ["Pattern Matching in Policy Rules" on page 405](#).

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 303](#), ["Event Correlation Tab" on page 303](#), ["Custom Attributes Tab" on page 302](#), ["Instructions Tab" on page 305](#), ["Advanced Tab" on page 299](#), 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 305](#).

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

UI Reference

This section includes:

- ["Actions Tab" on the next page](#)
- ["Advanced Tab" on page 299](#)
- ["Condition Tab" on page 300](#)

- ["Custom Attributes Tab" on page 302](#)
- ["Defaults Page" on page 302](#)
- ["Event Attributes Tab" on page 303](#)
- ["Event Correlation Tab" on page 303](#)
- ["Indicators Tab" on page 304](#)
- ["Instructions Tab" on page 305](#)
- ["Options Page" on page 305](#)
- ["Policy Data Page" on page 307](#)
- ["Policy Parameters Tab" on page 308](#)
- ["Policy Rules List" on page 309](#)
- ["Policy Variables Tab" on page 310](#)
- ["Properties Page" on page 310](#)
- ["Rules Page" on page 312](#)
- ["Source Page" on page 312](#)

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 echo or move), must be preceded by cmd /c. See the Windows help for more information on cmd.

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 %%password%%. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	<p>Name of the node on which the command will be started. You can also use the variable <\$MSG_NODE_NAME> to configure reusable policies for replicated sites.</p>
Append output of command as annotation to the event	<p>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.</p>
Close the event when the command is successful	<p>Closes the event automatically if the command is successful.</p>
Send event immediately	<p>Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.</p>
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	<p>Operator-initiated command that is attached to the event that the rule sends to BSM. This command can be started by the BSM user from the Operations Management Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.</p>

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 echo or move), must be preceded by cmd /c. See the Windows help for more information about cmd.
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 %%password%%. 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 <\$MSG_NODE_NAME> 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
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>

UI Element	Description
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 OPC_COND_EVT_LOG_SRC_PAT in the eaagt namespace to TRUE.</p>
Category equals	A classification of the event by the event source.
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> <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> <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

UI Element	Description
	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.
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](#), ["Instructions Tab" on page 305](#), and ["Advanced Tab" on page 299](#).

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.
Send with closed status	Sets the event's lifecycle status to Closed before sending it to BSM.

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.
Event Suppression	
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 Operations Management 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 Operations Management 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>
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 BSM.)









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 BSM when the input 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 BSM creates an event with the default values of the policy.</p> <div> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p> </div> <div> <p>Note:</p> <p>Windows event log, log file, measurement threshold, WMI and XML file policies: If several policies forward unmatched events to BSM, you could receive multiple events about a single input event.</p> </div>
are forwarded to BSM Server	Sends unmatched events to BSM.
are forwarded to BSM Server with state 'closed'	Sets the unmatched event's lifecycle status to Closed before sending it to BSM.
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) • \r Carriage return (CR) • \t Horizontal tab (HT) • \f Form feed (FF) • \v Vertical tab (VT) • \a Alert (BEL) • \b Backspace (BS) • \\ 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 _data.
	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><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.
	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>	<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>
	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

UI Element	Description
Rule Type	<p>The three rule types of event policies are:</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>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

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	<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
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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)

²(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 309](#), ["Condition Tab" on page 300](#), ["Event Attributes Tab" on page 303](#), ["Event Correlation Tab" on page 303](#), ["Custom Attributes Tab" on page 302](#), ["Advanced Tab" on page 299](#), and ["Actions Tab" on page 297](#).

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	<p>The agent sends an event if for some reason the event log is missing.</p> <p>Default value: not selected</p>

Read Mode	<p>The read mode of an event log policy indicates whether the policy processes the entire event log or only new entries.</p> <table border="1" data-bbox="418 336 1367 1537"> <tr> <td data-bbox="427 346 1156 982"> <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> </td><td data-bbox="1164 346 1359 982"> <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> </td></tr> <tr> <td data-bbox="427 993 1156 1526"> <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> </td><td data-bbox="1164 993 1359 1526"> <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> </td></tr> </table> <div data-bbox="427 1564 1359 1738" style="background-color: #f0f0f0; padding: 10px;"> <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> </div> <p>Default value: Read from last position</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>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>				

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 332](#).

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.

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

For more details, see ["Event Attributes Tab" on page 324](#), ["Event Correlation Tab" on page 325](#), ["Instructions Tab" on page 326](#), and ["Advanced Tab" on page 321](#).

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 330](#).

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 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 322](#) and ["Pattern Matching in Policy Rules" on page 405](#).

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 324](#), ["Event Correlation Tab" on page 325](#), ["Custom Attributes Tab" on page 323](#), ["Instructions Tab" on page 326](#), ["Advanced Tab" on page 321](#), 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 327](#).

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

UI Reference

This section includes:

- ["Actions Tab" on the next page](#)
- ["Advanced Tab" on page 321](#)

- ["Condition Tab" on page 322](#)
- ["Custom Attributes Tab" on page 323](#)
- ["Defaults Page" on page 324](#)
- ["Event Attributes Tab" on page 324](#)
- ["Event Correlation Tab" on page 325](#)
- ["Indicators Tab" on page 325](#)
- ["Instructions Tab" on page 326](#)
- ["Options Page" on page 327](#)
- ["Policy Data Page" on page 329](#)
- ["Policy Parameters Tab" on page 329](#)
- ["Policy Rules List" on page 330](#)
- ["Policy Variables Tab" on page 331](#)
- ["Properties Page" on page 332](#)
- ["Rules Page" on page 333](#)
- ["Source Page" on page 333](#)

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 echo or move), must be preceded by cmd /c. See the Windows help for more information on cmd.

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 %%password%%. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	<p>Name of the node on which the command will be started. You can also use the variable <\$MSG_NODE_NAME> to configure reusable policies for replicated sites.</p>
Append output of command as annotation to the event	<p>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.</p>
Close the event when the command is successful	<p>Closes the event automatically if the command is successful.</p>
Send event immediately	<p>Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.</p>
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	<p>Operator-initiated command that is attached to the event that the rule sends to BSM. This command can be started by the BSM user from the Operations Management Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.</p>









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 echo or move), must be preceded by cmd /c. See the Windows help for more information about cmd.
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 %%password%%. 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 <\$MSG_NODE_NAME> 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).


UI Element	Description
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.
	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.

UI Element	Description
Property	The name of the property that you want the rule to inspect. Properties must begin with a letter.
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> <div> <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.

UI Element	Description
	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" on the next page](#), ["Instructions Tab" on page 326](#), and ["Advanced Tab" on page 321](#).

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.




UI Element	Description
Send with closed status	Sets the event's lifecycle status to Closed before sending it to BSM.

Event Correlation Tab

UI Element	Description
Event Key	An identifier used to identify duplicates and for Close Events with Key.
Event Suppression	
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 Operations Management 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 Operations Management 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>
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 BSM.)
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 BSM when the input 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 BSM 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:</p> <p>Windows event log, log file, measurement threshold, WMI and XML file policies: If several policies forward unmatched events to BSM, you could receive multiple events about a single input event.</p>
are forwarded to BSM Server	Sends unmatched events to BSM.





UI Element	Description
are forwarded to BSM Server with state 'closed'	Sets the unmatched event's lifecycle status to Closed before sending it to BSM.
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.
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) • \r Carriage return (CR) • \t Horizontal tab (HT) • \f Form feed (FF) • \v Vertical tab (VT) • \a Alert (BEL) • \b Backspace (BS) • \\ 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.
	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
	<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.
	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.

UI Element	Description
<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>
	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	<p>The three rule types of event policies are:</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>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

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

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.
<\$MSG_ TEXT>	Returns the full text of the event. Sample output: SU 03/19 16:13 + tttyp7 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	<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).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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> <div> <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> </div>
Change Log	Text that describes what is new or modified in this version of the policy.

¹(globally unique identifier)
²(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 330](#), ["Condition Tab" on page 322](#), ["Event Attributes Tab" on page 324](#), ["Event Correlation Tab" on page 325](#), ["Custom Attributes Tab" on page 323](#), ["Advanced Tab" on page 321](#), and ["Actions Tab" on page 319](#).

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 %%password%%. 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> <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 %%<variable_name>%% or drag and drop the parameter from the Policy Parameters tab. When dropping a numeric parameter in a time field, the policy editor appends an s to the parameter to indicate that the parameter specifies the time in seconds (for example, %%interval%%s).</p>

<p>Query instance of class</p>	<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> <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. When dropping a numeric parameter in a time field, the policy editor appends an s to the parameter to indicate that the parameter specifies the time in seconds (for example, <code>%%interval%%s</code>).</p>
<p>Query the intrinsic event for these instances</p>	<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.</p> <p>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>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. When dropping a numeric parameter in a time field, the policy editor appends an s to the parameter to indicate that the parameter specifies the time in seconds (for example, <code>%%interval%%s</code>).</p>

Use global WQL filter	<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> <p><code>TargetInstance.InteractWithDeskTop = 1</code> <code>TargetNamespace.name = "CIMV2"</code></p>
------------------------------	--


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" on the next page](#)
- ["Mappings overview" on page 339](#)

Requirements for XML source files

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

- XML file requirements:
 - Use file rolling to create at least two or more XML input files. BSM Connector first reads the older file before starting to process the younger file. Each file should not be larger than 2 GB.

You can use wildcards in the **Log File Path / Name** field to match multiple file names. For example, to match the XML source file names events.1.xml and events.2.xml, use the pattern `<path>/events<*>.xml` in the Log File Path / Name field. For more information on pattern matching, see ["Pattern-Matching Details" on page 405](#).

Make sure the **Close after reading** check box is cleared when using file rolling.

- Make sure the polling interval is shorter than the frequency in which data is written to the file.
- XML format requirements:
 - 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.

Example:

```
<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>
```

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 358](#).

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 360](#).

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.

- 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.

- 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 351](#) and ["Indicators Tab" on page 350](#).

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.


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

For more details, see ["Event Attributes Tab" on page 350](#), ["Event Correlation Tab" on page 350](#), ["Custom Attributes Tab" on page 349](#), ["Instructions Tab" on page 351](#), and ["Advanced Tab" on page 346](#).

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 356](#).

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 347](#).

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 350](#), ["Event Correlation Tab" on page 350](#), ["Custom Attributes Tab" on page 349](#), ["Instructions Tab" on page 351](#), ["Advanced Tab" on page 346](#), 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 353](#).

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

UI Reference

This section includes:

- ["Actions Tab" on the next page](#)
- ["Advanced Tab" on page 346](#)
- ["Condition Tab" on page 347](#)
- ["Custom Attributes Tab" on page 349](#)
- ["Defaults Page" on page 349](#)

- ["Event Attributes Tab" on page 350](#)
- ["Event Correlation Tab" on page 350](#)
- ["Indicators Tab" on page 350](#)
- ["Instructions Tab" on page 351](#)
- ["Mappings Page" on page 351](#)
- ["Mappings Tab" on page 352](#)
- ["Options Page" on page 353](#)
- ["Pattern Matching Variables Tab" on page 355](#)
- ["Policy Data Page" on page 355](#)
- ["Policy Parameters Tab" on page 355](#)
- ["Policy Rules List" on page 356](#)
- ["Policy Variables Tab" on page 357](#)
- ["Properties Page" on page 358](#)
- ["Rules Page" on page 359](#)
- ["Sample Data Tab" on page 359](#)
- ["Source Page" on page 360](#)

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 echo or move), must be preceded by cmd /c. See the Windows help for more information on cmd.

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 %%password%%. A corresponding policy parameter should exist in the Policy Parameters tab.
Node	<p>Name of the node on which the command will be started. You can also use the variable <\$MSG_NODE_NAME> to configure reusable policies for replicated sites.</p>
Append output of command as annotation to the event	<p>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.</p>
Close the event when the command is successful	<p>Closes the event automatically if the command is successful.</p>
Send event immediately	<p>Sends an event to the BSM server as soon as a local automatic command starts on the node. This is the default setting.</p>
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	<p>Operator-initiated command that is attached to the event that the rule sends to BSM. This command can be started by the BSM user from the Operations Management Event Browser. The command might be a script that requires user input to solve the problem, or instructions that appear in a Web browser.</p>









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 echo or move), must be preceded by cmd /c. See the Windows help for more information about cmd.
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 %%password%%. 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 <\$MSG_NODE_NAME> 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).



UI Element	Description
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.
	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.

UI Element	Description
Property	<i>XML file policies:</i> 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	<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><i>XML file policies:</i> 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.</p> <div> <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_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> <ul style="list-style-type: none"> Description EtiHint HP_OPR_SAAS_CUSTOMER_ID NoDuplicateSuppression RelatedCiHint SourceCiHint SourcedFromExternalId SourcedFromExternalUrl SubCategory SubCiHint
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 351](#), and ["Advanced Tab" on page 346](#).



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.
Event Suppression	
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 Operations Management 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 Operations Management 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://

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 map to the map name if the variable has been created from sample data.
Data Input Property	<p><i>XML file policies:</i> XML element or attribute assigned to the custom variable.</p> <p>XML properties use the following syntax: <code><\$DATA:/<XML_property>></code></p> <p><code><XML_property></code> 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	<i>XML file policies:</i> Original value of the XML element or attribute.
Target Value	<i>XML file policies:</i> 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 BSM.)
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 BSM when the input 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 BSM creates an event with the default values of the policy.</p> <div> <p>Tip: If you want a policy to send events only with the default values, omit all rules from the policy.</p> </div> <div> <p>Note:</p> <p>Windows event log, log file, measurement threshold, WMI and XML file policies: If several policies forward unmatched events to BSM, you could receive multiple events about a single input event.</p> </div>
are forwarded to BSM Server	Sends unmatched events to BSM.

UI Element	Description
are forwarded to BSM Server with state 'closed'	Sets the unmatched event's lifecycle status to Closed before sending it to BSM.
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.
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) • \r Carriage return (CR) • \t Horizontal tab (HT) • \f Form feed (FF) • \v Vertical tab (VT) • \a Alert (BEL) • \b Backspace (BS) • \\ 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>

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
	<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.
	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.

UI Element	Description
<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>
	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	<p>The three rule types of event policies are:</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>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.

Variable	Description
<\$MSG_TEXT>	Returns the full text of the event. Sample output: SU 03/19 16:13 + tttyp7 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).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.
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> <div>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.</div>
Change Log	Text that describes what is new or modified in this version of the policy.

¹(globally unique identifier)

²(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 356](#), ["Condition Tab" on page 347](#), ["Event Attributes Tab" on page 350](#), ["Event Correlation Tab" on page 350](#), ["Custom Attributes Tab" on page 349](#), ["Advanced Tab" on page 346](#), and ["Actions Tab" on page 344](#).

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>

UI Element	Description
	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.
	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.
	Toggle Deduplication. Shows or hides duplicate values.
XML Properties	Shows all XML elements and attributes that match an XML event tag. (You can identify attributes based on the preceding at sign (@).) 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.
Values for <...>	Displays the values of the XML property selected in the XML Properties section.





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>You can use the following configurations to make your policy more flexible:</p> <ul style="list-style-type: none"> • Windows environment variables (for example, winnt or clusterlog). The syntax for these variables is <code><\$variablename></code>, for example <code><\$winnt></code>. • Script or command that returns the path and name of the log file you want to access. For example, type <code><'command'></code> where command is the name of a script that returns the path and name of the log file you want the policy to read. <p>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> <ul style="list-style-type: none"> • Pattern matching. The pattern-matching language enables you to very accurately specify the file names that you want the policy to match. For example, you can use the pattern <code><path>/events<*>.xml</code> to match XML source file names such as events.1.xml and events.2.xml. <p>For more information on pattern matching, see "Pattern-Matching Details" on page 405.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Note: The agent cannot process log files that are larger than 2 GB.</p> </div>
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. When dropping a numeric parameter in a time field, the policy editor appends an s to the parameter to indicate that the parameter specifies the time in seconds (for example, <code>%%interval%%s</code>).</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> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <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> </div> <p>Default value: UTF-8</p>
Send event if log file does not exist	<p>The agent sends an event if the specified XML file does not exist.</p> <p>Default value: not selected</p>
Close after reading	<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 syslog.log. Mondays at 23:59, the file is renamed to syslog.monday, and a new version of syslog.log is created for the Tuesday log. Without Close after reading being selected, the policy continues to read syslog.monday because the file handle refers to the original, renamed file.</p> <p>Default value: not selected</p>

Read Mode	The read mode of an XML 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 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	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>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>
	Opens the XML Sample Data dialog box. This dialog box displays the contents of the uploaded XML sample file.
XML Event Tag	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>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" on the next page](#)
- ["Templates" on the next page](#)
- ["Prerequisite for Importing SiteScope Templates" on the next page](#)
- ["Assigning and Deploying SiteScope Policy Templates" on page 367](#)

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 chooses 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

SiteScope policy templates must be assigned to the remote servers that you want to monitor with SiteScope. Before deploying the policy template, Operations Management replaces 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.

What to avoid:

- Do not assign SiteScope policy templates to the SiteScope server itself. The policy templates must always be assigned to the remote servers that will be monitored by SiteScope.
- Do not use the hostname of the CI to be monitored as value of the instance parameter representing the hosts to be monitored. For example, do not enter `ora.example.com` as instance parameter value. Instead, use the symbolic value `%%HOST%%` or set the parameter value based on the CI attribute `PrimaryDNSName`. The symbolic values are automatically resolved during deployment to the monitored CIs.

Tasks

This section includes:

- ["Prerequisite Tasks" below](#)
- ["How to Configure the Agent on the SiteScope System" on the next page](#)
- ["How to Connect to a SiteScope Server That Requires SSL" on page 370](#)
- ["How to Import Templates from a SiteScope Server" on page 371](#)
- ["How to Assign SiteScope Policy Templates to Remote Servers" on page 372](#)

Prerequisite Tasks

Before you can monitor a configuration item (CI) with SiteScope, you must complete the following steps:

1. Install and configure the agent on the SiteScope system:
 - a. Install the HP Operations Agent on the SiteScope system. For details, see the HP SiteScope Deployment Guide.
 - b. 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.

2. Prepare the agent on the SiteScope system for deployment:
 - a. Update the SiteScope configuration component `sisconfig`.
 - b. Configure the agent with the SiteScope user credentials. The SiteScope user credentials are required for the deployment of SiteScope policy templates.
 - c. 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" below](#).

3. Set up the SiteScope system as a connected server in Operations Management.

For details, see "Connected Servers" in the BSM Application Administration Guide.

4. Verify that a node CI has been created for the SiteScope system, access:

Admin > Operations Management > Setup > Monitored Nodes

5. Make sure the systems that SiteScope monitors are represented as node CIs in the RTSM, access:

Admin > Operations Management > Setup > Monitored Nodes

6. Configure templates in SiteScope and import them. For details, see ["Prerequisite for Importing SiteScope Templates" on page 366](#) and ["Importing HP SiteScope Templates" on page 364](#).

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. Update the SiteScope configuration component `sisconfig`:
 - a. On the BSM server, navigate to the following directory:

```
<OvInstallDir>/opr/subagents/sitescope
```
 - b. Open the following archive:

sisinstall-<version>.zip

where <version> is the installed agent version.

- c. Extract the following file from the archive and copy it to a temporary location on the SiteScope server:

oprsisconnector.jar

- d. On the SiteScope server, run the following command to stop the sisconfig component:

ovc -stop sisconfig

- e. Replace the following file with the file you copied from the SiteScope server:

Windows: <OvInstallDir>\java\oprsisconnector.jar

Linux: /opt/OV/java/oprsisconnector.jar

The sisconfig component is now updated to the version to be used with Monitoring Automation.

