(x) matters®

The relevance engine company.

xMatters (IT) engine for HP Operations Manager for Windows

AlarmPoint Systems, Inc. is now xMatters, inc. This change extends to how we name our products: the AlarmPoint Integration Agent is now the xMatters integration agent; AlarmPoint Enterprise is now xMatters enterprise; and so on. You can learn more about why we changed our name at www.xmatters.com. During the ongoing transition to the new naming conventions, legacy corporate and product names will still appear in some parts of our products, such as directory paths, logs, and messages. This document reflects the new names whenever possible, while respecting the need for clarity when referring to older products, legacy issues, existing knowledge base articles, etc.

Monday, June 25, 2012

Contacting xMatters

You can visit the xMatters Web site at: http:///www.xmatters.com

From this site, you can obtain information about the company, products, support, and other helpful tips. You can also visit the Customer Support Site from the main web page. In this protected area, you will find current product releases, patches, release notes, a product knowledge base, trouble ticket submission areas and other tools provided by xMatters, inc.

xMatters, inc.
Corporate Headquarters
4457 Willow Road, Suite 220
Pleasanton, CA 94588

Sales and Technical Support:

Telephone: 925-226-0300
Facsimile: 925-226-0310

support@xmatters.com
sales@xmatters.com
Customer Support Site: http://community.xMatters.com

This integration was designed and tested on an unmodified version of HP Operations Manager for Windows software, and this document describes how to configure xMatters to integrate with the default installation. If you have customized or altered your instance of HPOM for Windows, this integration may need to be modified for your deployment. Please note that these integration changes are not part of the services offered by xMatters Technical Support, but can be performed through xMatters's Professional Services department. For more information, contact your xMatters Sales representative.

Table of Contents

Chapter 1: Introduction

Welcome to xMatters (IT) for HP Operations Manager for Windows. This document describes how to install and configure the xMatters (IT) for HP Operations Manager for Windows software integration. The intended audience for this document is experienced consultants, system administrators and other technical readers.

1.1 Summary

xMatters is an interactive alerting application, designed to capture and enrich important events, to route those events to the right person on any communication device, and to give that person the ability to solve, escalate, or enlist others to resolve the events remotely.

xMatters allows you to take critical business information and contact the right people via voice phone, SMS, two-way pagers, instant message, and email.

Through integration modules, xMatters can become the voice and interface of an automation engine or intelligent application (the Management System, such as HP Operations Manager for Windows software). When HPOM for Windows detects something that requires attention, xMatters places phone calls, sends pages, messages, or emails to the appropriate personnel, vendors or customers.

xMatters is also persistent, escalating through multiple devices and personnel until someone accepts responsibility or resolves the problem. Once contacted, xMatters gives the notified person instant two-way communication with HP Operations Manager for Windows software. Responses are executed immediately on HPOM for Windows, enabling remote resolution of the event.

This integration supports event notifications (from HPOM for Windows to xMatters) through the use of web service calls via the xMatters integration agent. It also supports inbound actions (from xMatters to HPOM for Windows) to update events remotely.

You will need to modify this configuration to suit your particular business requirements and adjust it to suit your expected loads. For example, the default integration features automatic status annotations to the original event; in a high-volume production system, this can significantly affect performance. Consider your expected volume of injected events and your server capacity when designing your own integration with xMatters.

1.1.1 Benefits

With the xMatters integration, the appropriate technician can be notified directly via voice, email, pager, BlackBerry, or other device. Information about the failure will be presented to the event resolver and decisions can be made in real-time.

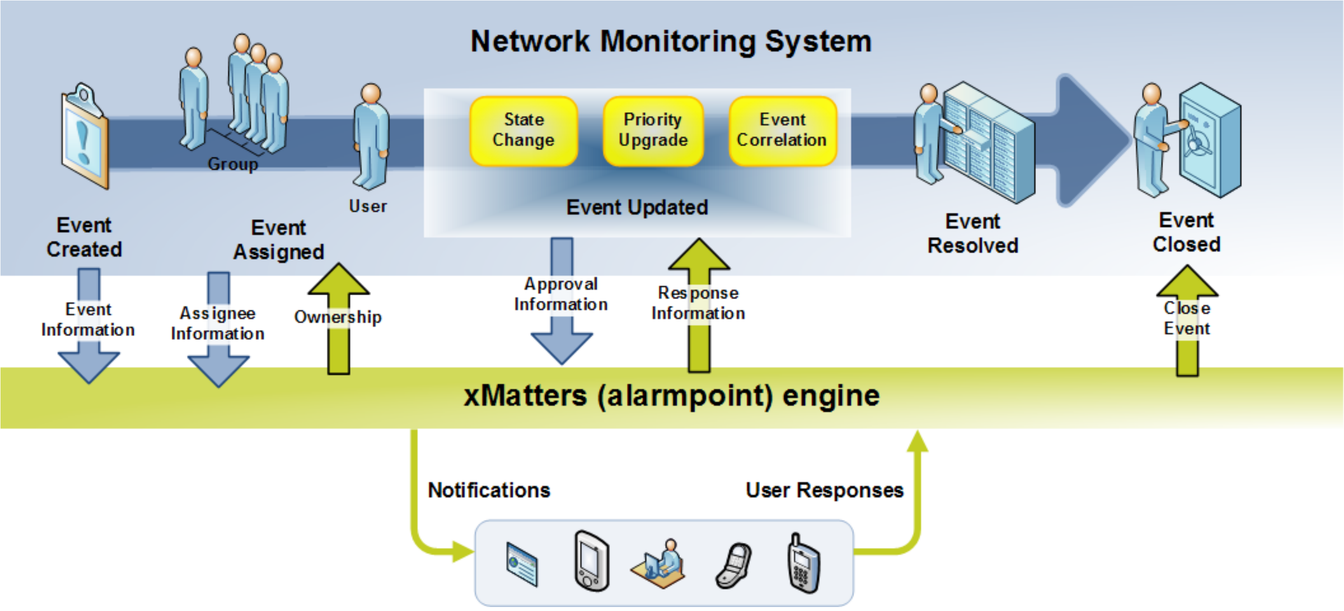
Once a response is selected on the recipient’s remote device, xMatters will update the HPOM for Windows event in real-time. The benefit is that this process is immediate – significantly faster than the time required for staff to notice the failures or malfunctions, determine who is on call, and manually notify the right person. In addition, the ability to take simple actions on the event from any device gives the event resolver a quick way to deal with many issues and communicate to other team members the current state of the event.

During the process, every notification, response, and action is logged in xMatters. In addition, xMatters automatically annotates the original event with status information.

The xMatters product features a self-service web user interface to allow accurate assignment of responsible personnel for each job. xMatters also includes a Subscription panel that allows both managed and self-subscription to HPOM for Windows events.

1.1.2 Information Workflow

The following diagram provides an example of a standard workflow in a network monitoring system, and how information from the management system can be passed into xMatters relevance engine:

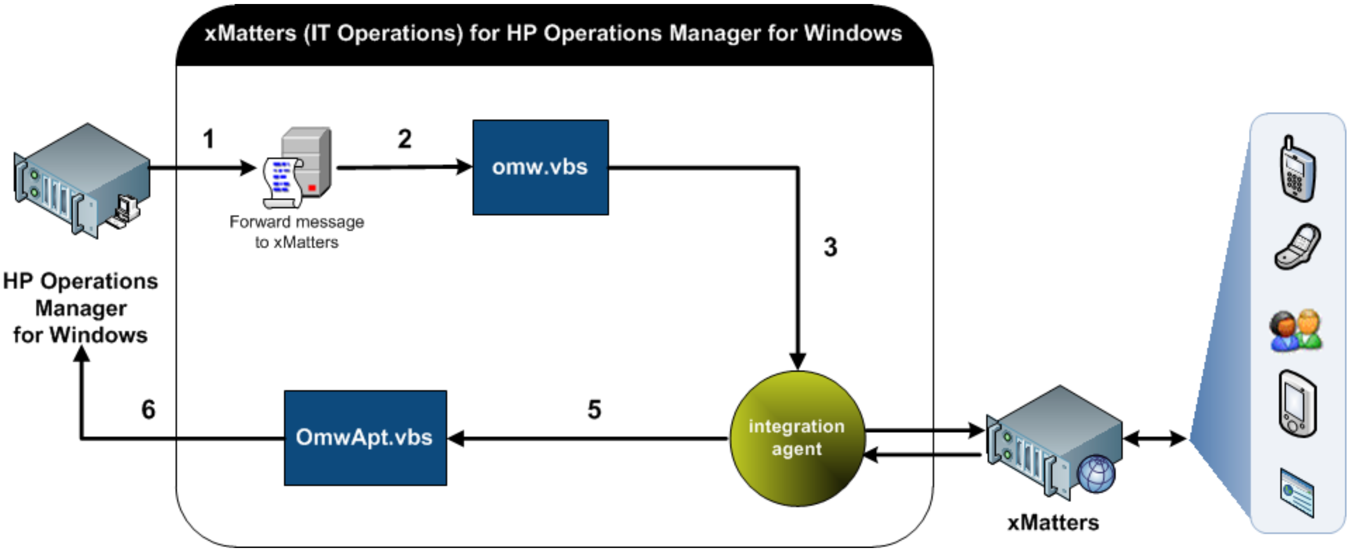


1.1.3 Integration Architecture

The software components in this integration include:

- xMatters relevance engine
- HP Operations Manager for Windows software
- xMatters integration agent

The following diagram illustrates the software processes used by this integration:


xMatters (IT Operations) for HP Operations Manager for Windows
HP Operations Manager for Windows
1
Forward message to xMatters
2
omw.vbs
3
integration agent
5
OmwApt.vbs
6
xMatters

The number for the following steps correspond to the numbers in the diagram:

1. When an event occurs on a system monitored by HPOM for Windows, it creates a message that triggers the "Forward message to xMatters" policy.
2. If the policy's conditions are true (the default setting is for any message of "Critical" severity), the message details are sent to omw.vbs.
3. The enriched details are then sent to the integration agent using an xMatters AddEvent via HTTP POST.
4. The integration agent sends the event to xMatters, which in turn notifies the Group defined in the originating message's Message Group field.
5. The notification response returns from xMatters to the integration agent, which sends an HPOM for Windows request to OmwApt.vbs via Response Action Scripting.
6. OmwApt.vbs sends a remote WMI action to HPOM for Windows to update the event.

1.2 System Requirements

The following products must be installed and operating correctly prior to integration:

- xMatters relevance engine 4.1 (patch 012 or later) or 5.x.
  - Note that to install xMatters 5.0 on Windows, patch 001 (or later) is required.
- xMatters integration agent 4.1 (patch 005 or later) or 5.x
  - Note that the integration agent MUST be installed on a Microsoft Windows machine.
- xMatters Developer IDE
- HP Operations Manager for Windows software 9

Note: *The integration agent must be installed on a different Windows computer than the one on which HPOM for Windows is installed, because an API call is required for the integration to accurately track user activity in the system. The call cannot be made from the same local system as HPOM for Windows due to security limitations in the API, so the integration agent uses a remote WMI call which allows xMatters to associate the correct user with the activity.*

1.2.1 Operating Systems

The following operating systems are supported by this integration:

- Microsoft Windows 2003 (validated)
- Microsoft Windows 2008 64-bit (validated)

1.3 Conventions and Terminology

This section describes how styles are used in the document, and provides a list of definitions.

1.3.1 Conventions

Some instructions appear in the following format: **MENU** > **OPTION**; for example, **File** > **Open** means click the **File** menu, and then click the **Open** menu option.

Words in **bold** typically reference text that appears on the screen. Words in `monospace` font represent the following:

- text that must be typed into the computer
- directory and file names
- code samples

Directory paths

Except where explicitly stated, the directory paths in this document are listed in Windows format. Unix users must substitute the given paths with the Unix equivalents.

The xMatters installation folder is referred to throughout the documentation as `<xMHOME>`.

- On Windows systems, the default for the 4.1 version of xMatters is `C:\Program Files\AlarmPointSystems\AlarmPoint`;for the 5.0 version, the default is `C:\Program Files\xMatters\`
- On Unix systems, the default for the 4.1 version of xMatters is `/opt/alarmpointsystems/alarmpoint`; for the 5.0 version, the default is `/opt/xmatters/`

The xMatters integration agent installation folder is referred to throughout the documentation as `<IAHOME>`.

- On Windows systems, the default is `C:\Program Files\AlarmPointSystems\IntegrationAgent` for the 4.1 version, and `C:\Program Files\xmatters\integrationagent` for the 5.0 version.
- On Unix systems, the default is `/opt/alarmpointsystems/integrationagent` for the 4.1 version, and `/opt/xmatters/integrationagent` for the 5.0 version.

The location to which you install the integration components on the HPOM for Windows server is referred to throughout the documentation as `<xMOMW>`.

- On a default HPOM for Windows installation, this is `C:\Program Files\HP\HP BTO Software\install\`.

1.3.2 Terminology

The following terms are used through the xMatters documentation.

