xMatters *(IT)* engine

FOR BMC PROACTIVENET PERFORMANCE MANAGEMENT

This manual provides information about xMatters. Every effort has been made to make it as complete and accurate as possible; however, the information it contains is subject to change without notice and does not represent a commitment on the part of xMatters No part of this document may be reproduced by any means without the prior written consent of xMatters

Tuesday, January 14, 2014

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
12647 Alcosta Blvd., #425
San Ramon, CA 94583

Sales and Technical Support:

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

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

This integration was designed and tested on an unmodified version of BMC ProactiveNet Performance Management, and this document describes how to configure xMatters to integrate with the default installation. If you have customized or altered your instance of BMC BPPM, 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 BMC ProactiveNet Performance Management. This document describes how to install and configure the xMatters (IT) for BMC ProactiveNet Performance Management software integration. The intended audience for this document is experienced consultants, system administrators and other technical readers.

1.1 Summary

xMatters enables any business process or application to trigger two-way communications (text, voice, email, SMS, push technology, etc.) throughout the extended enterprise. The company's cloud-based solution allows for enterprise-grade scaling and delivery during time sensitive events.

Through integration modules, xMatters can become the voice and interface of an automation engine or intelligent application (the Management System, such as BMC ProactiveNet Performance Management). When BMC BPPM 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 BMC ProactiveNet Performance Management. Responses are executed immediately on BMC BPPM, enabling remote resolution of the event.

This integration supports event notifications (from BMC BPPM to xMatters). It also supports inbound actions (from xMatters to BMC BPPM).

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 delivery 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.

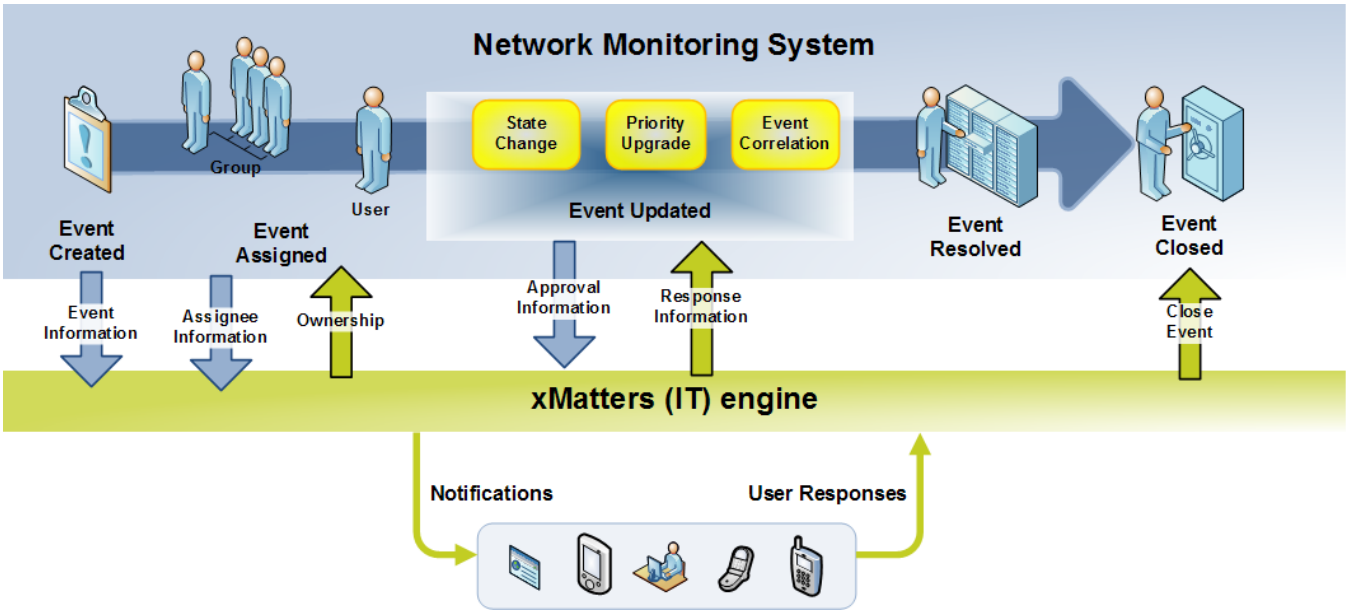
Once a response is selected on the recipient’s remote device, xMatters will update the BMC BPPM event in real-time. The benefit is that this process is immediate – significantly faster than the time required for staff to notice the failures or malfunctions, determine who is on call, and manually notify 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 BMC BPPM event with status information.

The xMatters product features a self-service web user interface to allow accurate assignment of responsible personnel for each job.

1.1.2 Information Workflow

The following diagram illustrates a standard incident workflow in a network monitoring system, and how information from the management system is passed into xMatters (IT) engine:



1.2 Integration features

This section describes the main features of the xMatters (IT) for BMC ProactiveNet Performance Management integration. Note that the following descriptions assume some familiarity with BMC BPPM terminology and concepts, such as Selectors, Notification Policies and Notification Services.

This integration supports the injection of events into xMatters from BMC BPPM, and the updating of BMC BPPM events by xMatters when users respond to notifications.

1.2.1 Automatic notifications

BMC BPPM injects events via Notification Policies; each Policy definition includes the following components:

- a Selector with search criteria that determine which events the policy will handle;
- a target to receive the notification of matching events; and,
- a Notification Service that delivers the events.

The injected events can be standard events or FYI events. FYI events have an FYI event token set to *true*, and have limited user response choices available in xMatters. While they are handled similarly to notifications generated by one-way subscriptions in xMatters, they are flagged as FYI within BMC BPPM.

The integration uses two xMatters Notification Services: one delivers standard events while the other delivers FYI events. BMC BPPM administrators can configure multiple Notification Policies that select events to be delivered as standard or FYI notifications.

1.2.2 Manual notifications

The integration includes a set of Knowledge Base files that define a set of Actions that are added to the Remote Actions / Diagnostics menu in BMC BPPM. These allow users to manually send standard or FYI notifications, or to request that an existing notification be stopped.

1.2.3 xMatters custom slots

The integration extends the definition of the EVENT class to add a slot called "is_replied_from_XM", used as follows:

- Whenever the xMatters integration agent processes a response from a user, it sets the is_replied_from_XM slot to "Yes" (and any other entries that may be added to the event Logs and Notes).

1.2.4 xMatters Collectors

The integration also includes a set of BMC BPPM Collectors, grouped under the heading of "Notified Events", that list events for which the is_replied_from_XM slot is "Yes".

1.2.5 User response choices

Users who receive event notifications via xMatters will have a set of response choices:

- Set the event status to Acknowledged
- Set the event status to Closed
- Accept the event (no status change, but the User becomes the assignee for the event)
- Ignore the event (no status change)

On voice, BES (BlackBerry), and email Devices, the User also has access to a set of diagnostic responses that will run ping and traceroute commands on the xMatters integration agent.

Note: *For more information about these features, see "Response choices" on page 27.*

1.3 Integration Architecture

The software components in this integration include:

- xMatters (IT) engine
- BMC ProactiveNet Performance Management
- BMC Impact Integration Web Services v9.0
- xMatters integration agent

BMC BPPM injects events into xMatters based on user-defined Notification Policies. Each Notification Policy refers to a BMC BPPM Selector that must be defined to select appropriate events according to the needs of the integration.These Notification Policies must use one of a pair of included Notification Services that inject events by executing xMatters Command Files that in turn execute APClient.bin to interact with the xMatters integration agent. The Command Files are also used to manually stop notification requests.

The integration agent updates events in BMC BPPM using an instance of the BMC Impact Integration Web Services v9.0 (IIWS) that must be installed and configured to connect to the cell associated with the BMC BPPM instance. Note that the IIWS are not used to inject events.

1.3.1 Event workflow

BMC BPPM can inject two types of events into xMatters using two different mechanisms.

Each event can be marked as standard or FYI at the time it is injected into xMatters. The difference is that FYI events will have a limited set of available response choices compared to standard events.

Note: *FYI events from BMC BPPM are unrelated to FYI notifications generated by xMatters as a result of one-way or FYI Subscriptions.*

Automatic notifications

The integration generates automatic notifications based on Notification Policies in BMC BPPM that can be configured by the Administrator. A Notification Policy references a Selector that selects events based on its search criteria: when an event is

updated or modified to match the Selector criteria, a notification is sent to the xMatters User or Group that is specified as the target of the Notification Policy.