- f. Issue the following command to restart the sisconfig component:

ovc -start sisconfig

2. Configure the agent with the SiteScope user credentials:

- a. On the SiteScope system, run the following command-line tool:

Windows: %OvInstallDir%\bin\sisconfig\sisSetCredentials.bat

UNIX or Linux: /opt/OV/bin/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

3. 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
```

How to Connect to a SiteScope Server That Requires SSL

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

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

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

- **Certificate from a certificate authority.** If the SiteScope certificate was signed with a certificate from a certificate authority, import the certificate to the SiteScope CA keystore and to the CA keystore of the BSM server hosting Monitoring Automation:

- a. Obtain the root certificate (and any other intermediate certificate) from the certificate authority.
- b. On the SiteScope server to which you want to deploy policies, import the root certificate (and any other intermediate certificate) to the SiteScope CA keystore, type:

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

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

- c. On the BSM server hosting Monitoring Automation to which you want to export SiteScope templates, import the root certificate (and any other intermediate certificate) to the BSM CA keystore, type:

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

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

- **SiteScope self-signed certificate.** If the SiteScope certificate is a self-signed certificate (for example, a certificate that was created and configured with the SiteScope tool **ssl_util**), export the self-signed certificate from SiteScope and import it to the CA keystores of Monitoring Automation and SiteScope:

- a. On the SiteScope server, export the self-signed certificate, type:

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

When prompted for the keystore password, type the password that was specified when using the **ssl_util** tool.

- b. On the SiteScope server, import the self-signed certificate to the SiteScope CA keystore, type:

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

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

- c. Copy the certificate to the BSM server hosting Monitoring Automation to which you want to export SiteScope templates.
- d. On the BSM server hosting Monitoring Automation, import the self-signed certificate to the BSM CA keystore, type:

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

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

How to Import Templates from a SiteScope Server

1. Make sure the SiteScope templates that you want to import meet the requirements listed in ["Prerequisite for Importing SiteScope Templates" on page 366](#).
2. On the OMi server running Monitoring Automation, open a command prompt and run the ConfigExchangeSIS command-line interface to import templates from a SiteScope server.

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

```
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
```

For more information on importing SiteScope templates, see ["ConfigExchangeSIS Command-Line Interface" on page 503](#).

How to Assign SiteScope Policy Templates to Remote Servers

1. *Prerequisites:* Make sure the prerequisite tasks described in ["Prerequisite Tasks" on page 367](#) and ["How to Configure the Agent on the SiteScope System" on page 368](#) have been completed.
2. Assign the SiteScope policy template to the remote servers (that is to the node CIs) that you want to monitor. Do not assign the template to the SiteScope server itself. For information about assigning a policy template, aspect, or management template to a CI, see ["Assignments and Tuning" on page 415](#).
3. Every SiteScope policy template includes an instance parameter that resolves to the remote server to be monitored. If this value is not already set, edit the value of the instance parameter during the assignment and enter the symbolic value %%HOST%%.

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

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

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



UI Reference

This section includes:

- ["Policy Data Page" on the next page](#)
- ["Policy Parameters Tab" on the next page](#)
- ["Properties Page" on page 374](#)





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).
Template ID	GUID ¹ assigned to the policy template when it is first created.
Version ID	GUID ² assigned to this version of the policy template when it is saved. Each version of a policy template has a unique ID.

¹(globally unique identifier)

²(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>

Developing Instrumentation

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 to upload your instrumentation into the RTSM. Production-ready instrumentation can be distributed to other BSM instances using content packs.

See also the HP Operations Manager for Windows and HP Operations Agent documentation for information about instrumentation.

To access:

The **ConfigExchange** command-line interface is located in:

`<BSM_Root_Directory>/opr/bin`

For details on ConfigExchange, see ["ConfigExchange Command-Line Interface" on page 486](#).

Learn More

This section includes:

- ["Development of Instrumentation" below](#)
- ["Deployment of Instrumentation Packages" below](#)
- ["Conventions for Naming of Instrumentation Packages" on the next page](#)
- ["Patching and Hotfix Strategy" on the next page](#)

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.

Note: Only base packages can be assigned to templates or aspects. If you try to assign a patch or hotfix, an error is displayed.

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.

Conventions for Naming of Instrumentation Packages

The following instrumentation artifacts exist:

- Instrumentation package (also referred as base package)

Instrumentation package names should only include alphanumeric characters and the underscore character (_) (similar to category names in HPOM).

- Instrumentation package patch

Patch names should only include alphanumeric characters, the underscore character (_), and include the following suffix: __PATCH__<num>.

- Instrumentation package hotfix

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 supersede 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.

Tasks

This section includes:

- ["How to Include Instrumentation Patches and Hotfixes Into Content Packs" below](#)
- ["How to Develop Instrumentation Base Packages for SPIs" below](#)
- ["How to Develop Instrumentation Patches or Hotfixes for SPIs" on the next page](#)

How to Include 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.

How to Develop Instrumentation Base Packages for SPIs

The following workflow outlines how to develop a new mySPI instrumentation package:

1. Create the directory structure for the mySPI instrumentation package:

ConfigExchange -createinstrumdir -output mySPI

2. Copy any mySPI files to the newly created directory structure.

3. Import to database for testing:

```
ConfigExchange -upload -input mySPI -instrumname mySPI
```

4. Continue development and fix bugs. Export package to the database:

```
ConfigExchange -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.

How to Develop Instrumentation Patches or Hotfixes for SPIs

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 -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 -upload -input mySPI -instrumname mySPI -patch 1
```

or when hotfixing the base package:

```
ConfigExchange -upload -input mySPI -instrumname mySPI -hotfix hf1 forpatch 0
```

or if you want a hotfix for patch 1:

```
ConfigExchange -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 -upload -input mySPI -instrumname mySPI -patch 1 -force
```

or

```
ConfigExchange -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.

Examples

This section includes:

- ["Upload Instrumentation" below](#)
- ["Download Instrumentation" on the next page](#)
- ["Merge Instrumentation" on the next page](#)
- ["Remove Instrumentation " on page 383](#)
- ["Create Instrumentation Directory" on page 383](#)
- ["List Instrumentation" on page 383](#)

Upload Instrumentation

- `ConfigExchange -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 -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 -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 -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 -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.

Download Instrumentation

- `ConfigExchange -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 -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 -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.

Merge Instrumentation

- `ConfigExchange -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

Remove Instrumentation

- ConfigExchange -remove -instrumname <categoryname> -hotfix hf1 -forpatch 0

Rolls back hotfix hf1 of the base instrumentation package <categoryname>.

- ConfigExchange -remove -instrumname <categoryname> -patch 1

Rolls back patch 1 and its hotfixes.

Note: Patches with higher version numbers than patch 1 are not downloaded.

Create Instrumentation Directory

- ConfigExchange -createinstrumdir -output <categoryname>

Generates an empty directory structure under <categoryname> which can be used to contain instrumentation files.

List Instrumentation

- ConfigExchange -list -instrumname <categoryname>

Lists all patches and hotfixes for instrumentation package <categoryname>.

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 at a command prompt.

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" on the next page](#)
- ["Source Object" on page 391](#)
- ["Session Object" on page 396](#)
- ["Rule Object" on page 397](#)

- ["ConsoleMessage Object" on page 398](#)
- ["ExecuteCommand Object" on page 402](#)

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: source object
VB Script Syntax:	Policy.Source(" <i>name</i> ")
Perl Syntax:	\$Policy->Source(" <i>name</i> ");
Description:	Returns the source object for the defined source and metric. Measurement type sources must use a separate source for each metric. Note: To improve performance, assign the source object to a variable instead of using the Source 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"> • NTPERFMON\\Object\\Counter\\Instance 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. Example: NTPERFMON\\Process\\Elapsed Time* • SNMP\\object id[\\hostname] 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 Example: SNMP\\.1.3.6.1.2.1.1.7.0\\onion.veg.com • PROGRAM\\command[\\monname] Run the specified command or script for gathering the monitored value. The command or script must at some point run the opcmom command to return the value associated with the monitor. If no monitor name is specified, then the default DynPROGRAM must be used. For example, to specify the monitor mymonname: opcmom mymonname=value; to specify the default, opcmom DynPROGRAM=value. Examples: PROGRAM\\opcmom DynPROGRAM=12 PROGRAM\\opcmom testmon=25\\testmon • EXTERNAL[\\monname] Wait for a value returned by the execution of the opcmom command. This is similar to the PROGRAM expression but a command is not directly carried out. An external command previously triggered by the ExecuteCommand object must provide the monitor value. The default value is DynEXTERNAL (opcmom DynExternal=10) Examples: EXTERNAL

Policy Method:	SourceEx
	<p>EXTERNAL\\testmon</p> <ul style="list-style-type: none"> WBEM\\namespace\\class name\\property name <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> <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 of 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 black; padding: 5px; margin-top: 10px;"> <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> ");
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:	Policy.Output(" <i>string</i> ")
Perl Syntax:	\$Policy->Output(" <i>string</i> ");
Description:	Appends the string to the annotation field of the event sent to BSM 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:	Policy.ExecuteEx(" <i>command</i> ")
Perl Syntax:	\$Policy->ExecuteEx(" <i>command</i> ");

Policy Method:	ExecuteEx
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:	StoreCollection
Parameters:	<ul style="list-style-type: none"> • <i>expression</i>: (An embedded performance component metric in the format: CODA\\data source\\collection\\metric name[\\category]) • <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: Policy.StoreCollection "CODA\\DBSPI\\TABLE\\SPACE",Source</p>

Policy Method:	SourceCollection
Parameters:	<ul style="list-style-type: none"> • <i>expression</i>: An embedded performance component metric in the format: CODA\\data source\\collection\\metric name. • <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:	Policy.SourceCollection (" <i>expression</i> ", <i>rangeofseconds</i> , <i>endtime</i>)
Perl Syntax:	\$Policy->SourceCollection (" <i>expression</i> ", <i>rangeofseconds</i> , <i>endtime</i>);
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</i> - <i>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: Policy.SourceCollection ("CODA\\\\CPU\\BYCPU_CPU_TOTAL_UTIL",300,0)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:	Sourceobj.Value()
Perl Syntax:	\$Sourceobj->Value();
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:	Sourceobj.Name()
Perl Syntax:	\$Sourceobj->Name();
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:	Sourceobj.InstanceCount()
Perl Syntax:	\$Sourceobj->InstanceCount();
Description:	Returns the number of instances that the source has.

Source Method:	Count
Parameter:	void

Source Method:	Count
Return Type:	VB Script: Int Perl: integer
VB Script Syntax:	Sourceobj.Count()
Perl Syntax:	\$Sourceobj->Count();
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:	Sourceobj.Item(<i>index</i>)
Perl Syntax:	\$Sourceobj->Item(<i>index</i>);
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:	Sourceobj.ValueOf(<i>index</i>)
Perl Syntax:	\$Sourceobj->ValueOf(<i>index</i>);
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:	Sourceobj.NameOf(<i>index</i>)
Perl Syntax:	\$Sourceobj->NameOf(<i>index</i>);

Source Method:	NameOf
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:	Sourceobj.Top(<i>number</i>)
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:	Sourceobj.Bottom(<i>number</i>)
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:	Sourceobj.Exclude(" <i>namepattern</i> ", " <i>valuepattern</i> ")
Perl Syntax:	<code>\$Sourceobj->Exclude("<i>namepattern</i>", "<i>valuepattern</i>");</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>
Return Type:	VB Script: IDispatch object of type "Source" Perl: source object
VB Script Syntax:	Sourceobj.Include("namepattern", "valuepattern")
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:	Sourceobj.Time()
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:	Source.TimeOf(<i>index</i>)
Perl Syntax:	<code>\$Sourceobj->TimeOf(<i>index</i>);</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:	Sourceobj.Add " <i>instancename</i> :", <i>value</i>

Source Method:	Add
Perl Syntax:	<code>\$Sourceobj->Add("instancename:", value);</code>
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;
Description:	Returns TRUE if the source object contains any value, otherwise, returns FALSE.

Source Method:	ValueOfInstance
Parameter:	<i>instancename</i>
Return Type:	VB Script: variant Perl: string
VB Script Syntax:	Sourceobj.ValueOfInstance(" <i>instancename</i> ")
Perl Syntax:	\$Sourceobj->ValueOfInstance(" <i>instancename</i> ");
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:	IsPresent
Parameter:	<i>key</i>
Return Type:	VB Script: Boolean Perl: integer
VB Script Syntax:	Session.IsPresent(" <i>key</i> ")
Perl Syntax:	\$Session->IsPresent(" <i>key</i> ");
Description:	Returns TRUE if a value for <i>key</i> exists. Returns FALSE if no value for <i>key</i> exists. Keys are set with the Session.Value method.

Session Method:	Remove
Parameter:	<i>key</i>
Return Type:	VB Script: void Perl: void

Session Method:	Remove
VB Script Syntax:	Session.Remove("key")
Perl Syntax:	\$Session->Remove("key");
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

Rule Method:	Status
VB Script Syntax:	for put: Rule.Status = <i>boolvalue</i> for get: boolvalue = Rule.Status
Perl Syntax:	for put: \$Rule.Status(<i>boolvalue</i>); for get: boolvalue = \$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 BSM. Events sent in this way are not intercepted by an open message interface policy, but instead are sent directly to the server. 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:	ConsoleMessage.Application = " <i>application</i> "
Perl Syntax:	\$ConsoleMessage->Application(" <i>application</i> ");
Description:	This optional method sets the content of Application in the event properties.

ConsoleMessage Method:	Object
Parameter:	<i>object</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ConsoleMessage.Object = " <i>object</i> "
Perl Syntax:	\$ConsoleMessage->Object(" <i>object</i> ");
Description:	This optional method sets the content of Object in the event properties.

ConsoleMessage Method:	MsgText
Parameter:	<i>msgtext</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ConsoleMessage.MsgText = " <i>msgtext</i> "
Perl Syntax:	<code>\$ConsoleMessage->MsgText("<i>msgtext</i>")</code> ;
Description:	This method sets the message text for the event.

ConsoleMessage Method:	Severity
Parameter:	<i>severity</i> (valid strings are: Unknown Normal Warning Minor Major Critical)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ConsoleMessage.Severity = " <i>severity</i> "
Perl Syntax:	<code>\$ConsoleMessage->Severity("<i>severity</i>")</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:	MsgGrp
Parameter:	<i>messagegroup</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ConsoleMessage.MsgGrp = " <i>messagegroup</i> "
Perl Syntax:	<code>\$ConsoleMessage->MsgGrp("<i>messagegroup</i>")</code> ;
Description:	Sets the value for the Message Group in event properties. If this method does not supply a value, Misc is used.

ConsoleMessage Method:	Node
Parameter:	<i>nodename</i> (IP address or fully qualified hostname)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ConsoleMessage.Node = " <i>nodename</i> "
Perl Syntax:	<code>\$ConsoleMessage->Node("<i>nodename</i>")</code> ;

ConsoleMessage Method:	Node
Description:	Sets the value for Primary Node Name that will be displayed in the event properties. 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:	ServiceId
Parameter:	<i>serviceid</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ConsoleMessage.ServiceId = " <i>serviceid</i> "
Perl Syntax:	<code>\$ConsoleMessage->ServiceId("<i>serviceid</i>");</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:	ConsoleMessage.MessageType = " <i>messagetype</i> "
Perl Syntax:	<code>\$ConsoleMessage->MessageType("<i>messagetype</i>");</code>
Description:	This optional method sets the value for the message type field of the event properties.

ConsoleMessage Method:	MessageKey
Parameter:	<i>messagekey</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ConsoleMessage.MessageKey = " <i>messagekey</i> "
Perl Syntax:	<code>\$ConsoleMessage->MessageKey("<i>messagekey</i>");</code>
Description:	This optional methods sets a key for event correlation.

ConsoleMessage Method:	AcknowledgeMessageKey
Parameter:	<i>messagekey</i> (string)

ConsoleMessage Method:	AcknowledgeMessageKey
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ConsoleMessage.AcknowledgeMessageKey = "messagekey"
Perl Syntax:	\$ConsoleMessage->AcknowledgeMessageKey("messagekey");
Description:	This optional method sets the message key to indicate which events are automatically closed.

ConsoleMessage Method:	TroubleTicket
Parameter:	<i>Booleanvalue</i>
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ConsoleMessage.TroubleTicket = <i>Booleanvalue</i>
Perl Syntax:	\$ConsoleMessage->TroubleTicket(<i>Booleanvalue</i>);
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:	ConsoleMessage.Notification = <i>Booleanvalue</i>
Perl Syntax:	\$ConsoleMessage->Notification(<i>Booleanvalue</i>);
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:	ConsoleMessage.AgentMSI = " <i>type</i> "
Perl Syntax:	\$ConsoleMessage->AgentMSI(" <i>type</i> ");
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:	ConsoleMessage.ServerMSI = " <i>type</i> "
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:	Send
Parameter:	void
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ConsoleMessage.Send()
Perl Syntax:	<code>\$ConsoleMessage->Send();</code>
Description:	This method sends the event to the BSM server. The MsgText method must set the message text before using this method. Multiple uses of the Send 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:	Command
Parameter:	<i>command</i> (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	ExecuteCommand.Command = " <i>command</i> "
Perl Syntax:	<code>\$ExecuteCommand->Command("<i>command</i>");</code>

ExecuteCommand Method:	Command
Description:	<p>This mandatory method is the name of the command to run with all necessary parameters.</p> <div> <p>Note: For scripts that will run on Windows systems, internal commands such as Copy, Rename, and DIR 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:	KillonTimeout
Parameter:	<i>seconds</i> (integer)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ExecuteCommand.KillonTimeout = <i>seconds</i>;</code>
Perl Syntax:	<code>\$ExecuteCommand->KillonTimeout(<i>seconds</i>);</code>
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:	UserName
Parameter:	username (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ExecuteCommand.UserName = "<i>username</i>"</code>
Perl Syntax:	<code>\$ExecuteCommand->UserName("<i>username</i>");</code>
Description:	User name under which the command should be run. Optional, default is \$AGENT_USER.

ExecuteCommand Method:	Password
Parameter:	password (string)
Return Type:	VB Script: void Perl: void
VB Script Syntax:	<code>ExecuteCommand.Password = "<i>password</i>"</code>

ExecuteCommand Method:	Password
Perl Syntax:	\$ExecuteCommand->Password("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
VB Script Syntax:	ExecuteCommand.Start()
Perl Syntax:	\$ExecuteCommand->Start();
Description:	Run the command specified by ExecuteCommand.Command 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:	ExecuteCommand.StartEx
Perl Syntax:	\$ExecuteCommand->StartEx();
Description:	<p>Run ExecuteCommand.Command 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 + tty2 user1-root
```

However, this line would not be matched, because it contains an entry concerning "user2":

```
SU 03/25 08:14 + tty2 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

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

The operators can also be combined to produce matches according to ranges of numbers:		
Matches numbers that belong to the interval, excluding the limits	<code>< n -lt [pattern] -lt n ></code>	<code><5 -lt [<#>] -lt 10></code> matches every number between 5 and 10 (but not 5 or 10)
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 (MA) 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 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.

Learn More

This section includes:

- ["Assignment Methods" below](#)
- ["Manual Assignments" on the next page](#)
- ["Tuning" on page 417](#)
- ["Deployment Jobs" on page 417](#)
- ["Assignment Synchronization" on page 418](#)

Assignment Methods

An assignment defines 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.

There are two different methods for creating assignments:

- **Manual Assignment**

When creating manual assignments, you manually select the CI to be monitored using the management template or aspect from a list of compatible objects. After creating the assignment, you enable the assignment to start the monitoring process, either as a part of creating the assignment, or afterward by manual intervention.

- **Automatic Assignment**

You can define automatic assignment rules; if a CI is modified or newly discovered, Monitoring Automation automatically evaluates any auto-assignment rules defined for its CI type.

If an automatic assignment rule evaluates to true, Monitoring Automation automatically assigns the items specified in the rule to the modified or newly discovered CI, and starts the corresponding deployment jobs.

There are several locations in the user interface where assignments can be created, deployed and managed:

- You can create and deploy manual assignments for management templates, aspects, and policy templates using the *Assignments and Tuning* screen.

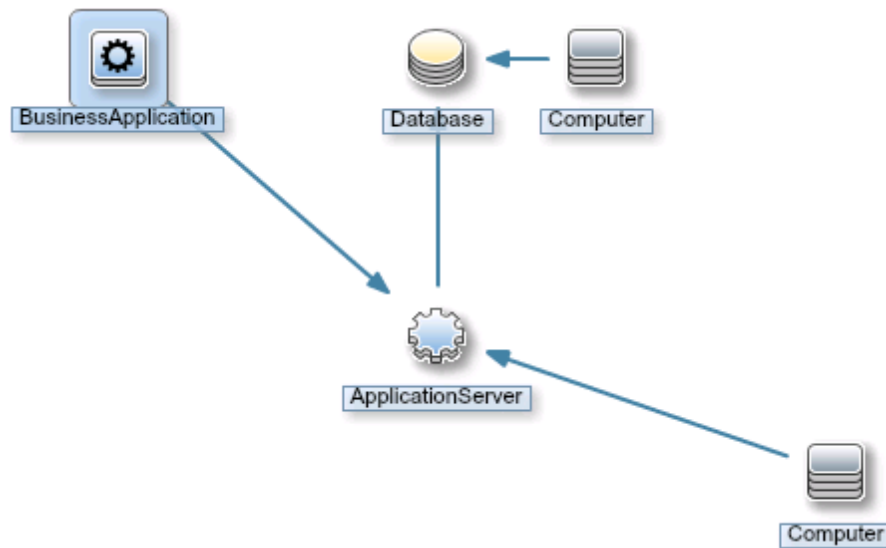
You can create automatic assignment rules using the *Automatic Assignment Rules* screen.

- You can view automatically created assignments for management templates and aspects in the *Assignments and Tuning* screen.
- You can assign management templates and aspects directly from the *Management Templates and Aspects* screen.
- You can assign policy templates directly from the *Policy Templates* screen.
- You can manage the deployments jobs generated by assignments using the *Deployment Jobs* screen.

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.

Tuning

Before starting the monitoring process, you may want to tune the values against which the CIs are monitored.

Tuning overrides the values set at lower configuration levels at deployment level, and allows you to fine-tune a selected subset of monitoring parameters to the environment in which your application or service operates while maintaining all presets defined in corporate and system monitoring standards.

For details on tuning, see ["How to Tune Parameter Values for Existing Assignments" on page 420](#).

Deployment Jobs

While the monitoring process is active, you can manage deployment jobs in the *Deployment Jobs* screen. For more information, see ["Deployment Jobs" on page 457](#).

Assignment Synchronization

Monitoring Automation keeps an inventory of the policies installed on the node. You can see which policies are installed on a node by synchronizing the policy template assignments of the node with Monitoring Automation.

It is possible for this inventory to become inaccurate in the following situations:

- After a policy is manually installed or removed on a node.
- After a policy is disabled or enabled locally on a node.
- In an environment with multiple servers, after a different server changes the policies on a node.

The policy inventory is updated every time you synchronize the policy template assignments of the node with Monitoring Automation. The first time the synchronization runs all policies that are installed on the node are uploaded to Monitoring Automation and displayed in the Policy Templates list. The next synchronization uploads only updates.

