



xMatters **(IT)** engine for BMC
Remedy Change 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.

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.

Tuesday, October 16, 2012

Copyright © 1994-2012. All rights reserved.

xMatters™, xMatters®, xMatters® Java Client, xMatters mobile access, xMatters integration agent, xMatters lite, xMatters workgroup, xMatters enterprise, xMatters service provider, xMatters on demand, and xMatters® Notification Server are trademarks of xMatters, inc.

All other products and brand names are trademarks of their respective companies.

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 Remedy Change 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 Remedy, 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 the xMatters Professional Services department. For more information, contact your xMatters Sales representative.

Proprietary and Confidential © 2012 xMatters, inc

Table of Contents

Chapter 1: Introduction	1
1.1 Summary	1
1.1.1 Benefits	1
1.1.2 Information Workflow	2
1.2 Integration architecture	2
1.2.1 Event workflow	3
1.2.2 Custom web services	3
1.2.3 Integration filters	3
1.2.4 Integration forms	3
1.3 System Requirements	4
1.3.1 Operating Systems	5
1.4 Conventions and Terminology	5
1.4.1 Conventions	5
1.4.2 Terminology	6
Chapter 2: Installation and Configuration	7
2.1 Installing the integration	7
2.1.1 Installing the integration service	7
2.1.2 Installing voice files	9
2.2 Configuring BMC Remedy	9
2.2.1 Importing workflow definition files	9
2.2.2 Configuring filters	10
2.2.3 Configuring ITSM user	12
2.2.4 Configuring Workflow-based notifications	13
2.3 Configuring xMatters	13
2.3.1 Importing Event Domain and scripts	14
2.3.2 Adding the Web Service User	15
2.3.3 Subscribing to alerts	16
Chapter 3: Integration Validation	18
3.1 Triggering a notification	18
3.2 Responding to a notification	19
3.3 Viewing response results	22
3.4 Testing Subscriptions	23
Chapter 4: Optimizing and Extending the Integration	24
4.1 Manually configuring xMatters	24

4.1.1 Importing the script package	24
4.1.2 Configuring the Event Domain	24
4.1.3 Response choices	30
4.2 Filtering and suppression	31
4.2.1 Configuration	31
4.3 Configuring SSL	32
4.3.1 Using self-signed certificates	32
4.3.2 Importing certificates	32
4.3.3 Updating HTTP to HTTPS	33
4.3.4 Optional Configuration	33
4.4 Adding new parameters	34
4.4.1 Adding new parameters to notification content	35
4.5 Changing and adding response choices	35
4.6 Annotations	36
4.7 Altering the duration of events	36
4.8 FYI Notifications	36
4.9 Constructing BES and email notifications	37
4.10 Uninstalling	37
Chapter 5: Configuration Variable Reference	39
5.1 Global configuration variables	39
5.2 Local Configuration Variable	39
5.2.1 FYI and Subscription Notification Variables	40

Chapter 1: Introduction

Welcome to xMatters (IT) engine for BMC Remedy Change Management. This document describes how to install and configure the xMatters (IT) engine for BMC Remedy Change Management 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 relevance engines, xMatters can become the voice and interface of an automation engine or intelligent application (the Management System, such as BMC Remedy). When BMC Remedy 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 Remedy. Responses are executed immediately on BMC Remedy, enabling remote resolution of the event.

This integration supports change request notifications (from BMC Remedy to xMatters). It also supports inbound actions (from xMatters to BMC Remedy).

Note that you may 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 change request that indicate each stage of delivery. In a high-volume production system, this constant stream of communications from xMatters to BMC Remedy may result in a significant amount of network traffic that can affect overall system 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.

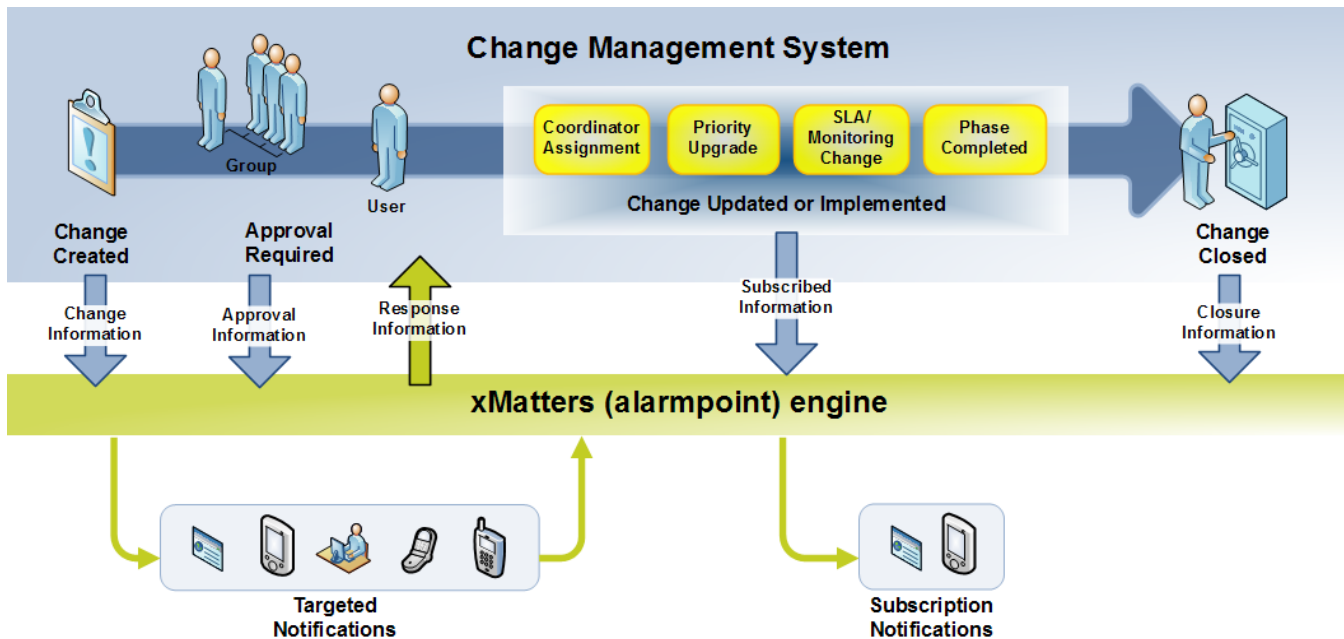
In the event of an approval notification, the recipient can select a response choice on their remote device, and xMatters will update the change request in BMC Remedy in real-time. The benefit is that this process is immediate – the ability to take simple actions on the approval process from any device gives the event resolver a quick way to deal with the event without needing to go to a computer and manually approve the change request.

During the process, every notification, response, and action is logged in xMatters. In addition, xMatters automatically annotates the original change request 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 BMC Remedy events.

1.1.2 Information Workflow

The following diagram illustrates a standard workflow in a change request management system, and how information from the management system is passed into xMatters relevance engine:



1.2 Integration architecture

The software components in this integration include:

- xMatters relevance engine
- BMC Remedy Change Management
- BMC Remedy Approval Server
- xMatters integration agent

The change management integration service runs in the integration agent and handles events and responses associated with change requests in BMC Remedy Change Management, and approval requests in BMC Remedy Approval Server. The integration is designed to work as a workflow-based notification, as described in the *BMC Remedy Approval Server Guide*. The integration involves the following steps when you create or update change requests, or interact with the approval request process:

1. BMC Remedy triggers one of the xMatters filters provided as part of the integration.
2. The filter pushes data to a backing form, which has an associated filter that sends a SOAP web service request to the integration service.
3. The integration service processes the request, using web services to obtain information about the change request that has been updated (or that is associated with the updated Approval).
 - This information is used to construct a message that is sent to xMatters.
4. In the case of an update to an approval, xMatters passes the recipient responses back to the integration agent.
5. The integration service handles user responses and automatically generated replies from xMatters, and updates the change request or approval in BMC Remedy via web services.

