xMatters On-Demand

FOR BMC REMEDY SERVICE DESK INCIDENT MANAGEMENT

(x)matters

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

Monday, May 8, 2017

Copyright © 1994-2017. All rights reserved.

xMatters™, xMatters®, xMatters® Java Client, xMatters mobile access, xMatters Integration Agent, 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.

Corporate Headquarters

12647 Alcosta Blvd., Suite 425
San Ramon, CA 94583
Telephone: 925.226.0300
Facscimile: 925-226-0310

Client Asistance:

International: +1 925.226.0300 and press 2
US/CAN Toll Free: +1 877.XMATTRS (962.8877)
EMEA: +44 (0) 20 3427 6333
Australia/APJ Support: +61-2-8038-5048 opt 2

Customer Support Site: https://support.xmatters.com

This integration was designed and tested on an unmodified version of BMC Remedy Incident 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.

Table of Contents

Chapter 1: Introduction to integrations

xMatters On-Demand reduces incident response time by finding the right person to solve the problem when system outages require you to manage on-call schedules and escalations.

- **Reduce downtime**: create and automate critical incident processes to get the right people on the job.
- **Aggregate and consolidate alert views**: closed loop integration between xMatters and BMC Remedy provides a single view of all alerts, no matter how diverse and distributed your environment may be.
- **Engage resolution teams**: determine message recipients based on on-call schedules, including substitutions and holidays, specific skill sets, escalation priority, and more.
- **Avoid alert fatigue**: reduce the noise with targeted notifications; alerts go only to the people that need them.
- **Manage issues from anywhere**: full-featured mobile apps allow you to stay in control wherever you are.

Through communication plans, xMatters can become the voice and interface of an automation engine or intelligent application. When a management system detects something that requires attention, xMatters places phone calls, sends messages, or emails 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 the management system. Responses are executed immediately on the original management system event, enabling remote updates and resolution.

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

1.1.1 Information workflow

The following diagram illustrates a standard workflow in an incident management system, and how information from the management system is passed into xMatters:
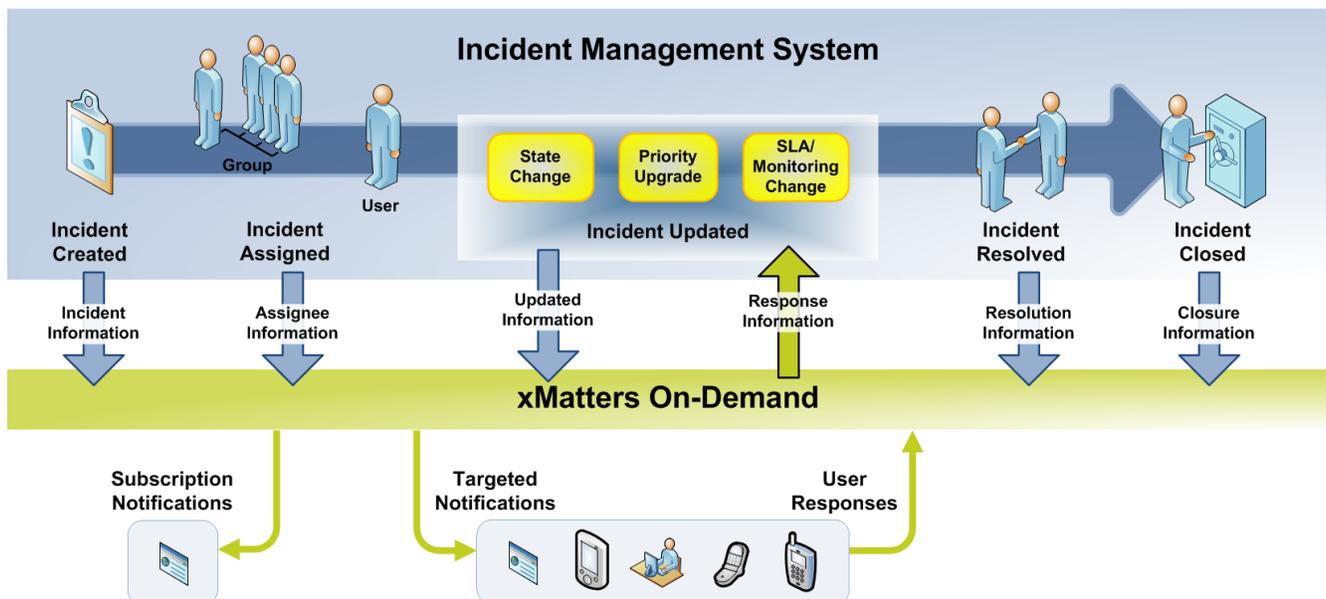
1.2 Integration architecture

The software components in this integration include:

- xMatters On-Demand
- BMC Remedy Incident Management
- xMatters Integration Agent

The incident integration service runs in the Integration Agent and handles events and responses associated with BMC Remedy incidents. The integration involves the following steps each time you create, delete, or update an incident within BMC Remedy:

1. BMC Remedy triggers one of the xMatters filters provided as part of the integration.
2. The filter sends a SOAP web service request to the integration service.
3. The integration service processes the request, using web services exposed by BMC Remedy to obtain information about the incident that has been updated.
    - This information is used to construct a message that is sent to xMatters via the xMatters REST API.
4. In the case of an incident update, xMatters notifies the appropriate recipients, and passes the recipient responses back to the Integration Agent.
5. The Integration Agent passes the response to the integration service, which updates the incident in BMC Remedy via web service requests.