The default integration includes templates for Notification Policies and Selectors that will inject standard and FYI events, but each xMatters deployment will need to create Notification Policies and Selectors to meet its requirements.

Manual notifications

A BMC BPPM user can inject events for notification manually using the BMC BPPM Operations Console. They can send standard or FYI event notifications to a specific User by selecting the Tools icon for an event and then choosing from the Remote Actions/Diagnostics menu. This menu also allows the user to send a stop notification request.

1.4 System Requirements

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

- xMatters (IT) engine 5.0 (patch 010 or later).
- xMatters integration agent 5.0 (patch 007 or later)
- BMC ProactiveNet Performance Management 9.0.50
- BMC Impact Integration Web Services v9.0

1.4.1 Operating Systems

The following component versions, operating systems, and databases are supported by this integration:

Integration Component	Version	Operating System	Database
xMatters (IT) engine	5.0 (patch 010 or later)	Microsoft Windows 2012 (validated) Linux CentOS 5.3 (validated)	Microsoft SQL Server 2008 (validated) Oracle 11g
xMatters integration agent	5.0 (patch 007 or later)	Microsoft Windows 2012 (validated) Linux CentOS 5.3 (validated)	
BMC ProactiveNet Performance Management	9.0.50	Microsoft Windows 2012 (validated with Microsoft SQL Server 2008) Linus CentOS 5.3 (validated) All operating systems supported by the xMatters integration agent	

1.5 Conventions and Terminology

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

1.5.1 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 is `C:\Program Files\xMatters\`
- On Unix systems, 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\integrationagent`.
- On Unix systems, the default is `/opt/integrationagent`.

1.5.2 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 monitoring or managing software that watches for events, and with which xMatters can combine; i.e., a synonym for BMC BPPM.
Device	The medium through which a recipient is contacted by xMatters; 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 user guide*.

Chapter 2: Installation and Configuration

This chapter provides information about installing the xMatters (IT) for BMC ProactiveNet Performance Management integration. This chapter also contains complete instructions on how to configure xMatters, BMC BPPM, and the integration components.

2.1 Installing the integration

The instructions in this chapter do not include information on how to install the xMatters (IT) engine, integration agent, BMC Impact Integration Web Services v9.0,or BMC ProactiveNet Performance Management. These components must be installed according to their related documentation, and operating properly before you can proceed with the integration.

The integration agent updates events in BMC BPPM using an instance of the BMC Impact Integration Web Services v9.0 (IIWS) that must be installed and configured to connect to the cell associated with the BMC BPPM instance.

For more information about installing xMatters (IT) 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
bmcbppm20.xml	The main configuration file for the integration; identifies the integration to the Integration Agent and specifies the mappings to xMatters event tokens of BPPM event slots provided by the APClient.bin command tool.
bppm-config.js	Defines constants used by other JavaScript files, including the endpoint URL of the BMC Impact Integration Web Services v9.0, name of the BMC BPPM cell, other IIWS constants, and the name of the event deduplicator filter.
xM-BMC-BPPM-20.xml	Event Domain package containing pre-configured Event Domain, Action scripts, predicates, and Event Domain Constants.

In addition, the integration depends on these files that will be installed in the BMC BPPM Knowledge Base (locations are relative to the root of the Knowledge Base):

File	Location	Description
xm_classes.baroc	classes	Adds xMatters-specific slots to the base EVENT class.
xm_actions.mrl	bin	Defines xMatters actions available on the tools menu for an event that allows manual notifications (normal and FYI) and stop notification requests.
xm_notification_policy.baroc	data	Defines template selectors and notification policies.
xm_notification_service.baroc	data	Defines notification services used by notification policies and remote actions.

File	Location	Description
xm_associate.mrl	rules	Defines Knowledge Base rules: • **correlate_for_stop_notification**:that issues a stop notification for a critical event if a non-critical event with similar host and object details is created.
xm_collectors.mrl	collectors	Defines the "Notified Events" collectors accessible in the BMC BPPM web user interface that filter events that have been notified via xMatters, or for which there has been a user response.
xm_send_notification.bat **xm_send_fyi_notification.bat** **xm_delete_notification.bat**	bin/w4	xMatters Windows command files that assemble BMC BPPM event slot information from environment variables and invoke APClient.bin.
xm_send_notification **xm_send_fyi_notification** **xm_delete_notification**	bin/l2	xMatters Linux command files that assemble BMC BPPM event slot information from environment variables and invoke APClient.bin.

2.1.2 Installing the integration service

To configure the integration agent for the BMC BPPM 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.

If you have more than one integration agent providing the BMC BPPM service, repeat the following steps for each one.

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-BMC-BPPM\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 `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\IAConfig.xml` and add the following line to the “service-configs” section:

```
<path>bmcbppm20/bmcbppm.xml</path>
```

4. Open the `<IAHOME>\integrationservices\bmcbppm20\bppm-config.js` file and modify the following variables:

Setting	Description
BBPM_CELL	Specifies the name of your BMC BPPM cell.
IIWS_URL	If the BMC Impact Integration Web Services v9.0 are running on the same server as the BMC BPPM server and the xMatters integration agent, this setting can be left unchanged. Otherwise, change the host name in the URL to that of the server on which IIWS is running.

Setting	Description
IIWS_BUFFER_TYPE	Specifies the bufferType parameter used by the IIWS Connect operations. The default value is BMCII_BUFFER_MODE_DEFAULT. For more information about other settings, see the BMC Impact Integration Web Services v9.0 documentation.
IIWS_SEND_EVENT_TIMEOUT	Specifies the timeout parameter for the IIWS SendEvent operation; default value is 3000 ms.
IIWS_RETRIEVE_QUERY_RESULTS_TIMEOUT	Specifies the timeout parameter used by the IIWS RetrieveQueryResults operation; default value is 3000 ms.
ANNOTATE_DELIVERY	If set to *true*, specifies that BMC BPPM should use Event Notes to record delivery of notifications to user devices.
DEDUPLICATOR_FILTER	Specifies the name of the filter used by the integration agent's deduplicator module, which prevents duplicate events from being injected into xMatters; the default value is "bmcbppm20". For more information about the deduplicator module, see "Filtering and suppression" on page 29. Note that the deduplication filter is cleared whenever the integration agent is restarted; this means that after a restart, events that would otherwise be filtered may be injected into xMatters.

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 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.

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 English voice files would be as follows:

```
<xMHOME>\node\phone-engine\Datastore\1\bmcbppm20\recordings\english\phrases
```

Note that if this is the first custom Event Domain you have created, the <FILE_IDENTIFIER> directory will not have been created yet. You can create it manually or log into xMatters and use the web user interface to add a new voice recording. If the Phone Device Engine is running, xMatters will create the directory structure and place the new voice recording in it.

2.2 Configuring xMatters

The following sections describe how to configure xMatters to combine with BMC BPPM.

2.2.1 Importing Event Domain

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 22.*

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 xM-BMC-BPPM-20.xml file extracted from the integration archive.
5. Click **Open**, and then click **Upload**.

xMatters imports the integration configuration settings and displays the new bmcbppm20 Event Domain.

Defining an Integration Service

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

To define an Integration Service:

1. In xMatters, on the Event Domains page, click the **bmcbppm20** 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**: bmcbppm20
   - **Description**: BMC BPPM Integration Service
4. Click **Save**.

Specifying connection parameters

Once you have imported the Event Domain package, you can specify the correct values for the imported Event Domain Constants.

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 bmcbppm20, 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):

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 xmattersurl 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 `$main.xmatters_url` variable.
bespushurl	http://localhost:8888/static	Used to specify the address of the BES device server. Populates the `$main.bes_pushurl` parameter.

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 23.*

2.2.2 Configuring Subscriptions

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

- Define a Subscription Domain
- Create a Subscription
- Create a fail-safe Group

The criteria you can use to create Subscriptions are based on the available Event Domain predicates, which are defined when you import the Event Domain package, as described in "Importing Event Domain" on page 9. For more information about the default predicates available, and instructions on how to modify them, see "Defining Event Domain predicates" on page 22.