1.2.1 Event workflow

The following table describes the interaction between BMC Remedy and xMatters during the course of a typical change request:

BMC Remedy process	Details	xMatters process
Change Request Created	A new change request is created.	An event is sent to xMatters. This results in FYI notifications being sent to the request's Change Manager and Change Coordinator.
Status Changes	The status of an existing change request is changed.	An event is sent to xMatters. This results in FYI notifications being sent to the request's Change Manager and Change Coordinator.
Approval Phase	A change request enters a state that requires approvals.	An event is sent to xMatters, resulting in two-way notifications being sent to the request's Approvers.

Note that the above table identifies the behavior of the default installation configuration. The integration is highly customizable, and can be configured to suit your specific deployment requirements.

1.2.2 Custom web services

The integration service relies on a set of custom web services implemented in BMC Remedy to access information about and change requests and approvals; for example, annotating the change request or recording the responses of approvers. Extending or modifying the behavior of the integration service will also typically require a change to the custom web services.

The integration service uses the following custom web services:

- **XM_CHG_InfrastructureChange_WS**: used to obtain information from CHG:InfrastructureChange, but should not be used to update change requests.
- **XM_CHG_ChangeInterface_WS**: used to update change requests. The default functionality is limited to adding worklog entries to change requests, as the approval or rejection of change requests is managed using the XM_CHG_ChangeAPDetailSignature_WS Web service (below).
- **XM_CHG_ChangeAPDetailSignature_WS**: exposes the CHG:ChangeAPDetailSignature form, the purpose of which is to allow the integration to update BMC Remedy with approve, reject and hold responses from change approvers..

1.2.3 Integration filters

This section identifies and describes the filters provided by the integration to enable the workflow explained in "Event workflow" on page 3.

- **XM:Change_NewStatus**: Attempts to inject an xMatters event when a BMC Remedy change has a new status.
- **XM:AP:Change_Workflow_Notification**: This filter is to be added to the filter guide AP:Workflow Notifications Guide. Its default setting is to run whenever AP:Workflow Notifications Guide runs. When it runs it will attempt to inject an xMatters event based on the triggering CHG:ChangeAPDetailSignature (Approval Request).

1.2.4 Integration forms

This section identifies and describes the forms provided by the integration to enable the workflow explained in "Event workflow" on page 3.

XM:Event Injection

The XM:Event Injection form is the staging area for sending events to the integration agent. Each event includes a BMC RemedyRequest ID which can be used to query for more information using web services and an Action keyword that describes what should be done in xMatters. The available actions are:

- **Add:** creates a new Event in xMatters
- **Delete:** deletes an existing Event from xMatters

The XM:Event Injection form is configured with a default Archive scheme to delete any XM:Event Injection instances after seven days:

Form Properties

- Basic
- Entry Points
- Results List Fields
- Sort
- Archive**
- Audit
- Indexes
- Permissions
- Subadministrator Permissions
- Change History
- Help Text

Archive

Archive Type:

Archive State:

Archive to Form:

☐ No Attachments ☐ No Diary Fields

Times Selected

Days of Month							Days of Week							Hours of Day			
1	2	3	4	5	6	7	Monday							12AM	1AM	2AM	3AM
8	9	10	11	12	13	14	Tuesday							4AM	5AM	6AM	7AM
15	16	17	18	19	20	21	Wednesday							8AM	9AM	10AM	11AM
22	23	24	25	26	27	28	Thursday							12PM	1PM	2PM	3PM
29	30	31	ALL	NONE			Friday							4PM	5PM	6PM	7PM
							Saturday							8PM	9PM	10PM	11PM
							Sunday										

Minutes after Hour:

Summary of selected Times

Every Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday at 12:00AM

Qualification

'Modified Date' < (\$TIMESTAMP\$ - (((60 * 60) * 24) * 7))

Archived from Form:

OK Cancel

XM:Action

This form is based on SYS:Action, and is used to separate the transactions of the BMC Remedy workflow from the workflow of sending event information to xMatters.

1.3 System Requirements

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

xMatters:

- xMatters relevance engine 4.1 (patch 011 or later) or 5.x
- xMatters integration agent 4.1 (patch 005 or later) or 5.x
- xMatters Developer IDE

Note that the version number of the xMatters integration agent, xMatters relevance engine, and xMatters Developer IDE must be the same. For example, if you are using the 4.1 version of the integration agent, then you must also use the 4.1 version of the xMatters relevance engine.

BMC Remedy:

- BMC Remedy Change Management 7.5 through 7.6.04 (Service Pack 2)
- BMC Remedy Mid Tier
- BMC Remedy Action Request System

1.3.1 Operating Systems

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

Integration Component	Version	Operating System	Database
xMatters relevance engine	4.1 patch 011	Linux CentOS 5.3 Microsoft Windows 2008 (validated)	Oracle 11g Microsoft SQL Server 2008
	5.0	Linux CentOS 5.3 (validated)	Oracle 11g (validated)
xMatters integration agent	4.1 patch 005	Linux CentOS 5.3 Microsoft Windows 2008 (validated)	
	5.0	Linux CentOS 5.3 (validated)	
BMC Remedy Change Management	7.5 through 7.6.04 (Service Pack 2)	Microsoft Windows 2008 (validated with Microsoft SQL Server 2008) All operating systems supported by the xMatters integration agent	
Note: <i>xMatters version 5.0 is currently available only for Linux/Oracle deployments. The integration agent is supported on multiple platforms.</i>			

For more information about the supported operating systems for xMatters, refer to the *xMatters installation and administration guide* and *xMatters integration agent guide*.

1.4 Conventions and Terminology

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

1.4.1 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.

1.4.2 Terminology

The following terms are used through the xMatters documentation.

Documentation terminology

Term	Meaning
Event	<p>An <i>event</i> 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.</p> <p>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 (i.e., change request), but can also collectively be called events.</p>
Management system	A management system is any sort of IT service management software, and with which xMatters can combine; i.e., a synonym for BMC Remedy.
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 <i>xMatters user guide</i> .

Chapter 2: Installation and Configuration

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

2.1 Installing the integration

This section describes the installation process for the xMatters (IT) engine for BMC Remedy Change Management integration.

Components

This integration includes the following components that must be modified for each deployment:

Component Name	Description
bmcremedychange.xml, configuration.js	The JavaScript and XML service configuration file that defines the integration service on the integration agent.
conf/deduplicator-filter.xml	The filtering mechanism used to suppress duplicate messages. The filter checks the values of certain parameters within injected events; if they are all the same within a specified timeframe, only the first message will be sent through to xMatters. You can customize these settings by adding or removing predicates in the filter, changing the suppression period or the number of messages that are compared by the integration agent. For more information about this feature, see "Filtering and suppression" on page 31.

2.1.1 Installing the integration service

To install the integration service, you must perform the following steps:

- Copy the folder containing 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.
- Modify the integration agent's IConfig.xml file to include the path for the new integration service.
- Modify the variables in the configuration.js file associated with the integration service.

If you have more than one integration agent providing the BMC Remedy 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*

Installing with other BMC Remedy integrations

If you are installing the xMatters (IT) engine for BMC Remedy Change Management integration on an integration agent that has a BMC Remedy integration already installed, note the following considerations:

This integration comes with a copy of the integrationservices\bmcremedy\lib folder and the integrationservices\bmcremedy\util.js which are the same as those bundled with the xMatters for BMC Remedy Incident Management and xMatters Data Load for BMC Remedy integrations. If you have not customized any of the files in integrationservices\bmcremedy\lib or the util.js file, then the installed files can be safely overwritten by the ones

included with this integration. If you have customized any of these files, do not overwrite the existing files. You will need to compare your customized files with the ones included with this integration, determine whether your changes will affect the integration, and merge your changes as necessary.