Documentation terminology

Term	Meaning
Event	An *event* refers to any situation or item of interest detected by the management system, and which requires attention. Event is also used to refer to the incident or situation as it progresses through the xMatters system, from injection to notification to resolution. Each event must generate at least one alert or notification. Event can also be a generic term used to refer to an incident, change request, message, or other specific item within the management system. Whenever possible, these situations are referred to using the management system's preferred terminology, but can also collectively be called events.
Management system	A *management system* is any sort of IT service management software, and with which xMatters can combine; i.e., a synonym for HPOM for Windows.
Device	The medium through which a recipient is contacted by xMatters is referred to as a *Device*; i.e., email, pager, phone, BlackBerry, etc.
User	In xMatters, people who can receive notifications are called *Users*. Each person in the xMatters system is defined by a set of User details, including ID number, user name, login password, and so on.
Group	*Groups* are used to collect and organize Users and Devices into notification schedules. For a complete explanation of Groups in xMatters, see the *xMatters engine user guide*.

Chapter 2: Installation and Configuration

This chapter provides information about installing the xMatters (IT) for HP Operations Manager for Windows integration. This chapter also contains complete instructions on how to configure xMatters, HPOM for Windows, and the integration components.

2.1 Installing the integration

The instructions in this chapter do not include information on how to install xMatters relevance engine, the xMatters integration agent, or HP Operations Manager for Windows software. These components must be installed according to their related documentation, and operating properly before you can proceed with the integration.

Note: *For more information about installing xMatters relevance engine and other xMatters products, refer to the xMatters web site at http:///www.xmatters.com.*

2.1.1 Integration components

The following table describes some of the notable components in the integration archive file:

Integration components

Component Name	Description
hpomw.xml	Contains the parameter mapping for messages injected for the hpomw Event Domain, and the Response Action Script which updates the event according to the response message from xMatters. Primary configuration file for the integration: • Specifies web services communication settings between xMatters and HPOM for Windows. • Identifies which event details will be forwarded from HPOM for Windows for xMatters to use when creating notification content.
omw.vbs	Enriches the data coming from the HPOM for Windows policy to include the primary node and node groups, along with a textual representation for severity and properly encoded XML characters. Also responsible for configuring the logging level of `xM-OMW-Inject.log`, which records when events are sent to xMatters from HPOM for Windows. Note that this script handles event injection only, and identifies the message by its GUID; all other enrichment should be performed by the Input Action Scripting to limit the scope of this script.
omw-forwarded.vbs	Contains logic to identify events that have been forwarded to xMatters for notification so they can be deleted from xMatters when they are Acknowledged in the HPOM for Windows console. Also responsible for configuring the logging level of `xM-OMW-Forwarded.log`, which records when "Del" events are sent from HPOM for Windows to terminate xMatters events. This script is called from a WMI policy that is triggered when events, as identified by their Message GUIDs, have been acknowledged.
OmwApt.vbs	Handles the responses generated by Users' Devices in xMatters; andlso configures the logging level of `xM-OMW-Responses.log`, which records User responses and message delivery annotations from xMatters to HPOM for Windows.

2.1.2 Installing the integration service and updating the integration agent

To configure the integration agent for the HPOM for Windows integration, you must copy the integration components into the integration agent; this process is similar to patching the application, where instead of copying files and folders one by one, you copy the contents of a single folder directly into the integration agent folder (`<IAHOME>`). The folder structure is identical to the existing integration agent installation, so copying the folder's contents automatically installs the required files to their appropriate locations. Copying these files will not overwrite any existing integrations.

Note: *The integration agent must be installed on a different Windows computer than the one on which HPOM for Windows is installed, because an API call is required for the integration to accurately track user activity in the system. The call cannot be made from the same local system as HPOM for Windows due to security limitations in the API, so the integration agent uses a remote WMI call which allows xMatters to associate the correct user with the activity.*

If you have more than one integration agent providing the "hpomw" service, repeat the following steps for each one. If you are not certain of the settings required in this section, consult your HPOM for Windows administrator.

Note: *If you have already installed an existing integration, ensure that you backup the* `deduplicator-filter.xml` *file (if one exists) in the* `<IAHOME>\conf` *folder before you install this integration.*

To install the integration service:

1. Copy all of the contents, including subfolders, of the `xM_HP_OM_Windows_3_0_0\components\integration-agent\` folder from the extracted integration archive to the `<IAHOME>` folder.
2. If you backed up an existing deduplicator file as indicated in the note above, merge the contents of your back up with the newly installed `<IAHOME>\conf\deduplicator-filter.xml` file: open both files in a text editor, and then copy the <filter> node from the backup file into the new deduplicator file after the last </filter> node. Save and close the file.
3. Open the `<IAHOME>\conf\IACongif.xml` file and add the following line to the “service-configs” section:

```
<path>hpomw/hpomw.xml</path>
```

4. Open the `<IAHOME>\integrationservices\hpomw\OmwApt.vbs` file and modify the omwHost setting to specify the IP address of the HPOM for Windows host machine:

```
# omwHost should be set to the host which is running HP Operations Manager Windows
omwHost = "localhost"
```

5. Restart the integration agent.
    - On Windows, the integration agent runs as a Windows Service; on Unix, it runs as a Unix daemon.

2.1.3 Installing the subscription files

To use the optional subscription panel, you must copy the folder containing the files required by the Subscription panel into the xMatters installation folder. If you have more than one web server, repeat the following steps for each one.

Note: *The optional subscription panel is provided for xMatters deployments on Microsoft Windows only. The libraries required by the subscription panel's auto-populate feature are Windows-based, and do not function on Unix systems.*

To install the JSP files:

1. Navigate to `<xMHOME>\webserver\webapps\cocoon\alarmpoint\jsp\subscription` folder, and create a new subfolder named `hpomw`.

2. Copy the contents of the `xM_HP_OM_Windows_3_0_0\components\xmatters\sub_panel\jsp` folder from the extracted integration archive into the `hpomw` folder you created in step 1.
3. Copy the contents of the `xM_HP_OM_Windows_3_0_0\components\xmatters\sub_panel\lib` folder from the extracted integration archive to `<xMHOME>\webserver\webapps\cocoon\WEB-INF\lib`.
   - Note that this change may require that you overwrite several files and directories on the xMatters server; if you have made any changes to these files, ensure that you create backups before overwriting your existing files.
4. Restart the web server.

2.1.4 Installing voice files

These files must be installed into any xMatters deployment running a voice Device Engine. For more information, refer to the *xMatters installation and administration guide*.

This integration provides a complete set of English voice files.

Note: *xMatters version 4.1 and 5.0 store voice files in different locations; ensure that you use the correct set of instructions for your version of xMatters.*

To install the voice files on xMatters version 4.1:

1. Copy all of the files in the `\components\xmatters\vox\hpomw\recordings\english\phrases` folder from the extracted integration archive to the following node installs folder:

`<xMHOME>\node\phone-engine\Datastore\domains\common\recordings\english\phrases`

To install the voice files on xMatters version 5.0:

1. Determine the value of the File Identifier associated with your Company.
   - To find your Company's File Identifier, log into the xMatters web user interface as the Super Administrator, and view the target Company's Details page (**Admin** tab > **Companies** > **Company name**).
2. Copy the contents of the `\components\xmatters\vox\` folder from the extracted integration archive to the following node installs folder:

`<xMHOME>\node\phone-engine\Datastore\<FILE_IDENTIFIER>\`

For example, if you were installing the integration for the Default Company on an out-of-the-box deployment, the installation path for the voice files would be as follows:

`<xMHOME>\node\phone-engine\Datastore\1\hpomw\recordings\english\phrases`

2.1.5 Installing host files

This integration includes a set of host files for use on HPOM for Windows servers, located in the `hp-omw` folder in the extracted integration archive.

To install and configure the xMatters host files:

1. Copy the `xM_HP_OM_Windows_3_0_0\components\hp-omw` folder from the extracted integration archive to the `C:\Program Files\HP\HP BTO Software\install\` directory on the HPOM for Windows server.
2. Create an environment variable named "XMOMW", and set the value to the location of the `hp-omw` directory (e.g., `C:\Program Files\HP\HP BTO Software\install\hp-omw`). Add the environment variable to the “path” environment variable.

Note: *You must use the 8.3 filename convention used by DOS, as it supplies a short name for the folders to eliminate spaces. To determine the 8.3 filename of a folder, type* `dir /x` *in a command line. For example, the default directory in the 8.3 convention is* `C:\PROGRA~1\HP\HPBTOS~1\install\hp-omw`

---

3. Navigate to the `C:\Program Files\HP\HP BTO Software\install\hp-omw` and open the `omw.vbs` file in a text editor.
4. Locate the `Const integrationAgentIP = "localhost"` line and change the value within quotes to the IP address of the machine on which you installed the integration agent.
5. Save and close the `omw.vbs` file.
6. Repeat steps 3 to 5 for the `omw-forwarded.vbs` file.
7. From the `<xMOMW>\tools` directory, execute the `xm_tools.bat` file to import the test tool into the xMatters tools folder within HPOM for Windows. (This tool will be used to verify the integration.)
8. To import the xMatters policies into HPOM for Windows, execute the `xm_policies.bat` file in the `$\policies` directory.

Warning

If you have already loaded the policies into HPOM for Windows once, and then attempt to delete and re-load the policies, HPOM for Windows will return a deployment error. The policies will be loaded, but you will be unable to deploy them on a node.

To work around this limitation, open the policy in HPOM for Windows and then click **File > Save As**. Save the policy with a different name (e.g., "Forward message to xMatters 2"), and then deploy the new policy.

2.2 Configuring a Windows User

The xMatters Windows User is used throughout the integration as the default user for WMI interaction to and from HPOM for Windows. You will need to create this user in Windows on the HPOM for Windows Server, and then associate the user with the appropriate Windows group.

To configure the Windows user:

1. In the Windows Control Panel, open **Administrative Tools > Computer Management**.
2. In the Computer Management window, expand **System Tools > Local Users and Groups**.
3. Right-click **Users** and select **New User**.
4. In the New User dialog box, type the following information:
   - **User name**: xMattersOMW
   - **Full name**: xMatters Integration User
   - **Description**: This user is required for WMI interaction between xMatters and HPOM for Windows
   - **Password**: xMattersOMW
   - **Confirm password**: xMattersOMW

Note: *xMattersOMW is the default user name and password used by the integration. If you want to specify a different user name or password, ensure that you use the correct combination when configuring the remaining components in the integration.*

---

5. Clear the **User must change password at next logon** check box, and then click **Create**.
6. In the Users pane, double-click the new **xMattersOMW** user.
7. In the xMattersOMW Properties dialog box, click the **Member Of** tab, and then click **Add**.

8. In the Select Groups dialog box, in the **Enter the object names to select** field, type `HP-OVE-ADMINS`, and then click **Check Names**.

Note: *You can also use the HP-OVE-OPERATORS group, but this may limit some actions within the integration; it is recommended that the user be added to the Admins group.*

9. Once the group is fully qualified, click **OK**.
10. Click **Apply**, and then click **OK**.

2.3 Configuring xMatters

The following sections describe how to configure xMatters to combine with HPOM for Windows.

2.3.1 Importing Event Domain and scripts

The integration package includes an XML file that was created using the xMatters "Export Integration" feature; this greatly simplifies the xMatters configuration process by enabling you to create the integration Event Domain, configure the predicates and Event Domain Constants, and import the integration script package in a single step.

Note: *For a description of how to import the script package and configure the Event Domain manually, refer to "Manually configuring xMatters" on page 27.*

To import the integration Event Domain package:

1. Log in to xMatters as a Company Administrator, and click the **Developer** tab.
2. In the Domains menu on the left side of the screen, click **Event Domains**.
3. On the Event Domains page, click **Import New**.
4. On the Import Integration page, click **Browse**, and then locate the `components\xmatters\event-domain\XM-HP-OM-W.xml` file extracted from the integration archive.
5. Click **Open**, and then click **Upload**.

xMatters imports the integration configuration settings and displays the new hpomw Event Domain.

Defining the integration services

For the installation to be successful, the integration service name must match the name specified in the `hpomw.xml` file installed on the integration agent.

To define an Integration Service:

1. In xMatters, on the Event Domains page, click the **hpomw** Event Domain.
2. On the Event Domain Details page, in the Integration Services area, click **Add New**.
3. Enter the following information into the form:
    - **Name**: hpomw
    - **Description**: HPOM for Windows Integration Service
    - **Path**: *Not required. (This field is used by the xMatters mobile access component, which is not included in this integration.)*
4. Click **Save**.

Specifying connection parameters

Once you have imported the Event Domain package and configured the Integration Service, you must specify an xMatters address that is reachable from within a notification so that responses can be processed.

Note: *A known issue in xMatters version 5.0 requires that all Event Domain Constants be defined in UPPERCASE.*

To specify the connection constants:

1. On the Event Domains page, in the Domains menu, click **Event Domain Constants**.
2. In the **Event Domain** drop-down list, select **hpomw**, and then click **Continue**.
    - xMatters displays the pre-configured Event Domain Constants for the integration:
3. In the Event Domain Constants list, specify the correct values for the following constants (click the name of a constant to edit its value and description):

Constant Name	Default Value	Description
xmattersurl	http://localhost:8888	Used to specify the address of the xMatters web server. The links provided in notification content use this value to locate the xMatters web server which would process the response. For these links to work, this address must be reachable from the Device where the User will receive the notification; normally, this is the IP address or fully-qualified host name of the xMatters web server.
bespushurl	http://localhost:8888/static	Used to specify the address of the BES device server.
MAINLOGO	/static/images/xmatters/ logos/xmatters_email.gif	Specifies the location of the xMatters logo displayed in email notifications. **Note**: This field not added as part of the Event Domain import process; it is required only on xMatters 4.1 deployments. You must add this constant using the tools on the Event Domain Constants page to have the xMatters logo appear as expected.
HPOMWOWNERTYPE	default	Specifies who should own the HPOM for Windows message for Own, Ack, or Change Severity Responses. Possible values are: • **default**: sets the owner to the value specified by the HPOMWOWNER constant, which should be set to a hostname\HPOM for Windows user account. • **custom-field**: Sets the owner to the value specified in the xMatters Custom Fields for the responding xMatters User; must be a valid HPOM for Windows account in the HOSTNAME\USER format. To use the "custom-field" setting, you must create two custom text fields in xMatters named HP OMW Login and HP OMW Password, and specify a valid HOSTNAME\USER accounts and password for each xMatters User that will respond to HPOM for Windows notifications. If this variable is set to "custom-field" but either Custom Field is not specified, the "default" setting is used instead. For more information about creating Custom Fields in xMatters, refer to the *xMatters installation and administration guide*.