Defining a Subscription Domain

The Subscription Domain is the reference point of the optional Subscription panel 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 with the new panel.

To create a Subscription Domain:

1. On the Developer tab, in the Domains menu, click **Subscription Domains**.
2. On the Subscription Domains page, click **Add New**.
3. In the **Event Domain** drop-down list, select **bmcbppm20**, and then click **Continue**.
4. On the Subscription Domain Details page, in the **Name** field, type `BMC BPPM`.
   - By default, Subscriptions are non-FYI (i.e., they support response options). To disable two-way Subscription notifications, select the **One-Way** check box.
5. In the **Type of Management** drop-down list, select **Both**.
6. Click **Continue**.
7. 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”, “Close”, “Accept” and “Ignore”. To enable two-way communications for Subscriptions, define all four response choices on the Select Appropriate Response Choices page. If you require only one-way, informational notifications, do not specify any response choices.

8. On the Select Appropriate Predicates page, add all of the predicates to the **Applied Predicates** list, and then click **Continue**.
9. 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.

Creating a Subscription

Once you have created a Subscription Domain, you can create and assign Subscriptions to notify recipients about events that match specific criteria.

To create a Subscription:

1. On the Alerts tab, in the Alerts menu, click **Assign Alerts**.
2. Select the BMC BPPM 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.
4. In the Recipients area, specify the Users that should receive notifications for this Subscription.
5. When you are satisfied with the criteria, click **Save** to create the Subscription.

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, xMatters sends 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 BMC BPPM 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 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 "Defining Event Domain Constants" on page 23.*

2.3 Configuring BMC BPPM

The following sections describe how to configure BMC BPPM to combine with xMatters.

2.3.1 Deploying integration files

The following variables refer to specific paths used within this section’s examples:

- `$CELL` refers to the integrated cell name.
- `$xM_CMD` refers to the extracted `\components\bmcbppm20\xM Command Files` folder

- $xM_KB refers to the extracted \components\bmcbppm20\kb folder
- $KB refers to the \pw\server\etc\$CELL\kb folder in the BMC BPPM installation directory.

Note: *For Unix installations, commands should be executed in the* /opt/mcell/bin *directory, unless this path has been added to the $PATH variable.*

2.3.2 Deploying the xMatters command files

1. In the extracted integration archive folder, locate the xm_send_notification, xm_send_fyi_notification, and xm_delete_notification files; by default, they are located in the $xM_CMD\windows or $xm_CMD/linux directory.
2. Open each file in a text editor and ensure the path of the xMatters integration agent is correct; for the default locations, refer to "Conventions and Terminology" on page 4.
3. Copy all three files to the $KB\bin\w4 (Windows) or $KB\bin\l2 (Linux) folder containing the command files on the integrated cell.

Note: *The account under which the cell is running must have permission to execute the command files.*

2.3.3 Deploying Baroc and Rule files

The next step is to deploy the .baroc and .mrl integration files into the $KB directory of the integrated cell. Load the following files into their appropriate directories on the integrated cell.

Note: *The .load files to be modified are read-only; their file properties must be changed before you can edit them.*

xm_actions.mrl (located in $xM_KB\bin)

1. Copy this file to $KB\bin.
2. Add a line containing “xm_actions” to the .load file located in $KB\bin.

Note: *The Actions defined in* xm_actions.mrl *allow users to manually send notifications to xMatters, and to request that a notification in xMatters be stopped. The action definitions include the roles that users must have assigned to them in order to access these actions in the Operations Console. Review the roles specified in* xm_actions.mrl *and ensure that they match the roles assigned to users who should have access to these actions.*

xm_classes.baroc (located in $xM_KB\classes)

1. Copy these files to $KB\classes.
2. Add a line containing “xm_classes” to the .load file located in $KB\classes.

xm_collectors.mrl (located in $xM_KB\collectors)

1. Copy this file to $KB\collectors.
2. Add a line containing “xm_collectors” to the .load file located in $KB\collectors.

xm_associate.mrl (located in $xM_KB\rules)

1. Copy this file to $KB\rules.
2. Add a line containing “xm_associate” to the .load file located in $KB\rules.

Workaround for BMC BPPM v9.0

A known issue with BMC BPPM v9.0 requires a change to the core BPPM Knowledge Base file im_policies.baroc.

Note: *The workaround is documented in the BMC BPPM release notes for BMC BPPM 8.6 patch 2. (Under "Open issues and workarounds in BMC ProactiveNet Server" the issue is listed with Tracking ID QM001711954.)*

To apply the workaround:

1. Open the file `$KB\classes\im_policies.baroc`.
2. In the definition of the IM_POLICY class, locate and change the line:

```
selector_ecf : ECF CORE_EVENT;
```

to

```
selector_ecf : ECF EVENT;
```

Compiling files

Execute the following command to re-compile the files added to the `$KB` directory of the integrated cell (`mccomp` is located in the `\pw\server\bin` folder within the BMC BPPM installation directory):

```
mccomp -n $CELL
```

If the command executed properly, the last line should state: “Compilation ended successfully”

`xm_notification_policy.baroc` and `xm_notification_service.baroc` (located in `$xM_KB\data`)

1. Copy these files to $KB\data.
2. To load the contents of these files into the BMC IM database, execute the following commands:

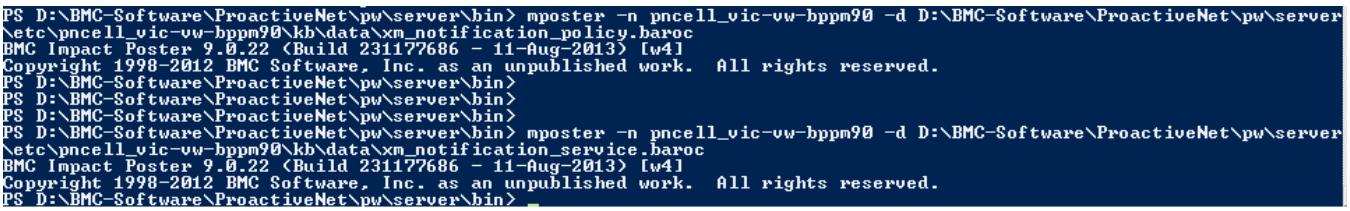
```
mposter -n $CELL -d $KB\data\xm_notification_policy.baroc
```

This command creates inactive Notification Policies which can be used as templates for new Notification Policies.

```
mposter -n $CELL -d $KB\data\xm_notification_service.baroc
```

This command creates Notifications Services that will be used by your new Notification Policies.

Successful execution of these commands should result in the following output:

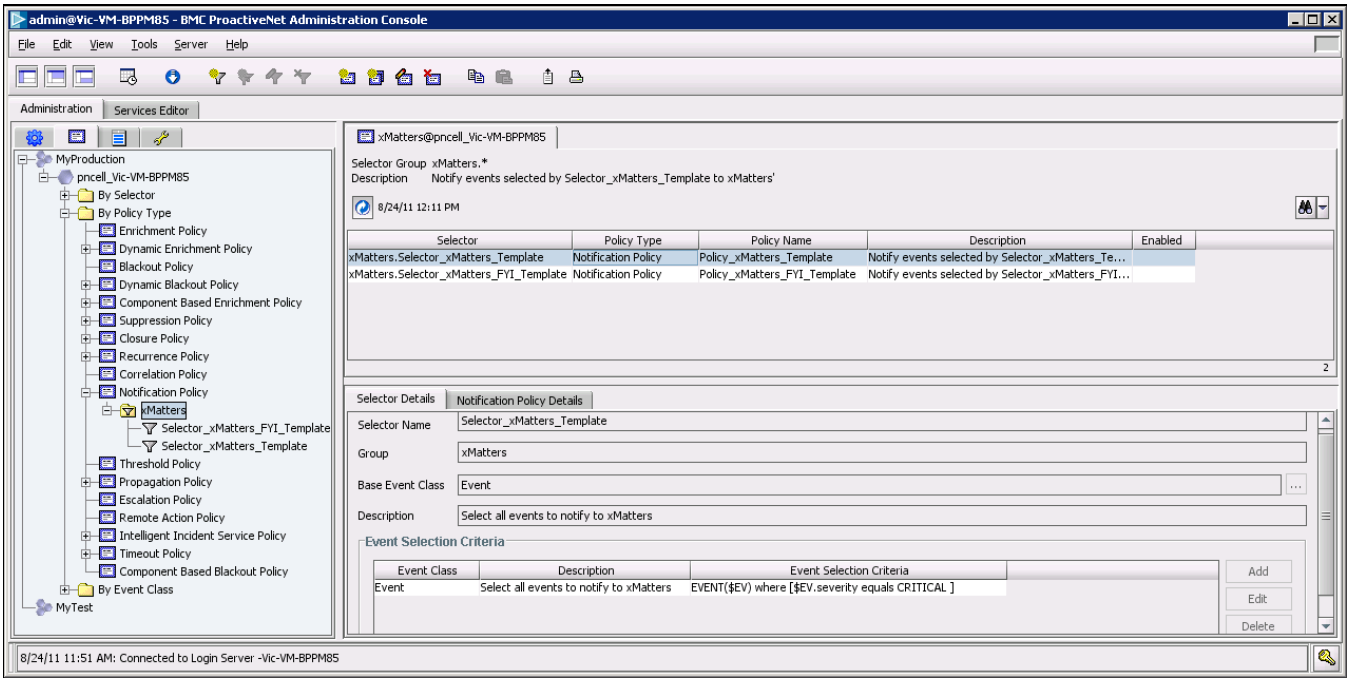


After completing the above steps, restart the BMC BPPM server.

To review the Notification Policies:

1. Launch the BMC ProactiveNet Administration Console.
2. Under the Administration tab, click the **Event Management Policies** tab.
3. Open the production node for your BMC BPPM cell.
4. Open the **By Policy Type** folder, and then open the **Notification Policy** folder.

Inside the Notification Policy folder should be a folder called xMatters, containing the selectors called "Selector_xMatters_ Template" and "Selector_xMatters_FYI_Template". These selectors should have Notification Policy details referring to policies called "Policy_xMatters_Template" and "Policy_xMatters_FYI_Template".

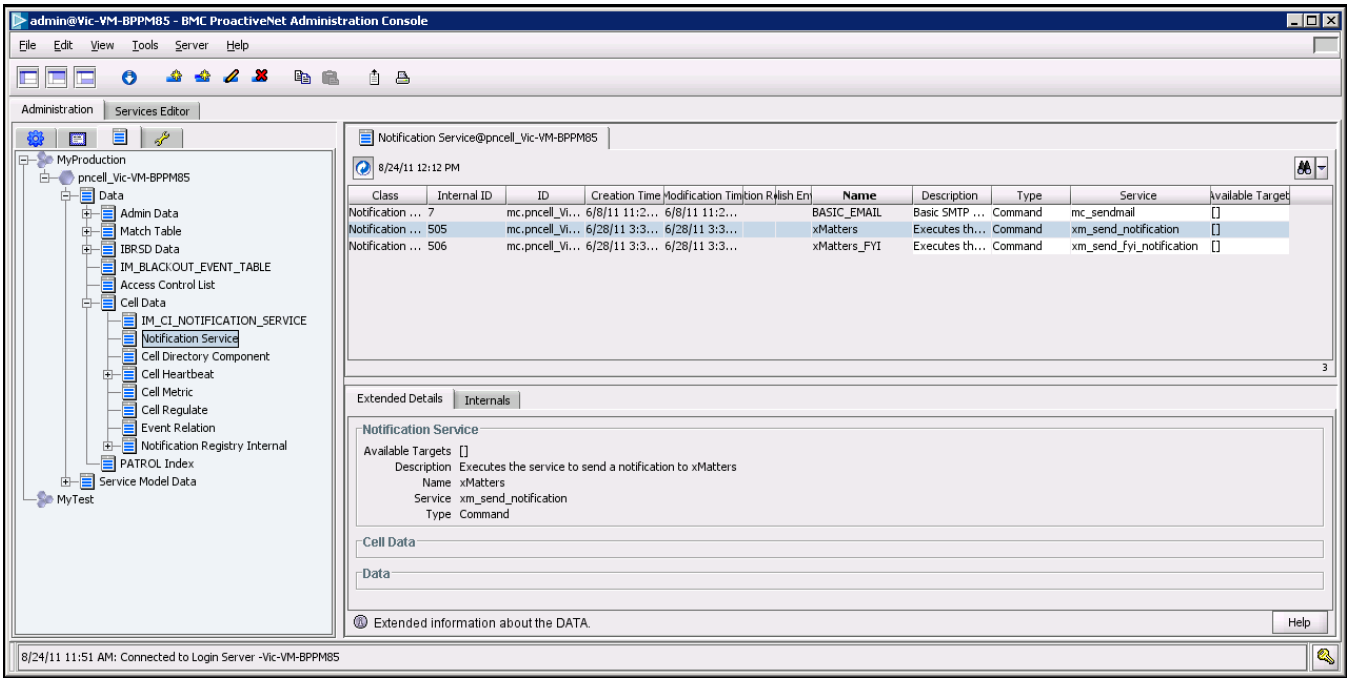


The Notification Policies should also reference Notification Services called "xMatters" and "xMatters_FYI".

To review the Notification Services

1. Launch the BMC ProactiveNet Administration Console
2. Under the Administration tab, click the **Dynamic Data Editor** tab.
3. Open the production node for your BMC BPPM cell.
4. Open the nodes **Data** and **Cell Data**, then click on the node **Notification Service**.

This should display a list of Notification Services, including services named "xMatters" and "xMatters_FYI".



2.3.4 Configuring notifications

After installing the integration, you must create your own Selectors and Notification Policies using the ProactiveNet Administration Console, or by creating and compiling baroc files in your BPPM Knowledge Base. You can use the template Selectors and Notification Policies as a starting point, or you can define your own Selectors and Notification Policies provided the Notification Policies you create refer to one of the xMatters Notification Services provided with the integration.

The xMatters and xMatters_FYI Notification Services can be used without modification and must be the Notification Services associated with any Notification Policy intended to forward events to xMatters.

If you create Notification Policies by copying the template Notification Policies supplied with the integration, make sure you enable your new Notification Policies.

Note: *For more information on defining Event Management Policies, see the BMC BPPM documentation.*

Chapter 3: Integration Validation

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

- BMC ProactiveNet Performance Management
- BMC Impact Integration Web Services v9.0
- xMatters (IT) 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 BMC BPPM for notification delivery and response.

3.1 Triggering a notification

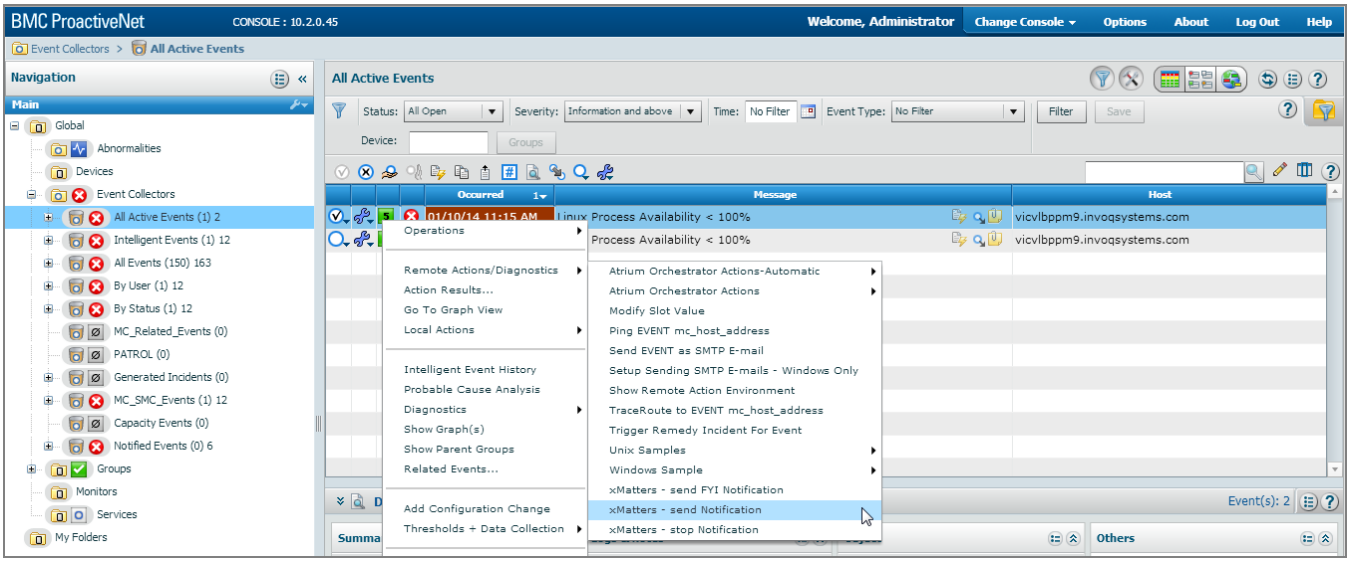
xMatters for BMC BPPM enables you to send manual and automatic notifications from BMC BPPM to xMatters. For both validation scenarios, confirm that you have a sample User in xMatters with a User ID of "bsmith" and an active Blackberry (BES) Device (the process is similar for other Devices).