To install the integration service:

1. Copy all of the contents of the `\components\integration-agent` folder from the extracted integration archive to the `<IAHOME>` folder.
2. Open the `IAConfig.xml` file found in `<IAHOME>\conf` and add the following line to the “service-configs” section:
`<path>bmcremedy/bmcremedychange/bmcremedychange.xml</path>`
3. Open the `configuration.js` files (now located in the `<IAHOME>\integrationservices\bmcremedy\bmcremedychange` folder), and set the values for the following variables:

Variable	Description
MID_TIER_HOSTNAME	Name of IP address of the network host on which the BMC Remedy web services are running.
MID_TIER_PORT	Port on which the BMC Remedy web services are running.
REMEDY_SERVER_NAME	The name of the BMC Remedy server hosting the web services.
REMEDY_WS_USERNAME	User name of the account used to access the BMC Remedy web services that support the integration. Note: This user account must be an Approval Server Process Administrator with Override Only Admin authority. For more information about configuring a process administrator, see the BMC Remedy Approval Server Guide.
REMEDY_WS_PASSWORD_FILE	Location of the file containing the web services user's password; for instructions on how to set the password for this user, see "Setting web services user password", below.
DEDUPPLICATOR_FILTER	Name of the deduplicator filter used to suppress duplicate notifications for this integration; i.e., the attribute name for the element filter in the <code>deduplicator-filter.xml</code> file. The default is <code>bmcremedychange</code> . For more information, see "Filtering and suppression" on page 31.

4. Save and close the files.
5. Restart the integration agent.
 - On Windows, the integration agent runs as a Windows Service; on Unix, it runs as a Unix daemon.

Setting web services user password

This integration includes an encrypted file, located in the `<IAHOME>\conf` folder, that stores the password for the web services user required for the management system. You will need to update the file with the correct password for the `REMEDY_WS_USERNAME` variable specified in the `bmcremedychange\configuration.js` file.

Password file name:

- `xm_chg_ws.pwd` stores the password for the `REMEDY_WS_USERNAME` user used by the `bmcremedychange` integration service. If you change the name of this file, you must also update the `configuration.js` file to point to the correct password file.

To specify a web service user password:

1. Open a command prompt, and then navigate to <IAHOME>\bin.
2. Run the following command, where <new_password> is the password for the web services user specified in the configuration.js file, <old_password> is the existing password (the default value for a newly installed integration is "password"), and <filename> is the name of the password file (xm_chg_ws.pwd).

```
iapassword.bat --new <new_password> --old <old_password> --file conf/<filename>.pwd
```

2.1.2 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\bmcremedychange\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\bmcremedychange\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 BMC Remedy

Configuring BMC Remedy to combine with xMatters requires the following steps:

- Import the workflow definition files
- Configure filters
- Configure the ITSM user
- Configure the workflow-based notifications

2.2.1 Importing workflow definition files

The workflow described in this document is provided in definition files that must be imported into BMC Remedy.

Note that this integration provides two versions of the definition files: one version, marked with `pre7604` is for BMC Remedy versions 7.5 to 7.6.03, and the other version, marked with `7604`, is for BMC Remedy version 7.6.04. These files are contained in the `bmcremedy` and `bmcremedy/pre7604` folders in the extracted integration archive; ensure that you install the correct definition files for your deployment.

The difference between the two versions is that the files intended for BMC Remedy version 7.6.04 have been exported as custom objects. The "pre7604" versions can be imported into BMC Remedy 7.6.04, but they will be created as origin objects and therefore not identifiable as customizations to a standard deployment. The "7604" versions of the definition files cannot be installed in previous versions of BMC Remedy.

To import the workflow definition files:

1. Log in to the BMC Remedy Developer Studio, and then select **File > Import**.
2. Select **BMC Remedy Developer Studio > Object Definitions**, and then click **Next**.
3. Select the AR System server into which you want to upload the integration objects, and then click **Next**.
4. Do one of the following:
 - Type in the location of the `xm_foundation_<version>.def` file.
 - Click the **Browse** button to the right of the text field and navigate to the location of the `xm_foundation_<version>.def` file. Select the file, and then click **Open**.
5. Click **Next**.
 - If you have already imported a workflow definition file, ensure that you select the **Replace Objects on the Destination Server** check box (do not select the other check boxes), but note that any changes you have made to those objects will be lost. If you are sure the changes you made are necessary for your installation, you will be required to re-apply those changes to the new version of the files being imported unless you applied those changes to overlay objects.
6. Repeat the above steps to import the `xm_change_<version>.def` file.
 - Note that this file must be imported after the foundation file.
7. Click **Finish**.

2.2.2 Configuring filters

The integration includes a filter and an escalation that use the Set Fields action to consume a web service; these objects need their endpoints changed to the address of the integration agent.

Filter:

- XM:EI:ChangeInjection_100

Escalation:

- XM:Change Injection Retry

Example of a change injection filter with a modified Endpoint field:

Developer - Modify Filter - XM:EI:ChangeInjection_100 on vic-vm-r7604-02 - BMC Remedy Developer Studio

File Edit Workflow Search Window Help

XM:EI:ChangeInjection_100

▶ **Error Handler** Enabled | XM:EI:EventInjectionError

▼ **If Actions (2)**

▶ **Set Fields** CURRENT TRANSACTION

▼ **Set Fields**

Data Source: WEB SERVICE

Server Name: vic-vm-r7604-02

WSDL File: C:\Documents and Settings\Administrator\Desktop\apia_http_bmcremedy.wsdl

Port: apia_http_bmcRemedyChangeSOAP

Use: WSDL

Endpoint: http://localhost:8081/http/bmcremedychange_bmcremedychange

Operation: triggerChange

Authentication: None

Input Mapping: ☐ Support XSI Type

For more information about changing these endpoints, consult your BMC Remedy administrator, or refer to the BMC Remedy documentation.

BMC Remedy version 7.5 Deployments

Note that BMC Remedy version 7.5 deployments require an additional configuration step, as described in the following section.

Located in the same directory as the *_pre7604.def workflow definition files is the `apia_http_bmcremedy.wsdl` file, which is required by BMC Remedy 7.5 to set the correct endpoint for the filters and escalations.

To update the endpoints, open the WSDL file in a text editor and locate the following element (near or at the bottom of the file):

```
<soap:address location="http://localhost:8081/http/bmcremedychange_bmcremedychange"/>
```

Change the addresses within the element to point to the correct address of the integration agent, and save and close the file.

To load the new values into BMC Remedy version 7.5:

1. Open the filter and escalation in the Remedy Developer Studio tool.
2. In the web service Set Fields action (the second one displayed), edit the **WSDL File** field to point to the `apia_http_bmcremedy.wsdl` file that was just edited. (If the field already contains a value, ensure that it is referencing the correct file and location.)

3. Click **Reload** .
 - Note that this causes BMC Remedy to reset the rest of the Set Fields action definition.
4. For the filter XM:EI:ChangeInjection_100 and the escalation XM:Change Injection Retry:
 - For the **Port** field, select **apia_http_bmcRemedyChangeSOAP**
 - For the **Operation** field, select **triggerChange**
5. The Input and Output Mappings also need to be recreated for all objects:
 - **action** should be set to **Action**
 - **id** should be set to **ID**
 - **requestType** should be set to **Request Type**
 - **status** should be set to **Status**
 - **description** should be set to **Short Description**
6. Save the objects.

2.2.3 Configuring ITSM user

The integration agent requires a dedicated ITSM user to interact with change requests.

Create an ITSM user

First, create a new ITSM user with the Infrastructure Change Master role in BMC Remedy; the user does not need to be Support Staff.