Policy synchronization ignores policy types not supported by Monitoring Automation (for example, server and event correlation policies). All other policy types, that is policy templates for HP Operations Agent, HP SiteScope, and HP ArcSight Logger are synchronized, including any parameter values and instruction texts used within the templates.

Policy synchronization does not synchronize aspect and management template assignments, for example:

- If a policy template that is assigned by an aspect is removed from a node, the synchronization removes the policy template assignment only. Aspect and management template assignments are not removed. Changing or redeploying the corresponding aspect or management template assignment redeployes the policy template to the node.
- If a policy template that is assigned by an aspect or a management template is migrated to another Monitoring Automation server, the synchronization creates direct assignments to the policy template on that server. Aspect or management template assignments are not created.
- If a policy template that is assigned by an aspect or a management template is disabled on a node, the synchronization only synchronizes the state and the parameters of the policy template. If the corresponding aspect or management template changes, the state and parameters of the aspect or management template propagate to the policy template and overwrite the synchronized state and parameters.

If a policy template with the same name and version but a different ID already exists in the Monitoring Automation database, a new policy template with a new name is created. If a template with the same name but a different version and a different ID already exists, a new version of the template will be created.



Note: The synchronization of policy template assignments imports the policies installed on a node but not the associated instrumentation. Therefore, do not use this method to migrate policies from another server. Use the ConfigExchange command instead to import policies with the associated instrumentation from HPOM. Alternatively, use content packs to exchange


policy templates and instrumentation between multiple Monitoring Automation instances.

Tasks

How to Monitor CIs Using a Management Template

To start monitoring from the *Assignments & Tuning* screen:

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 CIs matching the CIs in the view are listed in the View Browser. Alternatively, use the **Search** tab to find a CI.
2. In the list of CIs, click the CI that you want to monitor. The *Assignments* pane (top pane on the right) shows details of any existing assignments for that CI.
3. Click  **New Assignment** and select  **Assign Management Template**. The *Assign and Deploy* wizard opens at *Select Item to Assign*, which has a list of management templates that can be assigned to the CI type of the selected CI.
4. Select the management template to be deployed, and, if necessary, the appropriate **Version**. Click **Next** to go to *Required Parameters*.
5. Step *Required Parameters* lists all mandatory parameters in the management template that do not yet have a value. As they are mandatory, however, all listed parameters *must* be given a value before the management template can be deployed.

To change a parameter, double-click it, or select it in the list and click  **Edit**.

- For standard parameters, the *Edit Parameter* dialog opens.


Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the *Edit Instance Parameter* dialog 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**.

When finished, click **Next** to go to **All Parameters**, or click **Finish** to deploy the management template and close the wizard.

6. *Optional*. In step **All Parameters** tab, you can specify a value for each parameter at the deployment level. This value overrides any value defined on a lower level.

To change a parameter, double-click it, or select it in the list and click  **Edit**.

- For standard parameters, the *Edit Parameter* dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the *Edit Instance Parameter* dialog 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**.

When finished, click **Next** to go to *Configuration Options*, or click **Finish** to deploy the management template and close the wizard.

7. *Optional.* In step *Configuration Options*, clear the **Enable Assigned Objects** check box if you do not want to enable the assignment immediately. (You can enable assignments later.)
8. Click **Finish** to save the changes and close the wizard. The aspects in the management template are assigned to and deployed on the selected CI, as notified by the system. If **Enable Assigned Objects** was checked, any policy templates contained in the management template are activated on the appropriate agents. 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.

If a deployment job fails an event is sent to BSM.

How to Tune Parameter Values for Existing Assignments

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. Select a CI. The *Assignments* pane shows any existing direct or indirect assignments for that CI.
3. Click the assignment for which you want to tune parameters. The current parameter values are shown as *Assignment Details*.
4. Double-click the parameter you want to tune.
 - For standard parameters, the *Edit Parameter* dialog opens.
Click **Value**, specify the value, and then click **OK**.
 - For instance parameters, the *Edit Instance Parameter* dialog 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**.


5. Repeat the previous step for all parameters that require tuning.

Operations Management sends the new parameter values to the relevant HP Operations Agents.


How to Synchronize Policy Template Assignments

1. Select the node CI for which you want to synchronize policy template assignments.
2. Click  **Synchronize Policy Template Assignments**.

The server creates a deployment job to retrieve the inventory from the node.




To verify whether the synchronization process has been completed, click  **Refresh** to refresh the list of assignments and view any updates.

How to Display a Report for a CI

Select a CI and choose one of the available reports from the  **Generate Report** 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:** *Enabled only if exactly one assignment is selected.* Shows the details for the selected assignment.

The preconfigured report for the selected CI or assignment is displayed.

You can use  **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 Item to Assign

UI Element	Description						
List of Items to Assign	<p>List of items that can be assigned to the selected CI instances: management templates, aspects, and policy templates.</p> <p>The List of Items to Assign has the following columns:</p> <table><tr><td>Name</td><td>The name of the item.</td></tr><tr><td>Version</td><td>The version of the item. 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.</td></tr><tr><td>Description</td><td>A description of the item.</td></tr></table>	Name	The name of the item.	Version	The version of the item. 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.	Description	A description of the item.
Name	The name of the item.						
Version	The version of the item. 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.						
Description	A description of the item.						
Back	Moves back to the previous step.						
Next	Moves on to the next step.						
Finish	Accepts the values in all steps and creates the item.						
Cancel	Closes the wizard without creating the item.						
Help	Opens the relevant help in a new browser window.						


—Required Parameters




UI Element	Description
Required Parameters List	<p>This step lists all mandatory parameters in the management template that do not yet have a value. As they are mandatory, however, all listed parameters <i>must</i> be given a value before the management template can be deployed.</p> <p>If all required values are specified, you can choose one of the following actions:</p> <ul style="list-style-type: none">Click Finish to assign the configuration object to the selected CI and close the wizard or dialog.Click Next to go to <i>All Parameters</i>, where you can override the default value of any parameter, including those that are not required.






UI Element	Description										
	<p>Note: To access step <i>Configure Options</i>, click Next in this step, and Next again in step <i>All Parameters</i>.</p> <p>The toolbar provides the following controls:</p> <div>  <div> <p>Edit: Specify the value of the selected parameter.</p> <ul style="list-style-type: none"> For standard parameters, the <i>Edit Parameter</i> dialog opens. For instance parameters, the <i>Edit Instance Parameter</i> dialog opens. <p>For details on using the dialogs, see the relevant <i>UI Reference</i> section.</p> </div> </div> <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p> <table> <tr> <td>Target (Visible Only for Assignments of Management Templates)</td><td>The CI type of the item using the parameter.</td></tr> <tr> <td>Defined In (Visible Only for Assignments of Management Templates)</td><td>The management template, aspect or policy template in which the parameter is defined.</td></tr> <tr> <td>Instance Parameter (Visible Only for Assignments with Instance Parameters)</td><td>The instance parameter the parameter depends on.</td></tr> <tr> <td>Instance (Visible Only for Assignments with Instance Parameters)</td><td>The instance of the parameter.</td></tr> <tr> <td>Name</td><td>The name of the parameter.</td></tr> </table>	Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.	Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.	Instance Parameter (Visible Only for Assignments with Instance Parameters)	The instance parameter the parameter depends on.	Instance (Visible Only for Assignments with Instance Parameters)	The instance of the parameter.	Name	The name of the parameter.
Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.										
Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.										
Instance Parameter (Visible Only for Assignments with Instance Parameters)	The instance parameter the parameter depends on.										
Instance (Visible Only for Assignments with Instance Parameters)	The instance of the parameter.										
Name	The name of the parameter.										

UI Element	Description
	<p>Value</p> <p>The parameter value for this assignment.</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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.

—All Parameters

UI Element	Description
Parameter List	<p>Lists all parameters in the management template, aspect or policy template you are assigning to the configuration item.</p> <p>The toolbar provides the following controls:</p> <div>  <p>Edit: Specify the value of the selected parameter.</p> <ul style="list-style-type: none"> For standard parameters, the <i>Edit Parameter</i> dialog opens. </div>







UI Element	Description								
	<ul style="list-style-type: none"> For instance parameters, the <i>Edit Instance Parameter</i> dialog opens. <p>For details on using the dialogs, see the relevant <i>UI Reference</i> section.</p> <p> Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p> <p> Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p> <table> <tr> <td>Target (Visible Only for Assignments of Management Templates)</td><td>The CI type of the item using the parameter.</td></tr> <tr> <td>Defined In (Visible Only for Assignments of Management Templates)</td><td>The management template, aspect or policy template in which the parameter is defined.</td></tr> <tr> <td>Name</td><td>The name of the parameter.</td></tr> <tr> <td>Value</td><td>The parameter value for this assignment.</td></tr> </table> <p>An icon represents the type of parameter value, which can be one of the following:</p>	Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.	Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.	Name	The name of the parameter.	Value	The parameter value for this assignment.
Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.								
Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.								
Name	The name of the parameter.								
Value	The parameter value for this assignment.								












UI Element	Description
	<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, it is the default value. • If the icon is dimmed, the value is read-only. • If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.







—Configure Options





UI Element	Description
Enable Assigned Objects	If you do not want to enable the assignments immediately, clear the Enable Assigned Objects check box. To enable assignments after closing the wizard, use the <i>Assignments & Tuning</i> screen.
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.










Assignments Pane





UI Element	Description
Assignments	<p>Lists all assignments of management templates and aspects for the item selected in the View Browser:</p> <p>Note the following:</p> <ul style="list-style-type: none"> If you select an assignment, a list of contained parameters appears underneath the assignment list. <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: Only parameters that can be resolved for the target CI of the assignment are listed.</p> </div> <ul style="list-style-type: none"> You cannot delete indirect assignments. The assignments to the top level of the structure in which the selected assignment is contained are listed underneath the list of parameters with the header Direct Assignments in the <i>Assignment Details</i> pane. If you select no CI, or if you select the view in the View Browser, the list of assignments shows all <i>direct</i> assignments of all CIs in the view. If you select multiple CIs, nothing is shown. <p>The toolbar of the list of assignments provides the following controls:</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;">  </div> <div> <p>Refresh: Reloads the list of assignments for the selected CI.</p> </div> </div> <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="margin-right: 20px;">  <p>(Visible Only If a CI is Selected)</p> </div> <div> <p>New Assignment: Provides the following options:</p> <ul style="list-style-type: none">  Assign Management Template: Opens the <i>Assign and Deploy</i> wizard to assign a management template to the selected CI.  Assign Aspect: Opens the <i>Assign and Deploy</i> wizard to assign an aspect to the selected CI.  Assign Policy Template: Opens the <i>Assign and Deploy</i> wizard to assign a policy template to the selected CI. </div> </div> <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="margin-right: 20px;">  </div> <div> <p>Tune Assignment: Opens the <i>Tune Assignment</i> dialog to set parameter values defined for the</p> </div> </div>

UI Element	Description
	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. Operations Management removes the monitoring configuration from the relevant HP Operations Agents.
	Enable Assignment: Starts or resumes monitoring the selected CI with the management template, aspect, or policy template.
	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.
 (Visible Only If a CI is Selected)	Re-deploy Provides the following options: <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.
	Show/Hide Policy Template Assignments: Switches between showing and hiding policy template assignments for the selected CI.
 (Visible Only If a CI is Selected)	Show Only Assignments to this Node/Show Assignments to CIs on this Node: Switches between showing only assignments to the CI representing the selected node and showing all assignments to all CI hosted on the selected node.
	Generate Report: Provides the following options: <ul style="list-style-type: none">  Generate CI Configuration Report:




UI Element	Description
	<p>Describes how the selected CI is monitored.</p> <ul style="list-style-type: none"> •  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. •  Generate Assignment Report: Shows to which CIs a selected management template or aspect is assigned. The preconfigured report for the selected assignment is displayed. An Assignment Report is only available when a management template or aspect assignment is selected in the Assignments (right) pane. <p> Synchronize Policy Template Assignments: Synchronizes the policy templates installed on a node with the assignment inventory that the Monitoring Automation server keeps of the node. Policy template synchronization also uploads the policies installed on the node to the Monitoring Automation database, including any parameter values and instruction texts used within the templates. Management template and aspect assignments are not synchronized.</p> <p>Use this option if a node running HP Operations Agent is connected to more than one server, for example to a Monitoring Automation and an HPOM server or to multiple Monitoring Automation servers. For more information about managing a node with multiple servers, see "Connecting an Existing HP Operations Agent Installation" on page 476.</p> <p>Click  Synchronize Policy Template Assignments to start the synchronization of the policy template assignments. A message informs you that the synchronization process is started.</p> <p>To verify whether the synchronization process has been completed, click  to refresh the list of assignments and view any updates.</p>










UI Element	Description										
	<p data-bbox="581 310 1367 382">  Get Help: Opens the relevant help in a new browser window. </p> <p data-bbox="565 415 1133 445">The list of assignments has the following columns:</p> <table data-bbox="571 478 1367 1012"> <tr> <td data-bbox="571 478 597 508">D</td><td data-bbox="776 478 1367 655">✓ indicates that the aspect or policy template is assigned directly to the selected CI. — indicates it is assigned indirectly through the assignment of a management template or aspect that contains this aspect or policy template.</td></tr> <tr> <td data-bbox="571 676 695 739">Assigned Item</td><td data-bbox="776 676 1367 739">The name of the assigned management template, aspect, or policy template.</td></tr> <tr> <td data-bbox="571 760 669 789">Version</td><td data-bbox="776 760 1367 831">The version of the management template, aspect, or policy template that is currently assigned to the CI.</td></tr> <tr> <td data-bbox="571 852 734 882">Assigned By</td><td data-bbox="776 852 1367 915">The user name of the user who made the assignment.</td></tr> <tr> <td data-bbox="571 936 678 966">Enabled</td><td data-bbox="776 936 1367 1012">✓ indicates that the assignment is enabled, — indicates it is disabled.</td></tr> </table> <div data-bbox="792 1054 1360 1150"> <p>Note: When an assignment is disabled, monitoring is paused.</p> </div>	D	✓ indicates that the aspect or policy template is assigned directly to the selected CI. — indicates it is assigned indirectly through the assignment of a management template or aspect that contains this aspect or policy template.	Assigned Item	The name of the assigned management template, aspect, or policy template.	Version	The version of the management template, aspect, or policy template that is currently assigned to the CI.	Assigned By	The user name of the user who made the assignment.	Enabled	✓ indicates that the assignment is enabled, — indicates it is disabled.
D	✓ indicates that the aspect or policy template is assigned directly to the selected CI. — indicates it is assigned indirectly through the assignment of a management template or aspect that contains this aspect or policy template.										
Assigned Item	The name of the assigned management template, aspect, or policy template.										
Version	The version of the management template, aspect, or policy template that is currently assigned to the CI.										
Assigned By	The user name of the user who made the assignment.										
Enabled	✓ indicates that the assignment is enabled, — indicates it is disabled.										
Assignment Details—Parameters	<p data-bbox="565 1192 1367 1255">Parameters contained in the management template or aspect selected in the list of assignments.</p> <div data-bbox="565 1276 1367 1390"> <p>Note: Only parameters that can be resolved for the target CI of the assignment are listed.</p> </div> <p data-bbox="565 1411 1042 1440">The toolbar provides the following controls:</p> <table data-bbox="571 1465 1367 1612"> <tr> <td data-bbox="571 1465 604 1507">  </td><td data-bbox="776 1465 1367 1612"> <p>Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p> </td></tr> </table>		<p>Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p>								
	<p>Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p>										

UI Element	Description										
	<p>  Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p> <table> <tr> <td>Target (Visible Only for Assignments of Management Templates)</td><td>The CI type of the item using the parameter.</td></tr> <tr> <td>Defined In (Visible Only for Assignments of Management Templates)</td><td>The management template, aspect or policy template in which the parameter is defined.</td></tr> <tr> <td>Instance (Visible Only for Assignments with Instance Parameters)</td><td>The instance of the parameter.</td></tr> <tr> <td>Name</td><td>The name of the parameter.</td></tr> <tr> <td>Value</td><td> <p>The parameter value for this assignment.</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 </td></tr> </table>	Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.	Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.	Instance (Visible Only for Assignments with Instance Parameters)	The instance of the parameter.	Name	The name of the parameter.	Value	<p>The parameter value for this assignment.</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
Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.										
Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.										
Instance (Visible Only for Assignments with Instance Parameters)	The instance of the parameter.										
Name	The name of the parameter.										
Value	<p>The parameter value for this assignment.</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 										

UI Element	Description
	<ul style="list-style-type: none">  Password  String <p>Note the following:</p> <ul style="list-style-type: none"> If the value is dimmed, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
Assignment Details—Direct Assignments (Visible Only for Indirect Assignments)	<p>By default, the Direct Assignments list is collapsed. Click  to expand the direct assignments, which are the assignments to the top level of the structure in which the selected assignment is contained.</p> <p>You cannot delete indirect assignments until the assignment that triggered the indirect assignment was removed. The direct assignments list helps you to identify where to start.</p>

Edit Instance Parameter Dialog



UI Element	
Instance Values	<p>The toolbar provides the following controls:</p> <div>  <p>Create Instance Parameter: Open the <i>Edit Parameter</i> dialog. To create a new value, select Value and specify a value in the text box. Click OK to close the dialog and add the new value to the Instance Values list, or click Cancel to close the dialog without making changes.</p> </div> <div>  <p>Edit Instance Parameter: Open the <i>Edit Parameter</i> dialog. To change the instance value, edit the value in the text box. Click OK to close the dialog and replace the value in the Instance Value list with the new value, or click Cancel to close the dialog without making changes.</p> </div> <div>  <p>Delete Instance Parameter: Delete the selected instance value.</p> </div>
















UI Element					
	<div data-bbox="574 317 607 348"></div> <p>Move Up: Move the selected instance value up in the list.</p> <div data-bbox="574 405 607 436"></div> <p>Move Down: Move the selected instance value down in the list.</p>				
Dependent Values	<p>Lists the dependent values for the instance value selected in the Instance Values list.</p> <p>The toolbar provides the following controls:</p> <div data-bbox="574 663 607 695"></div> <p>Edit Show the <i>Edit Parameter Dialog</i> to specify a value for the parameter.</p> <div data-bbox="574 751 607 783"></div> <p>Hide/Unhide Expert Parameters: Show or hide expert parameters.</p> <p>The list has the following columns:</p> <table data-bbox="574 919 1156 1003"> <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 <p>Note the following:</p> <ul style="list-style-type: none"> If the value is dimmed, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value. 	Name	The name of the dependent value.	Value	The value of the dependent value.
Name	The name of the dependent value.				
Value	The value of the dependent value.				
OK	Applies all values and closes the dialog.				
Cancel	Closes the dialog without creating or updating the item.				


Edit Parameter Dialog

UI Element	Description
Value	Select Value if you want to set a specific default value for the parameter in this assignment. 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.
Remove Overwrite	The other choice offered is Remove Overwrite . Select this option if you want to use the default value defined in the policy template, aspect, or management template.
OK	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.





Tune Assignment Dialog

UI Element	Description
List of Parameters	<p>Lists the parameters that can be tuned for the selected assignment.</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: Specify the value of the selected parameter.</p> <ul style="list-style-type: none"> • For standard parameters, the <i>Edit Parameter</i> dialog opens. • For instance parameters, the <i>Edit Instance Parameter</i> dialog opens. <p>For details on using the dialogs, see the relevant <i>UI Reference</i> section.</p> </div> </div> <div style="margin-top: 20px;"> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;">  </div> <div> <p>Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p> </div> </div> </div>

UI Element	Description								
	<p>  Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p> <table> <tr> <td>Target (Visible Only for Assignments of Management Templates)</td><td>The CI type of the item using the parameter.</td></tr> <tr> <td>Defined In (Visible Only for Assignments of Management Templates)</td><td>The management template, aspect or policy template in which the parameter is defined.</td></tr> <tr> <td>Name</td><td>The name of the parameter.</td></tr> <tr> <td>Value</td><td> <p>The parameter value for this assignment.</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> </td></tr> </table>	Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.	Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.	Name	The name of the parameter.	Value	<p>The parameter value for this assignment.</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>
Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.								
Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.								
Name	The name of the parameter.								
Value	<p>The parameter value for this assignment.</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>								

UI Element	Description
	<ul style="list-style-type: none"> • If the value is dimmed, it is the default value. • If the icon is dimmed, the value is read-only. • If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
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>First, 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 tree structure in the area below the list with the selected view as its root.</p> <p>You can take the following actions:</p> <ul style="list-style-type: none"> • Select nothing, or click the view itself (the root of the tree structure) to list the direct assignments for all CIs included in the selected view. • Click a CI to select it and list the management templates, aspects and policy templates assigned to the CI in the <i>Assignments</i> pane. Hover the mouse over a CI to see the name of the CI followed by its CI type in parentheses. • CIs with contained CIs are preceded by . Click  to expand the CI and see the contained CIs. <p>Right-click the CI and select an action from the context menu.</p> <p>The toolbar provides the following controls:</p> <div>  Refresh: Refresh the view browser. </div> <div>  Clear All: Clear any selection in the view browser. </div>
Search Tab	<p>Specify a string in the Name box, and click Search to search for a View or CI with the specified string in its name, or an attribute with a value containing the string.</p> <p>The search results table has the following columns:</p>

UI Element	Description	
	Name	The name of the View or CI or the value of the attribute returned by the search.
	Type	The CI type or attribute name of the result.

Chapter 5: Automatic Assignment Rules

This section describes how to configure Automatic Assignment Rules using the *Automatic Assignment Rules* screen, accessible at **Monitoring > Automatic Assignment Rules**.

Learn More

Assignment Methods

An assignment defines 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.