3.1.1 Triggering a manual notification

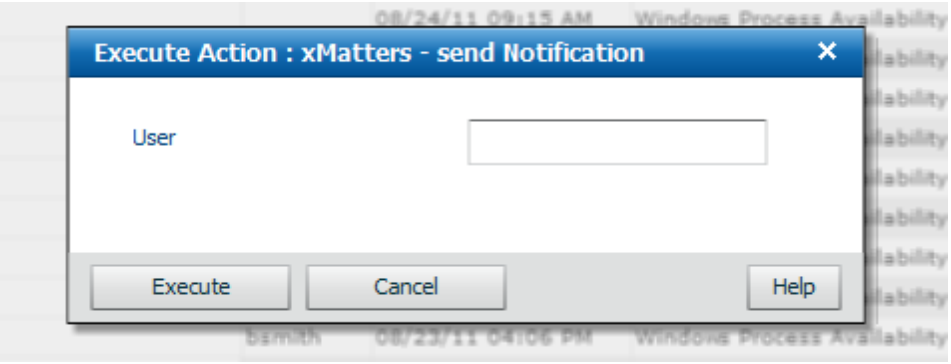
Use the following steps to trigger a manual notification.

To send a manual notification:

1. Log in to the BPPM Operations Console..
2. In the All Event Collectors pane, select the event for which you want to send a manual notification.
3. Click the **Tools** icon for the event, and then select **Remote Actions/Diagnostics > xMatters - send Notification**.
    - For FYI notifications, select **Remote Actions/Diagnostics > xMatters - send FYI Notification**.



4. In the Execute Action dialog box, enter the ID of the xMatters recipient you want to notify, and then click **Execute**:



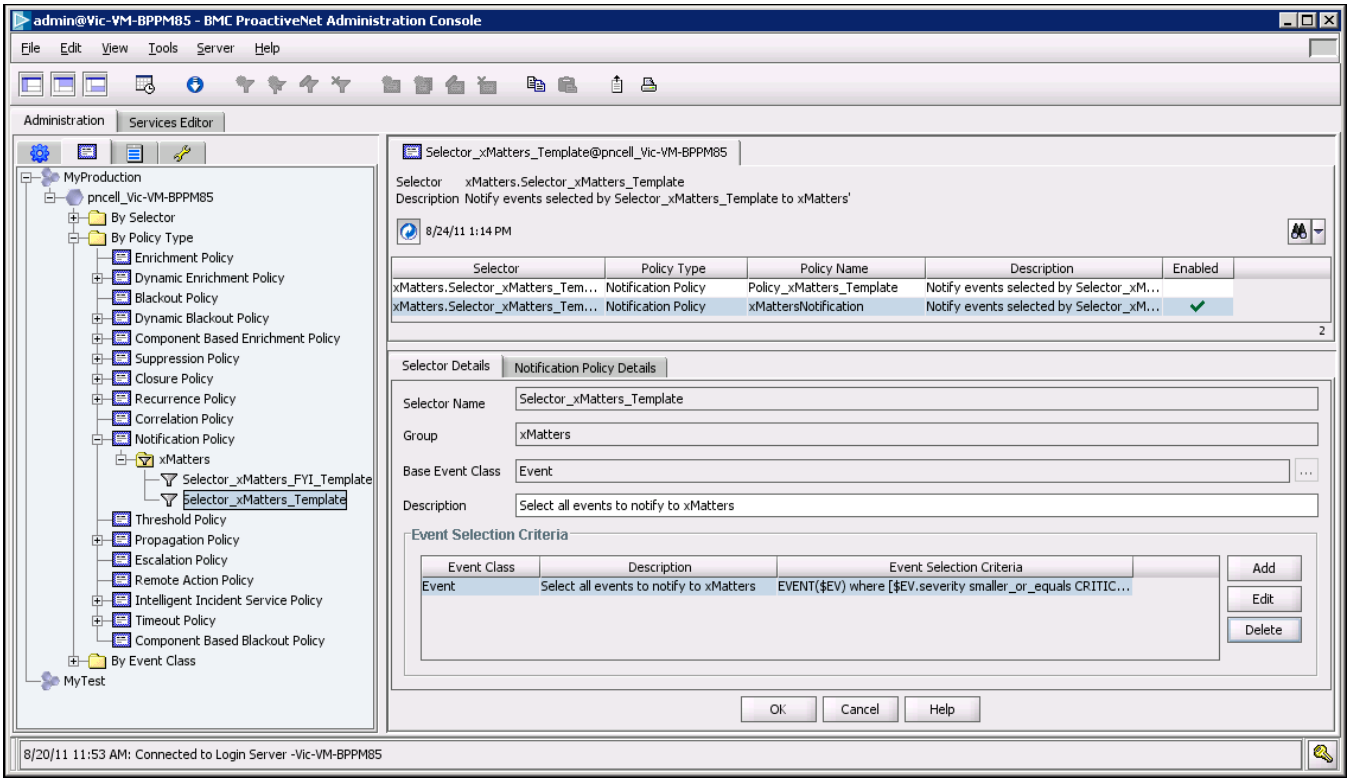
For information about viewing and responding to the notification, see "Responding to a notification" on page 19.

3.1.2 Triggering automatic notifications

Use the following steps to configure and send automatic notifications.

To send automatic notifications:

1. Log in to the BMC ProactiveNet Administration Console, and then select **Administration > Event Management Polices**.
2. To open the folders or nodes for your production cell, click **By Policy Type > Notification Policy > xMatters**.
3. Select **Selector_xMatters_Template**, and then select **Copy and Add Event Policy**.
4. Type a **Policy Name**, such as `xMatters_Notification`, and then enable the Policy.
   - Verify that the Notification Service is xMatters.
5. Edit the **Users to Notify** field, and add the User ID of the xMatters recipient you want to notify.
6. Click **OK** to save the new Notification Policy.
7. Click the **Selector Details** tab, and then click **Update Event Selector**.
8. Modify the selector criteria so the event severity is smaller than or equal to CRITICAL, as illustrated by the following figure:

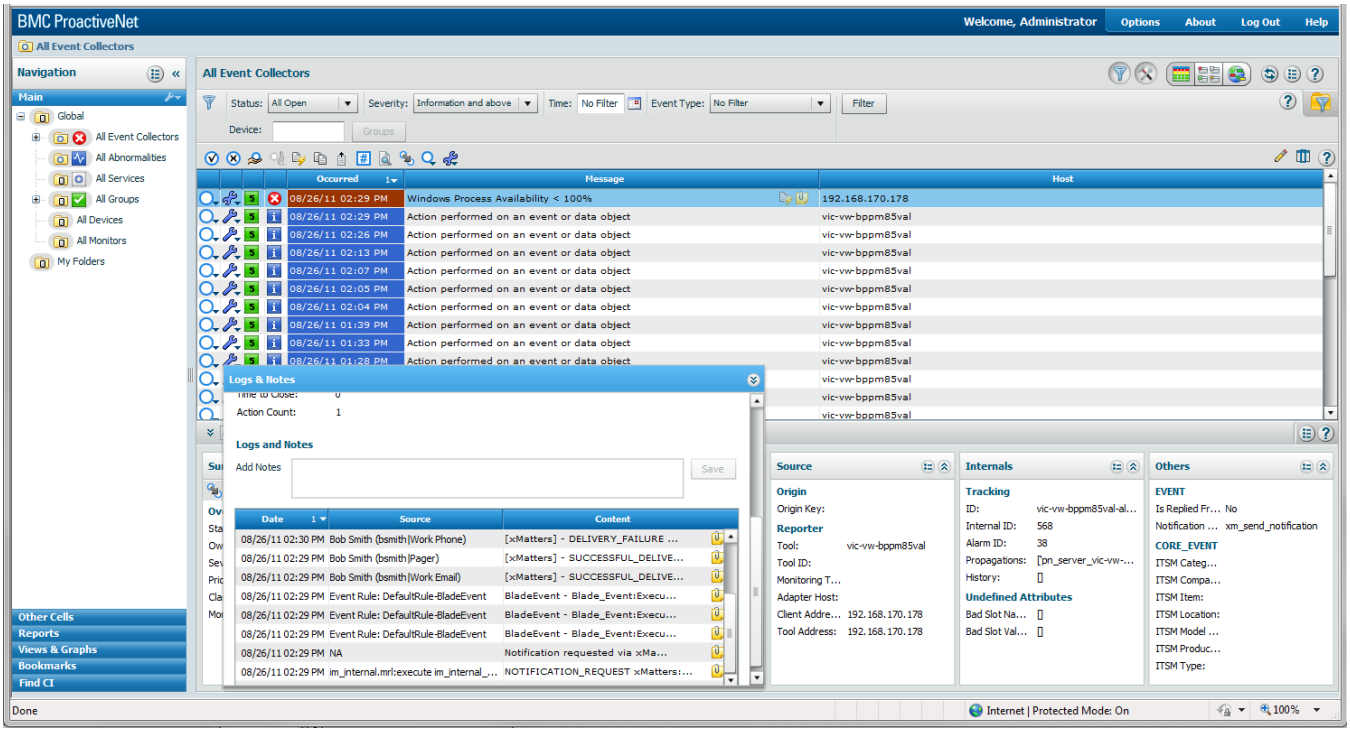


9. Click **OK** again to save changes.

Once you have configured the automatic notification, generate a new event in your BMC BPPM cell that will cause the recipient to receive a notification.

To view the event notification:

1. In the BPPM Operations Console., in the Navigation Pane, open **All Event Collectors > Notified Events > xMatters** and locate the event you generated.
2. Select the event, and then expand the **Logs and Notes** panel in the Details pane.
3. Ensure that there is an entry in the Operations Log stating that a NOTIFICATION_REQUEST was submitted to xMatters.
4. Close the Logs and Notes panel and wait for 30 seconds.
5. Re-open the panel and check the Operations Log: there should be entries confirming SUCCESSFUL_DELIVERY by xMatters to any validated User Devices:



For information about viewing and responding to the notification, see "Responding to a notification" on page 19.

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 via emai, but the process is similar for all Devices.

To respond to a notification:

1. When the notification arrives, open the email to view details about the BMC BPPM event:

Subject: xMatters (BPPM) Sev: CRITICAL Cell: pncell_vicvlbppm9.invoqsystems.com Incident: vicvlbppm9.invoqsystems.com-alr-62

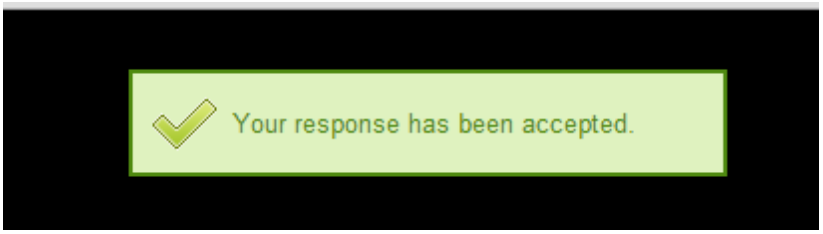
(x) matters
The relevance engine company.

BPPM - Automated Notification	
Target:	jquinn|Work Email
BPPM Event ID:	vicvlbppm9.invoqsystems.com-alr-62
Message:	Linux Process Availability < 100%
MC Host:	vicvlbppm9.invoqsystems.com
Severity:	CRITICAL
Event Time:	Monday, 13 Jan 2014 14:10:56 GMT-0800
Object:	Process = , Process Owner Name/ID = postfix/89
Object Class:	Linux Process
Tool:	vicvlbppm9.invoqsystems.com
Tool Class:	PNET
Parameter:	Availability

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

1. Acknowledge
2. Close
3. Accept
4. Ignore
5. Ping MCHostAddress
6. Ping EventOrigin
7. TraceRoute MCHostAddress
8. TraceRoute EventOrigin

2. Click a response choice at the bottom of the email to send that response back to BMC BPPM.
    - xMatters will open a browser window to indicate that the response was received and processed:

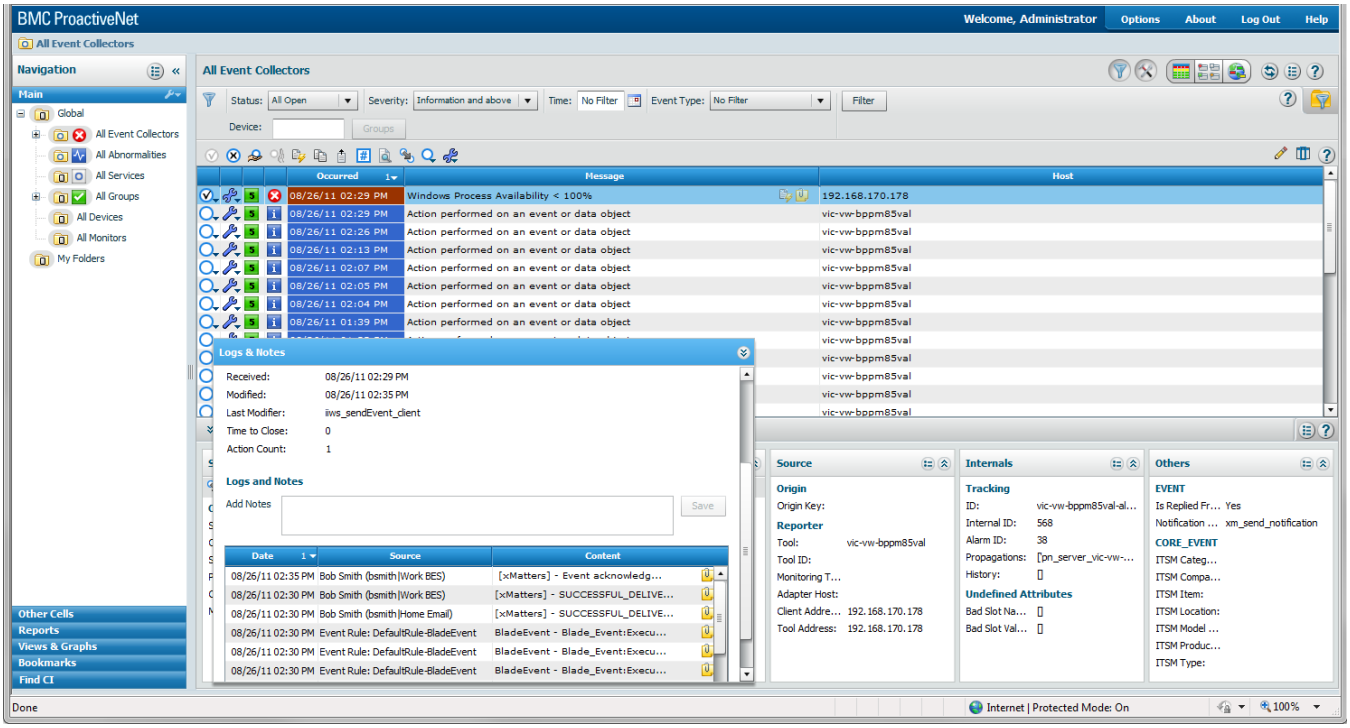


For more information about response choices, and changing the options available to Users, see "Response choices" on page 27.

3.3 Viewing response results

To view the results of the response, view the event Details in the BPPM Operations Console..

In the following example, the Status of the event has been updated to "Acknowledged", and the event Operations Log has been updated with additional entries to show the changes resulting from the User's response:



3.4 Testing the Subscription Panel

To test Subscriptions, ensure that you have created a Subscription (for more information, see "Creating a Subscription" on page 11). Trigger a notification that matches the criteria that you have configured your Subscription to match. You will receive a notification which may be informational-only, depending on your Subscription Domain configuration.