1.2.1 Event workflow

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

BMC Remedy process	Details	xMatters process
Incident Created	A new incident is created with priority of "Critical" or "High".	A notification is created for delivery to the assignee; if no assignee is specified, the notification is sent to the support group.
Incident Reassigned	The "Support Group" or "Assignee" is changed for an existing incident with priority of "Critical" or "High".	A notification event is created for delivery to the assignee; if no assignee is specified, the notification is sent to the support group. If a BMC Remedy user account assigns the ticket to itself, no notification is created.
Priority Changes	An existing incident's priority is changed to "High" or to "Critical".(This does not trigger if the priority is downgraded from "Critical" to "High".)	A notification event is created for delivery to the assignee; if no assignee is specified, the notification is sent to the support group.
SLM Status Changes	The "SLM Status" for an existing incident (with a Priority of "Critical" or "High") is changed to "All Service Targets Breached", "Service Targets Breached", or "Service Target Warning".	A notification event is created for delivery to the assignee; if no assignee is specified, the notification is sent to the support group.
Incident Terminated	The "Status" for an existing incident (with a Priority of "Critical" or "High") is changed to "Canceled", "Closed", or "Resolved".	All previous notification events associated with the incident are terminated.
Incident Re-opened	An incident (with a priority of "Critical" or "High") is re-opened.	A notification event is created for delivery to the assignee; if no assignee is specified, the notification is sent to the support group.

BMC Remedy process	Details	xMatters process
Incident Priority Downgraded	An existing incident has its priority changed from "Critical" or "High" to a lower value.	All previous notification events associated with the incident are terminated.
Self Assignment from Remedy	User assigns an incident to themselves.	All previous notification events associated with the incident are terminated.

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 changing incident status or assignment, or updated users and groups. 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.

Incident web services:

- **XM_HPD_HelpDesk_WS**: used to obtain information from HPD:Help Desk, but should not be used to update incidents. While this web service provides more information than HPD:IncidentInterface, HPD:IncidentInterface is the method supported by BMC Remedy to ensure workflow.

- **XM_HPD_IncidentInterface_WS**: used to update incidents. This web service is the supported method of interacting with HPD:Help Desk, and is therefore the end point for making updates. The out-of-box functions include adding a worklog entry, updating the assignee/assigned group, updating the ticket status, and resolving an incident.

- **XM_SupportGrp_SupportGrpAssoci_WS**: exposes the custom XM:SupportGrp_SupportGrpAssoci_join_form, which addresses the out-of-box behavior of the CTM:Support Group Association form where the Company, Support Organization, and Support Group fields are not populated. The join form is modeled after CTM:SupportGrp_ SupportGrpAssoci_join_from, which provides most of the same information. The xMatters version includes "Login ID" and "Fullname" fields.

Data load web services:

- **XM_CTM_People_WS**: exposes the fields belonging to CTM:People that can be used to create an xMatters User.

- **XM_CTM_Support_Group_Association_WS**: exposes CTM:Support Group Association; specifically, this web service exposes the Login ID of all members of the group specified in the Qualification. The Qualification can also be used to further limit which group members are returned, which should be a list of those members that will be made members of the corresponding xMatters group.

- **XM_CTM_Support_Group_WS**: exposes the fields belonging to CTM:Support Group that can be used to create an xMatters group.

- **XM_CTM_SupportGroupFunctionalRole_WS**: exposes the fields in CTM:SupportGroupFunctionalRole that can be used to obtain Support Group Functional Role data that can then be mapped to roles in xMatters.

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 2.

Incident filters (each filter begins with "XM:Incident" to help identify it as being required by the integration):

- **XM:Incident_Closed_899**: Attempts to delete xMatters events that have the same incident ID as a ticket in BMC Remedy when the related incident (with a priority of High or Critical) has its status changed to Resolved, Cancelled, or

Closed.

- **XM:Incident_PrioritySetCritical_899**: Attempts to inject an xMatters event when a BMC Remedy incident has a status of New, Assigned, In Progress, or Pending, and its priority is changed to Critical from Low, Medium, or High.
- **XM:Incident_PriorityUpgradeHigh_899**: Attempts to inject an xMatters event when a BMC Remedy incident has a status of New, Assigned, In Progress, or Pending, and its priority is changed to High from Low or Medium.
- **XM:Incident_Re-Assigned_899**: Attempts to inject an xMatters event when a BMC Remedy incident is re-assigned; i.e., an incident with a status of New, Assigned, In Progress, or Pending and a Priority of either High or Critical has its Assignee changed, or has its Assigned Group changed while the Assignee field is empty. Note the following exceptions:
  - An event will not be injected if the Assignee is the user currently modifying the incident through a BMC Remedy client.
  - An event will not be injected if the user currently modifying the incident is the BMC Remedy user that the Integration Agent uses to update incidents.
- **XM:Incident_Re-Opened_899**: Attempts to inject an xMatters event when a BMC Remedy incident is re-opened; i.e., the status is changed from Resolved, Cancelled, or Closed to New, Assigned, In Progress, or Pending, the Priority is either High or Critical, and the Assignee is not the user who re-opened the incident.
- **XM:Incident_SLMStatusRed_899**: Attempts to inject an xMatters event when a BMC Remedy incident has a Status of New, Assigned, In Progress, or Pending, and a priority of either High or Critical and the SLM Status is changed to either Service Targets Breached or All Service Targets Breached from No Service Target Assigned, Within the Service Target or Service Target Warning.
- **XM:Incident_SLMStatusYellow_899**: Attempts to inject an xMatters event when a BMC Remedy incident has a status of New, Assigned, In Progress or Pending and a priority of either High or Critical and the SLM Status is changed to Service Target Warning from No Service Target Assigned or Within the Service Target.
- **XM:Incident_Submitted_899**: Attempts to inject an xMatters event when a BMC Remedy incident is created with a status of New, Assigned, In Progress or Pending and a Priority of either High or Critical.
- **XM:Incident_TerminateEventsWhenDowngraded_899**: Attempts to delete xMatters events that have the same incident ID as a BMC Remedy incident when the corresponding BMC Remedy incident with a status of New, Assigned, In Progress or Pending has its priority changed to Low or Medium from either High or Critical.
- **XM:Incident_TerminateEventsWhenRe-AssignedToMe_899**: Attempts to delete xMatters events that have the same incident ID as a BMC Remedy incident when a user reassigns the incident to themselves using a BMC Remedy client; i.e., the corresponding incident with a status of New, Assigned, In Progress or Pending and a priority of either High or Critical is reassigned to the current user logged into BMC Remedy