The screenshot shows the 'People' configuration window in BMC Software. The window title is 'People (vic-vm-r7604-02)'. The main content area is divided into several sections:

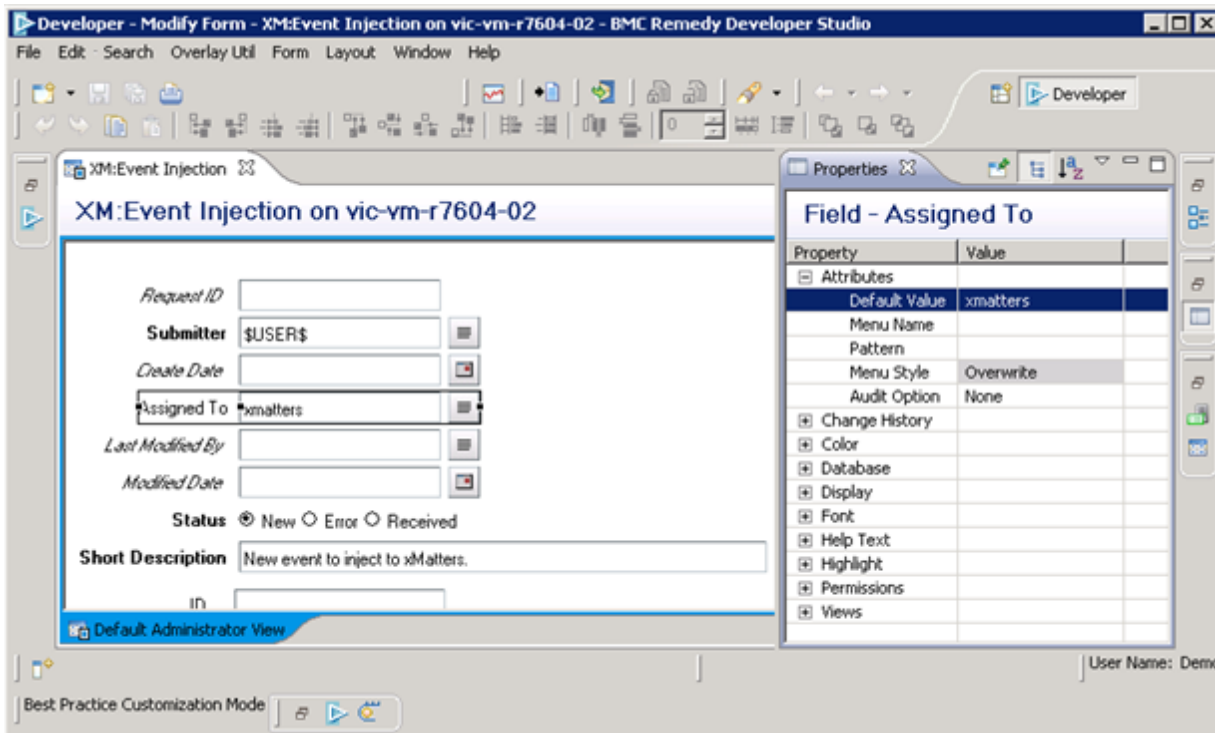
- Personal Information:**
 - First Name*: User
 - Middle Name: (empty)
 - Last Name*: xMatters
 - Client Type*: Office-Based Employee
 - Contact Type: (empty)
 - Support Staff*: No
 - Phone Number*: ####
 - Email Address: (empty)
- Organization Information:**
 - Company*: Calbro Services
 - Organization: (empty)
 - Department: (empty)
- Location Information:**
 - Site*: Amsterdam Support Center
 - Site Address: Boeing Avenue 245, Schiphol-Rijk, Amsterdam
- Login/Access Details:**
 - Login ID and Password:**
 - Login ID: xmatters
 - Password: (empty)
 - Licensing Preferences:**
 - License Type: Fixed
 - Full Text License Type: (empty)
 - Application Permissions:**
 - Permission Group: Infrastructure Change Master
 - Access Restrictions:**
 - Access Restriction: (empty)
 - Unrestricted Access: ☒ Yes

Buttons at the bottom include 'Add', 'Close', 'Update Permission Groups', 'Update Access Restrictions', and 'Click to Refresh'.

Note: *If you specify a Login ID of "xmatters" for this ITSM user, you can skip the following steps .*

Update the default assignee

The out-of-box permissions allow the Submitter and Assignee (and BMC Remedy administrators) to search instances of the XM:Event Injection form. This allows users who modify change requests to see the corresponding XM:Event Injection instance for their update. To allow the ITSM user to also see all of the Event Injection forms, modify the default value for the Assigned To field to the ITSM user you created.



2.2.4 Configuring Workflow-based notifications

This integration is designed to take advantage of workflow-based notifications in BMC Remedy Approval Server. According to the BMC Remedy documentation "workflow-based notification provides a way for approval events to be propagated to a customized notification system".

To configure this feature, add the filter XM:AP:Change_Workflow_Notification filter to the AP:Workflow Notification Guide filter guide.

Note: *For more information about modifying filter guides, refer to the BMC Remedy user documentation.*

By default XM:AP:Change_Workflow_Notification does not have a qualification meaning it should run anytime a filter associated with CHG:ChangeAPDetailSignature calls AP:Workflow Notification Guide. Integration administrators can add a qualification to XM:AP:Change_Workflow_Notification if they want to limit the approval events that are sent to xMatters.

2.3 Configuring xMatters

Configuring xMatters to combine with BMC Remedy requires the following steps:

- Import the Event Domain and define the integration service
- Configure the Web Services User

- Configuring a Subscription Domain and Subscriptions
- Review and configure the response choices

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.

To import the integration Event Domain package:

1. Log in to xMatters as a Company Administrator, and click the **Developer** tab.
2. On the Event Domains page, click **Import New**.
3. On the Import Integration page, click **Browse**, and then locate the `\components\xmatters\event-domain\xM-BMC-Remedy-CM.xml` file extracted from the integration archive.
4. Click **Open**, and then click **Upload**.

xMatters imports the integration configuration settings and displays the new "bmcremedychange" Event Domain. xMatters also creates the predicates for the Event Domain, and assigns common values as defaults. For more information about the created predicates, and instructions on how to modify them, see "Defining Event Domain predicates" on page 28.

Defining the integration service

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

To define an Integration Service:

1. In xMatters, on the Event Domains page, click the **bmcremedychange** 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:** bmcremedychange
 - **Description:** BMC Remedy Change 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 **bmcremedychange**, 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 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.

The following constants are used in a message that is sent to a user of the integration if, while processing the user's response to a notification, the integration encounters a serious error that indicates there may be a problem with the configuration of the integration.

ERRORCONTACT	xMatters/Remedy Integration Team	Administrator or Admin Group for the xMatters for BMC Remedy integration.
ERORCONTACTEMAIL	admin@defaultcompany.com	Email address for the error contact group.
ERRORCONTACTPHONE	555-555-5555	Phone number for the error contact group.

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 25.

2.3.2 Adding the Web Service User

This integration requires an xMatters Web Service User with permission to query existing events in xMatters before injecting a new event. 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 Service Users page, click **All**.
3. In the returned search results, click **IA_User**.
4. On the Details for IA_User page, confirm that the list of **Allowed Web Services** includes the following web services; if any of the following are not listed in the Allowed Web Services list, select them in the **Denied Web Services** list (Ctrl-click to select more than one), and then click **Add**:
 - Query Incident

5. Click **Save**.

2.3.3 Subscribing to alerts

You can use the Subscriptions feature in xMatters to subscribe to BMC Remedy change requests that match specific criteria. For example, you could configure a Subscription that would send an informational notification to a specific User each time an event entered the system with an urgency of "1-Critical", or whenever an event's status changed to "Closed".