There are two different methods for creating assignments:

- **Manual Assignment**

When creating manual assignments, you manually select the CI to be monitored using the management template or aspect from a list of compatible objects. After creating the assignment, you enable the assignment to start the monitoring process, either as a part of creating the assignment, or afterward by manual intervention.

- **Automatic Assignment**

You can define automatic assignment rules; if a CI is modified or newly discovered, Monitoring Automation automatically evaluates any auto-assignment rules defined for its CI type.

If an automatic assignment rule evaluates to true, Monitoring Automation automatically assigns the items specified in the rule to the modified or newly discovered CI, and starts the corresponding deployment jobs.

There are several locations in the user interface where assignments can be created, deployed and managed:

- You can create and deploy manual assignments for management templates, aspects, and policy templates using the *Assignments and Tuning* screen.

You can create automatic assignment rules using the *Automatic Assignment Rules* screen.

- You can view automatically created assignments for management templates and aspects in the *Assignments and Tuning* screen.
- You can assign management templates and aspects directly from the *Management Templates and Aspects* screen.
- You can assign policy templates directly from the *Policy Templates* screen.
- You can manage the deployments jobs generated by assignments using the *Deployment Jobs* screen.

Using Automatic Assignment Rules for Dynamic Monitoring

A view is a query that selects the CIs based on their CI type and their relations with other CIs. Management templates are assigned to one of the CIs in a particular view that is identified when the management template is created (see ["Configuring Management Templates" on page 27](#)).

- The CI the management template is assigned to is called the root CI of the management template.
- Related CIs are all CIs found by following the defined target paths starting from the root CI. Related CIs are not limited to the view; the view is only relevant with regard to defining the root CI.



If you create an automatic assignment rule for a management template, Operations Management automatically assigns the management template and the aspects it contains to the root CI and all its related CIs as they appear on the network, saving you from having to create the assignments manually.

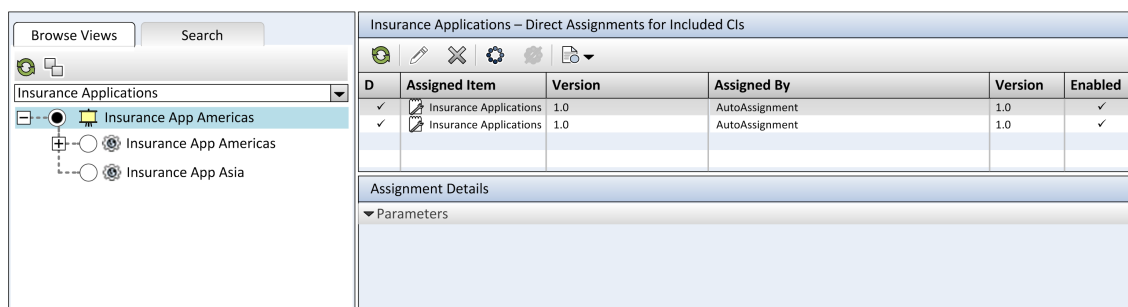
For example, you could create a view called Insurance Applications that selects CIs of CI type Insurance App and include the view in a management template called Monitor Business Applications.

To use the management template to monitor instances of Insurance App, you can create an automatic assignment rule for the management template Monitor Business Applications using the *Automatic Assignment Rules* screen, selecting Insurance Applications as the Target View, and management template Monitor Business Applications as the assigned item.

Operations Management then automatically assigns the aspects contained in the Monitor Business Applications management template to all instances of all CI types in the Insurance Applications view as soon as they are discovered, even if they are added to RTSM after the initial automatic assignment was created.

The following figure shows the *Assignments and Tuning* screen after the management template was assigned to the instance Insurance App Americas and Insurance App Asia.

Note that the column **Assigned By** shows the value AutoAssignment to indicate that the assignment was created by an automatic assignment rule. For such an assignment, if the column **Enabled** has the value , the automatic assignment rule is carried out as soon as the rule evaluates to true. A value of  indicates it is never carried out.



D	Assigned Item	Version	Assigned By	Version	Enabled
✓	Insurance Applications	1.0	AutoAssignment	1.0	✓
✓	Insurance Applications	1.0	AutoAssignment	1.0	✓

Assignment Details

Parameters

Now a new instance called Insurance App EMEA comes online and shows up in the RTSM. This instance, which has the CI type Insurance App, matches the criteria of the Insurance Applications view, and Operations Management automatically starts monitoring it by assigning the management

template Monitor Business Applications. The *Assignments and Tuning* screen changes as shown in the following figure:

D	Assigned Item	Version	Assigned By	Version	Enabled
✓	Insurance Applications	1.0	AutoAssignment	1.0	✓
✓	Insurance Applications	1.0	AutoAssignment	1.0	✓
✓	Insurance Applications	1.0	AutoAssignment	1.0	✓

Assignment Details

Parameters

Tasks

How to Automatically Assign Management Templates and Aspects

1. Go to the *Automatic Assignment Rules* screen (**Monitoring > Automatic Assignment Rules**). The screen consists of the *Auto-Assignment Rules* pane at the top, and a parameter list at the bottom.
2. Click **New Assignment** in the toolbar of the *Auto-Assignment Rules* pane and select the appropriate option. The *Create Auto-Assignment Rule* wizard is shown, at step *Select Target View*.
3. Select a view containing the CIs for which you want to create an automatic assignment, and click **Next** to go to *Select Item to Assign*.
4. In step *Select Item to Assign*, click the management template or aspect that you want to automatically assign to all CIs with a CI type appearing in the selected view.

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.

The latest version of the management template or aspect that you want to assign is selected by default. If required, select a different version in column **Version**.

Click **Next** to go to *Required Parameters*.


5. This step lists all mandatory parameters in the management template that do not yet have a value. As they are mandatory, however, all listed parameters *must* be given a value before the management template can be deployed.

If all required values are specified, you can choose one of the following actions:

- Click **Finish** to assign the configuration object to the selected CI and close the wizard or dialog.

- Click **Next** to go to *All Parameters*, where you can override the default value of any parameter, including those that are not required.

Note: To access step *Configure Options*, click **Next** in this step, and **Next** again in step *All Parameters*.

To change a parameter, double-click it, or select it in the list and click  **Edit**.


- For standard parameters, the *Edit Parameter* dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the *Edit Instance Parameter* dialog 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**.

6. *Optional.* In step *All Parameters*, specify a value for each parameter that needs to be monitored against a different value than the default value.

To change a parameter, double-click it, or select it in the list and click  **Edit**.

- For standard parameters, the *Edit Parameter* dialog opens.

Click **Value**, specify the value, and then click **OK**.

- For instance parameters, the *Edit Instance Parameter* dialog 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 go to the *Configure Options* tab, or **Finish** to save the assignment and close the wizard.

7. *Optional.* In step *Configuration Options*, clear the **Enable Assigned Objects** check box if you do not want to activate the assignment rule immediately. (You can activate automatic assignment rules later using the *Automatic Assignment Rules* screen at **Admin > Operations Management > Monitoring > Automatic Assignment Rules**.)
8. Click **Finish** to save the changes and close the wizard. The assignment rule is added to the list of auto-assignment rules.

As soon as the automatic assignment rule evaluates to true for a newly discovered CI, Operations Management creates an actual assignment for the CI, and starts the deployment jobs required 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.

An assignment may trigger an event to be sent to BSM if one of the following situations applies:

- A deployment job fails.
- An auto-assignment fails.
- An auto-assignment succeeds. This behavior can be configured in the Infrastructure Settings.

You can check if the automatic assignment rule successfully created the expected assignments as follows:


- Go the *Assignments and Tuning* screen (**Monitoring > Assignments and Tuning**).
- In the *Views* browser, select the view you identified when creating your automatic assignment rule.
- Expand the view, and select a node that corresponds to the root CI type of the assigned item. Assignments created as a result of Automatic Assignment Rules are shown in the list of assignments at the top of the right pane, and have the value *AutoAssignment* in the column **Assigned By**.











You can consider the following options for tuning the assignment:




- Use the *Automatic Assignment Rules* screen to tune the parameter values for all assignments triggered by the automatic assignment rule.
- Use the *Assignments and Tuning* screen to tune, redeploy, delete, and enable or disable individual assignments.






UI Reference

Automatic Assignment Rules Pane

UI Element	Description
Automatic Assignment Rules	<p>Lists all automatic assignment rules. Each line represents an automatic assignment rule; the assignment defined in the automatic assignment rule is created when the rule evaluates to true.</p> <p>After creating or changing an automatic assignment rule, it is <i>immediately</i> evaluated. If matching CIs are found the corresponding assignments will be created. After this initial evaluation, the evaluation of the rule is triggered in the following cases:</p> <ul style="list-style-type: none"> • Every time a CI was added, changed or deleted. • Every time a CI attribute was changed. • After a configurable time interval elapsed. The time interval is configured in the <i>Infrastructure Settings</i> screen. Scheduled evaluation guarantees that automatic assignments are created in case of issues with CI change notifications. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Note:</p> <ul style="list-style-type: none"> • Deleting an automatic assignment rule does not result in automatic removal of the assignments created by that rule. To remove the actual assignments, go to the <i>Assignments and Tuning</i> screen, select the appropriate CI and delete the assignments from the list. • You can view all assignments of an assignable item, including automatic assignments, in the <i>Management Templates and Aspects</i> screen. For details, see "Management Templates and Aspects" on page 9. • The behavior of automatic assignment rules does not depend on the installed license. </div> <p>The toolbar of the automatic assignment rules list provides the following controls:</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <div> <p>Refresh: Reload the list of automatic assignment rules.</p> </div> </div>




UI Element	Description
	<p>New Assignment: Provides the following options:</p> <ul style="list-style-type: none">  Assign Management Template: Opens the <i>Create Auto-Assignment Rule</i> wizard to create an automatic assignment rule for a management template.  Assign Aspect: Opens the <i>Create Auto-Assignment Rule</i> wizard to create an automatic assignment rule for an aspect.
	<p>Edit Item: Opens the <i>Edit Auto-Assignment Rule</i> dialog to set parameter values defined for the management template or aspect to a deployment-level value, which overrides any management template-level, aspect-level and policy template-level value, except for values that were tuned at assignment level.</p>
	<p>Delete Assignment: Deletes the selected automatic assignment rule.</p>
	<p>Activate Item: Activates the selected automatic assignment rule.</p>
	<p>Deactivate Item: Deactivates the selected automatic assignment rule, meaning that no assignments will be created automatically. To deactivate actual assignments, use the <i>Assignment and Tuning</i> screen.</p>
	<p>Generate Report: Provides the following options:</p> <p> Generate Assignment Report: Shows to which CIs the management template or aspect referenced in the selected automatic assignment rule is assigned. The preconfigured report for the referenced configuration object is displayed. An assignment report is only available when a management template or aspect assignment is selected.</p>
	<p>Get Help: Opens the relevant help in a new browser window.</p>
	<p>The list of assignment rules has the following columns:</p>

UI Element	Description
	<p>Topology View The name of the view to be used for evaluating the automatic assignment rule.</p> <p>Assigned Item The name of the management template or aspect to be automatically assigned.</p> <p>Version The version of the management template or aspect to be automatically assigned.</p> <p>Active ✓ indicates that the automatic assignment rule is carried out as soon as the rule evaluates to true, — indicates it is not carried out.</p>
Parameters	<p>Lists all parameters defined for the management template or aspect selected in the list of automatic assignment rules.</p> <p>The toolbar provides the following controls:</p> <div data-bbox="573 877 609 919"></div> <p>Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p> <div data-bbox="573 1035 646 1077"></div> <p>Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> • Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. • The search is not case-sensitive. • If a filter is active, click  No Filter to remove the filter and show all items in the list. <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p>

UI Element	Description
	<p>Target (Visible Only for Assignments of Management Templates) The CI type of the item using the parameter.</p> <p>Defined In (Visible Only for Assignments of Management Templates) The management template, aspect or policy template in which the parameter is defined.</p> <p>Instance (Visible Only for Assignments with Instance Parameters) The instance of the parameter.</p> <p>Name The name of the parameter.</p> <p>Value The parameter value for this assignment.</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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.










Create Auto-Assignment Rule Wizard

—Select Target View




UI Element	Description		
View List	<p>List all views. Select a view you want to create the automatic assignment rule for. The automatic assignment rule is evaluated on the root CI of the target view.</p> <p>The toolbar provides the following controls:</p> <p>  Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. <p>The list has the following columns:</p> <table> <tr> <td>Name</td><td>The name of the view.</td></tr> </table>	Name	The name of the view.
Name	The name of the view.		
Back	Moves back to the previous step.		
Next	Moves on to the next step.		
Finish	Accepts the values in all steps and creates the item.		
Cancel	Closes the wizard without creating the item.		
Help	Opens the relevant help in a new browser window.		




—Select Item to Assign





UI Element	Description
List of Items to Assign	<p>Lists all management templates and aspects that can be assigned to one of the CI types present in the target view. Select one of the objects to be automatically assigned when the rule evaluates to true.</p> <p>The toolbar provides the following controls:</p>

UI Element	Description						
	<p>  Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. <p>The list has the following columns:</p> <table> <tr> <td>Name</td><td>The name of the configuration object preceded by an icon denoting its object type ( for management templates and  for aspects).</td></tr> <tr> <td>Version</td><td>The version of the configuration object. The latest version is selected by default. To use a different version, select it from the drop-down list.</td></tr> <tr> <td>Description</td><td>A description for the configuration object.</td></tr> </table>	Name	The name of the configuration object preceded by an icon denoting its object type ( for management templates and  for aspects).	Version	The version of the configuration object. The latest version is selected by default. To use a different version, select it from the drop-down list.	Description	A description for the configuration object.
Name	The name of the configuration object preceded by an icon denoting its object type ( for management templates and  for aspects).						
Version	The version of the configuration object. The latest version is selected by default. To use a different version, select it from the drop-down list.						
Description	A description for the configuration object.						
Back	Moves back to the previous step.						
Next	Moves on to the next step.						
Finish	Accepts the values in all steps and creates the item.						
Cancel	Closes the wizard without creating the item.						
Help	Opens the relevant help in a new browser window.						


—Required Parameters










UI Element	Description		
Required Parameter List	<p>Lists all mandatory parameters contained in the management template or aspect to be assigned that do not yet have a value. Enter a value for each parameter in the list.</p> <p>The toolbar provides the following controls:</p> <table> <tr> <td></td><td>Edit: Specify the value of the selected parameter.</td></tr> </table>		Edit: Specify the value of the selected parameter.
	Edit: Specify the value of the selected parameter.		




UI Element	Description												
	<ul style="list-style-type: none"> For standard parameters, the <i>Edit Parameter</i> dialog opens. For instance parameters, the <i>Edit Instance Parameter</i> dialog opens. <p>For details on using the dialogs, see the relevant <i>UI Reference</i> section.</p> <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p> <table> <tr> <td>Target (Visible Only for Assignments of Management Templates)</td><td>The CI type of the item using the parameter.</td></tr> <tr> <td>Defined In (Visible Only for Assignments of Management Templates)</td><td>The management template, aspect or policy template in which the parameter is defined.</td></tr> <tr> <td>Instance Parameter (Visible Only for Assignments with Instance Parameters)</td><td>The instance parameter the parameter depends on.</td></tr> <tr> <td>Instance (Visible Only for Assignments with Instance Parameters)</td><td>The instance of the parameter.</td></tr> <tr> <td>Name</td><td>The name of the parameter.</td></tr> <tr> <td>Value</td><td> <p>The parameter value for this assignment.</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) </td></tr> </table>	Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.	Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.	Instance Parameter (Visible Only for Assignments with Instance Parameters)	The instance parameter the parameter depends on.	Instance (Visible Only for Assignments with Instance Parameters)	The instance of the parameter.	Name	The name of the parameter.	Value	<p>The parameter value for this assignment.</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)
Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.												
Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.												
Instance Parameter (Visible Only for Assignments with Instance Parameters)	The instance parameter the parameter depends on.												
Instance (Visible Only for Assignments with Instance Parameters)	The instance of the parameter.												
Name	The name of the parameter.												
Value	<p>The parameter value for this assignment.</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) 												

UI Element	Description
	<ul style="list-style-type: none"> •  Number •  Password •  String <p>Note the following:</p> <ul style="list-style-type: none"> • If the value is dimmed, it is the default value. • If the icon is dimmed, the value is read-only. • If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.

—All Parameters

UI Element	Description
Parameter List	<p>Lists all parameters contained in the management template or aspect. You can enter or change the default of a parameter in the list.</p> <p>The toolbar provides the following controls:</p> <div>  <p>Edit: Specify the value of the selected parameter.</p> <ul style="list-style-type: none"> • For standard parameters, the <i>Edit Parameter</i> dialog opens. • For instance parameters, the <i>Edit Instance Parameter</i> dialog opens. <p>For details on using the dialogs, see the relevant <i>UI Reference</i> section.</p> </div>

UI Element	Description								
	<p> Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p> <p> Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p> <table> <tr> <td>Target (Visible Only for Assignments of Management Templates)</td><td>The CI type of the item using the parameter.</td></tr> <tr> <td>Defined In (Visible Only for Assignments of Management Templates)</td><td>The management template, aspect or policy template in which the parameter is defined.</td></tr> <tr> <td>Name</td><td>The name of the parameter.</td></tr> <tr> <td>Value</td><td> <p>The parameter value for this assignment.</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 </td></tr> </table>	Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.	Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.	Name	The name of the parameter.	Value	<p>The parameter value for this assignment.</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
Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.								
Defined In (Visible Only for Assignments of Management Templates)	The management template, aspect or policy template in which the parameter is defined.								
Name	The name of the parameter.								
Value	<p>The parameter value for this assignment.</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 								






UI Element	Description
	<ul style="list-style-type: none">  Password  String <p>Note the following:</p> <ul style="list-style-type: none"> If the value is dimmed, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.






—Configure Options

UI Element	Description
Activate Auto-Assignment Rule	If you do not want the auto-assignment rule to start creating assignments immediately, clear the Activate Auto-Assignment Rule check box. To enable auto-assignment rules after closing the wizard, use the <i>Automatic Assignment Rules</i> screen.
Back	Moves back to the previous step.
Next	Moves on to the next step.
Finish	Accepts the values in all steps and creates the item.
Cancel	Closes the wizard without creating the item.
Help	Opens the relevant help in a new browser window.


Edit Auto-Assignment Rule Dialog











UI Element	Description
Parameter List	Lists all parameters contained in the management template or aspect to be auto-assigned.


UI Element	Description		
	<p>The toolbar provides the following controls:</p> <div data-bbox="573 373 605 405"></div> <p>Edit: Specify the value of the selected parameter.</p> <ul style="list-style-type: none"> For standard parameters, the <i>Edit Parameter</i> dialog opens. For instance parameters, the <i>Edit Instance Parameter</i> dialog opens. <p>For details on using the dialogs, see the relevant <i>UI Reference</i> section.</p> <div data-bbox="573 720 605 751"></div> <p>Hide/Unhide Expert Parameters: Show or hide expert parameters. If the management template, aspect, or policy template contains no expert parameters, clicking the button has no effect.</p> <div data-bbox="573 877 646 909"> </div> <p>Search/No Filter: Filter the items in the list:</p> <ul style="list-style-type: none"> Type a string or a number to narrow down the list to those items that have the specified string contained in their name and, if available, their description, value, or the name of the item they are defined in. The search is not case-sensitive. If a filter is active, click  No Filter to remove the filter and show all items in the list. <p>To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.</p> <p>The parameter list has the following columns:</p> <table border="0"> <tr> <td data-bbox="573 1507 743 1644"> Target (Visible Only for Assignments of Management Templates) </td> <td data-bbox="808 1507 1304 1539"> The CI type of the item using the parameter. </td> </tr> </table>	Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.
Target (Visible Only for Assignments of Management Templates)	The CI type of the item using the parameter.		

UI Element	Description
	<p>Defined In (Visible Only for Assignments of Management Templates)</p> <p>The management template, aspect or policy template in which the parameter is defined.</p> <p>Name</p> <p>The name of the parameter.</p> <p>Value</p> <p>The parameter value for this assignment.</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, it is the default value. If the icon is dimmed, the value is read-only. If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
OK	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.

Edit Instance Parameter Dialog

UI Element	
Instance Values	<p>The toolbar provides the following controls:</p> <p></p> <p>Create Instance Parameter: Open the <i>Edit Parameter</i> dialog. To create a new value, select Value and specify a value in the text box. Click OK to close the dialog and add the new value to the Instance Values list, or click Cancel to close the dialog without making changes.</p>

UI Element					
	<div data-bbox="573 317 607 348"></div> <p>Edit Instance Parameter: Open the <i>Edit Parameter</i> dialog. To change the instance value, edit the value in the text box. Click OK to close the dialog and replace the value in the Instance Value list with the new value, or click Cancel to close the dialog without making changes.</p> <div data-bbox="573 541 607 573"></div> <p>Delete Instance Parameter: Delete the selected instance value.</p> <div data-bbox="573 632 607 663"></div> <p>Move Up: Move the selected instance value up in the list.</p> <div data-bbox="573 722 607 753"></div> <p>Move Down: Move the selected instance value down in the list.</p>				
Dependent Values	<p>Lists the dependent values for the instance value selected in the Instance Values list.</p> <p>The toolbar provides the following controls:</p> <div data-bbox="573 978 607 1010"></div> <p>Edit Show the <i>Edit Parameter Dialog</i> to specify a value for the parameter.</p> <div data-bbox="573 1068 607 1100"></div> <p>Hide/Unhide Expert Parameters: Show or hide expert parameters.</p> <p>The list has the following columns:</p> <table data-bbox="573 1230 1156 1318"> <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 <p>Note the following:</p>	Name	The name of the dependent value.	Value	The value of the dependent value.
Name	The name of the dependent value.				
Value	The value of the dependent value.				