For more information on how to configure Subscriptions, see "Configuring Subscriptions" on page 10.

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 BMC ProactiveNet Performance Management 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. You must import the exported Event Domain for this integration to function, but the following sections explain how to manually configure and update the Event Domain Constants and predicates.

4.1.1 Configuring Users

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

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 user guide.

Defining Event Domain predicates

The default integration configuration uses the following Event Domain predicates:

- message
- status
- severity
- mc_priority
- mc_host
- client_address
- mc_object_class
- mc_object
- mc_parameter

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 26.*

To define Event Domain predicates:

1. In xMatters, click the **Developer** tab.
2. On the Event Domains page, click **bmcbppm20**.

3. On the Event Domain Details page, in the Predicates section, click **Add New**.
4. Add, remove, or modify the following predicates:

Event Domain predicates

Predicate	Type	Important	Values	Description
message	Text			Text description of the event.
status	List		• open • ack • assigned • closed • blackout	Status value of the event.
severity	List		• unknown • ok • info • warning • minor • major • critical	Severity value of the event.
mc_priority	List		• PRIORITY_5 • PRIORITY_4 • PRIORITY_3 • PRIORITY_2 • PRIORITY_1	Assigned priority of the event.
mc_host	Text			Fully-qualified name of the host on which the problem occured.
client_address	Text			Network address corresponding to the mc_host slot; can also contain some other type of information in situations in which a host value is not meaningful.
mc_object_class	Text			Identifies the class of an object
mc_object	Text			Sub-component of the host to which the event is related.
mc_parameter	Text			Name of the metric or property that triggered the event.

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 an xMatters client assistance representative before changing these values.

Note: *The values for the alarmpointurl 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 **bmcbppm20**.
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 xmattersurl 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 `$main.xmatters_url` variable.
bespushurl	http://localhost:8888/static	Used to specify the address of the BES device server. Populates the `$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.
enablediagnostics	true	Enables access to diagnostic menu options that allow Users to run ping and traceroute commands via the integration agent.
failsafegroup	BMC BPPM 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 (IT) engine and no subscriptions exist that match the event. Set this constant if you want to change the failsafe group from BMC BPPM Fail Safe to another group defined in xMatters.

Constant Name	Default Value	Description
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 `$use_emergency_devices` parameter.
trackdelivery	true	Track when each device is delivered to. Setting this to false may give a performance advantage, but you lose any information about whether a delivery was successful or not. Populates the `$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.

Constant Name	Default Value	Description
debug	false	Indicates whether to use the debug level for logging messages. Populates the `$main.debug` variable.

4.2 Adding new parameters

Additional data elements (or tokens) can be forwarded to xMatters by adding them in BMC BPPM. The following steps explain how to add a new event token to the event injected to xMatters.

Note: *For more information about which parameters may be available, refer to the BMC BPPM documentation.*

To add an event parameter:

1. Identify the name of the existing event slot you want to add as an event parameter.
2. On your BMC BPPM server, in the `bin\w4` (Windows) or `bin\l2` (Linux) Knowledge Base directory, open the xMatters command files, `xm_send_notification` and `xm_send_fyi_notification`.
   - These files assemble BMC BPPM event slot values taken from environment variables into a command line used to invoke `APClient.bin`.
3. Add the new parameter to the list of environment variables passed to `APClient.bin`.
4. Open the `bmcbppm20.xml` configuration file, and locate the mapped-input element.
5. Add an entry for the new parameter to the list in the mapped-input element.
   - Note that the order of the parameters in the mapped-input element must match the order listed in the xMatters command files. You can retain the name of the slot from BMC BPPM in the mapped-input element entries or assign a new name to the parameter.
6. Save and close the files.

4.2.1 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 BMC BPPM (BUSINESS) Script Package.
2. In the Presentation Action Script, add the following line to the email content creation section:

```
$content.message = $content.message & "TokenName: " & $event.tokenvalue    & "\n"
```

3. You can also add a check in the Initial script to confirm that the custom parameter was injected properly and exists within the Action Scripts:

```
IF ( ! EXISTS( $event. tokenvalue ) )
$event. tokenvalue = $undefined_default
IF ( $main.debug )
@script::log( $main.log_prepend & "Optional token ' tokenvalue '
not found, defaulting to '" & $event. tokenvalue & "'" )
ENDIF
ENDIF
```

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 Response choices

This integration allows recipients to respond to notifications with several default choices, some of which are injected back to the BMC BPPM 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, as described in "Adding annotation messages", below.

The diagnostic response options (email and voice Devices only) allow the User to execute the ping or traceroute command on the server that is hosting the xMatters integration agent. The user can specify the destination parameter for these commands to be either the event host address (slot mc_host_address, the host on which the problem occurred) or the event origin (slot mc_client_address, the host on which the adapter that sent the event is running).

Note that diagnostic responses have no xMatters job control, do not change event status or append annotation messages, and are not recorded in the event log in BMC BPPM.

The following is a list of the default response choices available with the integration, their availability based on the Device on which the notification is received, and their associated actions on the event in xMatters and the BMC BPPM event.

Response	BMC BPPM Update	xMatters Job Control	Device Availability
Acknowledge	Updates the status of the event to "Acknowledged", and records the response in the event log.	Delivered	BES, email, voice, text.
Ignore	No status change; records the response in the event log.	Delivered, notify next, delink responder.	BES, email, voice, text.
Accept	Updates the owner of the event to the responder (does not change the status), and records the response in the event log.	Delivered, delink all except responder	BES, email, voice, text.
Close	Updates the status of the event to "Closed", and records the response in the event log.	Delivered, delink all	BES, email, voice, text.
Annotate	No status change; adds the annotation text to the event notes in BMC BPPM.	Delivered	Email Devices only.

Note: *Users responding with voice Devices can also respond with "Event Details", which provides more information about the event than what is provided in the original notification.*

Job control definitions

The xMatters job controls in the above table are defined as follows:

- **Delivered**: marks the notification as delivered.
- **Notify next**: notifies the next recipient in the Group according to the defined escalation in xMatters.
- **Delink responder**: marks the notification as delivered, and stops the responder from performing any further action on the notification.
- **Delink all except responder**: marks the notification as delivered, and stops any recipients other than the responder from performing any further action on the notification.
- **Delink all**: marks the notification as delivered, stops any further action on the notification for all recipients, and terminates the event in xMatters.

The job control defined for each response choice is the default configuration for this integration; for more information about job control, and how to modify these actions in the scripts, see the *xMatters Online Developer's Guide*.

4.3.1 Changing and adding response choices

Changing or adding a response choice to the integration requires the following steps:

- Add or modify the response choice on the Subscription Domain (as described in "Defining a Subscription Domain" on page 10).
- Update the xMatters script to forward the response choice to the integration agent.
- Update the integration agent to send the response choice into BMC BPPM to perform the desired action on the originating event.

As an example, the following code illustrates adding a response choice of "Be there in 10 minutes" to the integration:

To forward the response choice to the integration agent, launch the xMatters Developer IDE and open the Handler script; make the following changes:

1. In the buildUserResponseMap script add:

```
@userResponseMap::put("be there in ten minutes", "be there in ten minutes")
```

2. In the processUserResponse script add:

```
IF ( $actionToken == "be there in ten minutes" )
GOSUB prepareAndSendServiceMessage

CALL sendAPDeliveredResponse
```

To send the response choice from the integration agent into BMC BPPM, open the `bmcbppm.xml` file, and add a new case block to the switch statement in the handleResponseAction function:

```
{
case "acknowledge":
bppmws.updateEvent(incidentId, bppmws.IMWS_STATUS_ACKNOWLEDGE, NO_ASSIGNEE, responder, notePrefix
+ "Event acknowledged by " + responder, annotation);
break;

...

case "be there in ten minutes":
<your code goes here>
break;

default:
throw "Unknown response Action: " + responseAction;
break;
}
```

The above is intended only as a brief overview of the required components. For more information about responses and scripting, refer to the xMatters Action Scripts and the xMatters Online Developer's Guide.