To allow Users to subscribe to specific criteria on injected events, you must configure the Subscription using the following steps:

- Define a Subscription Domain
- Create a Subscription
- Create a Fail-Safe Group

Defining a Subscription Domain

A Subscription Domain 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, in the Domains menu, click **Subscription Domains**.
2. On the Subscription Domains page, click the **Add New** link.
3. In the **Event Domain** drop-down list, select **bmcremedychange**, and then click **Continue**.
4. On the Subscription Domain Details page, in the **Name** field, type **bmcremedychange**.
5. Select the **One-Way** check box.
 - Note that no response choices are supported for subscription notifications with this integration.
6. Click **Continue**.
7. On the Select Appropriate Predicates page, add all of the predicates to the **Applied Predicates** list, and then click **Continue**.
8. 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

You can now subscribe to BMC Remedy events that match specific criteria. For example, you could configure a subscription that would send an informational notification to a specific User each time an event entered the system that was of extensive impact. These notifications do not affect the normal progression of an event through the system.

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 Remedy 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 25.*

Chapter 3: Integration Validation

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

- BMC Remedy Change Management
- 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 BMC Remedy for notification delivery and Subscription functionality.

3.1 Triggering a notification

Ensure that a Remedy Change Manager and Change Coordinator are defined in xMatters and have valid Devices. To trigger a notification, create a new change request in BMC Remedy and assign the Change Manager and Change Coordinator to the new change request.

The screenshot shows the 'People' configuration window in BMC Software. The window title is 'People (vic-vm-r7604-02)'. The main content area is divided into several sections:

- People**: Includes a 'Select Template' button and fields for 'First Name*' (User), 'Middle Name', 'Last Name*' (xMatters), 'Client Type*' (Office-Based Employee), 'Support Staff*' (No), 'Phone Number*+' (###), and 'Email Address'.
- Organization Information**: Includes 'Company*+' (Calbro Services), 'Organization', and 'Department'.
- Location Information**: Includes 'Site*+' (Amsterdam Support Center) and 'Site Address' (Boeing Avenue 245, Schiphol-Rijk, Amsterdam).
- Login/Access Details**: Includes 'Login ID and Password' (Login ID: xmatters, Password: |) and 'Licensing Preferences' (License Type: Fixed, Full Text License Type).
- Application Permissions**: Includes a list of 'Permission Group' (Asset Viewer, Infrastructure Change Master) and 'Access Restrictions' (Click to Refresh).

At the bottom, there are buttons for 'Update Permission Groups', 'Update Access Restrictions', and 'Unrestricted Access' (checked Yes). The window also has 'Add' and 'Close' buttons at the bottom left.

Both the Change Manager and Change Coordinator should receive FYI notifications.

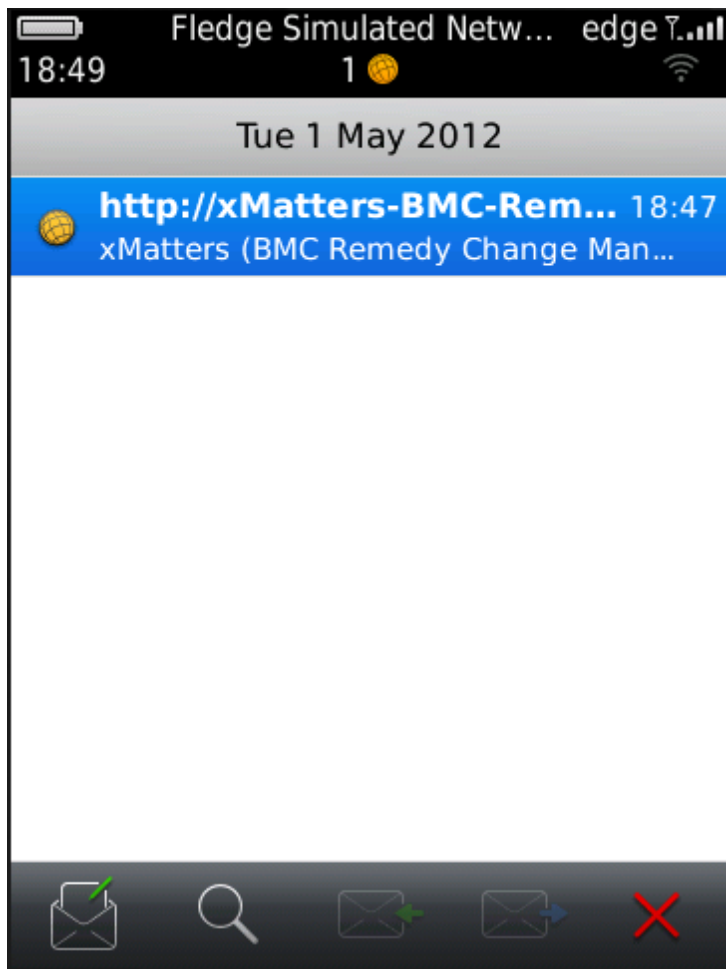
To test two-way notifications, ensure that a Remedy Change Approver is defined in xMatters and has a valid Device. Update the previously created change request to an Approval state such as "Request for Authorization" or "Request for Change". An approval should be created and associated to this change request. This should then cause an approval event to trigger a filter (for example, AP:Notify-000000000000009) which should call AP:Workflow Notifications Guide. This will run XM:AP:Change_Workflow_Notification, which attempts to inject an event to xMatters.

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 simulated 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:

http://xmatters-bmc-remedy-chan... edge 7.11

http://xmatters-bmc-remed... 2

(x) matters®
The relevance engine company.

BMC Remedy Change Management - Integration Notification

Time of Event:	Tuesday, 1 May 2012 18:43:50 GMT-0400
Target:	mary BlackBerry
Change ID:	CRQ0000000000001
Change Type:	Change
Summary:	Patch unix server cluster (group 1)
Status:	Request For Authorization
Risk Level:	Risk Level 2
Impact:	3-Moderate/Limited
Urgency:	3-Medium
Priority:	Medium
Change Manager:	Mary Mann
Requested By:	Allen Allbrook

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

http://xmatters-bmc-remedy-chan... edge

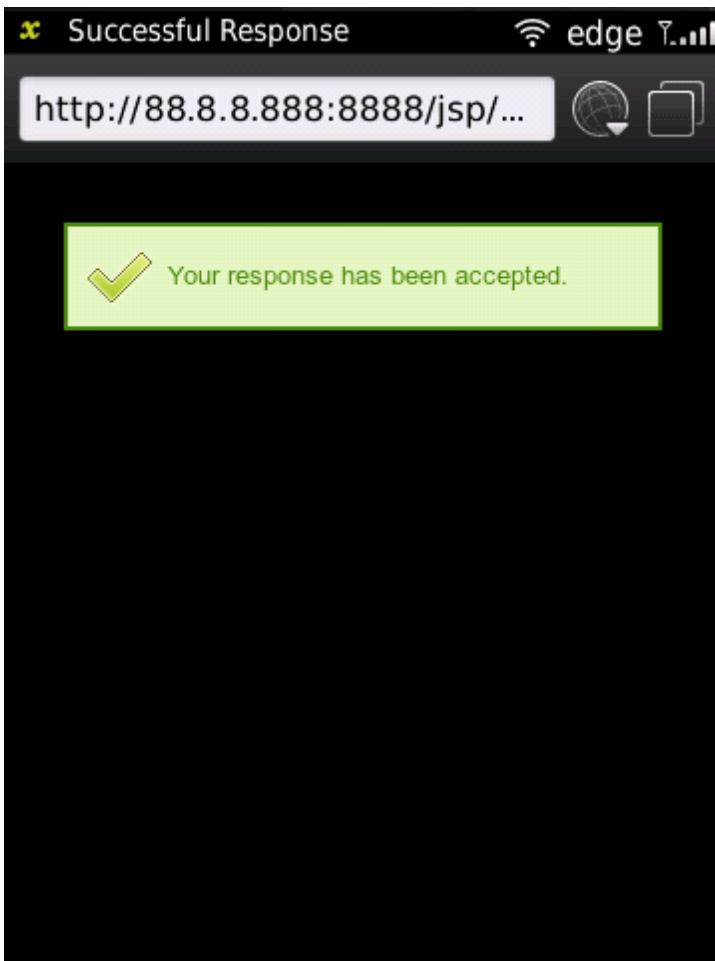
Change ID: CR0000000000001

Change Type:	Change
Summary:	Patch unix server cluster (group 1)
Status:	Request For Authorization
Risk Level:	Risk Level 2
Impact:	3-Moderate/Limited
Urgency:	3-Medium
Priority:	Medium
Change Manager:	Mary Mann
Requested By:	Allen Allbrook
Company:	Calbro Services
Phone:	1 212 555-5454 (11)
Requested For:	Allen Allbrook

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

1. [Approve](#)
2. [Reject](#)
3. [Hold](#)

4. To respond to the notification, the User clicks a response choice, and xMatters updates the event in BMC Remedy.



For more information about response choices, and changing the options available to Users, see "Response choices" on page 30.