Constant Name	Default Value	Description
HPOMWOWNER	hostname\xMattersOMW	Specifies the owner when "default" is set as the owner type; this value must be a valid HPOM for Windows account in the HOSTNAME\USER format.
HPOMWPASSWORD	xMattersOMW	Specifies the password when "default" is used for the HPOMWOWNERTYPE constant.

Note: *For more information about the Event Domain Constants included in the integration and how to configure them to suit your deployment, see "Defining Event Domain Constants" on page 29.*

2.3.2 Adding the Web Service User

This integration requires a Web Service User to query for events to be injected to xMatters. The following steps describe how to configure the default Web Service User, IA_User, for this integration.

To set up a Web Service User:

1. In xMatters, click the **Users** tab, and then click **Find Web Service Users**.
2. On the Find Web Services Users page, click **All**.
3. In the returned search results, locate and click **IA_User**.
4. On the Details for IA_User page, confirm that the list of Allowed Web Services includes the **Query Incident** web service; if Query Incident is not listed in the Allowed Web Services list, select it in the Denied Web Services list, and then click **Add**.
5. Click **Save**.

2.4 Configuring Subscriptions

The following sections describe how to manage Subscriptions in xMatters, including instructions on how to configure a Subscription panel and assign Subscriptions to Users.

To allow Users to subscribe to specific criteria on injected events, you must configure a Subscription panel, which requires the following steps:

- Define the Event Domain predicates
- Define a Subscription Domain
- Create a Subscription
- Create a Fail-Safe Group

2.4.1 Defining Event Domain predicates

The default integration configuration uses the following Event Domain predicates to which you can subscribe:

- SEVERITY
- PRIORITY
- STATE

These predicates are automatically created in the Event Domain when importing the Event Domain package, as described in "Importing Event Domain and scripts" on page 9. To modify these predicates, or to add other predicates that you consider important, see "Modifying Event Domain predicates" on page 28.

2.4.2 Defining a Subscription Domain

The Subscription Domain is the reference point for Subscriptions, and allows you to control who can create Subscriptions, how recipients can respond to Subscription notifications, and which Event Domain predicates can be used to create a Subscription. You must create a Subscription Domain before you can create Subscriptions.

To create a Subscription Domain:

1. On the Developer tab, the Developer menu, click **Subscription Domains**.
2. On the Subscription Domains page, click the **Add New** link.
3. In the **Event Domain** drop-down list, select **hpomw**, and then click **Continue**.
4. On the Subscription Domain Details page, in the **Name** field, type `hpomw`.
    - By default, Subscriptions are non-FYI (i.e., they support response options). To disable two-way Subscription notifications, select the **One-Way** check box. Note that you will not be prompted to enter response choices for one-way Subscriptions.
5. In the **Type of Management** drop-down list, select **Both**.
6. In the **Custom Page URL** field, enter the following path:

```
jsp\subscription\hpomw\OMWSubscriptionForm.jsp
```

7. Click **Continue**.
8. On the Select Appropriate Response Choices page, specify the available responses for this Subscription, and then click **Continue**.
    - By default, the scripts support the following response choices: "Acknowledge", "Own", “Ignore”, and “Annotate”. To enable two-way communications for Subscriptions, define all response choices on the Select Appropriate Response Choices page.
9. On the Select Appropriate Predicates page, add all of the predicates to the **Applied Predicates** list, and then click **Continue**.
10. On the Select Roles page, specify the Roles you want to be able to create Subscriptions on the Domain, and then click **Save**.

Note: *For more information about working with Event and Subscription Domains, see the* xMatters installation and administration guide.

2.4.3 Configuring the Subscription JSP

You can use one of the following methods to populate the predicate list values on the Subscription Panel:

- Manually specify the predicate list values in the web user interface (also referred to as "demonstration mode").
- Using web services, query HPOM for Windows for possible values, and automatically populate the predicate lists with the results of the web service call.

Note: *Changing Subscriptions by adding or removing Event Domain predicates may cause existing Subscriptions to fail. For more information about working with Event and Subscription Domains, see the* xMatters installation and administration guide.

Specifying predicate lists manually

You can choose to define the predicate values manually; this means that when you configure a Subscription and a search is performed on a predicate, the search results will result in the predefined list values only. The search results will not include database queries.

To configure the Subscription panel in a demonstration mode, using predefined predicate list values, you must modify the Subscription JSP.

To manually populate the predicate lists:

1. Navigate to the `<xMHOME>\webserver\webapps\cocoon\alarmpoint\jsp\subscription\` folder on the xMatters web server, and open the following files:
    - `OMSearchNode.jsp`
    - `OMSearchNodeGroups.jsp`
    - `OMSearchPolicy.jsp`
    - `OMSearchObject.jsp`
2. Within each JSP file, set the Boolean variable USE_PREDEFINED_LIST_VALUES to *true*.
3. Save and close the files.
4. In xMatters, click the **Developer** tab.
5. On the Event Domains page, click **hpomw**.
6. On the Event Domain Details page, click **NODE** in the Predicates list.
7. Add the values you want to appear in the NODE list predicate, and then click **Save**.
8. Repeat steps 6 and 7 for **NODE_GROUPS**, **MSG_OBJECT**, and **MSG_SOURCE** in the Predicates list.

Populating predicate lists automatically

If you want to populate the predicate values lists from HPOM for Windows through web service calls rather than the predefined predicate list values, you must configure the connection properties within the JSP file.

To configure the Subscription JSP to connect through web services:

1. Open the `<xMHOME>\webserver\webapps\cocoon\alarmpoint\jsp\subscription\hpomw\Configuration.jsp` file on the xMatters web server.
2. Within the JSP file, replace the values in quotes for each parameter as described in the following table:

Subscription JSP parameters

Parameter	Value
OM_HOST_URL	The IP address of the HPOM for Windows host machine.
OM_USER_NAME	User name of a Windows user on teh host machine of the HPOM for Windows Server; must be prefaced with `<Machine Name>\\` For example, if your machine name is "ESX-OMW810", and your user is "xmatters", you would use the following entry: `final string OM_USER_NAME = "ESX-OMW810\\xmatters` Note that this user should be the same Windows user as the user specifed in "Configuring a Windows User" on page 8.
OM_PASSWORD	Password for the specified Windows user.
JDBC_DRIVER_CLASS_NAME	Class name of the JDBC driver used to retrieve policies from HPOM for Windows.
JDBC_URL	URL at which the database can be queried.
JDBC_USERNAME	User anme with which to make database queries. Must be a user with the database access permisisons.
JDBC_PASSWORD	Password for the querying user.

3. Save and close the JSP.

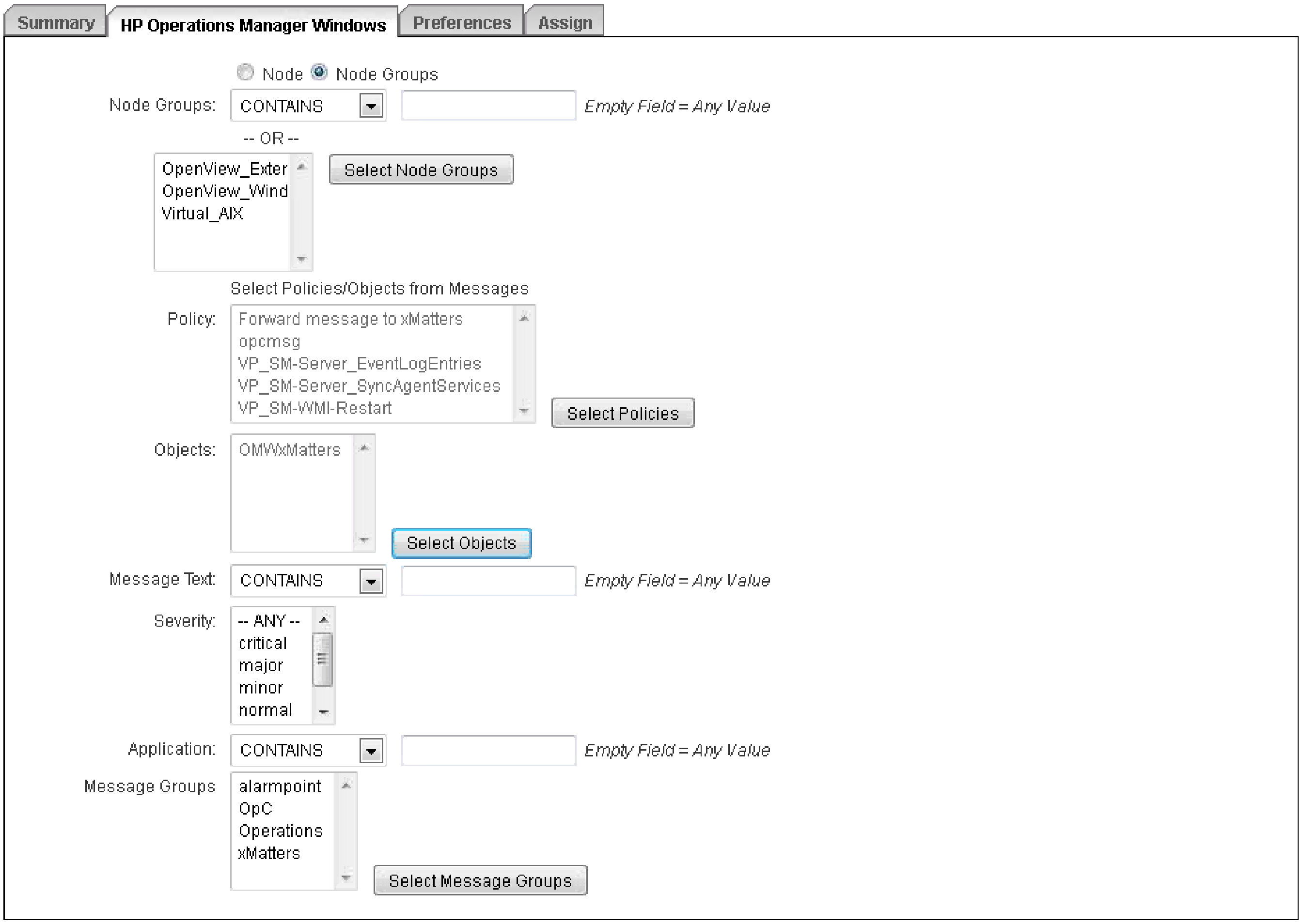
Creating a Subscription

You can now subscribe to HPOM for Windows events that match specific criteria. For example, you could configure a subscription that would send a notification to a specific User each time an event entered the system that was of critical severity.

To create a Subscription:

1. On the Alerts tab, in the Alerts menu, click **Assign Alerts**.
2. Select the **hpomw** Subscription Domain, and click the **Add New** link.
3. On the Subscription Details page, specify a name for the Subscription, and set the Subscription criteria and recipients using the tabbed pages of the Subscription panel.
4. When you are satisfied with the subscription details, click **Save** to create the Subscription.