4.3.2 Adding annotation messages

Two-way email Device notifications (not FYI) can add extra annotations that will be added to the BMC BPPM event as a message on the event. To add an extra annotation, respond to an email notification with the following format in the subject line:

```
RESPONSE <Choice> <Message>
```

`<Choice>` can be any of the response choices listed in the table above, and `<Message>` can be any content you want to add as the annotation.

Note: *This method of adding annotations does not work for the diagnostic (ping and traceroute) response options.*

4.3.3 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.

4.3.4 Responses for sync errors and quick messages

Sync Error and Quick Message notifications are based on the bmcbppm20 Event Domain. These create an event within xMatters and the available responses do not have any effect on the BMC BPPM system.

4.4 Annotations

This integration extensively annotates the originating BMC BPPM event, but this may not be desirable in all environments. To prevent the annotation of an incident, change the "annotate" Event Domain Constant to *false*. For more information, see "Defining Event Domain Constants" on page 23.

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**.

For more information about working with Event Domain Constants, see "Defining Event Domain Constants" on page 23.

4.6 Filtering and suppression

The xMatters integration agent's Portable Filtering and Suppression Module is a built-in module that maintains a rolling record of previously injected events, and allows for the suppression of duplicates (also referred to as "deduplication"). This helps avoid disruption of traffic due to inadvertent loads that can result when, for example, improperly configured management systems inject duplicated events.

4.6.1 Configuration

To configure the module, do the following:

- Define your required filters in the `<IAHOME>/conf/deduplicator-filter.xml` file.
- Ensure that in the integration configuration file (`bppm-config.js`), the value for the DEDUPLICATOR_FILTER value refers to the filter for this integration.

Note: *Each integration will usually have a single deduplication filter, but the* `deduplicator-filter.xml` *file may contain multiple filter definitions because it defines the filters for any integration installed in the integration agent.*

The following table identifies the attributes in a filter definition; the "Default Value" column identifies the out-of-the-box settings for the xMatters to BMC BPPM integration:

Deduplication filter attributes

Attribute	Description	Default Value
predicates	A list of incoming event tokens (or "predicates") that are considered relevant for the purpose of correlation.	incident_id state severity priority fyi recipients
suppression_period	The length of time (in seconds) to suppress duplicate.	1800
window_size	The maximum number of unique events to record.	100

The default filter for this integration is as follows:

```
<filter name="bmcbppm20">
  <predicates>
    <predicate>incident_id</predicate>
    <predicate>state</predicate>
    <predicate>severity</predicate>
    <predicate>priority</predicate>
    <predicate>fyi</predicate>
    <predicate>recipients</predicate>
  </predicates>
  <suppression_period>1800</suppression_period>
  <window_size>100</window_size>
</filter>
```

This default filter will suppress any notification within a 1800-second timeframe that has identical values for incident_id,. state, severity, priority, recipients, and fyi settings as an existing notification. All duplicate events are logged in the log file with a warning message: **Deduplicator Suppressed Notification**.

4.7 FYI Notifications

You can make all notifications informational only (i.e., the user is not offered any response choices) by setting the "forcefyi" Event Domain Constant to "on". This makes all normal and Subscription notifications one-way (FYI). For more information, see "Defining Event Domain Constants" on page 23.

Note: *All FYI events are set to priority LOW; this allows users to prevent the alerts from being sent to specific Devices by configuring their Devices to be used for only Medium and High priority alerts.*

4.7.1 Generating FYI notifications for Subscriptions

When using subscriptions to inform Users about service outages, you may want to remove responses from notifications generated for subscriptions.

To accomplish this, select the **One Way** check box on the Subscription Domain details page for the associated Subscription Domain.

4.8 Constructing BES and email notifications

You can configure xMatters to create BES and HTML email notifications.

This feature requires the xMatters Developer IDE. For installation instructions, refer to the xMatters Online Developer's Guide.

To enable BES and HTML email, the BMC BPPM (Business) script package set must be checked into the Developer IDE Database.

Note: *Some email clients, such as Microsoft Outlook 2007, may not display HTML elements correctly. It is recommended that you test the HTML compatibility of your email client before implementing the HTML email feature.*

To enable BES and/or HTML email:

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 .**bmcbppm20**.
3. On the Event Domain Constants page, do the following:
   - Set the **enablehtmlemail** constant to `true`.
   - Set the **uselogo** constant to `true` (if you want your HTML email to show a logo).
   - Set the **xmattersurl** constant to the base URL of your xMatters web server. (default is localhost).
   - If you are using BES, set the **bespushurl** constant to the URL of the BES server.

Note: *If the Event Domain Constants are not present, you can add them using the names specified above. For more information, see "Defining Event Domain Constants" on page 23.*

4. Optionally, you can also use the Developer IDE to make any of the following changes to the Global Configuration Variables section of the initial PROCESS script in the BMC BPPM (Business) Production script package::
   - Change `$main.HTML_form_url` to point to a JSP page that you want to process any responses from the HTML email. (the default setting should work out-of-the-box).
   - Change `$main.logo` to a URL that holds the image you want to display at the top of HTML emails (by default, it points to the xMatters logo).
   - Set `$main.logo_alt_text` to the text you wish to display when the logo cannot be fetched. This can be displayed if the email client is configured not to show images, or it could be displayed because the email client cannot access the xMatters web server directly and thus cannot respond by using the links in the HTML.
   - If you are using BES and have access to a BES server, you can set the URL to the BES server in the `$main.bes_pushurl` variable.
5. Save and validate the script, and check in the script package.

For more information about these and other configuration variables, see “Configuration Variable Reference” on page 55.

4.9 Troubleshooting

This section identifies and explains some issues with the integration that may be encountered during installation, configuration, or validation.

4.9.1 Voice files

Note that on multiple-Company deployments, the voice files must be installed to `<xMHOME>\node\phone-engine\Datastore\<company_id>\common\recordings\english\phrases`, where `<company_id>` is the database identifier of the Company where the servicenowim Event Domain has been created.

If the voice files have already been copied to the above location, but are still not playing in notifications, you can copy the voice files to the global location at `<xMHOME>\node\phone-engine\Datastore\global\common\recordings\english\phrases`. Note that this is the location for the out-of-box voice files; adding the integration specific files to this location may cause them to be played for notifications not related to BMC BPPM.

4.9.2 Actions not available in console

If you are unable to view and use the xMatters actions in the BMC BPPM Console, ensure that the role you are using has permissions to use the actions. These permissions are defined in the `xm_actions.mrl` file, as explained in "Deploying Baroc and Rule files" on page 12.

4.10 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 "Defining Event Domain Constants" on page 23; 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.HTML_form_url = $xmatters_URL & "/jsp/ProcessNotificationResponse.jsp"	Specifies the URL of the xMatters web server’s Process Notification Response JSP form, used by HTML email and BES to inject responses through the system.
$main.logo = $main.xmatters_url & "/static/images/logos/xmatters_email.gif"	Specifies the path to the graphic displayed on HTML (email and BES) notifications.
$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).
$main.numeric_pager_number = “555-1212”	The phone number to display for calling in to retrieve event information. This variable has a non-existent number as a default value; a real call-in number must be supplied, or a message indicating that an xMatters event has occurred.

5.2 Local Configuration Variable

These variables are available only in this script, and control how the script runs. For more information about the initial PROCESS script, consult the *xMatters Online Developer's Guide*.

5.2.1 FYI and Subscription Notification Variables

The following variables configure the behavior of informational-only, or FYI, notifications. The value assigned to each variable is the default value within the script.

Note: *For more information on the behavior associated with informational-only notifications, see "FYI Notifications" on page 30.*

FYI and Subscription variables

Variable	Description
$use_email_for_fyi = true	Configure Device filters for informational-only (FYI) notifications.
$use_phone_for_fyi = false	Setting these flags to false prevents that Device type from being notified with informational (FYI) messages.
$use_im_for_fyi = true	
$use_text_phone_for_fyi = true	
$use_text_pager_for_fyi = true	
$use_numeric_pager_for_fyi = true	
$use_bes_for_fyi = true	
$use_generic_for_fyi = true	

www.xMatters.com

12647 ALCOSTA BLVD., SUITE #425 SAN RAMON CA 94583 USA | P: 1-877-xMattrs + 1.877.962.8877
CENTRAL COURT 25 SOUTHAMPTON BUILDINGS, LONDON WC2A 1AL UK | P: +44 (0) 800 652 7711