3.3 Viewing response results

For FYI notifications sent as a result of updates to change requests, the results of the notification are displayed on the Work Detail tab. For approval requests, the notification and response results are recorded on the Work Detail tab of the associated change request's Work Detail tab:

Initiate
Review & Authorize
Approval
Plan & Schedule
Implement
Closed

Work Detail
Tasks
Relationships
Date/System

3 entries returned - 3 entries matched

Type	Notes	Files	Submit Date
General Information	[xMatters] - Response Approved from Mary Mann (mary@BlackBerry)		5/1/2012 3:37:07 PM
General Information	[xMatters] - SUCCESSFUL_DELIVERY to Mary Mann (mary@BlackBerry)		5/1/2012 3:32:24 PM
General Information	Status Transition: Draft > Request For Authorization > Request For Change > Planning In Progress > Sched		5/1/2012 2:09:18 PM

Add Work Info

Notes:

Attachment:
<File Name>

More Details

Add

Current Approval Phase
Business Approval

1 entries returned - 1 entries matched

Approval Status	Approvers	Name
Pending	Mary	Mary Mann

3.4 Testing Subscriptions

To test Subscriptions, ensure that you have created a Subscription (for more information, see "Creating a Subscription" on page 16). Trigger a notification that matches the criteria of the Subscription you created.

You will receive an FYI notification (informational only) which will not have any response choices available.

Chapter 4: Optimizing and Extending the Integration

This section describes some of the ways you can optimize or extend the xMatters (IT) engine for BMC Remedy Change Management integration.

4.1 Manually configuring xMatters

This integration includes an exported version of the xMatters Event Domain that includes a script package, Event Domain constants and predicates. If you do not want to use this 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 BMC Remedy Change Management that must be imported into the xMatters 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 IDE, and then configure the database connection.
2. Click **Workspace > Import**.
3. Select the `\components\xmatters\scripts\XM-BMC-Remedy-CM.apx` file extracted from the integration zip file, click **Open**., and then click **OK**.
4. When the script has finished importing, click **OK**.
5. Right-click the **BMC Remedy Change Management (BUSINESS)** folder, and then select **Validate**.
6. Right-click the folder again, and then select **Check In**.
7. In the Create Script Package dialog box, click **Create**.
8. In the Check In dialog box, click **Close**.

4.1.2 Configuring the Event Domain

By default this integration is set up to use an Event Domain of “bmcremedychange”; it is strongly recommended that you use this Event Domain name. 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 `bmcremedychange.xml`).

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

To define an Event Domain:

1. Sign on 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:** bmcremedychange
 - **Description:** BMC Remedy Change Management Integration
 - **Script Package:** BMC Remedy Change Management
5. Click **Save**.

Once you have defined the Event Domain, you can add the integration service, as described in "Defining the integration service" on page 14.

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 **XMATTERS** and **BESPUSHURL** constants should be modified to specify the address of the xMatters web server (to enable the HTML 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 **bmcremedychange**.
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.
 - Note that Event Domain Constant names in xMatters version 5.0 MUST be defined in uppercase.
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.*

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 <code>\$main.xmatters_url</code> variable.
BESPUSHURL	http://localhost:8888/static	Used to specify the address of the BES device server. Populates the <code>\$main.bes_pushurl</code> parameter.

Constant Name	Default Value	Description
FORCEFYI	disable	<p>Force notifications to be informational only (FYI), rather than requiring responses; this overrides the <code>fyi</code> behaviour specified on the injected event. Possible values:</p> <ul style="list-style-type: none"> • disable: Nothing is forced. • on: Notifications are forced to be FYI. • off: Notifications are forced not to be FYI. <p>Populates the <code>force_fyi</code> parameter.</p>
FAILSAFEGROUP	Remedy Fail Safe	<p>The fail-safe recipient to notify, typically a group.</p> <p>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 Remedy Fail Safe to another group defined in xMatters.</p>
FAILSAFE	enabled	<p>Controls fail-safe functionality, notifying the fail-safe recipient via EMAIL under certain circumstances; possible values are:</p> <ul style="list-style-type: none"> • 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. <p>Populates the <code>\$fail_safe</code> parameter.</p>
OVERRIDEFRAMEFRAMES	false	<p>Override Recipients Device Timeframes.</p> <p>Populates the <code>\$override_timeframes</code> parameter.</p>
USEEMERGENCYDEVICES	false	<p>Force the use of emergency Devices.</p> <p>Populates the <code>\$use_emergency_devices</code> parameter.</p>
TRACKDELIVERY	true	<p>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.</p> <p>Populates the <code>\$track_delivery</code> parameter.</p>
ANNOTATE	true	<p>Enables submission of annotations back to the management system.</p> <p>Populates the <code>\$main.annotate</code> parameter.</p>

Constant Name	Default Value	Description
SUBSCRIPTIONANNOTATE	true	Enables submission of Subscription annotations back to the management system. Populates the <code>\$main.subscription_annotate</code> parameter.
TRACKSUBSCRIPTIONDELIVERY	true	Track when each Device is delivered to for Subscriptions. Populates the <code>\$track_subscriptionDelivery</code> parameter.
TIMEOUT	259200	Amount of time (in seconds) the event is allowed to run before timing out. 259200 seconds = 72 hours. Populates the <code>\$main.timeout</code> parameter.
MAXINVALIDRESPONSES	3	Specifies the maximum number of invalid responses allowed before notification is no longer requeued. Populates the <code>\$main.maxInvalidResponses</code> parameter.
ENABLEHTMLMAIL	true	Enables HTML email functionality. Populates the <code>\$main.enable_HTML_Email</code> parameter.
USELOGO	true	Set this if you want the logo displayed within HTML email notifications. Populates the <code>\$main.use_logo</code> parameter.
MAINLOGO	<code>/static/images/logos/xmatters_email.gif</code>	Indicates the location of the image that will be displayed in HTML notification. The default is the location for xMatters version 5.0; for 4.1 deployments, the image location should be changed to: <code>/static/images/xmatters/logos/xmatters_email.gif</code>
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 <i>true</i> for xMatters on demand integrations.
DEBUG	false	Indicates whether to use the debug level for logging messages. Populates the <code>\$main.debug</code> variable.
ENABLESUBSCRIPTIONS	true	Indicates whether to enable processing of Subscriptions on incoming events.

Constant Name	Default Value	Description
SUBSCRIPTIONFYI	false	Indicates whether Subscriptions should be forced to be informational only (FYI).
<p>The following constants are used in a message that is sent to a user of the integration if, while processing the user's response to a notification, the integration encounters a serious error that indicates there may be a problem with the configuration of the integration.</p>		
ERRORCONTACT		Administrator or Admin Group for the xMatters for BMC Remedy integration.
ERORCONTACTEMAIL		Email address for the error contact group.
ERRORCONTACTPHONE		Phone number for the error contact group.

Defining Event Domain predicates

The default Event Domain provided with the integration includes a number of predicates that contain information about the incoming event. These predicates are created when you import the Event Domain, and assigned common values as defaults. You can modify or remove the default values to suit your deployment.