Data Load filters:

- **XM:Group_Add_600**: Runs when a new instance of CTM:Support Group is created.
- **XM:Group_Delete_600**: Runs when the Status field of a CTM:Support Group record is set to Delete.
- **XM:Group_Update_600**: Runs when an instance of CTM:Support Group is modified and the Status field does not have a value of Delete
- **XM:GroupMember_Add_600**: Runs when an instance of CTM:Support Group Association is created or modified, the Support Group ID field is not null, and the Status field is set to Enabled.
- **XM:GroupMember_Delete_600**: Runs when an instance of CTM:Support Group Association is deleted and the Support Group ID field is not null.
- **XM:GroupMember_Update_600**: Runs when an instance of CTM:Support Group Association is modified, the Support Group ID field is not null, and the field Assignment Availability is set to Yes.
- **XM:Person_Add_850**: Runs when an instance of CTM:People is created.
- **XM:Person_Delete_850**: Runs when an instance of CTM:People is modified and the field Profile Status has a value of Delete.

■ **XM:Person_Update_850**: Runs when an instance of CTM:People is modified and the field Profile Status does not have a value of Delete.

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 2.

XM:Event Injection

The XM:Event Injection form is the staging area for sending events to the Integration Agent. Each event includes a BMC Remedy ID, an Action keyword, a form URL and, optionally, an optional message added to the Remedy incident. The BMC Remedy ID can be used to query for more information using web services. The Action keyword describes what should be done in xMatters. The URL points to the form used to create the event in xMatters. Finally, the message is optional, and can be added to the Remedy incident work log when events are deleted.

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:

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.

XM:SupportGrp_SupportGrpAssoci_join_form

This form addresses the out-of-box behavior of the CTM:Support Group Association form where Company, Support Organizations, Support Group fields are not populated.

This join form is modeled after CTM:SupportGrp_SupportGrpAssoci_join_form, which provides most of the same information. The xMatters version includes the fields Login ID and Fullname.

1.3 System Requirements

The following component versions are supported by this integration.

Integration Component	Version
xMatters On-Demand	
xMatters Integration Agent	5.1 patch 008
BMC Remedy Incident Management	8.1

For a complete list of supported operating systems and other components, refer to the *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 Integration Agent installation folder is referred to throughout the documentation as <IAHOME>.

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

1.4.2 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 (i.e., incident), but can also collectively be called events.
Management system	A management system is any sort of IT service management software, and with which xMatters can combine; i.e., a synonym for BMC Remedy.
Device	The medium through which a recipient is contacted by xMatters; i.e., email, pager, phone, 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 On-Demand for BMC Remedy Service Desk Incident Management integration. This chapter also contains complete instructions on how to configure xMatters, BMC Remedy, and the integration components.

2.1 Configuring xMatters

Before you can configure xMatters for the integration, you need to download and extract the integration components.

To install the integration components:

1. Extract the integration archive file (`.zip` or `.tar.gz`) to a location on the computer hosting the Integration Agent.

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

Component Name	Description
bmcremedyincident.xml, bmcremedydataload.xml, configuration.js	The JavaScript and XML service configuration file that defines the integration service on the Integration Agent. This integration includes two versions of `configuration.js`: one for the incident management integration service, and one for the data load integration service.
BMCRemedyITSMIncident.zip, BMCRemedyITSMIntegratedProperties.zip	Pre-configured communication plans containing the necessary forms and properties for the integration.
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 41.

2.1.1 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 the following English voice files (.vox):

- a bmc remedy incident
- Accept
- and a summary of
- Ignore
- priority of
- Resolve

Note: *Ensure that the names of the recordings match the names of the files; file names are case-sensitive, and spacing must be respected.*

To install the voice files:

1. Log in to xMatters as a company administrator.
2. Click the **Developer** tab.
3. In the Phone Recordings menu, click **Add Phone Recording**.
4. On the Add a Phone Recording page, specify the following settings:
   - **Recording Phrase:** a bmc remedy incident
   - **Event Domain:** applications
5. Click **Save**.
6. On the "Edit Phone Recording Details for:" page, click **Add New**.
7. On the Add Phone Recordings page, click **Choose File**.
8. Navigate to `\components\xmatters\vox`, and select `a bmc remedy incident.vox`.
9. Click **Open**.
10. Click **Save**.
11. Repeat steps 3-10 for the remaining .vox files in `\components\xmatters\vox`.
    - Ensure that all files are added to the "applications" event domain.

2.1.2 Adding the web service and REST API users

Adding the web service user

This integration requires an xMatters web service user with permission to receive APXML in xMatters to receive user responses and notifications about event status changes. 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 are missing, select them in the **Denied Web Services** list, and then click **Add**:
   - Receive APXML
5. Click **Save**.

Adding the REST API user

To send, delete, and query events, the integration requires a separate xMatters user with permissions to access the integration's forms. By default, users with the Full Access User role have these permissions. To change this (for example, to limit the access to a specific user), you can modify forms permissions.