UI Element	
	<ul style="list-style-type: none"> • If the value is dimmed, it is the default value. • If the icon is dimmed, the value is read-only. • If the invalid icon  appears, the parameter is mandatory, and you need to specify a value.
OK	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.

Edit Parameter Dialog





UI Element	Description
Value	Select Value if you want to set a specific default value for the parameter in this assignment. 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.
Use Default Value	The other choice offered is Use Default Value . Select this option if you want to use the default value defined in the policy template, aspect, or management template.
OK	Applies all values and closes the dialog.
Cancel	Closes the dialog without creating or updating the item.

Chapter 6: Deployment Jobs

Deployment refers to the process of transferring policy templates, aspects, management templates, and instrumentation from the BSM server to one or more nodes.

Operations Management automatically creates a deployment job for a node whenever you create or remove an assignment to a policy template, aspect, or management template, or when you modify the assigned configuration.

Use the Deployment Jobs screen to manage deployment jobs. Some examples of tasks are:

- Investigate and repair jobs with the status  FAILED. Deployment jobs may fail when Operations Management cannot communicate with the node, for example because of network or certificate problems.
- Investigate and repair jobs remaining in the state  PENDING longer than expected. Pending jobs are jobs that are waiting to be executed on a node.
- Manually restart jobs with status  SUSPENDED after repairs or other updates. Jobs may be manually suspended by an Operations Management administrator. Jobs may also have the status  SUSPENDED if another job for the same node has failed.
- Monitor running jobs.


As soon as a deployment job is completed successfully, it is deleted from the list of pending jobs.

Tip: You can select multiple items by holding down the **Ctrl** or **Shift** key while selecting them.



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.

When you restart a deployment job, the state of all other jobs for the same node changes to  PENDING.

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.










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.





To restart jobs for deleted deployment jobs, click **Start jobs for undeployed deployments** .

UI Reference

Deployment Jobs

UI Element	Description
	Reload deployment jobs: Refresh the list of deployment jobs.
	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 because the associated jobs have been deleted.
State	<p>Indicates the state of the deployment job. The possible states are:</p> <ul style="list-style-type: none">  RUNNING  PENDING  SUSPENDED  FAILED
Node	Target system for the deployment job.
Assigned Item	The management template, aspect, or policy template that was used for the assignment.
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.
Automatically reload jobs	Reloads the list of deployment jobs every few seconds.

Deployment Job Details

UI Element	Description
State	Indicates state of the deployment job. The possible states are: <ul style="list-style-type: none">•  RUNNING•  PENDING•  SUSPENDED•  FAILED
Description	Overview of the deployment job. If a deployment job has failed, the description shows the details of the error or exception.
Deployment Job ID	ID of the deployment job.
Node	Target system for the deployment job.
Scope	Describes the artifacts included in the deployment job (for example, policy templates, aspects, or management templates).
Date created	Date and time the deployment job was created.
Date modified	Date and time the status of a deployment job was last modified.
Executed on gateway	Name of the BSM Gateway Server that initiated the deployment.
CI Name and Type	The name of the CI to which the item was assigned, followed by the CI type in parentheses
Assigned Item	The management template, aspect, or policy template that was used for the assignment.
Assigned Item Version	The version of the assigned item that was used for the assignment.
Assigned Item Version ID	The ID of the assigned item version.

Chapter 7: 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 462](#)

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. " on the next page](#)
- ["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** .
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 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: Opens the <i>Add License</i> browser allowing you to select a license file to add.
	Expand All: Expand all multi-level list entries.
	Collapse All: Collapse all multi-level list entries.
	Show/Hide Columns: Opens the <i>Choose Columns to Display</i> dialog. 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 its checkbox is not checked.

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 8: Migrating Configuration Data

There are several types of configuration information you may want to copy or move between servers. This section covers the following topics:

- ["Copying Configurations Between Servers" below](#)
- ["Importing Configuration Data from HP Operations Manager" on the next page](#)

Copying Configurations Between Servers

You can export configuration content from one system and import it to other systems using the Content Manager, accessible at **Admin > Platform > Content Packs**.

To enable exporting the configuration, create a content pack with the required data on the primary server. To ensure that the entire configuration is exported, the following configuration objects must be included in the Content Pack:

- **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 the links to the aspects, management templates, policy templates that are assigned to a CI is not supported.

When the content pack is complete, select it in the list of Content Pack Definitions (left pane) and click  **Export Content Pack Definitions and Content** to export the data to the file system as an archive with the extension zip. Transfer the archive to the file system of the secondary server, start BSM, and go to the Content Manager. Click  **Export Content Pack Definitions and Content**, browse to the transferred Content Pack, and click **Import**. The configuration is now uploaded to the secondary server.

Importing Configuration Data from HP Operations Manager

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. Monitoring Automation provides the command-line interface **ConfigExchange** that enables you to import policies from HPOM so that you can include them in aspects, and also deploy them directly from Monitoring Automation.

Learn More

This section includes:

- ["Migrating HPOM Configuration Data" below](#)
- ["Forwarding of HPOM Data" on page 467](#)
- ["Validating HPOM Policies" on page 467](#)
- ["Limitations" on page 467](#)

Migrating HPOM Configuration Data

You can migrate the following types of configuration data from HPOM to Monitoring Automation:

- **Policy templates.** HPOM supports agent, server, and Event Correlation Services (ECS) policies. You can export agent policies from HPOM and import them to Monitoring Automation. Any associated instructions are also migrated. Server and ECS policies cannot be migrated.
- **SiteScope templates.** SiteScope templates can be imported in the following ways:
 - The template can be imported directly from a SiteScope server. For more information, see ["Importing HP SiteScope Templates" on page 364](#).
 - The template may have been imported to HPOM for UNIX or Linux earlier, in which case it is stored on HPOM for UNIX or Linux as a policy. This policy can then be transferred to Monitoring Automation together with other policies.
- **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 HPOM and import them into Monitoring Automation. 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 HPOM 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 Monitoring Automation. You can deploy the instrumentation categories with individual policies, and you can add the instrumentation to aspects.

- **Script parameters in measurement threshold policies.** 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 Monitoring Automation policy template parameters.

- **Automatic and operator-initiated commands.** HPOM policies can create events (called messages in HPOM) that include automatic and operator-initiated actions (also known as commands in HPOM for Windows):
 - Automatic actions can run locally on a managed node when the HP Operations Agent detects the event.

HPOM can run automatic actions on the management server or a managed node when the event arrives on the management server. HPOM can also run remote automatic actions. Operators can restart automatic actions manually from the HPOM message browser.

A remote automatic action is an action that is attached to an event sent by a node and configured to run on another node.

BSM Operations Management can run automatic and remote automatic actions on managed nodes. Automatic actions can also run on the BSM Operations Management server if an HP Operations Agent is installed. You can restart an automatic or remote action on any node manually from the BSM Operations Management Event Browser.

- HPOM operators can start operator-initiated actions manually from the HPOM message browser, after evaluating the details of the event.

Similarly, BSM Operations Management users can start operator-initiated actions manually from the BSM Operations Management Event Browser.

Operations Management checks the Originating Server event attribute to determine which server should start the action. If the Originating Server attribute is empty, Operations Management starts the action. If the originating server is an HPOM server, the action request is transferred to the HPOM server for execution. The originating server is the server that initially

forwarded the original event along the chain of servers configured in a flexible management environment.

When you import policies from HPOM to Monitoring Automation, any automatic and operator-initiated actions are included. Actions that include the variable <\$OPC_MGMTSV> only run on HPOM management servers, not on BSM Operations Management servers. To run these actions on the BSM Operations Management server, replace the variable <\$OPC_MGMTSV> with the name of the server.

Note: Migrating configuration data from Monitoring Automation to HPOM is not supported.

Forwarding of HPOM Data

The following types of data can be forwarded dynamically from HPOM to Operations Management :

- Messages (including message operations such as acknowledgment, annotations, and so on)
- Action requests and responses for tools executed on the agent through HPOM
- Topology changes, including addition, modification, and deletion of nodes, node groups, and services

For the initial synchronization, you need to forward all the topology data that already exists on an HPOM management server. (You can do this using the tool **startInitialSync** on the source HPOM server.)

Validating HPOM Policies

You can use the command-line interface **ConfigExchange** to check and validate whether HPOM policies are compatible with Monitoring Automation. The tool generates a Policy Parser Report, which contains the following information:

- Summary of the number and types of problems and incompatibilities
- Policies without problems
- Policy files containing Event Correlation Services (ECS)
- Policy file problem details

After the import to Monitoring Automation, you can use the policy editors to edit each policy with reported problems and change the policy to comply with Monitoring Automation policy templates. It is important that all problems are corrected before deploying the policy templates to an agent.

Limitations

The following data *cannot* be imported from HPOM to Operations Management:

- Event Correlation Services (ECS) policies
- Users, user profiles, and responsibility matrices
- Message groups
- Tool definitions
- Assignments (for example, the assignment of policy groups to nodes)
- Server-related policies and configuration data (for example, trouble tickets, notification definitions, message-stream configuration data, configuration settings, and instruction text interface definitions)
- Heartbeat monitoring configurations

Tasks

This section includes:

- ["How to Export Policies from HPOM for Windows" below](#)
- ["How to Export Policies from HPOM on UNIX or HPOM on Linux" on the next page](#)
- ["How to Validate and Import Policies from HPOM" on the next page](#)

How to Export Policies from HPOM for Windows

You can export policies, policy groups, and instrumentation from HPOM for Windows using the **ovpmutil** tool on the HPOM for Windows management server:

```
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 policy group path can be constructed similar to the path to a 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.

Example policy group path: "\Samples\Flexible Management\Follow the Sun"

- 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 on ovpmutil, see the HPOM for Windows online help.

How to Export Policies from HPOM on UNIX or HPOM on Linux

To download policies, policy groups, and instrumentation from HPOM for UNIX or Linux, you can use the Administration UI or the **opcpolicy** command-line interface:

- **Administration UI.** 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**, select the policy groups and instrumentation categories that you want to download, and then click **Choose an action > Download Shopping Cart**. Type a comment, and then click **OK**.
 - e. Click **Browse > Downloads**, select the sub-folder with your download data, and then click **Choose an action > Archive as ZIP**. Click **View Archive Directory**, and then click the name of the archive file to download it.

The downloaded data is also available in the following directory on the management server:

```
/opt/OV/OMU/adminUI/data/clipboard/
```

- **opcpolicy.** opcpolicy downloads policies and policy groups and associated instrumentation.

To export policy group *<policyGroup>* and associated instrumentation from HPOM for UNIX or Linux to the directory *<downloadDir>*, run the following command on the HPOM for UNIX or Linux server:

```
opcpolicy -download pol_group=<policyGoup> dir=<downloadDir>
```

You can also export a single policy instead of a policy group. For example, to export version 1.0 of the open message interface policy Oracle messages and the associated instrumentation, run the following command:

```
opcpolicy -download pol_name="Oracle messages" pol_type="Open_Message_Interface"  
version=1.0 dir=/tmp
```

For more information, see the opcpolicy man page.

How to Validate and Import Policies from HPOM

Validate and import the downloaded HPOM policies, policy groups, and instrumentation:

1. Copy the output folder or archive file from the HPOM server to the BSM server, and if necessary extract the files from archive.

- Exported policy files are stored in the following folder:

`<downloadDir>/<policyVersionId>_<suffix>`

- Exported policy groups are stored in the following folder:

`<downloadDir>/PolicyConfig_<policyGroupId>.xml`

- Exported instrumentation files are stored in the following folder:

`<downloadDir>/Instrumentation/<categoryName>`

2. On the BSM server, check if the policies copied from HPOM to Monitoring Automation are compatible with Monitoring Automation and log the results to log file `<logFile>`. Run the following command:

`ConfigExchange -check -policyfile <policyDir> -logfile <logFile>`

3. On the BSM server, upload the HPOM policies, policy groups, and instrumentation using the ConfigExchange command-line tool:

`ConfigExchange -username <username> -password <password> -uploadOM -input <folder>`

- Replace `<username>` with the user name of a BSM user with permission to create policy templates.
- Replace `<password>` with the password of the BSM user.
- Replace `<folder>` with the path to a folder that contains the policy data and instrumentation. The folder must be the output of ovpmutil (HPOM for Windows) or a download started from the Administration UI or opcpolicy (HPOM for UNIX or HPOM for Linux).

Example:

The following command uploads policies, policy groups, and instrumentation from a folder called 'example_policy_group':

```
c:\HPBSM\opr\bin\ConfigExchange.bat -username admin -password password -
uploadOM -input c:\Users\Administrator\Desktop\example_policy_group
```

4. Check the generated log file that contains the policy parser report. For each policy file with reported errors, using the policy editors, modify the policy to suit your requirements.

For details on ConfigExchange, see ["ConfigExchange Command-Line Interface" on page 486](#).

Examples

Policy Parser Report for HPOM Policies

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 opcmoma 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:

...

Configuration Data Exchange on Linux

The following commands show the migration of the configuration data set english InfraSPI from HPOM for UNIX or Linux to an OMi Linux system running Monitoring Automation:

1. Run the following commands on the HPOM for UNIX or Linux server:

```
/opt/OV/bin/OpC/utls/opcpolicy -list_groups |grep -i infra
```

```
/opt/OV/bin/OpC/utls/opcpolicy -download pol_group="/Infrastructure Management/en"  
dir=/tmp/infraspiDown
```

```
scp -r /tmp/infraspiDown <MAserver>:/tmp
```

2. Run the following commands on the OMi server running Monitoring Automation:

```
/opt/HP/BSM/opr/bin/ConfigExchange.sh -check -policyfile /tmp/infraspiDown -logfile  
/tmp/infraspiVal.log
```

```
/opt/HP/BSM/opr/bin/ConfigExchange.sh -username myU -password myPW -uploadOM  
-input c:/cygwin/tmp/infraspiDown
```

Configuration Data Exchange on Windows

The following commands show the migration of the configuration data set english SPI for Databases from HPOM for Windows to an OMi Windows system running Monitoring Automation:

1. Run the following command on the HPOM for Windows server:

```
cfg pol dnl C:\temp /p "\SPI for Databases" /instrum
```

2. Copy the output folder C:\temp\SPI for Databases from the HPOM server to the OMi server running Monitoring Automation.
3. Run the following commands on the OMi server running Monitoring Automation:

```
C:\HPBSM\opr\bin\ConfigExchange.bat -check -policyfile "C:\temp\SPI for Databases"  
-logfile C:\temp\infraspiVal.log
```