- The HPOM for Windows tab (Ctrl-click to select more than one value):



○ Node ● Node Groups

Node Groups: CONTAINS *Empty Field = Any Value*

-- OR --

OpenView_Exter
OpenView_Wind
Virtual_AIX

Select Policies/Objects from Messages

Policy:
Forward message to xMatters
opcmsg
VP_SM-Server_EventLogEntries
VP_SM-Server_SyncAgentServices
VP_SM-WMI-Restart

Objects:
OMWxMatters

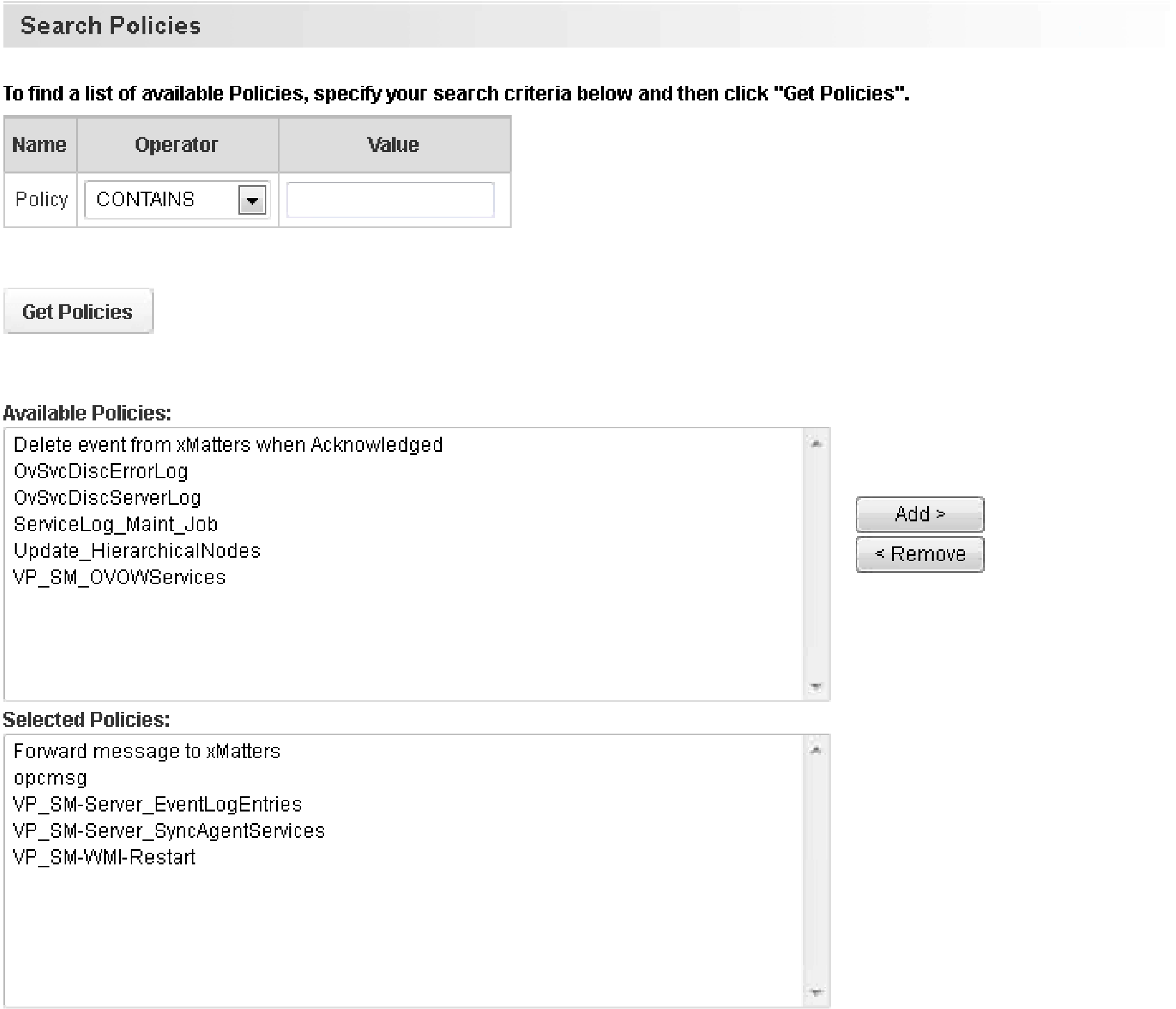
Message Text: CONTAINS *Empty Field = Any Value*

Severity:
-- ANY --
critical
major
minor
normal

Application: CONTAINS *Empty Field = Any Value*

Message Groups
alarmpoint
OpC
Operations
xMatters

- The Search Policies dialog box:



Search Policies

To find a list of available Policies, specify your search criteria below and then click "Get Policies".

Name	Operator	Value
Policy	CONTAINS	

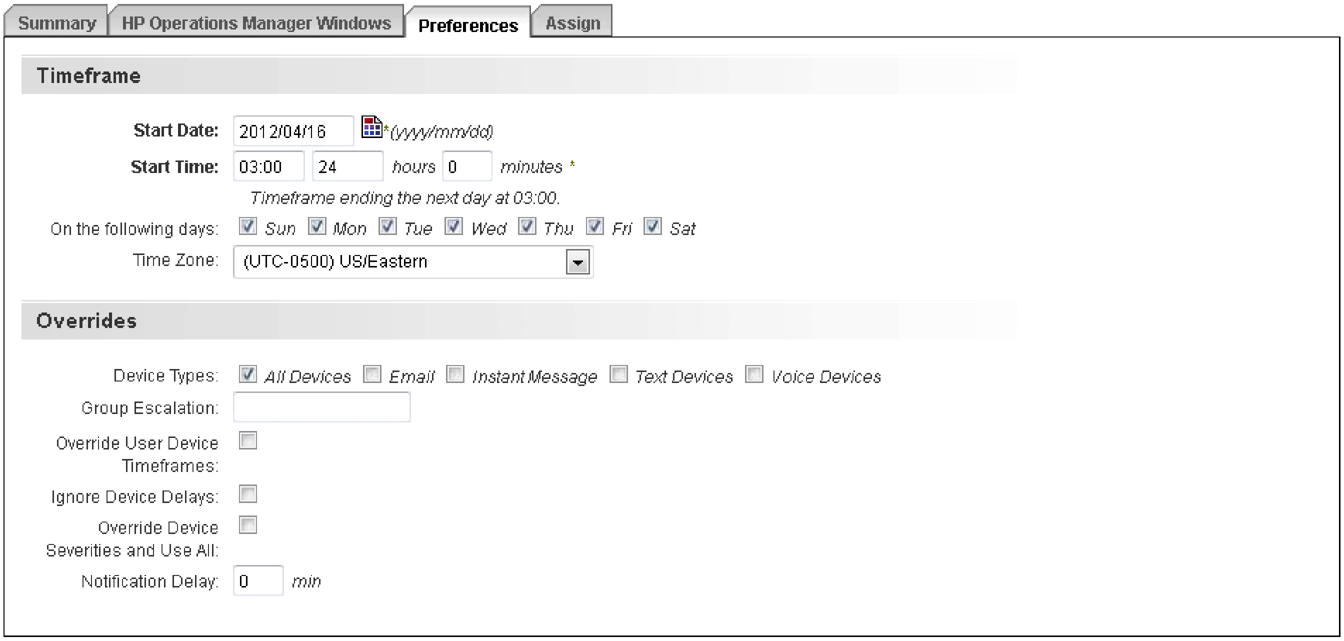
Available Policies:

Delete event from xMatters when Acknowledged
OvSvcDiscErrorLog
OvSvcDiscServerLog
ServiceLog_Maint_Job
Update_HierarchicalNodes
VP_SM_OVOWServices

Selected Policies:

Forward message to xMatters
opcmsg
VP_SM-Server_EventLogEntries
VP_SM-Server_SyncAgentServices
VP_SM-WMI-Restart

- The Preferences tab (defines the Timeframe and Overrides applied to events for Subscription notifications):



Timeframe

Start Date: 2012/04/16 *(yyyy/mm/dd)

Start Time: 03:00 24 hours 0 minutes *

Timeframe ending the next day at 03:00.

On the following days: ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time Zone: (UTC-0500) US/Eastern

Overrides

Device Types: ☑ All Devices ☐ Email ☐ Instant Message ☐ Text Devices ☐ Voice Devices

Group Escalation:

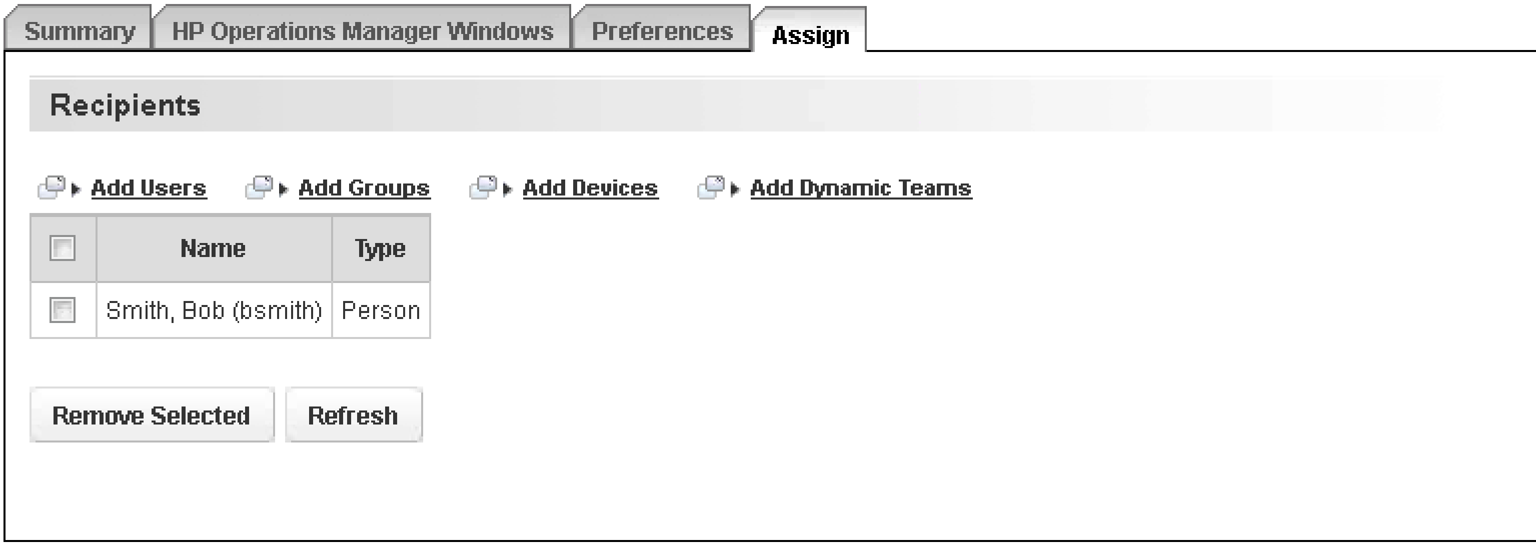
Override User Device Timeframes: ☐

Ignore Device Delays: ☐

Override Device Severities and Use All: ☐

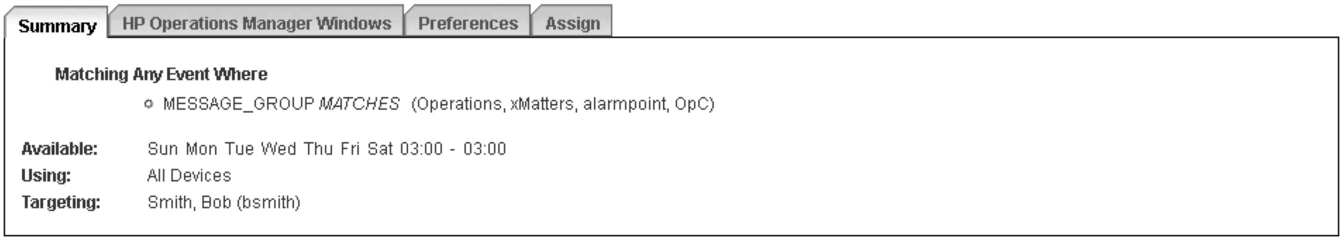
Notification Delay: 0 min

- The Assign tab:



☐	Name	Type
☐	Smith, Bob (bsmith)	Person

- You can review the Subscription details at any time on the Summary tab:



Matching Any Event Where

- MESSAGE_GROUP *MATCHES* (Operations, xMatters, alarmpoint, OpC)

Available: Sun Mon Tue Wed Thu Fri Sat 03:00 - 03:00
Using: All Devices
Targeting: Smith, Bob (bsmith)

Creating a fail-safe Group

If an event is submitted to xMatters when the fail-safe functionality is enabled, and there is no subscription that matches the event, xMatterssends the notification to the fail-safe recipient. The fail-safe recipient is typically a Group, but can be configured as a User.

To create a fail-safe Group:

1. In xMatters, click the Groups tab.
2. Create a new Group named HP OMW Fail Safe, with at least one User as a Team member to receive notifications.

For more information about creating Groups and Teams, see the xMatters engine user guide.

Note: *If you want to use an existing Group or a different Group name, modify the value for the failsafegroup Event Domain Constant. You can also eliminate notifying any fail-safe group by setting the failsafe constant to* disabled. *For more information, see "Configuring the Event Domain" on page 28.*

2.5 Configuring HPOM for Windows

The following sections describe how to configure HPOM for Windows to combine with xMatters.

2.5.1 OM-W Integration Module Distribution Components

The integration module components are distributed as a compressed archive with the following component structure:

Component	Description
Environment Variables	As described in "Installing host files" on page 7, the XMOMW environment variable is required, and must default to the location of the `hp-omw` directory (e.g., `C:\Program Files\HP\HP BTO Software\install\hp-omw`). Additionally, the xMatters integration agent must be installed on a machine other than the HPOM for Windows server.
xm_policies.bat	This script is located in the `<xMOMW>\policies` directory, and is used to import the default xMatters policies to activate the integration within HPOM for Windows.
xm_tools.bat	This script is located in the `<xMOMW>\tools` directory, and is used to import the xMatters test tool into the xMatters tools folder.
apt_tls.mof	This file contains the test tool that will be imported into HPOM for Windows. It was created by HPOM for Windows when the tool was exported for distribution, and will be accessed by the `xm_tools.bat` file during the tool import process.
OmwApt.vbs	This script is located in the `<IAHOME>\integrationservices\hpomw` directory, and contains the logic to handle response injections from xMatters to HPOM for Windows. It processes messages from xMatters to HPOM for Windows, using the same GUID in support of the two-way integration.