To set up a REST API user:

1. In the xMatters web user interface, click the **Users** tab.
2. Click **Add User**.
3. On the Add a User page, specify the following settings:
   - **User ID**: Type the value you configured as INITIATOR_USER_ID in the `configuration.js` file. The default is "Remedy".
   - **First Name**: Remedy
   - **Last Name**: ITSM

4. In the Available Roles list, select **Full Access User**, and then click **Add**.
   - The role you select must match the role configured under Permissions in the integration form.
5. Click **Save**.
6. On the Change Web Login page, specify the following settings:
   - **Web Login ID**: Type the value you configured as INITIATOR in the `configuration.js` file. The default is "remedyincident".
   - **New Password** and **Verify New Password**: Type the password you encoded in INITIATOR_PASSWORD_FILE.

7. Click **Save**.

2.1.3 Importing and configuring the communication plan

The integration package includes a .zip file that was created using the xMatters "Export Plan" feature; this greatly simplifies the xMatters configuration process by enabling you to create the integration communication plan, forms, event properties, and responses in a single step.

To import the plan:

1. Log in to xMatters as a company administrator, and click the **Developer** tab.
2. On the Communication Plans page, click **Import Plan**.
3. In the Import Communication Plan File dialog box, click **Choose File**, and then locate the `\components\xmatters\plans\BMCRemedyITSMIncident.zip` file extracted from the integration archive.
4. Click **Open**, and then click **Import Plan**.
5. Click **Plan Disabled** to enable the plan.
6. In the **Edit** drop-down list, select **Forms**.
7. In the **New Incident Alerts** form, in the **Not Deployed** drop-down list, click **Create Event Web Service**.
   - After you create the web service, the drop-down list label will change to **Web Service Only**.
8. In the **Web Service Only** drop-down list, click **Permissions**.
9. Enter the REST API user created in "Adding the web service and REST API users" on page 9.
10. Click **Save Changes**.

After importing the communication plan, review the list of properties in the forms to ensure that they match the values of list properties in your configuration.

Accessing web service URLs

To get the web service URL for a form, in the **Web Service Only** drop-down list, click **Access Web Service URL**. Copy the highlighted URL at the top of the dialog box.

Note: *The Access Web Service URL option appears twice in the drop-down menu. Ensure that you click the option just below Create Event Web Service.*

2.1.4 Installing the data load components

The data load integration includes several components that must be imported into xMatters

---

Note: *The configuration steps described in the following sections may require the assistance of your xMatters On-Demand client success manager.*

Import the event domain

By default the data load integration is uses an event domain of "bmcremedydataload"; 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.

To import and define the 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 **Import New**.
4. On the Import Integration page, click **Choose file**.
5. Locate the `components\xmatters\event-domain\xM-BMC-Remedy-DL.xml` file within the extracted integration archive, click **Open**, and then click **Upload**.
6. On the Event Domains page, click the **bmcremedydataload** link.
7. On the Event Domain Details page, in the Integration Services area, click **Add New**.
8. Enter the following information into the form:
   - **Name**: bmcremedydataload-5-1-2
   - **Description**: BMC Remedy Data Load Integration Service
   - **Path**: *Leave blank; this field is not required.*
9. Click **Save**.

Specifying connection parameters

Once you have imported the event domain package and configured the integration service, you must specify the connection parameters for the data load integration.

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 **bmcremedydataload**, 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.

2.1.5 Installing the integration services

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 `IAConfig.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.*

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. If you backed up an existing deduplicator file as indicated in the note above, merge the contents of your backup with the newly installed `<IAHOME>\conf\deduplicator-filter.xml` file: open both files in a text editor, and then copy the <filter> node from the backup file into the new deduplicator file after the last </filter> node. Save and close the file.
3. Open the `IAConfig.xml` file found in `<IAHOME>\conf` and add the following line to the "service-configs" section:
   ```
   <path>remedy81/remedyincident-5-1-2/bmcremedyincident.xml</path>
   <path>remedy81/bmcremedydataload-5-1-2/bmcremedydataload.xml</path>
   ```
4. In the `external-service-request` section, ensure that the "mode" attribute is set to "indirect".
5. Ensure that the `service-gateway` section is enabled.
6. Save and close the file.
7. Open the `<IAHOME>\integrationservices\remedy81\remedyincident-5-1-2\configuration.js` file in a text editor, and set the values for the following variables:

Variable	Description
MID_TIER_HOSTNAME	Name or 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 have the Incident Master role. For more information, see "Configuring ITSM user" on page 15.
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.

Variable	Description
DEDUPLICATOR_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 `deduplicator-filter.xml` file. The default is bmcremedyincident-5-1-2. For more information, see "Filtering and suppression" on page 41.
WEB_SERVICE_URL	Specifies the web service URL of the New Incident Alerts form, which is used to create events in xMatters. You can locate the web service URL for this form on the BMC Remedy relevance engine after you have imported it into xMatters. Typically, it has the following format: `http://<IPaddress>/reapi/2015-01-01/forms/<UID>/triggers` For more information, see "Importing and configuring the communication plan" on page 10.
FORMS	This array maps each of the form names used in BMC Remedy filters to the corresponding relevance engine form web service URLs. **Note**: You will need a web service URL for each form used in the integration. For more information, see "Importing and configuring the communication plan" on page 10.
INITIATOR	The web login ID of a separate xMatters user for authenticating REST API requests to xMatters. The user, or its role, must have permission to access the integration's forms. The default login ID is "remedyincident". For more information, see "Adding the web service and REST API users" on page 9.
INITIATOR_PASSWORD_FILE	Location of the file containing the password of the xMatters user configured as INITIATOR. **Note**: The password must be encoded with `iapassword` utility, as explained in "Setting web services user password", below.
INITIATOR_USER_ID	The user ID of the xMatters user that authenticates REST API calls. The default user ID is "Remedy".
RESPONSE_OPTIONS_WHEN_ASSIGNED_TO_USER	Configure this variable with the response identifiers of both Accept and Resolve for all forms used by the integration. For more information, see "Changing and adding response choices" on page 45.
XMATTERS_COMPANY_NAME	Specifies the xMatters company to use when making web service calls from the Integration Agent to xMatters.