You can also use the following steps to add other predicates that you consider important and which you plan to add to the integration. For more information, see "Adding new parameters" on page 34. For more information about predicates, including the available types and how the Important flag works, refer to the *xMatters installation and administration guide*.

To define the Event Domain predicates:

1. In xMatters, click the **Developer** tab.
2. On the Event Domains page, click **bmcremedychange**.
3. On the Event Domain Details page, in the Predicates section, add to or modify the following predicates:

Event Domain predicates

Predicate	Type	Important	Description
infrastructure_change_id	Text		
requestType	List		<p>A list of request types that indicate what kind of BMC Remedy object changed to trigger the event being injected into xMatters; possible values are :</p> <ul style="list-style-type: none"> • approval • change

Predicate	Type	Important	Description
change_request_status	List	Yes	<p>A list of Status values that may be listed on change requests; possible values are:</p> <ul style="list-style-type: none"> • Draft • Request for Authorization • Request For Change • Planning In Progress • Scheduled For Review • Scheduled For Approval • Scheduled • Implementation In Progress • Pending • Rejected • Completed • Closed • Cancelled
impact	List		<p>A list of Impact values in BMC Remedy that may be listed on change requests; possible values are:</p> <ul style="list-style-type: none"> • 1-Extensive/Widespread • 2-Significant/Large • 3-Moderate/Limited • 4-Minor/Localized
urgency	List	Yes	<p>A list of Urgency values in BMC Remedy that may be listed on change requests; possible values are:</p> <ul style="list-style-type: none"> • 1-Critical • 2-High • 3-Medium • 4-Low
priority	List		<p>A list of Priority values in BMC Remedy that may be listed on change requests; possible values are:</p> <ul style="list-style-type: none"> • Critical • High • Medium • Low
Support_Group_Name	Text		Name of the Support Group.
ASGRP	Text		Change Coordinator Group
serviceci	Text		The Service CI from the BMC Remedy change request.

4.1.3 Response choices

This integration allows recipients to respond to notifications with several default choices, some of which are injected back to the BMC Remedy server, updating the original change request. Users notified on email Devices also have the ability to respond with an extra annotation message which will be logged in the change request, as described in "Adding annotation messages", below.

The following is a list of the default response choices (and their short forms) 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 change request in BMC Remedy.

Response	BMC Remedy Update	xMatters Job Control	Device Availability
Approve (App)	Sets the status of the approval request to Approved.	Delivered, delink all.	BES, email, voice, text.
Reject (Rej)	Sets the status of the approval request to Rejected.	Delivered, delink all.	BES, email, voice, text.
Hold (Hld)	Sets the status of the approval request to Hold.	Delivered.	BES, email, voice, text.
Annotate (Ann)	No status change; adds the annotation text to the change request log.	Delivered	Email Devices only.

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*.

Adding annotation messages

Two-way email Device notifications (not FYI) can add extra annotations that will be added as a message on the change request in BMC Remedy. 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.

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.

4.2 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.

Each integration that uses a deduplication filter must define the variable `DEDUPPLICATOR_FILTER` in the integration service configuration file; this integration defines the variable within the `configuration.js` file as follows:

```
var DEDUPPLICATOR_FILTER = "bmcremedychange";
```

The value assigned to `DEDUPPLICATOR_FILTER` must correspond to the name of a filter defined in `<IAHOME>\conf\deduplicator-filter.xml`. If you have multiple integration services using deduplication, your `deduplicator-filter.xml` file must contain a filter definition for each integration service, and each filter definition must have a unique name.

4.2.1 Configuration

To configure the module, add your required filters to the `<IAHOME>\conf\deduplicator-filter.xml` file. You can change the default filter configuration, but must use the following filter attributes; the "Default Value" column identifies the out-of-the-box settings for the 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 status slm_status urgency priority impact recipients
suppression_period	The length of time (in seconds) to suppress duplicates.	1800
window_size	The maximum number of unique events to record.	100

The default filter for this integration is as follows:

```
<filter name="bmcremedyincident">
  <predicates>
```

```

    <predicate>incident_id</predicate>
    <predicate>status</predicate>
    <predicate>slm_status</predicate>
    <predicate>urgency</predicate>
    <predicate>priority</predicate>
    <predicate>impact</predicate>
    <predicate>recipients</predicate>
  </predicates>
  <suppression_period>1800</suppression_period>
  <window_size>100</window_size>
</filter>

```

This default filter will suppress any notification within an 1800-second timeframe that has identical values for the indicated predicates as an existing notification. All duplicate events are logged in the log file with a warning message: ****Deduplicator Suppressed Notification****.

4.3 Configuring SSL

This integration supports SSL communication between the integration agent and BMC Remedy and between the integration agent and xMatters.

4.3.1 Using self-signed certificates

The SSL support has been configured out of the box to support self-signed certificates. This is not recommended for production systems due to security reasons, unless you are aware and accepting of the security implications of self-signed certificates.

To modify the SSL configuration:

1. Open the `<IAHOMES>\integration\services\bmcremedy\lib\javascript\webservices\wsutil.js` file and modify the `ACCEPT_ANY_CERTIFICATE` variable as follows:
 - Set to *true* to use SSL but trust any certificate (including self-signed ones).
 - Set to *false* to accept only Certificate Authority (CA) certified certificates (recommended in production environments).

4.3.2 Importing certificates

The next step required to enable SSL support is to import the certificate used by the BMC Remedy web server to the cacerts keystore of the Java Virtual Machine (JVM) bundled with the integration agent.

Using the keytool executable located at `<IAHOMES>\jre\bin`, execute the following command on the integration agent to import the certificate, replacing the variables with the appropriate values as described in the list below:

```
keytool -import -alias <your.alias> -file <path>/<certificate>.cer -keystore
<dir>/jre/lib/security/cacerts -storepass <password>
```

- **<your.alias>**: an identifier for the certificate within the keystore; for example, you can use the string "bmcremedychange".
- **<path>**: path to the certificate
- **<certificate>**: the certificate's file name
- **<dir>**: the directory in which the integration agent is installed.
- **<password>**: the password for the cacerts keystore; the default password is "changeit".

If you want to configure SSL support between the integration agent and xMatters, use the above command to import the trusted certificate for xMatters into the integration agent keystore (for information on setting up SSL in xMatters, consult the xMatters Community site at <http://connect.xMatters.com>).

4.3.3 Updating HTTP to HTTPS

The next step is to update the `PROTOCOL` in the

`<IAHOME>\integrationservices\bmcremedy\bmcremedychange\configuration.js` file to use the HTTPS protocol instead of HTTP.

The modified value should resemble the following:

```
var PROTOCOL = "https";
```

Note: For trusted certificates, "localhost" in the `MID_TIER_HOSTNAME` variable should be replaced with the `COMMON NAME (CN)` specified in the certificate and the port should be set to the port specified in the SSL configuration for BMC Remedy.

To configure the integration agent to use HTTPS when communicating with xMatters:

1. In a text editor, open the `<IAHOME>\conf\IAConfig.xml` file.
2. Modify the URL for the `<primary-servers>` and `<secondary-servers>` elements to use the HTTPS protocol instead of HTTP; the section should resemble the following:

```
<primary-servers>
<!--
| 0 or more URL elements that specify the primary location of each xMatters server's
| RegisterIntegrationAgent Web Service. The URLs must begin with either http:// or https://
| and cannot have a query or fragment component. The URLs must be resolvable from this IA.
+-->
<url>https://localhost:8443/api/services/AlarmPointWebService</url>
</primary-servers>

<!--
| These servers are assumed to be connected to the same xMatters database,
| which can be different than the primary servers' database.
+-->
<secondary-servers>
<!--
| 0 or more URL elements that specify the secondary location of each xMatters server's
| RegisterIntegrationAgent Web Service. The URLs must begin with either http:// or https://
| and cannot have a query or fragment component. The URLs must be resolvable from this IA.
+-->
<url>https://localhost:8443/api/services/AlarmPointWebService</url>
</secondary-servers>
```

Note: For trusted certificates, "localhost" should be replaced with the `COMMON NAME (CN)` specified in the certificate and the port should be set to the port specified in the SSL configuration for the xMatters server.