2.5.2 Policies and Tools

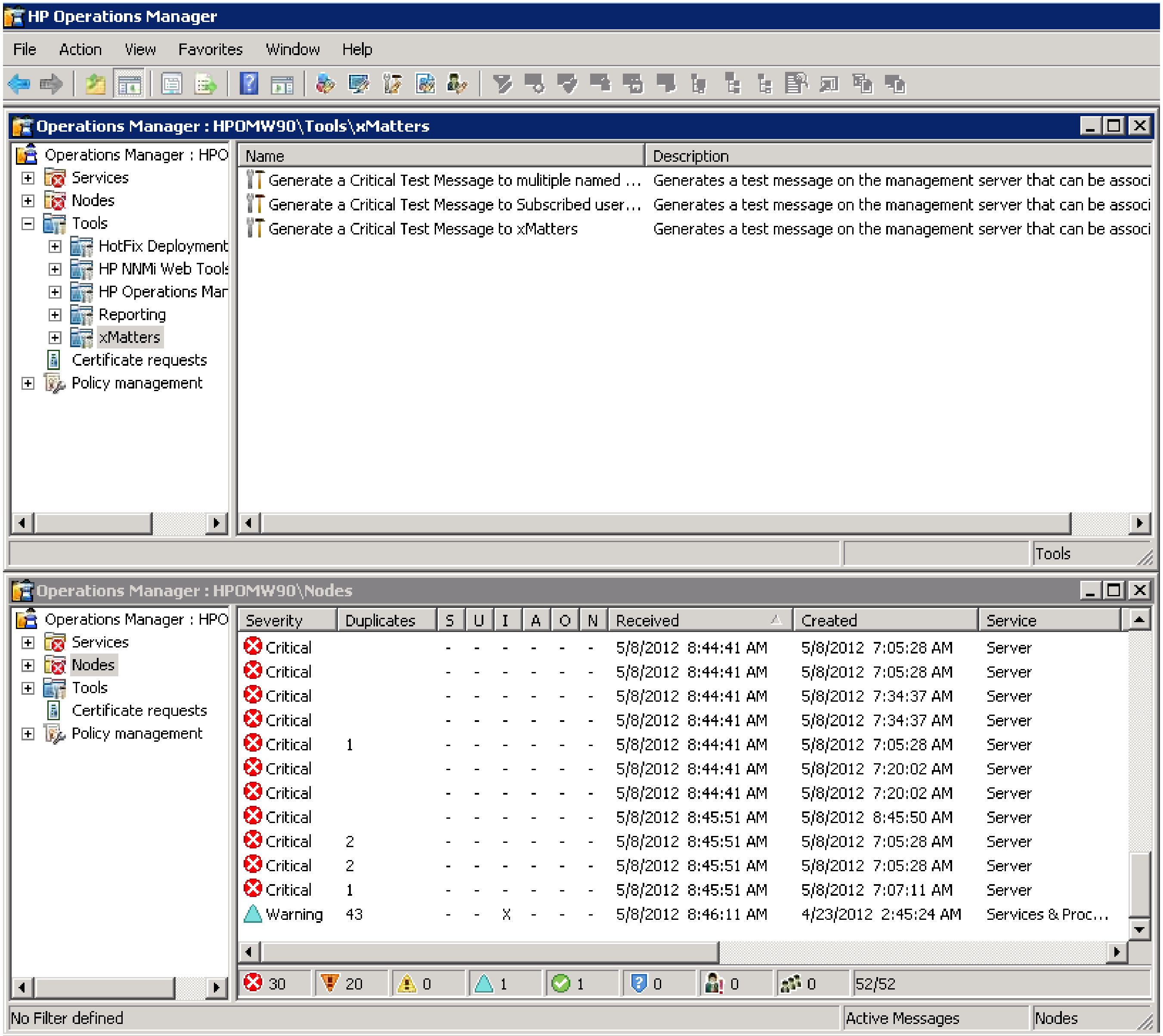
When creating, updating or maintaining HPOM for Windows Policies, you may need to add or remove tokens that are being passed to xMatters. When doing so, you must duplicate your changes to the tokens being passed by the policy in the following files:

- `omw.vbs`: Any changes to the tokens being passed out of HPOM for Windows must be reflected here, specifically in the `ProcessArguments()` and `injectEvent()` subroutines.
- `hp_operations_manager_win.xml`: The data map is defined in the `<mapped-input method="add" subclass="action">` and must reflect the changes made to the policy and the `omw.vbs` file.

Note: *It is important to consider all policies that will be using this integration when you make your changes; be careful not to remove tokens used by other policies and ensure that you provide default values for tokens that are not supplied by every policy. For an example of adding tokens, see "Adding new parameters" on page 32.*

Policy/Tool Name	Policy Type	Tool Type	Description
Forward message to xMatters	WMI		Forwards messages to xMatters from HPOM for Windows.
Delete event from xMatters when Acknowledged	WMI		Forwards a “del” event to xMatters when an Operations Event is acknowledged in the Console.

Policy/Tool Name	Policy Type	Tool Type	Description
Generate a Critical Test Message to xMatters		WMI	Generates a critical test message, triggering an alert via xMatters for a single User/Group; runs on the management server only; can be associated with a service and/or Node. The "Forward message to xMatters" Policy must be deployed on the management server before using this command.
Generate a Critical Test Message to multiple named recipients in xMatters		WMI	Generates a critical test message, triggering an alert via xMatters for multiple Users/Groups; runs on the management server only; can be associated with a service and/or Node. The "Forward message to xMatters" Policy must be deployed on the management server before using this command.
Generate a Critical Test Message to Subscribed users in xMatters		WMI	Generates a critical test message triggering an alert via xMatters for a subscribed User; runs on the management server only; can be associated with a service and/or Node. The "Forward message to xMatters" Policy must be deployed on the management server before using this command.



Name	Description
Generate a Critical Test Message to mulitiple named …	Generates a test message on the management server that can be associ
Generate a Critical Test Message to Subscribed user…	Generates a test message on the management server that can be associ
Generate a Critical Test Message to xMatters	Generates a test message on the management server that can be associ

Severity	Duplicates	S	U	I	A	O	N	Received	Created	Service
Critical		-	-	-	-	-	-	5/8/2012 8:44:41 AM	5/8/2012 7:05:28 AM	Server
Critical		-	-	-	-	-	-	5/8/2012 8:44:41 AM	5/8/2012 7:05:28 AM	Server
Critical		-	-	-	-	-	-	5/8/2012 8:44:41 AM	5/8/2012 7:34:37 AM	Server
Critical		-	-	-	-	-	-	5/8/2012 8:44:41 AM	5/8/2012 7:34:37 AM	Server
Critical	1	-	-	-	-	-	-	5/8/2012 8:44:41 AM	5/8/2012 7:05:28 AM	Server
Critical		-	-	-	-	-	-	5/8/2012 8:44:41 AM	5/8/2012 7:20:02 AM	Server
Critical		-	-	-	-	-	-	5/8/2012 8:44:41 AM	5/8/2012 7:20:02 AM	Server
Critical		-	-	-	-	-	-	5/8/2012 8:45:51 AM	5/8/2012 8:45:50 AM	Server
Critical	2	-	-	-	-	-	-	5/8/2012 8:45:51 AM	5/8/2012 7:05:28 AM	Server
Critical	2	-	-	-	-	-	-	5/8/2012 8:45:51 AM	5/8/2012 7:05:28 AM	Server
Critical	1	-	-	-	-	-	-	5/8/2012 8:45:51 AM	5/8/2012 7:07:11 AM	Server
Warning	43	-	-	X	-	-	-	5/8/2012 8:46:11 AM	4/23/2012 2:45:24 AM	Services & Proc…

Forward message to xMatters

This policy provides the logic to determine which events warrant the generation of an alert via xMatters notification processing. Any message may be used to generate a notification by simply adding a rule to this policy, and modifying the Automatic command with the appropriate parameters. This policy passes the entire TargetInstance ID of the current message to the `omw.vbs` script so that it may process the components into an appropriate integration agent call.

The example policy forwards all CRITICAL messages to xMatters for processing. After eliminating any messages generated by the integration itself, the policy checks for messages with a CRITICAL Severity (a value of 32). The automatic action calls the integration script, injecting a list of parameters defined within the Rule for the Policy. This injected message will be enriched by omw.vbs, which links the Node and Node Groups associated with the message and injects it to xMatters for notification.

This policy is intended only as an example of how to forward messages to xMatters. Using this policy as a guide, you must create policies that match your specific business requirements for event notification.

Delete event from xMatters when Acknowledged

When an event is acknowledged within the Operations Console, it is considered closed and no further actions are allowed other than to re-open the event. The “Delete event from xMatters when Acknowledged” Policy forwards a “del” event to xMatters, closing the associated xMatters Event. This prevents the xMatters User from taking actions on a closed event.

2.5.3 Policy Notification Activation

Once the scripts have been placed in their appropriate directories, and the default policies have been imported into HPOM for Windows, activate the integration by deploying the policy to the HPOM for Windows Server:

1. From within HPOM for Windows’s xMatters policy group (**Operations Manager > Policy Management > Policy Groups > xMatters**), right-click the **Forward message to xMatters** policy and select **All tasks > deploy on**.
2. Expand the **Nodes** tree and select only the check box for your server, **SERVER (Management Server)**.
3. Click **OK** to deploy the policy.
4. Repeat the above steps for the "Delete event from xMatters when Acknowledged" policy.

The "Forward Message to xMatters" Policy may be customized by adding additional rules. Each rule can call a separate `omw.vbs` script to handle and enrich specific parameters.

2.5.4 Debugging Visual Basic Scripts

This integration incorporates three Visual Basic scripts used for passing messages to and from HPOM for Windows to the xMatters integration agent. To aid in troubleshooting the intermediate VB scripts, the scripts include the logType flag.

You can specify the amount of logging performed on the Visual Basic scripts by setting the debugLogLevel variable for each of the `forward.vbs`, `omw.vbs`, and `OmwApt.vbs` files. The debugLogLevel can be set to one of the following values:

Value	Description
false (default)	Shows critical logging only; excludes INFO logging
true	Shows all messages, including INFO logging. (Note that INFO messages contain a lot of data, and can cause large log files.)

The log files for each of the Visual Basic scripts are located as follows:

Visual Basic Script	Log File
`omw-forwarded.vbs`	`$XMOMW\logs\XM-OMW-Forwarded.log`
`omw.vbs`	`$XMOMW\logs\XM-OMW-Inject.log`
`OmwApt.vbs`	`$APIA_HOME\logs\XM-OMW-Response.log`

By default, debugging information is written to a file. You can also choose to annotate the debug information to the original HPOM for Windows event, or disable the logging behavior entirely. To log a debug message, you must set the message to write in the logText variable, specify the type of logging behavior in the logType variable, and then call the WriteLog method.

The logType flag may specify one of the following behaviours:

Value	Description
toFile	Logs the debug message to a file.

Value	Description
toEvent	Annotates the debug message to the HPOM for Windows event.
toBoth	Logs the debug message to a file, and annotates the message to the HPOM for Windows event.

If any other value is supplied, the logging behavior is disabled.

Note: *The messageGUID must be associated with a valid HPOM for Windows event for the annotating to work.*

Chapter 3: Integration Validation

After configuring xMatters and HPOM for Windows, you can validate that communication is properly configured. It is recommended that you start the components in the following order:

- HP Operations Manager for Windows software
- xMatters relevance engine
- xMatters integration agent

Consult the respective user manuals for details on starting these applications.

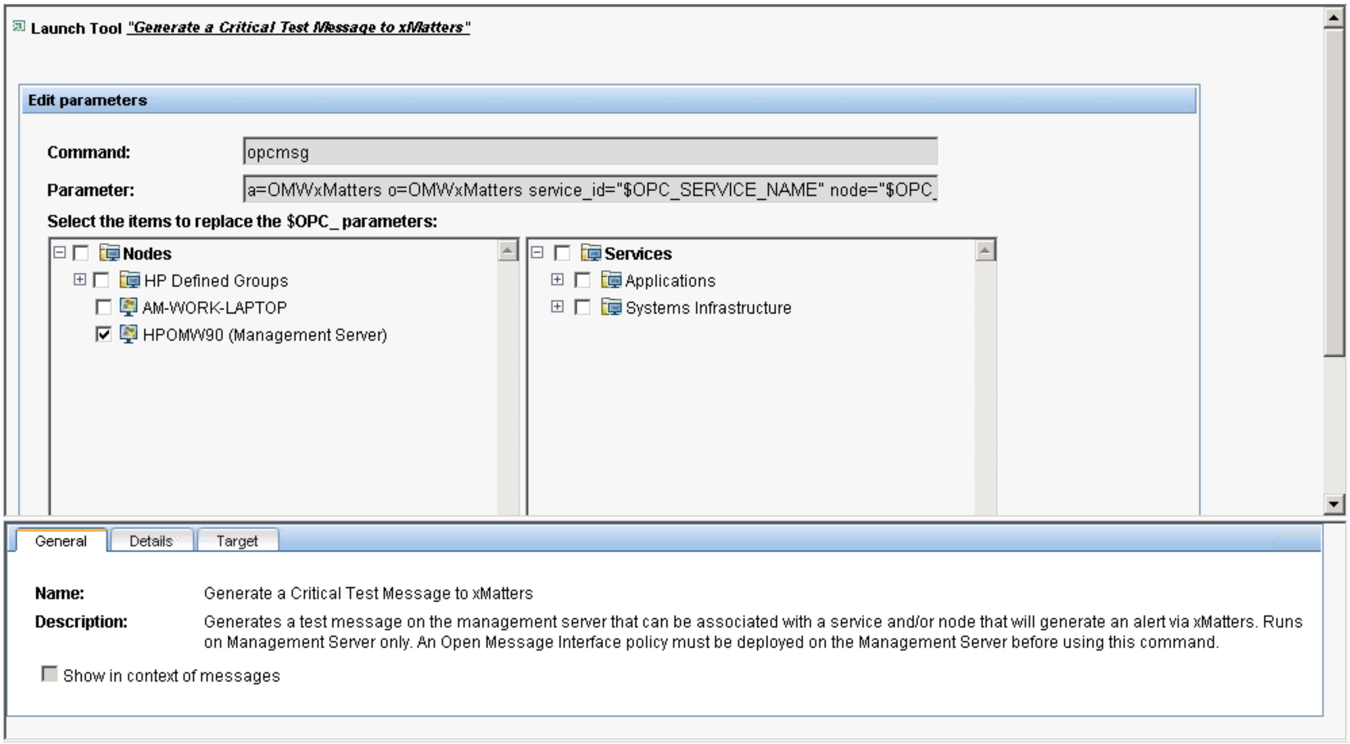
The following sections will test the combination of xMatters and HPOM for Windows for notification delivery and response, and Subscription Panel functionality.