8. Save and close the file.
9. 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 `remedyincident-5-1-2\configuration.js` file.

Password file name:

- `xm_hpd_ws.pwd` stores the password for the `REMEDY_WS_USERNAME` user used by the bmcremedyincident-5-1-2 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, and <old_password> is the existing password (the default value for a newly installed integration is "password"):

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

To configure the xMatters REST API 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 INITIATOR user specified in the `configuration.js` file, and <old_password> is the existing password (the default value for a newly installed integration is "password"):

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

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
- Disable automatic assignments

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.

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_8_1.def` file.
    - Click the **Browse** button to the right of the text field and navigate to the location of the `xm_foundation_8_1.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_dataload_8_1.def` and `xm_incident_8_1.def` files.

   - Note that these files must be imported after the foundation file.

7. Click **Finish**.

2.2.2 Configuring filters

The integration includes a filter that uses the Set Fields action to consume a web service; this object needs its endpoint changed to the address of the Integration Agent.

Filter:

- XM:EI:EventInjection_100

Example of an event injection filter with a modified Endpoint field (from BMC Remedy 8.1):

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

2.2.3 Configuring ITSM user

The Integration Agent requires a dedicated ITSM user to interact with incidents.

Create an ITSM user

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

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

Update the filter qualification

The XM:Incident_Re-Assigned_899 filter contains the following qualification criteria:

```
($USER$ != "xmatters")
```

This qualification prevents the integration from sending a second notification based on an incident's assignment changing because of a user response to an earlier notification. Replace xmatters with the name of the ITSM user created in Step One.
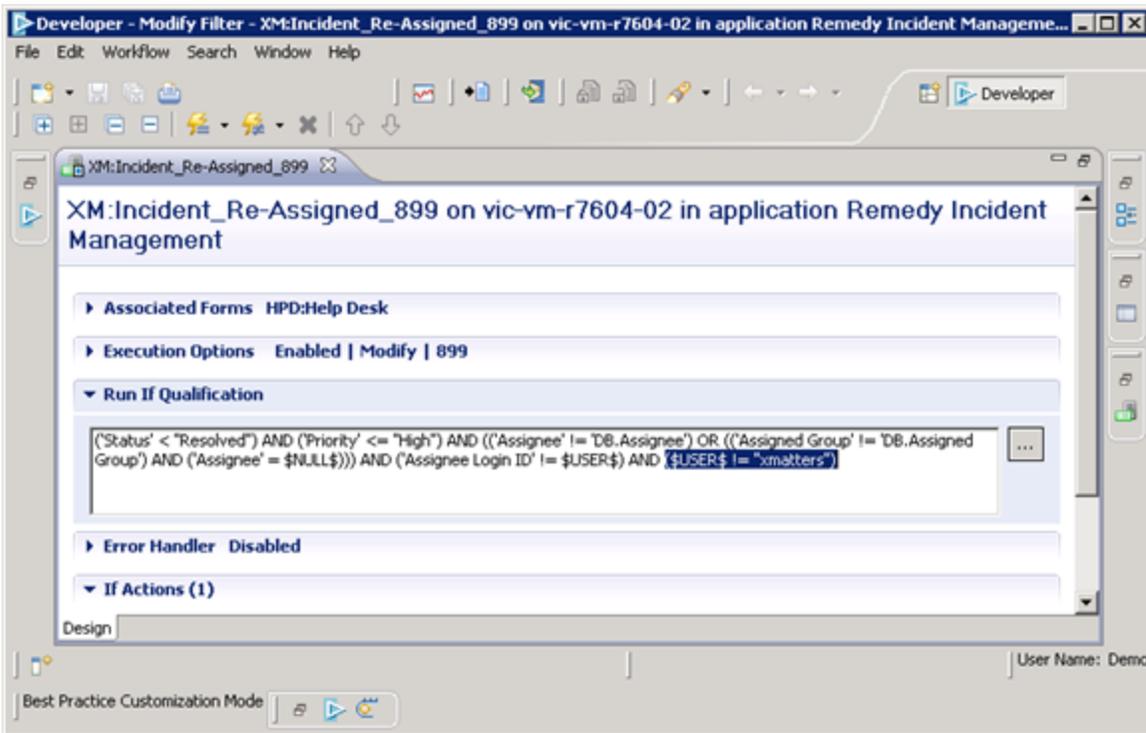
Update the default assignee