```
C:\HPBSM\opr\bin\ConfigExchange.bat -username myU -password myPW -uploadOM -i  
"c:\temp\SPI for Databases"
```

Troubleshooting

Troubleshooting Configuration Upload

For information on troubleshooting configuration upload, see ["ConfigExchange Command-Line Interface" on page 486](#).

For information on troubleshooting SiteScope template import, see ["Importing HP SiteScope Templates" on page 364](#).

Chapter 9: Connecting HP Operations Agents to HP Operations Manager i

HP Operations Agent is a server performance monitoring application that resides on a server and collects detailed information about system metrics related to faults and performance. It is designed to provide information about servers used to run critical business applications, enables outage troubleshooting, performance optimization and capacity planning. The agent can take autonomous action if a metric breaches a threshold value, adjusting those values based on actual performance that it tracks over time. HP Operations Agent can send alerts or events to HP Operations Manager i (BSM).

New Installations of HP Operations Agent

HP Operations Agent 11.12 is available on the HP Operations Agent media DVD, which is included in the BSM 9.20 media kit. The latest agent updates can be downloaded from HP Software Support Online (<http://h20230.www2.hp.com/selfsolve/patches>). After the installation of the HP Operations Agent software on the system to be monitored, you must connect the agent to OMi and then grant the agent's certificate request in BSM Operations Management. For details, see "[Connecting a New HP Operations Agent Installation](#)" below.

Once the communication between the agent and the OMi server is established and the agent processes are running, a node CI is created in the RTSM for the monitored node. You can then deploy management templates, aspects, policies, and instrumentation to the node. Alternatively, if the node matches an automatic assignment rule, BSM Operations Management creates an assignment for the CI, and starts the deployment jobs required to transfer the monitoring configuration to the node. After the agent has started monitoring the system, it begins to send events to OMi, which you can view in the Operations Management Event Browser.

Existing HP Operations Agent Installations

HP Operations Agents that are already connected to HP Operations Manager (HPOM) can be configured to send events to BSM, run actions, and accept policies from BSM. For details, see "[Connecting an Existing HP Operations Agent Installation](#)" on page 476.

Connecting a New HP Operations Agent Installation

To connect an agent-monitored system to Monitoring Automation in BSM Operations Management, you must first ensure that the HP Operations Agent is installed on that system, connect the agent to BSM, and grant the required certificates.

Note: The HP Operations Agent is licensed separately.

Tip: Include agent installation in your virtual machine cloning, in your general software distribution process, or use a distribution tool, such as SCP, for remote installation.

For details, refer to the HP Operations Agent documentation.

To connect an HP Operations Agent to a BSM server with HP Monitoring Automation installed, follow these steps:

1. *Prerequisite:* Install HP Operations Agent on the system that you want to monitor with Monitoring Automation. When installing the agent, specify the BSM gateway server as the agent's management server.

For information about installing the HP Operations Agent, see *HP Operations Agent and HP Operations Smart Plug-ins for Infrastructure Installation and Configuration Guide*.

If the agent is installed in inactive mode, for example for pre-installation in a virtual machine image, manually connect the agent to BSM:

- a. Log on to your systems where the HP Operations Agent is installed.
 - b. Navigate to the following location:
 - Windows 64-bit: %OvInstallDir%\bin\win64\OpC\install
 - Windows 32-bit: %OvInstallDir%\bin\OpC\install
 - %OvInstallDir% default: C:\Program Files\HP\HP BTO Software\
 - AIX, HP-UX, Linux, and Solaris: /opt/OV/bin/OpC/install/
 - c. Run the following script at a command prompt:
 - Windows: cscript opcactivate.vbs -srv <BSM_Gateway_Server>
 - AIX, HP-UX, Linux, and Solaris: opcactivate.sh -srv <BSM_Gateway_Server>
2. In the BSM user interface under **Operations Management > Setup > Certificate Requests**, accept the new certificate request. For details, see the BSM Operations Management online help.

Tip: You can grant certificates automatically using pre-configured IP ranges or a groovy script.

3. *Optional:* Check HTTPS communication in both directions using the command:

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

If the connection is successful, the command returns status=eServiceOK.

Connecting an Existing HP Operations Agent Installation

HP Operations Manager (HPOM) managed nodes already have the HP Operations Agent installed. By default, these agents send messages to HPOM, and accept policies and packages as well as action execution requests from the HPOM management server. By default, the HPOM management server is the primary manager of the agents.

If HPOM is integrated with BSM Operations Management, the HPOM management server forwards all messages to BSM based on a flexible management policy. Instruction and action execution requests sent from the BSM server are executed on the HPOM server.

With Monitoring Automation installed, you can connect HPOM managed nodes directly to BSM and configure the agents to accept policies and action execution requests from BSM.

Note: You can also configure the agent to directly send events to BSM. However, to ensure successful retrieval of instruction texts it is recommended that the agent sends all events to the HPOM management server from where they are forwarded to BSM.

Learn More

This section includes:

- ["Primary, Secondary, and Action-Allowed Managers" on the next page](#)
- ["Policy Management" on the next page](#)
- ["Instructions" on page 478](#)
- ["Actions" on page 478](#)
- ["Architecture" on page 479](#)
- ["Limitations" on page 480](#)

Primary, Secondary, and Action-Allowed Managers

By default, only the node's primary manager has the right to deploy policies and instrumentation and to start actions. In addition, the primary manager by default receives all events from a node. Discovery data is also always sent to the primary manager, regardless of the flexible management configuration.

By configuring the BSM server as secondary and action-allowed manager, the BSM server is granted permission to deploy policies and instrumentation to the HPOM managed nodes and to execute actions on the nodes. You configure secondary and action-allowed servers by specifying these servers in a flexible management policy and deploying the policy to the nodes.

When you switch the primary manager of an agent from the HPOM server to the BSM server, the BSM server will by default receive all events and topology data sent from the HPOM managed nodes. Switching a node's primary manager from HPOM to BSM can be accomplished by running the `ovconfpar` command-line tool on the BSM server running Monitoring Automation.

Note: It is not recommended that you make the BSM server the primary manager until the complete HPOM configuration has been migrated to Monitoring Automation. Otherwise instruction text retrieval may not be successful.

Policy Management

All secondary managers of a node have permission to deploy policies to the node and to keep an inventory of the policies installed on the node. You can see which policies are installed on a node by viewing the node's policy inventory. The policy inventory is updated every time you synchronize the policy template assignments of the node with Monitoring Automation.

The first time the synchronization runs all policies that are installed on the node are uploaded to Monitoring Automation and displayed in the Policy Templates list. Policy types not supported by Monitoring Automation (for example, server and event correlation policies) are ignored. The next synchronization uploads only updates.

Note: The synchronization of policy template assignments also imports the policies installed on a node but not the associated instrumentation. Therefore, do not use this method to migrate policies from another server. Use the `ConfigExchange` command instead to import policies with the associated instrumentation. For details, see "[ConfigExchange Command-Line Interface](#)" on page 486.

If you want to modify HPOM policies in Monitoring Automation, you must download the policies in HPOM and then upload the policies to Monitoring Automation using the `ConfigExchange` command-line tool. `ConfigExchange` can also upload instrumentation. Monitoring Automation policies cannot be uploaded to HPOM.

Instructions

Instructions are configured in the policy that generates the event. Events do not contain the actual instructions but a reference to the corresponding policy (or for some HPOM for UNIX or Linux events, a link to an external instruction provider).

When you open the instructions associated with an event in the BSM Operations Management Event Browser, the browser first attempts to retrieve the instruction from the server to which you are logged on. If this fails because the server is unable to find the corresponding policy that contains the instructions, the server tries to retrieve the instructions from the originating server (that is, the HPOM management server). The HPOM message browser always searches for instruction texts in the management server's policy database.

Actions

Policies can create events that include automatic and operator-initiated actions (also known as commands in HPOM for Windows):

- Automatic actions can run locally on a managed node when the HP Operations Agent detects the event.

HPOM can run automatic actions on the management server or a managed node when the event arrives on the management server. HPOM can also run remote automatic actions. Operators can restart automatic actions manually from the HPOM message browser.

A remote automatic action is an action that is attached to an event sent by a node and configured to run on another node.

BSM Operations Management can run automatic and remote automatic actions on managed nodes. Automatic actions can also run on the BSM Operations Management server if an HP Operations Agent is installed. You can restart an automatic or remote action on any node manually from the BSM Operations Management Event Browser.

- HPOM operators can start operator-initiated actions manually from the HPOM message browser, after evaluating the details of the event.

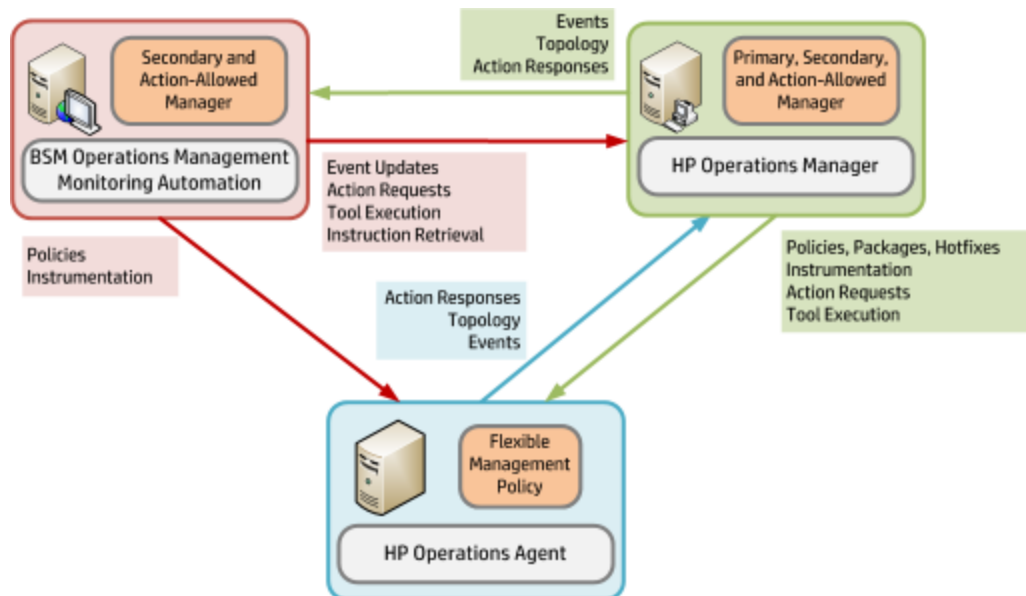
Similarly, BSM Operations Management users can start operator-initiated actions manually from the BSM Operations Management Event Browser.

Operations Management checks the Originating Server event attribute to determine which server should start the action. If the Originating Server attribute is empty, Operations Management starts the action. If the originating server is an HPOM server, the action request is transferred to the HPOM server for execution. The originating server is the server that initially forwarded the original event along the chain of servers configured in a flexible management environment.

When you import policies from HPOM to Monitoring Automation, any automatic and operator-initiated actions are included. Actions that include the variable <\$OPC_MGMTSV> only run on HPOM management servers, not on BSM Operations Management servers. To run these actions on the BSM Operations Management server, replace the variable <\$OPC_MGMTSV> with the name of the server.

Architecture

The following figure shows the architecture of a deployment where both HPOM and Monitoring Automation manage an agent:



- **HPOM:**

Is the primary, secondary, and action -allowed manager of an HP Operations Agent.

Deploys policies, packages, hotfixes, and instrumentation to the agent.

Runs actions and tools on the agent.

Forwards events and topology to BSM Operations Management.

- **Monitoring Automation:**

Is the secondary and action-allowed manager for the HP Operations Agent.

Deploys policies and instrumentation to the agent.

Forwards event updates to HPOM.

Uses HPOM as the action server for running actions on the agent.

Uses HPOM as the instruction text server for retrieving instruction texts from HPOM policies.

- **HP Operations Agent:**

Accepts configuration from both HPOM and Monitoring Automation.

Sends events and topology to HPOM only.

Limitations

- Only HP Operations Agents version 11.12 or later can be integrated with Monitoring Automation.
- HPOM for Windows management servers require patch OMW_00177 (32-bit) or OMW_00178 (64-bit).

HPOM for UNIX or Linux management servers do not require a patch for the HPOM-Monitoring Automation integration.

- Policy synchronization in HPOM for Windows:

HPOM for Windows management servers can synchronize their policy inventory with nodes that are managed by both HPOM for Windows and Monitoring Automation. If such nodes have parameterized Monitoring Automation policy templates, the HPOM server associates these policies with the policy type "Unknown". The HPOM server does not receive the contents of the policy, so the policies cannot be changed, enabled, disabled, removed, or deployed to other nodes.

- Monitoring Automation does not support heartbeat polling.
- Monitoring Automation cannot deploy agent hotfixes or patches to the nodes.

Tasks

This section includes:

- ["How to Manage an Existing HP Operations Agent with HPOM and Monitoring Automation" below](#)
- ["How to Switch the Primary Server of an Agent Managed by Monitoring Automation" on page 483](#)

How to Manage an Existing HP Operations Agent with HPOM and Monitoring Automation

This task describes how to configure an existing HP Operations Agent to be managed by both HPOM and OMi running Monitoring Automation:

1. *Prerequisite:* Make sure the HPOM management server is integrated with the BSM Operations Management server running Monitoring Automation. If it is not, follow the instructions in the BSM - Operations Manager Integration Guide to integrate both products.
2. Update the trusted certificates on the nodes. The tools in the following procedure retrieve the currently trusted certificates from the certificate server and install them as trusted certificates on the nodes.

HP Operations Manager for Windows managed nodes:

- a. In the console tree, click **Tools > HP Operations Manager Tools > Certificate Management**.
- b. In the details pane, double-click **Update trusted certificates**. A dialog box opens, which lists nodes and services.
- c. Select the nodes on which to update the trusted certificates. To update trusted certificates on all existing nodes, select the **Nodes** check box. Alternatively, you can select check boxes for individual nodes or node groups.
- d. Click **Launch....** The Tool Status dialog box opens and shows progress.

HP Operations Manager for UNIX or Linux managed nodes:

In the Operator UI, right-click the managed nodes on which to update the trusted certificates and select **Start > Certificate Tools > Update Trusts** from the context menu. The output of the tool displays in a new workspace pane window

3. *Optional:* Import HPOM policies and instrumentation into Monitoring Automation. Once the HPOM policies are available in Monitoring Automation, you can apply the advanced monitoring features of Monitoring Automation to them (for example, parameterization, management templates, and aspects). For details, see ["Importing Configuration Data from HP Operations Manager" on page 465](#).
4. Configure and deploy an agent-based flexible management policy in HPOM:
 - a. Create or edit an agent-based flexible management policy in HPOM. Add both the BSM server and the HPOM server as secondary and action-allowed servers. \$OPC_ALWAYS and \$OPC_PRIMARY_MGR configure the agent to always send events to the current primary manager (that is, the HPOM management server).

Hostname and IP address in flexible management policies:

You can specify either the IP address or host name of each management server. If you are specifying only a host name, enter the IP address 0.0.0.0.

For management servers in clusters, specify the IP address or host name of the virtual management server. In addition, you must add the core ID of the virtual management server.

Core ID in flexible management policies:

You must add the core ID for standalone management servers if you have not set up a node to represent these management servers on the management server from which you intend to deploy the policy.

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

```
ovcoreid -ovrg server
```


If the management server is in a cluster, make sure that you start the above command on the cluster node that is currently active.

Example:

```
TIMETEMPLATES
#none
RESPMGRCONFIGS
RESPMGRCONFIG
  DESCRIPTION "Defines HPOM and Monitoring Automation as responsible servers"
SECONDARYMANAGERS
SECONDARYMANAGER
  NODE IP 0.0.0.0 "hpom.example.com" ID "e11fd362-cc28-754b-1bdd-936b7e932019"
  DESCRIPTION "FQDN of HPOM management server"
SECONDARYMANAGER
  NODE IP 0.0.0.0 "ma.example.com" ID "814aee82-84d3-754b-1acd-8c4ca610810d"
  DESCRIPTION "OMi/MA server: FQDN of gateway server"
ACTIONALLOWMANAGERS
ACTIONALLOWMANAGER
  NODE IP 0.0.0.0 "hpom.example.com" ID "e11fd362-cc28-754b-1bdd-936b7e932019"
  DESCRIPTION "FQDN of HPOM management server"
ACTIONALLOWMANAGER
  NODE IP 0.0.0.0 "ma.example.com" ID "814aee82-84d3-754b-1acd-8c4ca610810d"
  DESCRIPTION "OMi/MA server: FQDN of gateway server"
MSGTARGETRULES
MSGTARGETRULE
  DESCRIPTION "always send all messages to current primary manager"
MSGTARGETRULECONDS
MSGTARGETMANAGERS
MSGTARGETMANAGER
  TIMETEMPLATE "$OPC_ALWAYS"
  OPCMGR IP 0.0.0.0 "$OPC_PRIMARY_MGR"
```

For more information on creating a flexible management policy in HPOM, see the HPOM documentation.

- b. Deploy the flexible management policy to the nodes that you want to co-manage with Monitoring Automation.
5. *Recommended:* To see which policies are installed on the node, synchronize the node's policy template assignments with Monitoring Automation:

- a. On the BSM Operations Management server running Monitoring Automation, navigate to **Admin > Operations Management > Monitoring > Assignments & Tuning**.
- b. Select the node CI for which you want to synchronize policy template assignments.
- c. Click  **Synchronize Policy Template Assignments**.

You may have to refresh the list to see the assignments.

How to Switch the Primary Server of an Agent Managed by Monitoring Automation

This task describes how to switch the primary server of an HP Operations Agent that is managed by a BSM Operations Management server running Monitoring Automation to another BSM server:

1. *Prerequisites:* Configure trust and a flexible management policy:

- a. Exchange trusted certificates between the BSM Operations Management servers, and update the trusted certificates on the agents.

For details on exchanging trusted certificates between the BSM Operations Management servers, see "How to Establish a Trust Relationship for a Server Connection" in the BSM Application Administration Guide or the BSM Help.

To update the trusted certificates on the nodes, run `ovcert -updatetrusted` on each agent system. The command retrieves the currently trusted certificates from the certificate server and installs them as trusted certificates on the node.

- b. Configure the new primary server as a secondary and action-allowed server of the nodes. You do this by deploying a flexible management policy to the nodes from the current primary server. For details, see ["Connecting an Existing HP Operations Agent Installation" on page 476](#).

Hostname and IP address in flexible management policies:

You can specify either the IP address or host name of each server. If you are specifying only a host name, enter the IP address 0.0.0.0.

Core ID in flexible management policies:

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

```
ovcoreid -ovrg server
```

Example:

```
RESPMGRCONFIGS
RESPMGRCONFIG DESCRIPTION "Prepare for primary manager switch"
SECONDARYMANAGERS
  SECONDARYMANAGER NODE IP 0.0.0.0 "oldserver.example.com"
    ID "e77b4992-5d78-753f-1387-c01230fe2648"
  SECONDARYMANAGER NODE IP 0.0.0.0 "newserver.example.com"
    ID "68f01602-8bfa-7557-0403-8467ba97477a"
ACTIONALLOWMANAGERS
  ACTIONALLOWMANAGER NODE IP 0.0.0.0 "oldserver.example.com"
    ID "e77b4992-5d78-753f-1387-c01230fe2648"
  ACTIONALLOWMANAGER NODE IP 0.0.0.0 "newserver.example.com"
    ID "68f01602-8bfa-7557-0403-8467ba97477a"
MSGTARGETRULES
MSGTARGETRULE
  DESCRIPTION "always send all events to current primary manager"
MSGTARGETRULECONDS
MSGTARGETMANAGERS
MSGTARGETMANAGER
  TIMETEMPLATE "$OPC_ALWAYS"
  OPCMGR IP 0.0.0.0 "$OPC_PRIMARY_MGR"
```

In addition to configuring "oldserver.example.com" and "newserver.example.com" as secondary and action-allowed managers, the policy always sends all events (\$OPC_ALWAYS) to the agent's primary server (\$OPC_PRIMARY_MGR).

For more information on the syntax used in flexible management policies, see ["Configuring Flexible Management Policies" on page 125](#).

2. Switch the node's primary manager. Complete the following steps on the new server for each node that you want to switch to the new server:

- a. Make sure the new server can contact the agent and that the agent processes are running on the node that you want to switch. On the new server, type the following command:

```
ovrc -ovrg server -host <FQDN of the node> -status
```

The command output should report that the ovcd, confd, and ovbbccb processes are running.

For more information on ovrc, run `ovrc -help`.

- b. Change the OPC_PRIMARY_MGR configuration parameter on the node. On the new server, type the following command:

```
ovconfpar -change -host <FQDN of the node> -src-ovrg server -ns eaagt -set OPC_
PRIMARY_MGR <FQDN of new BSM Operations Management server>
```

For more information on ovconfpar, run `ovconfpar -help`.


- c. Check the new configuration on the node. On the new server, type the following command:

```
ovconfpar -get -host <FQDN of the node> -src-ovrg server -ns eaagt
```

The output should include the following line:

```
OPC_PRIMARY_MGR="FQDN of new BSM Operations Management server"
```

Tip: If an open message interface policy is deployed to the node, you can send a message to the open message interface on the node and check that the corresponding event arrives in the Event Browser of the new server.

3. *Optional:* To see which policies are installed on the node, synchronize the node's policy template assignments with the Monitoring Automation policy database on the new server:
 - a. On the new server, navigate to **Admin > Operations Management > Monitoring > Assignments & Tuning**.
 - b. Select the node CI for which you want to synchronize policy template assignments.
 - c. Click  **Synchronize Policy Template Assignments**.

You may have to refresh the list to see the assignments.

Chapter 10: Tools

This section describes the following tools that are useful when managing Monitoring Automation configurations:

- ["ConfigExchange Command-Line Interface" below](#)
- ["ConfigWsTool Command-Line Interface" on page 497](#)
- ["ConfigExchangeSIS Command-Line Interface" on page 503](#)
- ["HP Operations Manager i and HP Operations Agent Command-Line Interfaces" on page 506](#)

Note: The syntax descriptions in this section use the following conventions:

1. {choice1|choice2|...} represents one of the choices choice1, choice2, ...
2. *<argument>* is a placeholder for an argument passed to an option. When issuing the command you should replace it with an appropriate string as explained for the option in question. To be able to use spaces and other reserved characters in the string, enclose it in quotation marks, for example -label "Category 5-7". (Note: Leading and trailing white space is removed.)
3. Everything enclosed in square brackets [...] is optional.
4. The rest of the notation is to be interpreted as literal.

Most command elements can be abbreviated. The option -force, for example, is listed in the syntax reference as {-force|-f}, meaning that either the fully qualified option -force, or the abbreviation -f may be used. For clarity, the abbreviations have been omitted from the command summaries and the examples, but they are included in the command reference.

ConfigExchange Command-Line Interface

You can use the ConfigExchange command-line interface (CLI) for the following tasks:

- Migrating policies from the HP Operations Manager (HPOM) to Monitoring Automation. These tasks make use of operations referred to in this section as <omOperation>.
- Development and management of instrumentation packages:
 - Creating a compatible file structure for instrumentation development.
 - Uploading and downloading instrumentation packages or elements thereof. An element of an instrumentation package can be the base package, a patch or a hotfix.

These tasks make use of operations referred to in this section as <instrumOperation>.

Location

`<BSM_Root_Directory>/opr/bin/ConfigExchange`

Synopsis

`ConfigExchange [<connection>] [<authentication>] {<toolInfo> | <omOperation> | <instrumOperation>}`

Options

Syntax for <connection>

`[{-server <gatewayServer> [-port <port>] [-ssl] | -url <url>}]`

Note: If <connection> is omitted, the command is executed on the server to which you are logged on.

Option	Description
<code>{-port -p} <port></code>	Uses port <port> to connect to the target Gateway Server. Default value of <port>: 80 for HTTP connections. 443 for HTTPS connections.
<code>-server <gatewayServer></code>	Sets the target Gateway Server, using <gatewayServer> as the hostname or IP Address to locate it. Default value of <gatewayServer> is the FQDN of the BSM gateway.
<code>-ssl</code>	When this flag is specified, the HTTPS protocol is used to connect to the target Gateway Server. If omitted, the HTTP protocol is used. This option cannot be used in conjunction with the option: url.
<code>{-url -u} <url></code>	Sets the target Gateway Server, using <url> as the URL to locate it. Default value of <url> is: <code>http://<BSM gateway FQDN>:80/opr-config-server/rest</code>

Syntax for <authentication>

`{-username <userName> -password <password> | -customer <customerID> | -jks <JAVAKeyStore> -jksPassword <password> | -smartcard | -winCrypto}`

Option	Description
{-customer -cu} <customerID>	The identification number associated with a particular customer in a HP Software-as-a-Service environment. Default value of <customerID> is 1.
{-jks -j} <JAVAKeyStore> {-jksPassword -jp} <password>	Use the JAVA Key Store located in directory <JAVAKeyStore> for authentication, and access it using the password <password>.
{-password -pw} <password>	Uses the password <password> for user <username>, which is used to execute ConfigExchange operations on the target Gateway Server. The default value of <password> is an empty string.
{-smartcard -sc}	Use certificate stored on smart card or security token for authentication.
{-username -user} <username>	Sets the username to be used to execute ConfigExchange operations on the target Gateway Server to <username>. The specified user must be a BSM user with permission to create policy templates.
{-winCrypto -wc}	Use Windows Certificate Store for authentication. This option can only be used on Windows systems.

Syntax for <toolInfo>

{-help | -version}

Option	Description
{-examples -ex}	Displays a number of examples of how to use the ConfigExchange tool.
{-help -h}	Display a summary of the ConfigExchange command options.
-version	Prints version information for the ConfigExchange tool.

Syntax for <omOperation>

{-check | -uploadOM} <arguments>

Option	Description
{-check -c} {-policyfile -pf} <fileOrDir> {-logfile -lf} <logFile>	Checks the policy contained in the policy file or directory <fileOrDir> for incompatibilities, and logs the results to <logFile>. Typically, policy files or directories are obtained through exports from HPOM. For more information on checking and migrating

Option	Description
	<p>policies from HPOM to Monitoring Automation, see "Importing Configuration Data from HP Operations Manager" on page 465.</p>
<p>{-uploadOM -uom} {-input -i} <inputDir></p>	<p>Note: <authentication> is required.</p> <p>Uploads the HPOM policies, policy groups, and instrumentation exported from HPOM for Windows or HPOM for UNIX or Linux to the Monitoring Automation database, using directory <inputDir> as the input directory.</p>

Syntax for <instrumOperation>

{-createinstrumdir | -download | -list | -merge | -remove | -upload} <arguments>

Option	Description
<p>{-createinstrumdir -cin} {-output -o} <outputDir></p>	<p>Creates an empty directory layout for an instrumentation package in the file system in directory <outputDir>.</p> <ul style="list-style-type: none"> • If a directory structure already exists at the specified location, the directory structure is merged in the existing one. • If the specified directory does not exist, it is created, including any higher-level directories. <p>When developing instrumentation, it is recommended to use this structure to ensure you apply the correct layout required by HPOM.</p>
<p>{-download -dl} {-output -o} <outputDir> {-instrumname -inn} <instrum> [-patch <patchNr>] [{-hotfix -hf} <hotfixName>] {-forpatch -fp} <patchNr>]</p>	<p>Note: <authentication> is required.</p> <p>Extracts the content of a specific configuration folder, a specific element of an instrumentation package or a policy from the database and downloads it to the file system in directory <outputDir>.</p> <ul style="list-style-type: none"> • Use -download -output <outputDir> -instrumname <instrum> to download the base package labeled <instrum>. • Use -download -output <outputDir> -instrumname <instrum> -patch <patchNr> to download patch

Option	Description
	<p><i><patchNr></i> for instrumentation <i><instrum></i>.</p> <ul style="list-style-type: none"> Use <code>-download -output <outputDir> -instrumname <instrum> -hotfix <hotfixName> -forpatch <patchNr></code> to download hotfix <i><hotfixName></i> for patch <i><patchNr></i> for instrumentation <i><instrum></i>. <p>Note: To download an entire package, including all its patches and hotfixes, use the <code>-merge</code> operation.</p>
{-list -l} {{-instrumname -inn} <i><instrum></i> ALL}	<p>Note: <i><authentication></i> is required.</p> <p>Lists all patches and hotfixes for instrumentation package <i><instrum></i>, or use ALL to list all instrumentation packages in the database (Note: ALL is case-sensitive).</p>
-merge {-output -o} <i><downloadDir></i> {-instrumname -inn} <i><instrum></i>	<p>Note: <i><authentication></i> is required.</p> <p>Downloads the instrumentation package with the label <i><instrum></i> and all its patches and hotfixes to the file system and places it in directory <i><downloadDir></i>. Data is merged in the following order:</p> <p>The base package and any patches and hotfixes are downloaded in the order they are applied to an agent:</p> <ol style="list-style-type: none"> 1. The base package is downloaded first. 2. Next, the highest patch is downloaded and applied to the base package. 3. Then the hotfixes for this patch are downloaded and applied in alphabetical order. 4. The previous steps are repeated for the next highest patch until all patches have been downloaded. <p>Note: To download a specific element of a package, use the <code>-download</code> operation.</p>

Option	Description
<pre>{-remove -rm} {-instrumentname -inn} <instrum> [{-patch -p} <patchNr>] [{-hotfix -hf} <hotfixName> {-forpatch -fp} <patchNr>]</pre>	<p>Note: <i><authentication></i> is required.</p> <p>Removes an instrumentation package or an element thereof from the database:</p> <ul style="list-style-type: none"> • Use <code>-remove -instrumentname <instrum></code> to completely remove the instrumentation package labeled <i><instrum></i> (including patches and hotfixes). • Use <code>-remove -instrumentname <instrum> -patch <patchNr></code> to remove all patches with a patch number \leq <i><patchNr></i> (including hotfixes) from instrumentation package <i><instrum></i>. • Use <code>-remove -instrumentname <instrum> -hotfix <hotfixName> -forpatch <patchNr></code> to remove hotfix <i><hotfixName></i> for patch <i><patchNr></i> from instrumentation package <i><instrum></i>. <p>Use <code>-remove -instrumentname <instrum> -hotfix <hotfixName> -forpatch 0</code> to remove hotfix <i><hotfixName></i> from the base package of instrumentation package <i><instrum></i>.</p>
<pre>{-upload -ul} {-input -i} <inputDir> {-instrumentname -inn} <instrum> [-label <label>] [{-description -de} <descr>] [{-patch -p} <patchNr>] [{-hotfix -hf} <hotfixName> {-forpatch -fp} {<patchNr> 0}][{-force -f}]</pre>	<p>Note: <i><authentication></i> is required.</p> <p>Uploads instrumentation data from directory <i><inputDir></i> to the database as an instrumentation package with object name <i><instrum></i>.</p> <p>An upload error occurs if a configuration object with the name <i><instrum></i> already exists in the database. In this case, you can use the option <code>-force</code> to work around the upload error and upload the package using the existing name.</p> <p>Caution: Using <code>-force</code> overwrites the existing package with the uploaded package, meaning the existing data is lost.</p> <p>When the instrumentation is uploaded to the database, a label and a description are attached to the package, which are used as the name and</p>

Option	Description
	<p>description of the package in the Operations Management user interface.</p> <ul style="list-style-type: none"> Specify option <code>-label <label></code> to name the instrumentation <code><label></code>. If <code>-label</code> omitted, <code><instrum></code> is used as label. Specify option <code>-description <descr></code> to set the text to go into the description to <code><descr></code>. If <code>-description</code> is omitted, the description is left blank. <p>Packages can be uploaded as base packages, patches, or hotfixes.</p> <ul style="list-style-type: none"> Use <code>-upload -input <inputDir> -instrumname <instrum></code> to upload a base package prepared in <code><inputDir></code> and name it <code><instrum></code>. Use <code>-upload -input <inputDir> -instrumname <instrum> -patch <patchNr> [-label <label>]</code> to upload a patch prepared in <code><inputDir></code> as patch <code><patchNr></code> for instrumentation package <code><instrum></code>. Use <code>-upload -input <inputDir> -instrumname <instrum> -hotfix <hotfixName> -forpatch <patchNr></code> to upload a hotfix prepared in <code><inputDir></code> as hotfix <code><hotfixName></code> for patch <code><patchNr></code> for instrumentation package <code><instrum></code>. Use <code>-upload -input <inputDir> -instrumname <instrum> -hotfix <hotfixName> -forpatch 0</code> to upload a hotfix for the base package of instrumentation package <code><instrum></code>.

Exit Status

Exit Status	Description	Output
0	Successful completion of the requested operation	No output.
1	Failure of the requested operation	An error message stating why the operation failed, followed by the ConfigExchange man page.

Exit Status	Description	Output
300-399	HTTP Redirection (300-399)	An error message stating the HTTP error number and description. For more information about HTTP error status values, see publicly available HTTP documentation.
400-499	HTTP Client Error (400-499)	
500-599	HTTP Internal Server Error (500-599)	

Restrictions

Some operations require authentication. The specified user must be a BSM user with permission to create policy templates. If *<authentication>* is required, *<authentication>* must be specified and valid.

If *<authentication>* is omitted when requesting an operation requiring authentication, **ConfigExchange** does not execute the requested operation, and exits with the following error:

Username may not be null. Operation requires authentication. Please enter the login name and password.

The error can be fixed by inserting an *<authentication>*.

Examples

This section shows a number of real-life examples you can use as a starting point for developing your own **ConfigExchange** commands.

- **Upload Instrumentation, Policies and Policy Groups from HPOM**

A policy was exported from OM to the directory */usr/myOMPpolicy*. Issue the following command to upload the policy:

```
ConfigExchange -username myU -password myPwd -uploadOM -input /usr/myOMPpolicy
```

- **Upload Instrumentation Packages, Patches, and Hotfixes**

- A new instrumentation package was prepared in the directory */usr/myCustomInstrum*. Issue the following command to overwrite existing instrumentation *myInstrum* with the new package:

```
ConfigExchange -username myU -password myPwd -upload -input /usr/myCustomInstrum  
-instrumname myInstrum -force
```

- A new instrumentation package was prepared in the directory */usr/myCustomInstrum*. Issue the following command to upload the new package as a patch for instrumentation *myInstrum* with patch number 3 and label the patch *myFix*:

```
ConfigExchange -username myU -password myPwd -upload -input /usr/mydir -instrumname  
myInstrum -patch 3 -label myFix
```

- A new instrumentation package was prepared in the directory /usr/myCustomInstrum. Issue the following command to upload the new package as a hotfix with name hf_CPUfix for patch number 3 of instrumentation myInstrum, and attach the description MyCP hotfix for patch 3; fix CPU issue:

```
ConfigExchange -username myU -password myPwd -upload -input /usr/myCustomInstrum  
-instrumname myInstrum -hotfix hf_CPUfix -forpatch 3 -force -description "hotfix for patch 3;  
fixes CPU issue"
```

- A new instrumentation package was prepared in the directory /usr/myCustomInstrum. Issue the following command to upload the new package as a hotfix with name hf_CPUfix for the base package of instrumentation myInstrum:

```
ConfigExchange -username myU -password myPwd -upload -input /usr/myCustomInstrum  
-instrumname myInstrum -hotfix hf_CPUfix -forpatch 0
```

- **Download an Instrumentation Package from the Database to the Local File System**

Issue the following command to download the entire package for instrumentation package myInstrum from the database, and place it in directory myDownloads:

```
ConfigExchange -merge -output myDownloads -instrumname myInstrum
```

- **Download the Contents of a Configuration Folder from the Database to the Local File System**

Issue the following command to download the configuration objects in configuration folder myInstrum from the database, and place them in directory myDownloads:

```
ConfigExchange -download -output myDownloads -startId  
7d6468fb-486d-b7cd-8bff-f6c26b34c305
```

- **Download Specific Elements of an Instrumentation Package from the Database to the Local File System**

- Issue the following command to download the base package for instrumentation package myInstrum from the database, and place it in directory myDownloads (patches and hotfixes are *not* downloaded):

```
ConfigExchange -username myU -password myPwd -download -output myDownloads  
-instrumname myInstrum
```

- Issue the following command to download patch number 1 for instrumentation package myInstrum from the database, and place it in directory myDownloads (the base package and any hotfixes for the patch are *not* downloaded):

```
ConfigExchange -username myU -password myPwd -download -output myDownloads  
-instrumname myInstrum -patch 1
```

- Issue the following command to download hotfix hf_CPUFix for patch number 1 for instrumentation package myInstrum from the database, and place it in directory myDownloads (the base package and the patch the hotfix is for are *not* downloaded):

```
ConfigExchange -username myU -password myPwd -download -output myDownloads  
-instrumname myInstrum -hotfix hf_CPUFix -forpatch 1
```

- The same command used in the previous example can be shortened using command element abbreviations, in which case it looks as follows:

```
ConfigExchange -user myU -pw myPwd -dl -o myDownloads -inn myInstrum -hf hf_CPUFix  
-fp 1
```

- **Remove Instrumentation Packages or Elements Thereof from the Database**

- Issue the following command to remove instrumentation package MyInstrum, including all associated patches and hotfixes, from the database:

```
ConfigExchange -user myU -pw myPwd -remove -instrumname myInstrum
```

- Issue the following command to roll back hotfix hf_CPUFix for patch number 1 from instrumentation package MyInstrum (the base package and the patch are *not* removed):

```
ConfigExchange -user myU -pw myPwd -remove -instrumname myInstrum -hotfix hf_  
CPUFix -forpatch 1
```

- Issue the following command to roll back patches with a patch number ≤ 1 and all their hotfixes (the base package and any patches with a patch number > 1 are *not* removed):

```
ConfigExchange -user myU -pw myPwd -remove -instrumname myInstrum -patch 1
```

- **Create a Directory Structure to be Used as a Template for Preparing an Instrumentation Package from Scratch with the Intention to Upload It**

Issue the following command to create a directory structure for instrumentation MyInstrum in the directory /usr/myCustomInstrum:

```
ConfigExchange -createinstrumdir -output /usr/myCustomInstrum
```

- **Investigate Which Patches and Hotfixes are Installed for a Certain Instrumentation Package**

Issue the following command to list all patches and hotfixes for instrumentation myInstrum:

```
ConfigExchange -username myU -password myPwd -list -instrumname myInstrum
```

Troubleshooting

General Troubleshooting

Some of the errors reported by ConfigExchange can be classified as warnings and can be ignored. The policy upload process ignores these errors and continues. The following sections describe some of these errors.

Operation failed. HTTP Status: 400 (Bad Request)

- **Problem:** An instrumentation with dirName "<name>" already exists.

The tool re-attempts uploading an instrumentation after encountering import problems. In this case the error may happen because an instrumentation with the same name, ID, or version already exists in the database, having been created during the first attempt.

Solution: Can be ignored.

- **Problem:**

Template "<name>" already exists with a different ID (<ID>) in the database.

Template version "<name>" <version> (version ID <ID>) is already in the database.

The tool attempts to import a policy template. In this case the error may happen because a policy template with the same name but with a different ID already exists in the database.

You may be attempting to upload a policy with the same version number as a policy already uploaded to the database. For example, if an HPOM policy is uploaded to Monitoring Automation, and is then modified in both Monitoring Automation and HPOM, the same policy version numbers are created with different policy content. If you then attempt to re-import the HPOM-modified policy to Monitoring Automation, ConfigExchange generates an error.

Solution: Delete the policy version in Monitoring Automation and re-import the HPOM policy. A policy should have a dedicated master. Do not modify a policy in both Monitoring Automation and HPOM to avoid version conflicts.

- **Problem:** Object [templateVersion] is read-only.

ConfigExchange attempts to re-import the same policy version. However either the policy was modified without leading to a new version on the HPOM server or instrumentation was missing during the first upload. For example, ConfigExchange imports a policy although some instrumentation categories are missing. When importing the same policy for a second time, ConfigExchange assumes that new categories were added to the policy.

Solution: Can be ignored.

Operation failed. HTTP Status: 404 (Not Found)

- **Problem:** No template with id: "<ID>" found.

A policy group contains a policy that cannot be uploaded to Monitoring Automation, for example because the policy type is not supported in Monitoring Automation.

Solution: Can be ignored.

- **Problem:** No instrumentation with id: "<ID>" found.

This may occur when importing further versions of same policy name.

Solution: Can be ignored.

ConfigWsTool Command-Line Interface

You can use the **ConfigWsTool** command-line interface (CLI) to interact with Monitoring Automation using the Monitoring Automation web service API.

The tool enables using the web service API without having to set up a REST-based communication channel. It accepts commands and flat input files, and handles the communication details, making it especially useful for development and troubleshooting of external applications using the Monitoring Automation web service.

Location

<BSM_Root_Directory>/opr/bin/ConfigWsTool

Synopsis

```
ConfigWsTool [<connection>] <authentication> {<toolInfo> | <request>} [{-verbose|-v}] [{-output|-o} <outputFile>]
```

Note the following with respect to the optional parameters:

- Specifying `-verbose` results in verbose output.
- By default, the output is directed to the console. To redirect the output to an output file, specify the `-output <outputFile>` option, where the file name *<outputFile>* may contain path information. If path information is omitted, the file is stored in the current working directory.
- All output and input files are formatted as XML.

Options

<connection>

{-server <gatewayServer> [-port <port>] [-ssl] | -url <url>}

Note: If <connection> is omitted, the command is executed on the server to which you are logged on.

Option	Description
{-port -p} <port>	Uses port <port> to connect to the target Gateway Server. Default value of <port>: 80 for HTTP connections. 443 for HTTPS connections.
-server <gatewayServer>	Sets the target Gateway Server, using <gatewayServer> as the hostname or IP Address to locate it. Default value of <gatewayServer> is the FQDN of the BSM gateway.
-ssl	When this flag is specified, the HTTPS protocol is used to connect to the target Gateway Server. If omitted, the HTTP protocol is used. This option cannot be used in conjunction with the option: url.
{-url -u} <url>	Sets the target Gateway Server, using <url> as the URL to locate it. Default value of <url> is: http://<bsm-gateway-server>:80/opr-config-server

<authentication>

-username <userName> -password <password> -customer <customerID> | -jks
<JAVAKeyStore> -jksPassword <password> | -smartcard | -winCrypto}

Option	Description
{-customer -cu} <customerID>	The identification number associated with a particular customer in an HP Software-as-a-Service environment. Default value of <customerID> is 1.
{-jks -j} <JAVAKeyStore> {-jksPassword -jp} <password>	Use the JAVA Key Store located in directory <JAVAKeyStore> for authentication, and access it using the password <password>.
{-password -pw} <password>	Uses the password <password> for user <username>, which is used to execute ConfigWSTool operations on the target Gateway Server. The default value of <password> is an empty string.
{-smartcard -sc}	Use certificate stored on smart card or security token for authentication.
{-username -user} <username>	Sets the username to be used to execute ConfigWSTool operations on the target Gateway Server to <username>.

{-winCrypto -wc}	Use Windows Certificate Store for authentication. This option can only be used on Windows systems.
------------------	---

<toolInfo>

{-help | -version}

Option	Description
{-help -h}	Display a summary of the ConfigWSTool command options.
-version	Prints version information for the ConfigWSTool tool.

<request>

{-create_assignment | -create_assignment_by_mgmt_template | -delete_assignment | -get_draft_assignment | -get_draft_assignment_for_mgmt_template | -list_assignment | -list_assignment_by_ci | -list_assignment_by_mgmt_template | -list_assignment_by_mgmt_template_version | -list_deployment_job | -list_deployment_job_by_assignment | -list_mgmt_template | -list_mgmt_template_by_citype | -list_mgmt_template_version } <arguments>

Option	Description
{-create_assignment -ca} {<CIID>{ ,} <mtVersionID> {-input -i} <inputFile>}	<p>Creates a new assignment of a specific management template version. You can specify the management template version to be assigned and the CI it is to be assigned to in one of the following ways:</p> <ul style="list-style-type: none"> • Provide a literal <mtVersionID><CIID> combination, separated by either a space or a comma. If this method is used, the parameter values used to create the assignment parameters are set to their default values. To override parameter values, use the -input option. • Specify the -input option, together with an input file name <inputFile>, where the input file is structured as a draft assignment returned by the -get_draft_assignment option for the CI and management template version combination. <p>The file name <inputFile> may contain path information. If path information is omitted, the file is assumed to be in the current working directory.</p> <p>Note: If the options for both methods are specified, the input file takes precedence.</p>

<pre>{-create_assignment_ by_mgmt_ template -camt} {<CIID>{ ,><mtID> -input -i} <inputFile>}</pre>	<p>Creates a new assignment of the latest version of a management template. You can specify the management template to be assigned and the CI it is to be assigned to in one of the following ways:</p> <ol style="list-style-type: none"> 1. Provide a literal <i><mtID></i> <i><CIID></i> combination, separated by either a space or a comma. If this method is used, the parameter values used to create the assignment parameters are set to their default values. To override parameter values, use the <i>-input</i> option. 2. Specify the <i>-input</i> option, together with a input file name <i><inputFile></i>, where the input file is structured as a draft assignment returned by the <i>-get_draft_assignment</i> option for the CI and management template combination. <p>The file name <i><inputFile></i> may contain path information. If path information is omitted, the file is assumed to be in the current working directory.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Note: If the options for both methods are specified, the input file takes precedence.</p> </div>
<pre>{-delete_ assignment -da} [<assignmentID>]</pre>	<p>Deletes the assignment with the ID <i><assignmentID></i>.</p>
<pre>{-get_draft_ assignment -gda} <CIID> <mtVersionID> {- output -o} <outputFile></pre>	<p>Returns a draft request for assigning the management template version with the version ID <i><mtVersionID></i> to the CI with ID <i><CIID></i>. The response is stored as file <i><outputFile></i>. You can modify the response and subsequently use it as an input file for a request to create a new assignment.</p>
<pre>{-get_draft_ assignment_for_ mgmt_ template -gdamt} <CIID><mtID> {- output -o} <outputFile></pre>	<p>Returns a draft request for assigning the latest version of the management template with the ID <i><mtID></i> to the CI with ID <i><CIID></i>. The response is stored as file <i><outputFile></i>. You can modify the response and subsequently use it as an input file for a request to create a new assignment.</p>
<pre>{-list_assignment -la} [<assignmentID>]</pre>	<p>Lists all assignments of all management template versions. To return a single assignment, provide the parameter <i><assignmentID></i>.</p>
<pre>{-list_assignment_by_ ci -laci} <CIID></pre>	<p>Lists all assignments for the CI with ID <i><CIID></i>.</p>

{-list_assignment_by_ mgmt_template -lamt} <mtID>	Lists all assignments of the management template with ID <mtID>.
{-list_assignment_by_ mgmt_template_ version -lamtv} <mtVersionID>	Lists all assignments of the management template version with ID <mtVersionID>.
{-list_deployment_ job -ldj} [<deploymentJobID>]	Lists all deployment jobs for all current management template assignments. To return a single deployment job, provide the parameter <deploymentJobID>.
{-list_deployment_ job_by_ assignment -ldja} <assignmentID>	Lists all deployment jobs for the assignment with ID <assignmentID>.
{-list_mgmt_ template -lmt} [<mtID>]	Lists all management templates in the database. To return a single management template, provide the parameter <mtID>.
{-list_mgmt_ template_by_ citype -lmtcit} [<CITYPE>]	Lists all management templates that can be assigned to CIs of the CI type <CITYPE>.
{-list_mgmt_ template_ version -lmtv} [<mtVersionID>]	Lists all versions of all management templates in the database. To return a single management template version, provide the parameter <mtVersionID>.

Exit Status

Exit Status	Description	Output
0	Successful completion of the requested operation	No output.
1	Failure of the requested operation	An error message stating why the operation failed, followed by the ConfigWsTool man page.

Exit Status	Description	Output
300-399	HTTP Redirection (300-399)	<p>An error message stating the HTTP error number and description.</p> <p>Note: The exit status values 300-599 correspond to standard HTTP-status values. For more information about HTTP error status values, see publicly available HTTP documentation.</p>
400-499	HTTP Client Error (400-499)	
500-599	HTTP Internal Server Error (500-599)	

Restrictions

All operations require authentication. The specified user must be a BSM user with permission to execute the requested operations. The user rights needed to execute an operation using the tool are aligned with the user rights needed to execute the same operation using the user interface.

If *<authentication>* is omitted when requesting an operation requiring authentication, **ConfigWsTool** does not execute the requested operation, and exits with the following error:

Username may not be null. Operation requires authentication. Please enter the login name and password.

The error can be fixed by inserting a valid *<authentication>*.

Examples

This section shows a number of examples you can use as a starting point for developing your own **ConfigWsTool** commands.

All examples use basic authentication with the credentials myU/myPwd, and are executed on the local host.

- **List All Management Templates That Can Be Assigned to a Specific CI Type**

Issue the following command to list all CI Types that can be assigned to a CI of the type myCIType:

```
-lmtcit myCIType
```

The management template IDs to be used for subsequent lists or assignments can be parsed from the response.

- **List All Management Template Versions Currently Assigned to a Specific CI**

Issue the following commands to list all Management Template Versions that are currently assigned to a CI with the ID 5e2cef17df64ec4b35a0459e7ba33c8c:

- a. `-laci 5e2cef17df64ec4b35a0459e7ba33c8c`
- b. The response lists all current assignments for the CI. Parse the response, and for each assignment ID in the list, denoted as `assgldK`, issue the following command:

```
-la assgldK
```

The management template version IDs to be used for subsequent lists or assignments can be parsed from the response.

- **Create an Assignment Using an Explicitly Specified Combination of CI and Management Template**

Issue the following command to assign the management template version with version ID 430738c-796e-cfbd-9653-ee9fab02388a to the CI with the ID 5e2cef17df64ec4b35a0459e7ba33c8c:

```
configwstool -u myU -pw myPwd -ca 5e2cef17df64ec4b35a0459e7ba33c8c c430738c-796e-cfbd-9653-ee9fab02388a
```

- **Create an Assignment Using an Input File**

Issue the following command to create an assignment using the XML input file `\tmp\myAssg.xml`:

```
configwstool -u myU -pw myPwd -ca -i \tmp\myAssg.xml
```

- **Create an Assignment From a Draft Assignment**

Issue the following command to retrieve a draft assignment of the management template version with version ID 430738c-796e-cfbd-9653-ee9fab02388a to the CI with the ID 5e2cef17df64ec4b35a0459e7ba33c8c:

```
configwstool -u myU -pw myPwd -gda 5e2cef17df64ec4b35a0459e7ba33c8c c430738c-796e-cfbd-9653-ee9fab02388a -o \tmp\myDraft.xml
```

The draft is stored as `\tmp\myDraft.xml`. Modify the file as required and save it, for example as file `\tmp\myModifiedDraft.xml`. Then, create a new assignment using the modified file as input file by issuing the following command:

```
configwstool -u myU -pw myPwd -ca -i \tmp\myModifiedDraft.xml
```

ConfigExchangeSIS Command-Line Interface

The ConfigExchangeSIS command-line interface enables you to import templates from a SiteScope server.

Location

<BSM_Root_Directory>/opr/bin/ConfigExchangeSIS

Synopsis

```
ConfigExchangeSIS
  -help |
  -sis_group_container <directory>
  -sis_user <username>
  -sis_passwd <password>
  -bsm_user <username>
  -bsm_passwd <password>
  [ -sis_hostname <hostname> ]
  [ -sis_port <port> ]
  [ -sis_ssl ]
  [ -bsm_hostname <hostname> ]
  [ -bsm_port <port> ]
  [ -bsm_root_dir <dir> ]
  [ -bsm_ssl ]
  [ -verbose true ]
```

Options

Option	Description
-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_user	The user name of a SiteScope user with permission to read the templates.
-sis_passwd	The password of the SiteScope user.
-bsm_user	The user name of a BSM user with permission to create policy templates.
-bsm_passwd	The password of the BSM user.
-sis_hostname	<i>Optional.</i> 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_port	<i>Optional.</i> The port of the SiteScope server (default: 8080).

Option	Description
-sis_ssl	<i>Optional.</i> Opens an HTTPS connection to the SiteScope server (default: HTTP). To connect to a SiteScope server that requires SSL, Monitoring Automation must trust the root certificate that was used to sign the SiteScope certificate. For details, see "How to Connect to a SiteScope Server That Requires SSL" on page 370 .
-bsm_hostname	<i>Optional.</i> 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_port	<i>Optional.</i> The port of the BSM server (default: 80).
-bsm_root_dir	<i>Optional.</i> The base path of the BSM server (default c:\HPBSM\).
-bsm_ssl	<i>Optional.</i> Opens an HTTPS connection to the BSM server (default: HTTP).
-verbose	<i>Optional.</i> Displays verbose information (default: false).

Exit Status

This command exits with value 0 after successful operation. In case of errors, 1 is returned and a descriptive text is printed to standard out.

Restrictions

The specified SiteScope user must be a SiteScope user with permission to read the templates.

The specified BSM user must be a BSM user with permission to create policy templates.

Examples

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
```

Troubleshooting

General Troubleshooting

Use the -verbose option with the -uploadOM operation to ensure you are provided with all the details.

The log files resulting from using -verbose are placed in the following folder:

<BSM_Root_Directory>/Temp/tmp_sis/templsdwnld/ <processId of ConfigExchangeSIS command>.

Import Problems Caused By Parameter Definitions

Problem: The SiteScope parameter definitions in the following file may contain errors:

<BSM_Root_Directory>/Temp/tmp_sis/dwnld/ <processId of ConfigExchangeSIS command>/ <SISgroupContainer>/ <templateName>.xml

Solution: Make sure the parameter definitions are correct. See also ["Prerequisite for Importing SiteScope Templates" on page 366](#).

HP Operations Manager i and HP Operations Agent Command-Line Interfaces

HP Operations Manager i (OMi) provides a number of command-line interfaces to manage processes, certificates, and the communication infrastructure in general (for example, ovc, ovconfchg, and ovcert). In addition to these interfaces, HP Operations Agent includes tools to manage specific agent types (for example, opcmon to send data to the monitor agent or opcmsg to feed the message interface).

For more information on these tools, see the HP Operations Agent Reference Guide. Alternatively, to get more information about a command, type the name of the command followed by the -help parameter (for example, ovc -help).

The following command-line interfaces are particularly useful in Monitoring Automation environments:

ovconfpar

The ovconfpar command-line interface sets and returns configuration parameters remotely. On the BSM server running Monitoring Automation, run the tool with the -host <hostname> parameter to connect to a system monitored by HP Operations Agent. The -change and -get parameters enable you to change and retrieve configuration values.

For example, to change the primary manager of an agent, run the following command on the secondary or backup server running Monitoring Automation:

ovconfpar -change -host <FQDN of the node> -src-ovrg server -ns eaagt -set OPC_PRIMARY_MGR <FQDN of secondary or backup BSM Operations Management server>

For more information on ovconfpar, run ovconfpar -help.

ovpolicy

The ovpolicy command-line interface installs, manages, and removes both local and remote policies. The Monitoring Automation server does not have any policies deployed locally but you can use the command to manage policies on remote HP Operations Agent systems.

For example, you can use it on the BSM server running Monitoring Automation to connect to an agent system and list the policies that are installed there:

```
ovpolicy -list -host <FQDN of the node>
```

For more information on ovpolicy, run ovpolicy -help.

ovrc

The ovrc command-line interface remotely controls the starting and stopping, event notification, and status reporting of all components registered with the HP Operations Control service on a node.

For example, on the BSM server running Monitoring Automation, run the tool with the -host <hostname> -status parameter to connect to a system monitored by HP Operations Agent and to retrieve status information from that system:

```
ovrc -host <FQDN of the node> -status
```

For more information on ovrc, run ovrc -help.

Chapter 11: 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 HP Operations Agent or HP SiteScope. You can access the *Monitored Nodes* screen at **Admin > Operations Management > Setup > Monitored Nodes**.

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 in *Learn More > Node Filters*. You can create custom node filters if the predefined node filters do not suit your needs (see task *How to Create Custom Node Filters*). You can also group specific nodes together into node collections; these also function as filters by narrowing down the list to members of the collection (see task *How to Create Node Collections*).

- **List of monitored nodes** (middle pane)

The list of monitored nodes, filtered according to the filter selected in the *Node Views* browser. The name of the active filter, followed by the filter category is shown in the list's title bar.

Note: You can view all nodes by selecting **Predefined Node Filters > All Nodes**.


- **Node Details** (right pane)

Details for the node selected in the list of monitored nodes.


Learn More

Node Filters


The following filtering methods can be applied:

- To apply a predefined node filter, click  to expand **Predefined Node Filters** and select the desired filter.
- You can create a filter yourself if the nodes you want to single out have a common attribute that can be used as a selection criterion. The following attributes can be used as criteria for custom node filters:
 - Primary DNS Name (or a substring thereof)
 - IP Address (or a substring thereof)
 - Routing Domain (or a substring thereof)

- Monitored By (or a substring thereof)
- Operating System (or a substring thereof)
- View the node is contained in.

To apply a custom node filter, click  to expand **Custom Node Filters** and select the desired filter. For detailed information on creating custom node filters see *How to Create Custom Node Filters* in section *Tasks*.


- Node collections are sets of manually selected nodes. The nodes in a node collection do not need to have anything in common. To group nodes together in a node collection, create the collection, and then select a number of nodes and add them to the collection.

To list all nodes in a node collection, click  to expand **Node Collections** and select the desired collection. For detailed information on creating node collections see *How to Create Node Collections* in section *Tasks*.


Note: Node collections are modeled in the RTSM as CIs of type CI Collection with attribute monitored_by set to OM.

Tasks

How to Create Custom Node Filters


1. Select the root folder Custom Node Filters or one of its subfolders in the *Node Views* browser.
2. Click  **New Custom Node Filter** in the toolbar of the Node Views browser. The *Create New Custom Node Filter* dialog 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 to be matched and enter an appropriate value for each selected criterion.
5. Click **OK**. The dialog closes and the new filter is added to the list of custom filters in the *Node Views* browser.

How to Create a Node Collection



1. Select the root folder Node Collection or one of its subfolders in the *Node Views* browser.
2. Click  **New Node Collection** in the toolbar of the *Node Views* browser. The *Create New Node Collections* dialog opens.

3. Enter the **Display Name** for the new node collection and a **Description**, if required.
4. Select the desired **Parent Collection**, or Root Collection if the collection shouldn't have a parent collection.
5. Click **OK**. The dialog closes and the new node collection is added to the Node Collections category.

How to Change an Existing Node Collection

1. Select the node collection to be changed in the *Node Views* browser.
2. Click  **New Node Collection** in the toolbar of the *Node Views* browser. The *Edit Node Collections* dialog opens.
3. If required, you can change the node's **Display Name** and its **Description**.
4. You can move the collection in the tree structure by selecting a different **Parent Collection**, or remove the node's parent collection by selecting Root Collection as the Parent Collection.
5. Click **OK** to apply the changes and close the dialog.

How to Create a New Monitored Node



1. Make sure a node filter (from any of the filter categories) is selected in the **Node Views** browser.
2. Click  **New Node** in the toolbar of the list of monitored nodes 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 Nodes* dialog opens.
3. Enter the new node's **Primary DNS Name** and click another control, for example the list of IP addresses. The system uses DNS lookup to resolve all IP addresses associated with the specified DNS name, and enters them in the list of IP addresses.
4. If any IP addresses associated with the node are not shown in the list, you can enter them manually using  **New Item**.
5. *Optional*. Enter the **Operating System**, **Processor Architecture** and a **Description** for the node.
6. Click **OK**. The dialog is closed and the new node is created and added to the list of monitored nodes.

Tip: Always specify the operating system when creating a node manually. If the operating system is not specified, you could face the following issues:


- The assignment of templates with specific operating system fails and generates an error.
- Management templates and aspects for which an operating system is defined are not listed as items that can be assigned to the node.

How to Change an Existing Monitored Node


To change a node's properties:

1. Make sure a node filter returning the node to be edited is selected in the **Node Views** browser.
2. Select the node to be edited in the list of monitored nodes and click  **Edit Item** in the toolbar of the list of monitored nodes. The *Edit Monitored Nodes* dialog opens.
3. You can use the dialog to change the node's properties, for example:
 - You can change the node's **DNS Name** or its **Description** by editing the text in the corresponding text boxes.
 - You can change the node's **Operating System** or **Processor Architecture** by selecting a different value from the corresponding list.
 - You can change or delete **IP Addresses** in the corresponding list. If any IP addresses associated with the node are not shown in the list, you can enter them manually using  **New Item**.
4. Click **OK**. The dialog is closed and the new node is created and added to the list of monitored nodes.

To move a node to a different node collection:

1. Make sure a node filter returning the node to be edited is selected in the **Node Views** browser.
2. Select the node to be edited in the list of monitored nodes and click  **Add to Node Collection** in the toolbar of the list of monitored nodes. The *Add Node to a Node Collection* dialog opens.
3. Use the dialog to add the node to set or change the **Parent Collection**.


How to Add a Node to a Node Collection

1. Select one or more nodes in the list of monitored nodes and click the  button. The *Add Node to a Node Collection* dialog opens.
2. Select the node collection to which you want to add the selected nodes as the **Parent Collection**.
3. Click **OK**. The dialog closes and the selected nodes are added to the node collection, as can


be verified by expanding **Node Collections** and, if appropriate, the node's parent collection(s) in the *Node Views* browser.

How to Delete a Node from a Node Collection




To remove a node from a node collection:

1. Expand **Node Collections** and select the node collection from which you want to remove a node. The nodes in the node collection are shown in the list of monitored nodes (middle pane).
2. Select one or more nodes in the list of monitored nodes and click  **Remove from Node Collection**. The selected nodes are removed from the selected node collection.

How to Display a Report for a Node

Select a node in the list of monitored nodes (middle pane) and click  **Generate Node Report** in the pane's toolbar.

The preconfigured *Node Configuration Report* 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  **Expand** and  **Collapse** to expand or collapse the assigned CI information.  **Show All Values/Show Customized Values Only** toggles between displaying all values or only the customized values.

UI Reference





Create New/Edit Custom Node Filter Dialog

UI Element	Description
ID	The system-assigned ID of the custom node filter.
Display Name	The name by which the custom node filter is shown in the user interface.
Description	A description for the custom node filter.

UI Element	Description
Filter Criteria	<p>The criteria for filtering the nodes managed by the system. To use a criterion:</p> <ol style="list-style-type: none">1. Check the checkbox in front of the criterion. The input field is activated.2. Enter or select the value to be matched in the input field. <p>If the value to be matched is a string, the following considerations apply:</p> <ul style="list-style-type: none">• The matching process is case-sensitive.• Using an asterisk (*) as a wildcard causes the specified value to be interpreted as a substring. Specifying 192.* in the IP Address field, for example, will return all nodes with an IP address starting with 192. if the filter is activated.
OK	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard/dialog without creating/updating the item.
Help	Opens the relevant help in a new browser window.

Create New/Edit Monitored Node Dialog

UI Element	Description
ID	The system-assigned ID of the node.
Node Type	The CI Type of the node.
Primary DNS Name	Fully qualified DNS hostname of the node, which also determines the name of the node as shown in the nodes list as well as topology views.

UI Element	Description
IP Addresses	<p>All IP addresses of the node. After specifying the DNS hostname of a node, the system will prefill the list automatically with all IP addresses it finds for the hostname using DNS lookup. You can specify any additionally required IP addresses manually.</p> <p>The toolbar provides the following controls:</p> <p> New Item: Opens the <i>Create New IP Address</i> dialog used to specify a new IP address and add it to the list.</p> <p> Edit Item Opens the <i>Edit IP Address</i> dialog used to edit an existing IP address.</p> <p> Delete Item: Removes the selected IP addresses from the list.</p> <p>The list has the following columns:</p> <p>IP Address The IP address of the node.</p> <p>DHCP  if the IP addresses was assigned by a DHCP server, or empty if it was not.</p> <p>Routing Domain The routing domain for the IP address, or \$(DefaultDomain) if the default domain is used.</p>
Operating System	The node's operating system.
Processor Architecture	The node's processor architecture.
Description	A description for the node.
OK	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard/dialog without creating/updating the item.
Help	Opens the relevant help in a new browser window.

Create New/Edit Node Collection Dialog



UI Element	Description
Display Name	The name by which the node collection is shown in the user interface.
Description	A description for the node collection.

UI Element	Description
Parent Collection	<p>The node collection to contain the new node collection.</p> <p>You are not limited to having the collection selected in the Node Views browser as parent collection:</p> <ul style="list-style-type: none"> You can select any existing node collection by expanding the tree structure and selecting the desired parent collection. If you want to create a node collection without parent, select Node Collections. The new node collection is placed on the highest level in the Node Collections category.
OK	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard/dialog without creating/updating the item.
Help	Opens the relevant help in a new browser window.





Create New/Edit IP Address Dialog

UI Element	Description
IP Address	The IP address to be added to the list of IP addresses.
DHCP	If checked, the IP address is marked as having been assigned to the node by a DHCP server.
Routing Domain	By default, the system enters \$(DefaultDomain). If the node's routing domain is different from the BSM server's routing domain, replace the default with the node's routing domain.
OK	Applies the values in all screens and closes the dialog.
Cancel	Closes the wizard/dialog without creating/updating the item.
Help	Opens the relevant help in a new browser window.







Details Pane





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.

Node Views Browser

UI Element	Description
	Refresh: Reloads the content of the <i>Node Views</i> browser.
	New Node Collection: <ul style="list-style-type: none"> If the Custom Node Filter root folder or an item in it is selected, this button opens the <i>Create New Custom Node Filter</i> dialog to create a new custom node filter. If the Node Collection root folder or an item in it is selected, this button opens the <i>Create New Node Collection</i> dialog to create a new node collection.
	Edit Item: <ul style="list-style-type: none"> If an item in the Custom Node Filters root folder is selected, this button opens the <i>Edit Custom Node Filter</i> dialog to edit the selected custom node filter. If an item in the Node Collections root folder is selected, this button opens the <i>Edit Node Collections</i> dialog to edit the selected node collection.
	Delete Item: Deletes the selected filter or collection.

Nodes List

UI Element	Description
	Refresh: Reloads the nodes list.
	New Node: Opens the <i>Create New Monitored Node</i> dialog to create a new node. Types of commonly found nodes are available from the selections in the drop-down menu, for example, Computer > Unix , or Net Device > Router . If no suitable predefined node type is available, select Generic Node .
	Edit Item: Opens the <i>Edit Monitored Nodes</i> dialog to edit the selected node.
	Delete Item: Opens a confirmation dialog asking you whether you are sure you want to delete the selected object. Click Yes to delete the selected nodes, or No to cancel deletion.
	Add to Node Collection: Opens the <i>Add Node to Node Collection</i> dialog to add the selected nodes to a node collection.
	Remove from Node Collection: Deletes the selected nodes from the active node collection.

UI Element	Description
	<p>Open Node Report: Opens the predefined report for the selected node.</p> <p>You can use  Expand and  Collapse to expand or collapse the aspects and templates information.  Show 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>
Nodes List	To sort the list by the values in a particular column, click the column header. At the right side of the sort column the ascending ▼ or descending ▲ sort order indicator is shown.
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	Indicates the type of node, for example, Windows 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).

Troubleshooting

Troubleshooting Node Configuration Reports

If Operations Management is not be able to generate a report for one or more selected nodes, the following error messages may appear in the report. To troubleshoot the problem, attempt one of the possible solutions below the error message.

Hostname of node is not resolvable

Possible Causes:

- Incorrect DNS configuration.
- Incorrect or incompatible node IP address.

Possible Solutions:

- Make sure the node name corresponds to the Primary DNS Name of the corresponding node CI.
- Use the nslookup command-line tool to check the IP address of the node. If nslookup fails, contact our DNS administrator.

Connection to node could not be established

Possible Causes:

- A required agent process is not running.
- A certificate is missing.
- The firewall configuration is incorrect.

Possible solutions:

Run the following command on the BSM server:

```
bbcutil -ping <node hostname>
```

The command should return the following message:

```
status=eServiceOK.
```

If the command returns status eServiceOK, the problem no longer exists, and you can attempt to run the report again.

If the command returns a status other than eServiceOK, take one of the following actions to resolve the problem:

- status=eHostUnavailable: The node is not running or the node name cannot be resolved. Start the node, make sure it can access the network, and make sure the network is not experiencing problems.
- status=eCBUnavailable: A required agent processes is not running on the node. Access the operating system on the node and make sure the agent is running by the following command:

```
ovc
```

- If the command is not found, the agent may not be installed.
- If ovc returns "ovcd is not yet started" or if it shows that some processes have stopped, run the following command to call to restart all required agent processes:

```
ovc -start
```

- status=eServiceError: Required certificates are missing. Check the certificates on the node and make sure they are installed and correct. For more information on the required certificates, see the agent documentation.

If all actions fail, make sure there is no firewall blocking communication between the BSM server and the node.

Not authorized to list installed policies on node

Possible Causes:

- Incorrect server hostname or server core ID.
- Internal error accessing policies.

Possible Solutions:

Make sure the node is configured with the correct server and the correct server core ID by running the following command on the node:

```
ovconfget sec.core.auth
```

The command output will be similar to the following:

```
MANAGER=<server hostname>  
MANAGER_ID=<server core ID>
```

Inspect the value of MANAGER:

1. If MANAGER is different from the BSM server hostname, the node is probably managed by an HPOM management server. In this case, use one of the following methods to deploy monitoring configurations to the node:

- Change the server managing the node to the BSM server.
- Create a Flexible Management policy template that contains the BSM server as secondary manager.
- If available, use an installed Flexible Management policy template. To find out if a Flexible Management policy template is installed on the system:

- i. Run the following command on the node:

```
ovpolicy -l -poltype mgrconf -level 2
```

- ii. Open the following file:

```
<OvDataDir>/datafiles/policies/mgrconf/<policy id>_data
```

Find the section defining the secondary managers, which looks like the following example:

```
SECONDARYMANAGER  
NODE IP <server IP address> " <server hostname>" ID " <server core ID>"
```

This section must contain a line where the values *<server IP address>*, *<server hostname>* and *<server core ID>* are configured with values corresponding to the BSM server.

2. If MANAGER is set to the BSM server hostname, run the command `ovcoreid -ovrg server` on

the BSM server and compare the output with the value of `MANAGER_ID`. If the values don't match, change the `MANAGER_ID` on the node by running the following command on the node:

```
ovconfchg -ns sec.core.auth -set MANAGER_ID <server core ID>
```

using the BSM server core ID as the value for parameter `<server core ID>`.

If these settings are all correct, investigate the installed policies using the BSM content manager and make sure all required policies are installed and can be access without generating internal errors..

We appreciate your feedback!

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Monitoring Automation for HP Operations Manager i Administrator Guide (Business Service Management 9.23)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to ovdoc-asm@hp.com.