3. Modify the value for the `<service-gateway>` element to use SSL; note that the service-gateway host IP must be resolvable from the xMatters servers:

```
<service-gateway ssl="true" host="localhost" port="8081"/>
```

4. Restart the integration agent.

4.3.4 Optional Configuration

The following scenarios illustrate the common configuration options available when using SSL.

Scenario 1

- BMC Remedy certificate: CA-certified
- xMatters certificate: CA-certified

In `wsutil.js`, set the variable `ACCEPT_ANY_CERTIFICATE` to *false*.

This will ensure ALL communication between the integration agent and BMC Remedy and the integration agent and xMatters uses the appropriate CA certified certificates

Scenario 2

- BMC Remedy certificate: CA-certified
- xMatters certificate: self-signed

In `wsutil.js`, set the variable `ACCEPT_ANY_CERTIFICATE` to *false*.

In `xmatterws.js`, add the following line at the end of the `init()` method:

```
this.ACCEPT_ANY_CERTIFICATE = true;
```

This will allow communication between the integration agent and xMatters to use self-signed certificates while maintaining more complete security between the integration agent and BMC Remedy.

Scenario 3

- BMC Remedy certificate: self-signed
- xMatters certificate: CA-certified

In `wsutil.js`, set the variable `ACCEPT_ANY_CERTIFICATE` to *true*.

In `xmatterws.js`, add the following line at the end of the `init()` method:

```
this.ACCEPT_ANY_CERTIFICATE = false;
```

This will allow communication between the integration agent and BMC Remedy to use self-signed certificates while maintaining more complete security between the integration agent and xMatters.

Scenario 4

- BMC Remedy certificate: self-signed
- xMatters certificate: self-signed

In `wsutil.js`, set the variable `ACCEPT_ANY_CERTIFICATE` to *true*.

This will allow ALL communication between the integration agent and BMC Remedy and between the integration agent and xMatters to use self-signed certificates.

4.4 Adding new parameters

Additional data elements (or tokens) can be forwarded to xMatters by adding them in BMC Remedy. 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 Remedy documentation.*

Each time BMC Remedy triggers the integration service to inject a new event into xMatters, the APXML message is assembled in the function `makeApxmlFrom()` in the file `bmcremedychange.js`. The tokens added to the APXML message are created in two ways:

- Any of the XML elements contained in response of the GetChange operation of the XM_CHG_InfrastructureChange_WS web service will be directly mapped to APXML tokens where the name of the token added will be the same as the name of the XML element:

```
new xMattersWS().addEventTokensFromObject(apxml, changeRequest);
```

- The makeApxmlFrom() function can additionally add APXML tokens based on settings in configuration.js or other program logic; this occurs in the code that follows the call to addEventTokensFromObject().

Adding a new event token therefore requires that you modify the XM_CHG_InfrastructureChange_WS web service or the logic of makeApxmlFrom() (or both), depending on the source of the information that defines the new token.

The XM_CHG_InfrastructureChange_WS web service is provided by the integration to directly obtain information from CHG:InfrastructureChange. It is important to remember that this web service should only be used to obtain information from, and NOT push information to CHG:InfrastructureChange. XM_CHG_ChangeInterface_WS and XM_CHG_ChangeAPDetailSignature should be used to push information into the BMC Remedy workflow.

Once you have chosen the new fields you want to be injected into xMatters, add them to the Output Mapping section of the GetChange operation by using the BMC Remedy Developer Studio. These new fields will then be added to the response sent by BMC Remedy for calls to the GetChange operation.

4.4.1 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:

- Open the xMatters Developer IDE and check out the BMC Remedy Change Management (BUSINESS) Script Package.
- In the Presentation Action Script defaultContent, add the following line to the email content creation section:

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

Your custom parameter should now appear in the notification content for Email Devices.

4.5 Changing and adding response choices

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

- Modify the scripts that present the choices to the notification recipient
- Update the xMatters script to forward the response choice to the integration agent.
- Update the integration agent to send the response choice into BMC Remedy to perform the desired action on the originating change request.

As an example, the following steps illustrate how to add a response choice of "Be there in 10 minutes" to the integration.

Step One: Modifying the presented choices

To present the recipient with the new or modified response choices:

- Launch the xMatters Developer IDE and open the INTERACTION > deviceResponses script.
- Modify the parts of the script that add entries to the \$content.choices variable.

Note that there is logic in the default implementation of this script to add options specific to email Devices and FYI notifications, and to display truncated response option text on limited Devices such as pagers.

Step Two: Forwarding the response to the integration agent

To forward the response choice to the integration agent, 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
```

Step Three: Sending the response into BMC Remedy

To send the response choice from the integration agent into BMC Remedy, open the `bmcremedychange.js` file, and add a new case block to the switch statement in the `handleResponse` function:

```
switch (String(responseAction).toUpperCase())
{
    case RESPONSE_ACTION_HOLD:
var qualification = XM_CHG_CHANGE_AP_DETAIL_SIGNATURE_WS_GET_APPROVAL_BY_ID_QUALIFICATION.replace
("${REQUEST_ID}", String(responseTokens.get("requestId")));
...
    break;
...
    case "be there in ten minutes":
        <your code goes here>
    break;
...
    default:
        throw("Unknown responseAction [" + 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 Online Developer's Guide`.

4.6 Annotations

This integration extensively annotates the originating BMC Remedy change request, but this may not be desirable in all environments. To prevent the annotation of change requests, change the "annotate" Event Domain Constant to *false*. For more information, see "Defining Event Domain Constants" on page 25.

4.7 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 **259200**.

For more information about working with Event Domain Constants, see "Defining Event Domain Constants" on page 25.

4.8 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 25.

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.*

4.9 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 Remedy Change Management (Business) script package set must be checked into the Developer IDE Database. If the script package has not been checked in already, see the instructions in "Importing the script package" on page 24.

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 **bmcremedychange**.
3. On the Event Domain Constants page, do the following:
 - Set the **ENABLEHTML** 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 25.*

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 Remedy Change Management (Business) Production script package::
 - Change `$main.HTML_form_url` to point to a JSP page that you want to process any responses from the HTML email. (the default setting should work out-of-the-box).
 - Set `$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.
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.

4.10 Uninstalling

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

To remove the BMC Remedy objects installed as part of this integration:

1. Open the BMC Remedy Developer Studio
2. Locate and remove the following packing lists:
 - XM:Foundation Packing List
 - XM:Change Packing List

These list all of the objects that are part of the integration. Deleting the objects contained in these lists, and the lists themselves, removes all objects imported into BMC Remedy as part of this integration.

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 25; 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
<code>\$main.use_logFile = false</code>	Specify whether to use an alternate log file for debugging messages. This variable is ignored unless <code>\$main.debug</code> is also set to true.
<code>\$main.logFile = "../logs/"</code>	Defines the file used to log debugging information (only if <code>\$main.use_logfile</code> is set to true).
<code>\$main.HTML_form_url = \$main.xmatters_url & "/jsp/ProcessNotificationResponse.jsp"</code>	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.
<code>\$main.logo = \$main.xmatters_url & "/static/images/logos/xmatters_email.gif"</code>	Specifies the path to the graphic displayed on HTML (email and BES) notifications. Note: For xMatters 4.1 deployments, the path should be changed to: <code>/static/images/xmatters/logos/xmatters_email.gif</code>
<code>\$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.]"</code>	The alternate text to display if the HTML email logo is unavailable. Note: If the logo does not display, it is unlikely that the <code>HTML_form_url</code> is valid and responses will not be injected from HTML Devices (email and BES).
<code>\$main.numeric_pager_number = "555-1212"</code>	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 36.*

FYI and Subscription variables

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



1-877-xMatters

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