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 incidents 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.
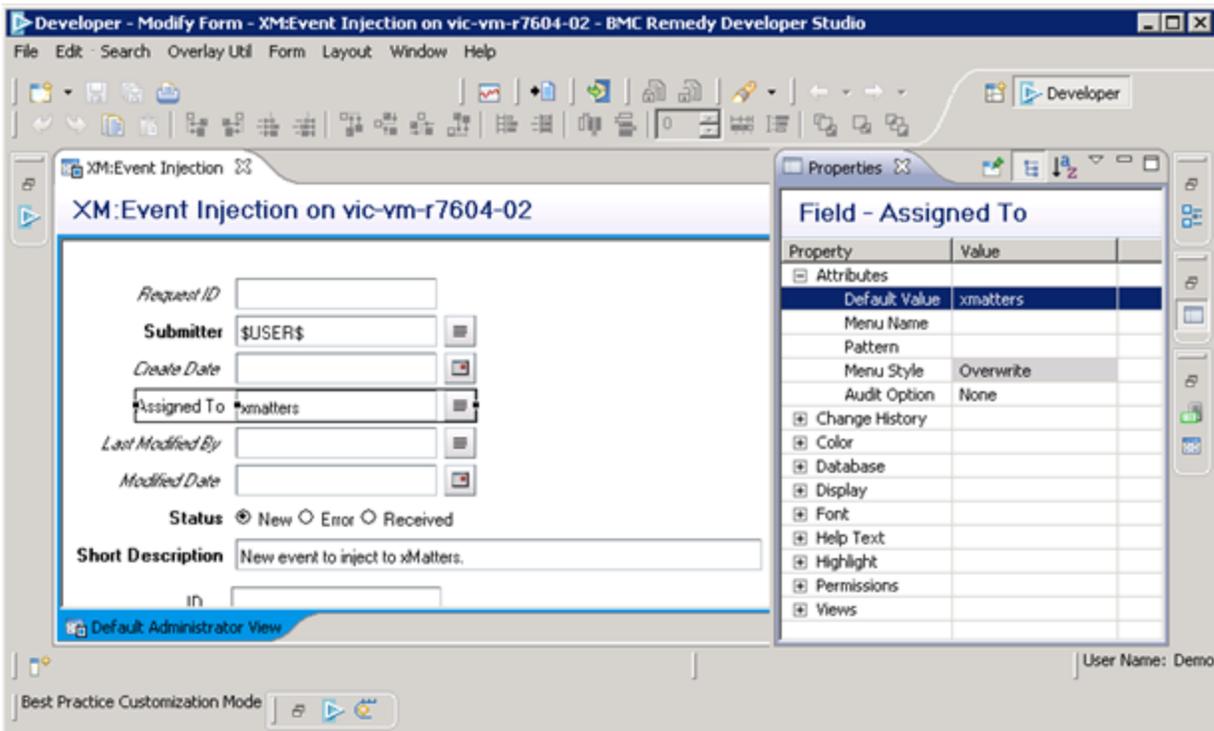
2.2.4 Disabling automatic assignment

To allow xMatters to control assignments, you must turn off the automatic assignment feature in BMC Remedy.

Note: *To perform this step, you will need to login as a user with Administrator permission.*

To disable automatic assignments:

1. Log in to the BMC Remedy Mid Tier web server.
2. Click **Applications**, and then click the **Application Console** left-menu item.
3. Click **Application Administration Console**.
4. In the new window, expand **Incident Management**, and then expand **Advanced Options**.
5. Select **Rules**, and then click **Open**.
6. Search for all existing "Configure Incident Rules".
7. For each existing rule, do the following:
     - Select the rule, and in the **Assignment Process** drop-down list, select **(clear)**.
     - Click **Save**.

Repeat steps 7 and 8 for all companies that will be a participant in the xMatters integration.

2.3 Configuring data load

This integration supports one-way data load of users, devices, support groups, and support group associations from BMC Remedy to xMatters. When one of these objects is created, modified, or deleted in BMC Remedy, the change is propagated to xMatters.

To configure the data load process for your deployment, modify the configuration files included with your deploymentas described in the following sections.

2.3.1 Data load configuration files

The data load configuration files are installed to `<IAHOME>\integrationservices\remedy81\remedyincident-5-1-2\` as described in "Installing the integration services" on page 11, and consist of the following files:

- `configuration.js`: defines the default values for objects loaded into xMatters, and controls the logging of data load result.
- `dataSyncList.js`: defines whether the data load will update existing objects or only add new objects, and specifies the list of included or excluded objects (referred to as the "sync list").

These files define the default values that control the behavior of data load operations; you can modify the behavior of the data load process by specifying the parameters in the following tables.

Data load settings: configuration.js file

To configure the data load integration service:

1. Open the `<IAHOME>\integrationservices\remedy81\remedyincident-5-1-2\configuration.js` file in a text editor, and set the values for the following variables:

Variable	Description	Default
XM_CTM_WS_USERNAME	Connection information and credentials used to access the BMC Remedy web services that support the integration. The user chosen here must have read access to the following forms: • CTM:People • CTM:Support Group • CTM:SupportGroupAssociation	xmatters
XM_CTM_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" on page 14	conf/xm_ctm_ws.pwd
MID_TIER_HOSTNAME		localhost
MID_TIER_PORT		8080
REMEDY_SERVER_NAME		ARServer
XMATTERS_COMPANY_NAME	Specifies the xMatters Company to use when making web service calls from the Integration Agent to xMatters; this value is required by xMatters On-Demand.	
SEND_SYNC_SUMMARY	Determines whether the data load summary should be sent to the user specified in XMATTERS_ADMINISTRATOR. This summary is written to the Integration Agent logs.	true
XMATTERS_ADMINISTRATOR	The xMatters user ID to which you want to send the data load summary.	companyadmin
XM_CTM_PEOPLE_WS_BATCH_QUALIFICATION	Selects a subset of BMC Remedy users for transfer to xMatters.	
XM_CTM_SUPPORT_GROUP_WS_BATCH_QUALIFICATION	Selects a subset of BMC Remedy groups for transfer to xMatters.	
DEFAULT_SUPERVISOR	The xMatters user ID of the default supervisor for users and groups in xMatters.	companyadmin
DEFAULT_XMATTERS_ROLES	The default roles assigned to users in xMatters.	Standard User
MAP_REMEDY_USER_ROLES	If this variable is *false*, all xMatters users will be assigned the role or roles defined by DEFAULT_XMATTERS_ROLES, irrespective of what BMC Remedy roles the individual users have. If *true*, the xMatters roles assigned to individual users will be based on their roles inBMC Remedy and the role mappings defined by the roleMap variable.	false
DEFAULT_USER_SITE	Determines the site to which any new xMatters user should belong.	Default Site