3.1 Triggering a notification

In this example, the Test Tool included with the integration is used to trigger a CRITICAL event in HPOM for Windows. The xMatters policy detects that a CRITICAL event has occurred, and sends notifications to xMatters.

To trigger a CRITICAL event:

1. Open the HPOM for Windows Console, and expand the tree in the left pane (**Tools > xMatters**) to display the test tool.
2. Double-click **Generate a Critical Test Message to xMatters**.
    - The Launch tool opens:



Launch Tool "Generate a Critical Test Message to xMatters"

Edit parameters

Command: opcmsg

Parameter: a=OMWxMatters o=OMWxMatters service_id="$OPC_SERVICE_NAME" node="$OPC_

Select the items to replace the $OPC_ parameters:

☐ Nodes
  ☐ HP Defined Groups
  ☐ AM-WORK-LAPTOP
  ☑ HPOMW90 (Management Server)

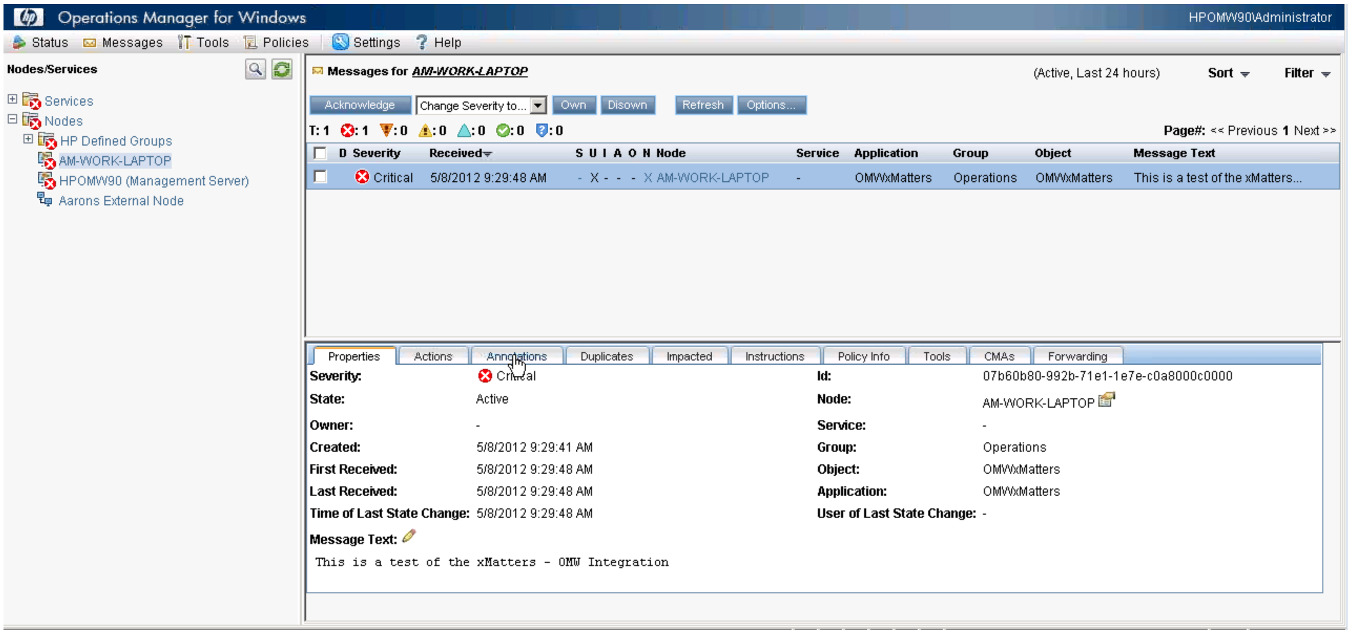
☐ Services
  ☐ Applications
  ☐ Systems Infrastructure

Name: Generate a Critical Test Message to xMatters

Description: Generates a test message on the management server that can be associated with a service and/or node that will generate an alert via xMatters. Runs on Management Server only. An Open Message Interface policy must be deployed on the Management Server before using this command.

☐ Show in context of messages

3. Select the check box next to the Management Server you want to use.
4. Click **Next**, and then click **Launch**.
    - The Nodes area displays the CRITICAL event:



Messages for AM-WORK-LAPTOP (Active, Last 24 hours)

T: 1 :1 :0 :0 :0 :0 :0

☐	D	Severity	Received	S	U	I	A	O	N	Node	Service	Application	Group	Object	Message Text
☐		Critical	5/8/2012 9:29:48 AM	-	X	-	-	-	X	AM-WORK-LAPTOP	-	OMWxMatters	Operations	OMWxMatters	This is a test of the xMatters...

Severity: Critical

State: Active

Owner: -

Created: 5/8/2012 9:29:41 AM

First Received: 5/8/2012 9:29:48 AM

Last Received: 5/8/2012 9:29:48 AM

Time of Last State Change: 5/8/2012 9:29:48 AM

Id: 07b60b80-992b-71e1-1e7e-c0a8000c0000

Node: AM-WORK-LAPTOP

Service: -

Group: Operations

Object: OMWxMatters

Application: OMWxMatters

User of Last State Change: -

Message Text:

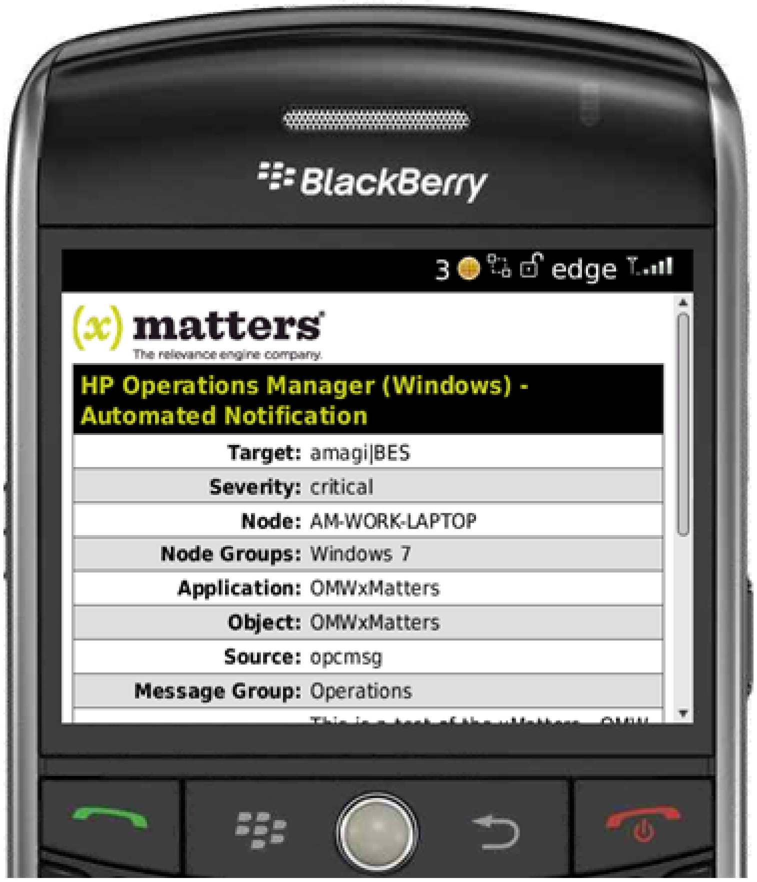
```
This is a test of the xMatters - OMW Integration
```

3.2 Responding to a notification

This section describes how to respond to a notification from xMatters. In the following example, the notification is received on a BlackBerry Device, but the process is similar for all Devices.

To respond to a notification:

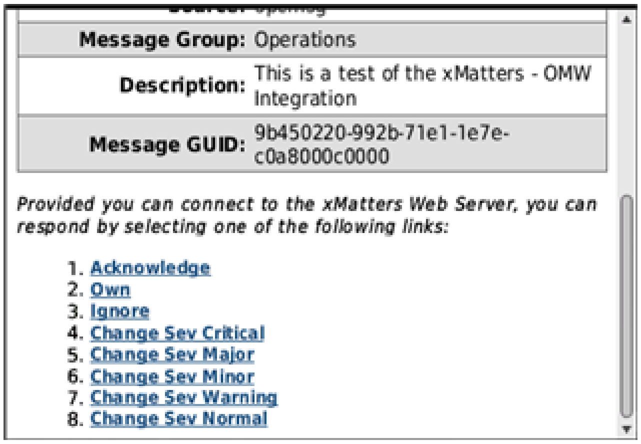
1. When a notification arrives for the User, the Device indicates the number of calls received.
2. Opening the notification displays its details:



HP Operations Manager (Windows) - Automated Notification

Target:	amagi|BES
Severity:	critical
Node:	AM-WORK-LAPTOP
Node Groups:	Windows 7
Application:	OMWxMatters
Object:	OMWxMatters
Source:	opcmsg
Message Group:	Operations

3. Scrolling down will display the remainder of the details, and the list of possible replies:

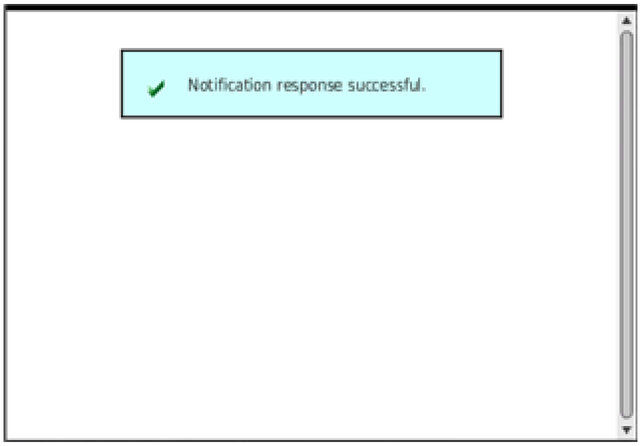


Message Group:	Operations
Description:	This is a test of the xMatters - OMW Integration
Message GUID:	9b450220-992b-71e1-1e7e-c0a8000c0000

Provided you can connect to the xMatters Web Server, you can respond by selecting one of the following links:

1. Acknowledge
2. Own
3. Ignore
4. Change Sev Critical
5. Change Sev Major
6. Change Sev Minor
7. Change Sev Warning
8. Change Sev Normal

4. To respond to the notification, the User clicks a response choice, and xMatters updates the event in HPOM for Windows.



Notification response successful.

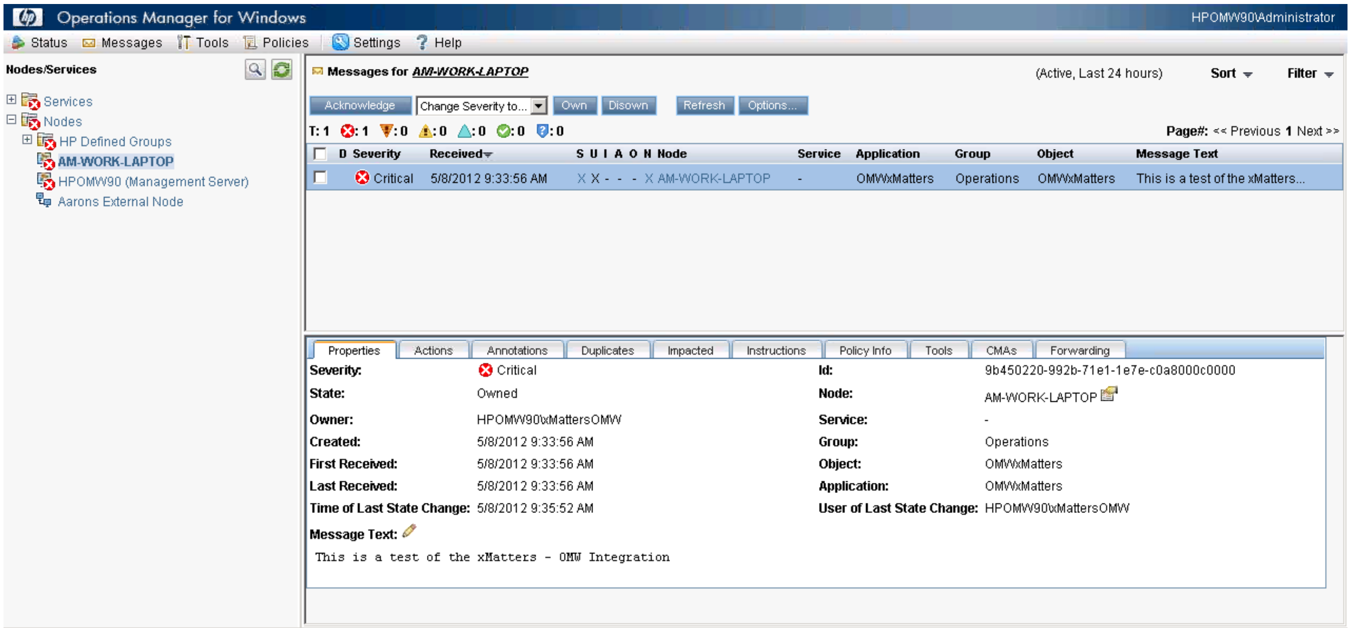
For more information about response choices, and changing the options available to Users, see "Response Choices" on page 34.