Variable	Description	Default
EXTERNALLY_OWN_USERS	Determines whether users created in xMatters should be marked as "Externally Owned". For more information about externally-owned users and groups, consult the online help available from within xMatters.	false
EXTERNALLY_OWN_GROUPS	Determines whether groups created in xMatters should be marked as "Externally Owned".	false
WEB_LOGIN_TYPE	Specifies the method of web login to use for users created in xMatters; possible values are "NATIVE" (uses xMatters web login credentials) or "LDAP".	NATIVE
WEB_LOGIN_LDAP_DOMAIN	Specifies the LDAP domain to use if WEB_LOGIN_TYPE is set to "LDAP".	company.com
roleMap	If MAP_REMEDY_USER_ROLES is set to true, this setting specifies how to map BMC Remedy support groups functional roles to xMatters roles.	
countryCodes	Associates international country dialing prefixes with ISO 3166-1 alpha-2 codes required by xMatters.	The default mapping converts a dialing code of "1" to the country code "US"
DEVICE_NAME_<type>	These parameters are used to set the default device name in xMatters for the BMC Remedy device; this list includes the following parameters and defaults: ```var DEVICE_NAME_EMAIL = "Work Email";` `var DEVICE_NAME_PHONE_NUMBER_BUSINESS = "Work Phone";` `var DEVICE_NAME_PHONE_NUMBER_MOBILE = "Mobile Phone";` `var DEVICE_NAME_PHONE_NUMBER_HOME = "Home Phone";` `var DEVICE_NAME_PHONE_NUMBER_FAX = "Other Phone";```	
PROVIDER_NAME_<type>	These parameters are used to set the default protocol provider in xMatters for phone and email devices; this list includes the following parameters and defaults: ```var PROVIDER_NAME_EMAIL = "SMTP Email";` `var PROVIDER_NAME_VOICE = "PHONE Engine";```	
XMATTERS_COMPANY_NAME	Specifies the xMatters Company to use when making web service calls from the Integration Agent to xMatters; this value is required by xMatters On-Demand.	company
REMOVE_USERS_FROM_ALL_TEAMS_IN_GROUP	Controls how removing a user from a BMC Remedy group will affect users in xMatters. If *false*, removing a user from a group in BMC Remedy will remove the user only from the default team in the corresponding xMatters group. If set to *true*, the user is removed from all teams in the xMatters group.	false

2. Save and close the file.
3. Restart the Integration Agent.
   - On Windows, the Integration Agent runs as a Windows Service; on Linux, it runs as a daemon.

Data load settings: dataSyncList.js file

The following settings can be modified or adjusted in the `dataSyncList.js` file; for more information about these settings and how they interrelate, see the following section, "Data load process":

Variable	Description
SYNC_ACTION	Defines whether the users and groups specified in the syncList parameter (defined below) should be included or excluded in the data load.
USER_SEED_ONLY	If set to true, user objects will be added to xMatters only when they are initially loaded, and not updated. If set to false, any modifications to the object in BMC Remedy will be synchronized with the object in xMatters, overwriting any changes that may have been made to the object in xMatters.
GROUP_SEED_ONLY	If set to true, group objects will be added to xMatters only when they are initially loaded, and not updated. If set to false, any modifications to the object in BMC Remedy will be synchronized with the object in xMatters, overwriting any changes that may have been made to the object in xMatters. Note that the update process will preserve existing xMatters team information, such as type and rotation settings, and the rotation order and delay settings for existing members.
syncList	An XML document defining user and group names that should be excluded or included, as explained in the following sections.

2.3.2 Data priority and sources

The data load integration service uses the following rules for creating and updating the individual properties of users, groups, and teams in xMatters:

1. New objects are created from a combination of BMC Remedy object information and configured defaults provided by the integration service file.
2. When an object in BMC Remedy is changed and the corresponding user or group in xMatters is updated:
   - Any properties that are populated with information from BMC Remedy will be updated based on BMC Remedy information even if the property has been changed in xMatters.
   - Any properties that are populated with configured defaults will not be updated, and any changes in xMatters will be preserved.

Note: *It may take up to five minutes for users in xMatters to be removed from the database after you remove them from the system.*

The following tables describe the source for the data used to populate the fields users, groups and devices in xMatters.

User data

The data for user details in xMatters that is obtained from BMC Remedy is provided by the XM_CTM_People_WS web service which exposes fields belonging to CTM:People.

xMatters Field	Source
Active	BMC Remedy: Profile_Status
User ID	BMC Remedy: Remedy_Login_ID
First Name	BMC Remedy: First_Name
Last Name	BMC Remedy: Last_Name
User Devices	BMC Remedy
Roles	Configuration file OR BMC Remedy Support group functional roles **Note**: Role information is sent to xMatters only when a user record is initially synchronized. The information is not sent if the user record is modified after the initial sync.
User Site	Configuration file
Supervisors	Configuration file
Externally Owned	Configuration file
Web Login Type	Configuration file
LDAP Domain	Configuration file

Group data

The data for group details in xMatters that is obtained from BMC Remedy is provided by the XM_CTM_Support_Group_WS web service which exposes fields belonging to CTM:Support Group.

xMatters Field	Source
Group Name	BMC Remedy: the xMatters group name is constructed as <Company>*<Support_Organization>*<Support_Group_Name>
Active	BMC Remedy: Status (the xMatters group is marked as active if the status is "Enabled")
Description	BMC Remedy: Description
Externally Owned	Configuration file

User Devices

The data for device details in xMatters is provided by the XM_CTM_People_WS web service which exposes fields belonging to CTM:People.