3.3 Viewing response results

In the HPOM for Windows Console, the message will be cleared from the message pane once it has been acknowledged.

To view the notification results:

1. Right-click Nodes, and then select View > Acknowledged Messages.
2. Select the message from the list, and view the Properties tab:



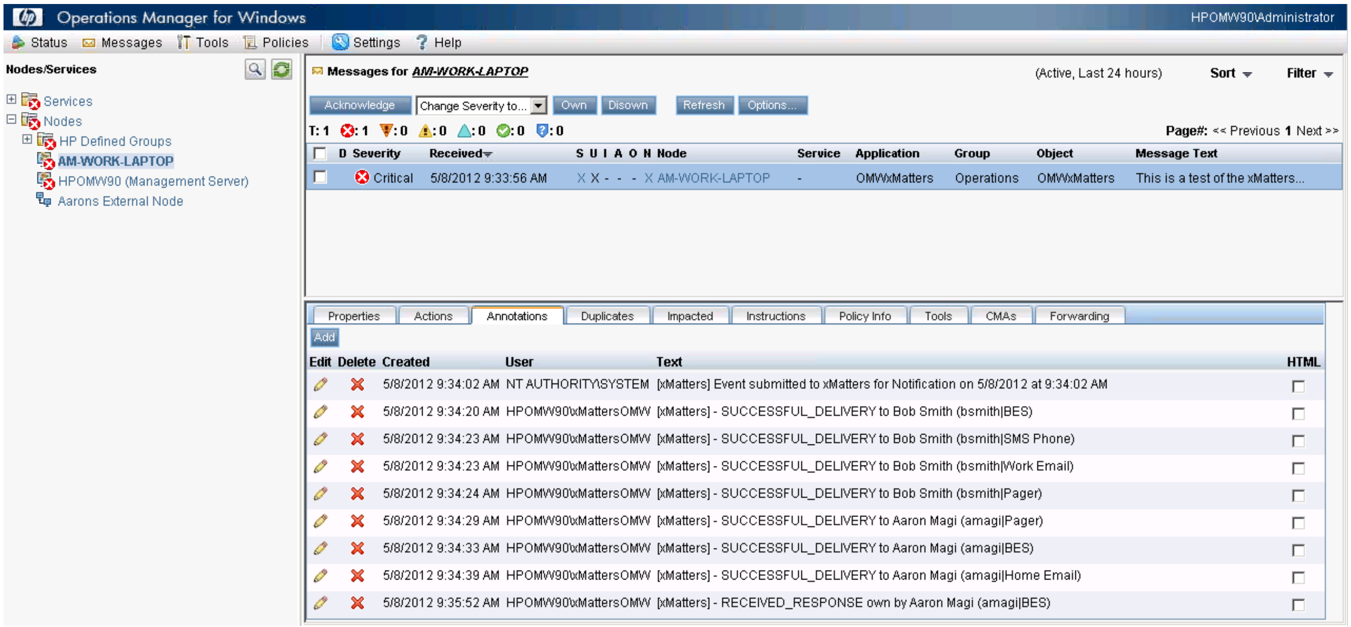
☐	D	Severity	Received	S	U	I	A	O	N	Node	Service	Application	Group	Object	Message Text
☐		Critical	5/8/2012 9:33:56 AM	X	X	-	-	-	X	AM-WORK-LAPTOP	-	OMWxMatters	Operations	OMWxMatters	This is a test of the xMatters...

Severity:	Critical	**Id:**	9b450220-992b-71e1-1e7e-c0a8000c0000
State:	Owned	**Node:**	AM-WORK-LAPTOP
Owner:	HPOMW90\xMattersOMW	**Service:**	-
Created:	5/8/2012 9:33:56 AM	**Group:**	Operations
First Received:	5/8/2012 9:33:56 AM	**Object:**	OMWxMatters
Last Received:	5/8/2012 9:33:56 AM	**Application:**	OMWxMatters
Time of Last State Change:	5/8/2012 9:35:52 AM	**User of Last State Change:**	HPOMW90\xMattersOMW

Message Text:

```
This is a test of the xMatters - OMW Integration
```

3. To display the messages annotated to the event, click the Annotations tab:



☐	D	Severity	Received	S	U	I	A	O	N	Node	Service	Application	Group	Object	Message Text
☐		Critical	5/8/2012 9:33:56 AM	X	X	-	-	-	X	AM-WORK-LAPTOP	-	OMWxMatters	Operations	OMWxMatters	This is a test of the xMatters...

Edit	Delete	Created	User	Text	HTML
		5/8/2012 9:34:02 AM	NT AUTHORITY\SYSTEM	[xMatters] Event submitted to xMatters for Notification on 5/8/2012 at 9:34:02 AM	☐
		5/8/2012 9:34:20 AM	HPOMW90\xMattersOMW	[xMatters] - SUCCESSFUL_DELIVERY to Bob Smith (bsmith|BES)	☐
		5/8/2012 9:34:23 AM	HPOMW90\xMattersOMW	[xMatters] - SUCCESSFUL_DELIVERY to Bob Smith (bsmith|SMS Phone)	☐
		5/8/2012 9:34:23 AM	HPOMW90\xMattersOMW	[xMatters] - SUCCESSFUL_DELIVERY to Bob Smith (bsmith|Work Email)	☐
		5/8/2012 9:34:24 AM	HPOMW90\xMattersOMW	[xMatters] - SUCCESSFUL_DELIVERY to Bob Smith (bsmith|Pager)	☐
		5/8/2012 9:34:29 AM	HPOMW90\xMattersOMW	[xMatters] - SUCCESSFUL_DELIVERY to Aaron Magi (amagi|Pager)	☐
		5/8/2012 9:34:33 AM	HPOMW90\xMattersOMW	[xMatters] - SUCCESSFUL_DELIVERY to Aaron Magi (amagi|BES)	☐
		5/8/2012 9:34:39 AM	HPOMW90\xMattersOMW	[xMatters] - SUCCESSFUL_DELIVERY to Aaron Magi (amagi|Home Email)	☐
		5/8/2012 9:35:52 AM	HPOMW90\xMattersOMW	[xMatters] - RECEIVED_RESPONSE own by Aaron Magi (amagi|BES)	☐

Chapter 4: Optimizing and Extending the Integration

This section describes some of the available methods you can use to optimize or extend the xMatters (IT) for HP Operations Manager for Windows integration.

4.1 Manually configuring xMatters

This integration includes an exported version of the xMatters script package and Event Domain, including Event Domain constants and predicates. If you do not want to use the included XML file to create and configure the required Event Domain and Action Scripts, the following sections describe how to manually configure these components.

4.1.1 Importing the script package

This integration includes a set of customized Action Scripts specific to HPOM for Windows that must be imported into the xMatters scripts. The default callout scripts in a standard xMatters deployment are not configured to use web services to annotate the originating event, and must be updated to inject messages back to the HPOM for Windows integration action scripts.

Note: *This step requires the xMatters Developer IDE. For installation instructions and more information about scripting in xMatters, refer to the xMatters Online Developer's Guide.*

To import the xMatters Script Package:

1. Launch the xMatters Developer IDE, and then configure the database connection.
2. Click **Workspace > Import**.
3. Select the `xM_HP_OM_Windows_3_0_0\components\scripts\xM-HP-OMW.aps` file extracted from the integration zip file, and then click **OK**.
4. When the script has finished importing, click **OK**.
5. Right-click the Default Company folder, and then select **Validate**.
6. Right-click the Default Company folder, and then select **Check In**.
7. In the Create Script Package dialog box, click **Create**., and then click **Close**.

4.1.2 Configuring Users

Each xMatters User that will be notified and respond to notifications must be configured to allow xMatters to communicate with HPOM for Windows as that User. Note that each User must also be configured in HPOM for Windows.

To configure a User:

1. In xMatters, click the **Users** tab.
2. Use the Find Users page to locate the User you want to configure and view their details.
3. In the Common Tasks pane, click **User Devices**.
4. Verify that an appropriate Device exists and that it is enabled.
5. Click **Save**.

Note: *If you have no Users in the system, you can use the default demonstration User, "bsmith". If this User does not exist, create a User with the User ID "bsmith", and add a virtual text phone Device. For more information and instructions on how to perform these tasks, refer to the* xMatters engine user guide.

4.1.3 Configuring the Event Domain

By default this integration is set up to use an Event Domain of “hpomw”; it is strongly recommended that you use this default Event Domain. For the integration to be successful, the Event Domain name must match the value in the integration agent configuration file for the integration service (i.e., the <domain> tag in `hpomw.xml`).

The xMatters relevance engine web server must be running to perform this portion of the integration.

To define an Event Domain:

1. Log in to xMatters as a Company Administrator, and click the **Developer** tab.
2. In the Developer menu on the left side of the screen, click **Event Domains**.
3. On the Event Domains page, click **Add New**.
4. Enter the following information into the form:
    - **Name**: hpomw
    - **Description**: HPOM for Windows Integration
    - **Script Package**: HP Operations Manager for Windows
5. Click **Save**.

Once you have defined the Event Domain, you can add the integration service, as described in "Defining the integration services" on page 9.

Modifying Event Domain predicates

The default predicates for the integration are automatically created in the Event Domain when importing the Event Domain package, as described in "Importing Event Domain and scripts" on page 9. The following instructions are included to explain how to add or modify these predicates, and explain how the default configuration relates to event details in HPOM for Windows.

Note: *You can also use the following steps to add other predicates that you consider important and which you plan to add to the integration as explained in "Adding new parameters" on page 32.*

To define Event Domain predicates:

1. In xMatters, click the **Developer** tab.
2. On the Event Domains page, click hpomw.
3. On the Event Domain Details page, click **Add New**.
4. Add the following predicates to the Event Domain:

Event Domain predicates

Predicate	Type	Important	Values
NODE	List	Yes	None; automatically populated.
NODE_GROUPS	List		None; automatically populated.
NODE_GROUPS_TEXT	Text		
APPLICATION	Text	Yes	
MESSAGE_GROUP	Text		
MSG_OBJECT	List		None; automatically populated.

Predicate	Type	Important	Values
MSG_SOURCE	List		None; automatically populated.
MSG_TEXT	Text		
SEVERITY	List	Yes	Manually entered; populate with the following values: • normal • warning • minor • major • critical

Note: *For more information about populating list values for the NODE, NODE_GROUPS, MSG_OBJECT, and MSG_ SOURCE predicate, see .*

Defining Event Domain Constants

Company Administrators and Developers can create Event Domain Constants that will be available in scripting for all event objects associated with an Event Domain.This integration uses Event Domain Constants to define custom values for the integration script package.

The integration script package uses the names of the constants defined in the table below to look up the values; it is strongly recommended that you use the names specified, or speak to your xMatters client assistance representative before changing these values.

Note: *The values for the xmattersurl and bespushurl constants should be modified to specify the address of the xMatters web server (to enable the HMTL response options) and the BES device server.*

To add an Event Domain Constant:

1. In xMatters, click the **Developer** tab, and then, in the menu on the left side of the screen, click **Event Domain Constants**.
2. In the **Event Domain** drop-down list, select **hpomw**.
3. On the Event Domain Constants page, click **Add New**.
4. Define a **Constant Name**, **Value**, and **Description** for the new constant, according to the table below.
5. Click **Save**.
6. Repeat the above steps for each of the constants you want to add.
   - Note that if the constants are not defined in the web user interface, the scripts will use the values listed in the Default Values column of the following table.

Note: *Shaded rows indicate **mandatory** settings that are specific to your deployment. You must change the default settings to match your instance.*

Event Domain Constants

Constant Name	Default Value	Description
xmattersurl	http://localhost:8888	Used to specify the address of the xMatters web server. The links provided in notification content use the alarmpointurl constant value to locate the xMatters web server which would process the response. For these links to work, this address must be reachable from the Device where the User will receive the notification; normally, this is the IP address or fully-qualified host name of the xMatters web server. Populates the `$main.alarmpoint_url` variable.
bespushurl	http://localhost:8888/static	Used to specify the address of the BES device server. Populates the `$main.bes_pushurl` parameter.
forcefyi	disable	Force notifications to be informational only (FYI), rather than requiring responses; this overrides the fyi behaviour specified on the injected event. Possible values: • **disable**: Nothing is forced. • **on**: Notifications are forced to be FYI. • **off**: Notifications are forced not to be FYI. Populates the `force_fyi` parameter.
failsafegroup	HP OMW Fail Safe	The fail-safe recipient to notify, typically a group. The fail-safe group identifies the recipient that will be notified if an event is injected to xMatters relevance engine and no subscriptions exist that match the event. Set this constant if you want to change the failsafe group from HP OMW Fail Safe to another group defined in xMatters.
failsafe	enabled	Controls fail-safe functionality, notifying the fail-safe recipient via EMAIL under certain circumstances; possible values are: • **enabled**: Notify if no subscriptions match or no notifiable recipients. • **for-subscriptions**: Notify if subscription functionality is enabled AND no subscriptions match. • **for-recipients**: Notify if no notifiable recipients. • **disabled**: Disable fail-safe functionality. Populates the `$fail_safe` parameter.
overridetimeframes	false	Override Recipients Device Timeframes. Populates the `$override_timeframes` parameter.
useemergencydevices	false	Force the use of emergency Devices. Populates the `$use_emergency_devices` parameter.

Constant Name	Default Value	Description
trackdelivery	true	Track when each device is delivered to. Setting this to false may give a performance advantage, but you lose any information about whether a delivery was successful or not. Populates the `$track_delivery` parameter.
annotate	true	Enables submission of annotations back to the management system. Populates the `$main.annotate` parameter.
subscriptionannotate	true	Enables submission of Subscription annotations back to the management system. Populates the `$main.subscription_annotate` parameter.
tracksubscriptiondelivery	true	Track when each device is delivered to for Subscriptions. Populates the `$track_subscriptionDelivery` parameter.
timeout	259200	Amount of time (in seconds) the event is allowed to run before timing out. 259200 seconds = 72 hours. Populates the `$main.timeout` parameter.
maxinvalidresponses	3	Specifies the maximum number of invalid responses allowed before notification is no longer requeued. Populates the `$main.maxInvalidResponses` parameter.
enablehtmlemail	true	Enables HTML email functionality. Populates the `$main.enable_HTML_Email` parameter.
uselogo	true	Set this if you want the logo displayed within HTML email notifications. Populates the `$main.use_logo` parameter.
useurlalias	false	Indicates how Response Choices are presented to xMatters to ensure that the user is authenticated in the correct company so the notification can be updated.; set to *true* for xMatters on demand integrations.
debug	false	Indicates whether to use the debug level for logging messages. Populates the `$main.debug` variable.
enablesubscriptions	true	Indicates whether to enable processing of Subscriptions on incoming events.
subscriptionfyi	false	Indicates whether Subscriptions should be forced to be informational only (FYI).
numericpagernumber	555-1212	The callback number to be used as the subject for outgoing notifications to numeric pagers.

4.2 Adding new parameters

Additional data elements, or tokens, can be forwarded to xMatters by adding them to the policy in HPOM for Windows or retrieving them via WMI in the `omw.vbs` enrichment and injection script. The following steps explain how to add a custom data element to inject the OriginalText for the OV_Message to xMatters and displayit within the notification content.

Note: *For more information about which parameters may be available, refer to the HPOM for Windows documentation.*

4.2.1 Adding custom parameters to the policy

If you have already configured a custom policy for your integration to forward messages to xMatters, edit your custom policy rather than the Forward message to xMatters policy.

To add a data element to the policy for forwarding messages:

1. Open the Operations Manager Console and under Policy Management, click **Policy Group > xMatters**.
2. Open the **Forward message to xMatters** policy for editing.
3. Within the Rules section, select the rule to which you want to add the custom data element and click **Modify**.
4. On the Actions Tab of the Rule pop-up, click **Automatic command**.
5. Add the data element to the end of the command line.
   - For example, `"<$WBEM:TargetInstance.OriginalText>"`
6. Click **OK**, and then click **OK** again.
7. On the Rules tab of the policy, under Rule Summary, locate the **Start Automatic Command** block, and verify that the new parameter has been added.

The following is a representation of the Start Automatic Command block with the added custom data element. The custom parameter is the original text of the Event, "<$WBEM:TargetInstance.OriginalText>":

```
Start Automatic command (cmd /c cscript.exe /NoLogo %XMOMW%omw.vbs
"hpomw" "OPERATIONS MANAGER EVENT" "no"
"<$WBEM:TargetInstance.Severity>" "<$WBEM:TargetInstance.Id>"
"<$WBEM:TargetInstance.MessageGroup>" "<$WBEM:TargetInstance.NodeName>"
"<$WBEM:TargetInstance.Application>" "<$WBEM:TargetInstance.Object>"
"<$WBEM:TargetInstance.TimeCreated>" "<$WBEM:TargetInstance.TimeReceived>"
"<$WBEM:TargetInstance.ServiceId>" "<$WBEM:TargetInstance.Source>"
"<$WBEM:TargetInstance.OriginalText>")
```

Within the `omw.vbs` enrichment and injection script, this custom parameter must be retrieved from the injected message received from HPOM for Windows.

To retrieve the custom parameter from the injected message:

1. Determine an appropriate name for the parameter and instantiate it within the Globals section at the beginning of the script.
   - For example, `Dim apdt_original_text`
2. To retrieve this parameter add a line to the ProcessArguments Sub method:

```
apdt_original_text = Trim( args.Item( 13 ) )
```

Note: *The* `args.item(#)` *must match the location of the custom parameter within the Start Automatic Command block of the policy. This number starts at 0, where 0 matches* `"hp_operations_manager_win"`*, the first parameter after the executed application name (*`%APOMW%\omw.vbs`*).*

Alternately, you can retrieve custom parameters through WMI Objects within the `omw.vbs` script.

To retrieve a parameter using WMI:

1. Determine if the parameter is associated with the OV_Message or OV_ManagedNode Objects, and the name of the desired field
2. The WMI Object Browser is useful in making this determination.
3. Within the retrieveNodeAndNodeGroups Sub method, after the Node or Message Object has been retrieved, set the custom parameter to the value of the associated field:

```
apdt_original_text = HPWMIMessageObject.OriginalText
```

OriginalText is an example field, and is the same as the parameter injected through the xMatters policy in HPOM for Windows.

4.2.2 Adding new parameters to notification content

Once you have injected the new data elements, you can add the token as a parameter to the notification content for Devices. The following steps explain how to add the custom parameter to email notifications; adding content for other Device types is similar and requires the presentation script to be modified for the specific Devices.

To add a new token to email notification content:

1. Open the xMatters Developer IDE and check out the HP Operations Manager for Windows (BUSINESS) Script Package.
2. Open the PRESENTATION > deviceContentEmail script, and locate the following line:

```
@messageContent::put( "Duplicate Count", $event.duplicate_count )
```

3. Add the following below the Duplicate Count line; replace "custom_token" with the name of the custom token you added in the previous section:

```
@messageContent::put( "custom_token", $event.custom_token )
```

4. Save, validate, and check in the script.

Your custom parameter should now appear in the notification content for email Devices. Repeat the above steps for each Device content creation section (such as deviceContentBES for BlackBerry Devices) to which you want to add the new parameter.

4.3 Policy Customizations

Each time you want to add additional conditions for notification, you must add an additional rule to the integration's **Forward message to xMatters** Policy.

4.3.1 FYI Notifications

FYI notifications are informational only; they are delivered to recipients with no expectation that the recipients will act upon the notification. Regular, or non-FYI, notifications are delivered to recipients with an expectation that the recipients will act upon the event.

To generate FYI notifications from xMatters, the policy must be specifically changed to instruct the integration to deliver the notifications as FYI. In the out-of-the-box integration, the third parameter injected to the `omw.vbs` script is used to indicate whether the policy is generating FYI or non-FYI notifications.

Non-FYI:

```
cmd /c cscript.exe /NoLogo "%XMOMW%\omw.vbs" "hpomw" "OPERATIONS MANAGER EVENT" "no"
"<$WBEM:TargetInstance.Severity>" "<$WBEM:TargetInstance.Id>"
"<$WBEM:TargetInstance.MessageGroup>" "<$WBEM:TargetInstance.NodeName>"
"<$WBEM:TargetInstance.Application>" "<$WBEM:TargetInstance.Object>"
```

```
"<$WBEM:TargetInstance.TimeCreated>" "<$WBEM:TargetInstance.TimeReceived>"
"<$WBEM:TargetInstance.ServiceId>" "<$WBEM:TargetInstance.Source>"
```

FYI:

```
cmd /c cscript.exe /NoLogo "%XMOMW%\omw.vbs" "hpomw" "OPERATIONS MANAGER EVENT" "yes"
"<$WBEM:TargetInstance.Severity>" "<$WBEM:TargetInstance.Id>"
"<$WBEM:TargetInstance.MessageGroup>" "<$WBEM:TargetInstance.NodeName>"
"<$WBEM:TargetInstance.Application>" "<$WBEM:TargetInstance.Object>"
"<$WBEM:TargetInstance.TimeCreated>" "<$WBEM:TargetInstance.TimeReceived>"
"<$WBEM:TargetInstance.ServiceId>" "<$WBEM:TargetInstance.Source>"
```

Note: *Do not submit all HPOM for Windows events for notification. Tailor the policies to fit your specific business requirements and the capacity of your HPOM for Windows Server, xMatters Server and communications infrastructure.*

4.4 Response Choices

This integration allows recipients to respond to notifications with several default choices, some of which are injected back to the HPOM for Windows server, updating the original event. Users notified on email devices also have the ability to respond with an extra annotation message which will be logged in the original event.

The following is a list of the default response choices available with the integration and their associated actions on the xMatters Event and the HPOM for Windows event:

Response Choice	xMattersAction	HPOM for Windows Update	Default Device Availability
Acknowledge	Delinks everyone from the xMatters event (deletes/terminates the event), and halts notifications from being delivered. **Note**: If FYI Subscriptions are being delivered, they are allowed to finish.	Removes the message for the active messages browser view and puts it in the acknowledged message browser.	Email, BES, Browser. For other non-FYI mobile devices an Acknowledge is represented as an Ack.
Own	Delinks all users other than the responder from the event, not allowing them to submit responses. The owner will not be notified further, but has the ability to affect the event by responding on one of their Devices or from the browser. For example, a User owns the event in xMatters, and then changes the severity of the event. They may also acknowledge or annotate the owned event.	The owner gains exclusive read/write access to the message. Other users can see the message, but have limited access.	All non-FYI devices.

Response Choice	xMattersAction	HPOM for Windows Update	Default Device Availability
Ignore	Signifies that the User rejects the notification. The rejection causes the action script to escalate to the next recipient in the Group.	A reject message is sent back to HPOM for Windows and logged as an Annotation; it has no effect on the state of the message.	Email, BES and Browser. For other non-FYI mobile Devices an Ignore is represented as an Ign.
Change Severity	Halts delivery of notifications to any other Devices the responding User may have configured. Delinks all Users other than the User changing the severity.	Handles the changing of the message severity. Possible severities: • Critical • Major • Minor • Warning • Normal Owns the HPOM for Windows message as though the severtity was changed in the console.	Email, BES and Browser. If notified on a phone Device, the option to change severity is provided as a phone menu. (Can only change the severity up or down, but have unlimited number of times to do so; i.e., it requires four times to go from critical to warning.)
Annotate	Halts delivery of notifications to any other Devices the responding User may have configured.	Allows the User to provide a message to be posted to the annotation of the message. When an annotation is provided the state of the message does not change.	This functionality is available for text-based Devices only.

4.4.1 Responses for FYI notifications

FYI notifications do not have any response choices available, except for FYI notifications sent to voice Devices. Voice FYI notifications offer the following response choices so that Users can navigate between multiple notifications. (This navigation is not required on other Devices.)

Voice Device responses for FYI notifications

Response	Description
Delete	Removes the notification from the User’s list. This option is most likely to be selected.
Save	Saves the notification and stops attempting to deliver it to the User’s other Devices. Users may select this option to delay listening to the notification when it is delivered, and access the details by calling in, or via the xMatters web user interface, at a later time.
Repeat	Replays the notification content.

4.5 Altering the duration of events

You can modify the amount of time xMatters will send out notifications for a particular event before it times out by changing the "timeout" Event Domain Constant. This constant stores the number of seconds the notifications will be allowed to continue before timing out.

For example, if you wanted to change the event duration to two hours, you could change the value for the timeout constant to **7200**.

Note: *For more information about working with Event Domain Constants, see "Configuring the Event Domain" on page 28.*

4.6 Uninstalling

For instructions on removing an xMatters deployment, refer to the *xMatters installation and administration guide*.

Chapter 5: Configuration Variable Reference

This section outlines and describes the configuration variables available in the initial PROCESS Action Script.

Note that many of the configuration variables are configurable using the Event Domain Constants, as described in "Configuring the Event Domain" on page 28; those variables are not listed here.

5.1 Global configuration variables

These variables are available throughout the script package, and are parameters of the “main” object. The value assigned to each variable is its default value within the script.

Gobal variables

Variable	Description
$main.use_logFile = false	Specify whether to use an alternate log file for debugging messages. This variable is ignored unless $main.debug is also set to true.
$main.logFile = "../logs/"	Defines the file used to log debugging information (only if $main.use_logfile is set to true).
$main.logo_alt_text = “[If the logo does not appear you may be blocking images or you may be outside a firewall. If the latter, the links will not work for responding and you should respond by replying to this email as described below.]”	The alternate text to display if the HTML email logo is unavailable. **Note**: If the logo does not display, it is unlikely that the HTML_form_url is valid and responses will not be injected from HTML Devices (email and BES).

(x) matters

1-877-xMattrs

12647 Alcosta Blvd., #425
San Ramon, CA 94583 USA
+ 1.877.962.8877

Central Court 25 Southampton Buildings,
London WC2A 1AL UK
+ 44.0.20.3427.6326