Note:	*For these devices to be loaded, you may need to add the device names into xMatters. For more information about adding device types and device names, see the xMatters installation and administration guide.*

xMatters Device Name	xMatters Device Type	BMC Remedy Field
Work Email	Email	Internet_Email

xMatters Device Name	xMatters Device Type	BMC Remedy Field
Work Phone	Voice	Phone_Number_Business
Mobile Phone	Voice	Phone_Number_Mobile
Home Phone	Voice	Phone_Number_Home
Other Phone	Voice	Phone_Number_Fax
Numeric Pager	Pager	Phone_Number_Pager

Note that the data load uses the following rules when processing phone number information from BMC Remedy:

1. The integration uses the country code, area code, number, and extension fields from BMC Remedy to populate the xMatters device information.

2. The number field is required, and the device will not be transferred to xMatters if the number is not specified. All other fields are optional.

3. The BMC Remedy fields are used as is; invalid characters (such as "(" and ")") are not removed. The fields must contain values acceptable to xMatters, or the device may not work even if the transfer succeeds.

4. The BMC Remedy country code / numeric dialing prefix is converted to an xMatters Country Code Override that uses the two-character codes form the ISO 3166-1 alpha 2 standard, and the mappings defined by the countryCodes variable in `configuration.js`.

The default integration behavior is to map the dialing prefix 1 to the Country Code Override "US". To change this, or to add additional mappings, see "Changing country code mapping" on page 1.

2.3.3 Data load process

The data load integration transfers user and group information between BMC Remedy and xMatters in two ways:

- Batch data load: the batch data load happens only when a BMC Remedy user manually initiates the process. You must create and save a new instance of XM:Event Injection with an Action field value of "Load"; this instructs the integration to retrieve lists of qualifying users and groups from BMC Remedy and transfer them to xMatters one at a time.

- Dynamic data load: The integration automatically triggers dynamic data load operations whenever users and groups are created or updated in BMC Remedy. In this case, the integration is instructed which object to process, and retrieves the necessary information from BMC Remedy to update the matching object in xMatters.

In both cases, the data is transferred between BMC Remedy and xMatters via the Integration Agent, which uses SOAP web service requests to fetch the data from BMC Remedy and send it to the xMatters instance. The web service on the BMC Remedy server is provided by xMatters and installed as part of the integration (as described in "Custom web services" on page 3).

The rules which govern the data load process are the same for batch and dynamic operations, with the following exceptions:

- The batch operation processes only those users and groups that meet the qualification criteria defined in the `configuration.js` files described in the preceding section. Dynamic updates will process any user or group for which BMC Remedy sends a request. If this user or group does not meet the batch qualification criteria, they will be processed and may result in an update to an existing xMatters user, but will not be added if they do not already exist.

- The batch operation will only add new or update existing users and group. The dynamic process can also delete users and groups from xMatters.

The following sections explain the data load process in more detail.

Batch user data load

The USER_SEED_ONLY variable determines how users are treated when loading them into xMatters:

If the USER_SEED_ONLY variable is set to *true*:

- If (user ID **does not exist** in xMatters) AND (user meets batch qualification criteria) AND [(user ID is not in excluded list) OR (user ID is in included list)]:
    - New user is created in xMatters
    - User information is populated
    - User devices are added to xMatters
- IF (user ID **already exists** in xMatters):
    - No changes are made to any users or devices

If the USER_SEED_ONLY variable is set to *false*:

- If (user ID **does not exist** in xMatters) AND (user meets batch qualification criteria) AND [(user ID is not in excluded list) OR (user ID is in included list)]:
    - New user is created in xMatters
    - User information is populated
    - User devices are added to xMatters
- IF (User ID **already exists** in xMatters):
    - User information is updated
    - User devices are added to match settings in BMC Remedy

Dynamic user data load

The dynamic data load follows the same behavior defined above for batch data loads, with the following additions:

If USER_SEED_ONLY is set to *false*:

- IF the request from BMC Remedy indicates that the user has been deleted:
    - The user is deleted from xMatters
    - User is removed from any team memberships
- IF (the user is updated) AND (user **already exists** in xMatters) AND (user currently does not meet batch qualification criteria:
    - User will be updated in xMatters
- IF (the user is updated) AND (user ID **does not exist** in xMatters) AND (user currently does not meet batch qualification criteria):
    - Nothing is changed or updated

Usage notes:

Dynamic updates to users do not result in the integration service updating their group associations. For example, if a user is updated in BMC Remedy and newly qualifies for inclusion in xMatters, their group memberships will not be reviewed, with the result that they will not be added to any xMatters groups associated with the BMC Remedy groups to which they belong.

When a BMC Remedy user who previously has not met the batch update qualification and does not exist in xMatters is updated and added to a BMC Remedy support group for the first time, the resulting update to xMatters will not add them to a corresponding xMatters group. In this case the User must be manually added to the group in xMatters.

The integration is not able to change the User ID of xMatters users. If a Login ID of a user in Remedy is changed, the resulting update to xMatters will create a new user and leave the original xMatters user unchanged.

BMC Remedy statuses map to xMatters statuses as follows:

- BMC Remedy users with a status of 'Enabled' will have a status of 'Active' in xMatters.
- BMC Remedy users with statuses of 'Proposed', 'Offline', 'Obsolete' or 'Archive' will have a status of 'Inactive' in xMatters.
- BMC Remedy users with a status of 'Delete' will be removed from xMatters.
- Users that are permanently deleted from BMC Remedy will be deleted from xMatters.

Batch group data load

The GROUP_SEED_ONLY variable determines how groups are treated when loading them into xMatters.

Note: The "Escalation Types" field for a rotation team is overwritten whenever group or team members are updated. This is default xMatters web services behavior.

If the GROUP_SEED_ONLY variable is set to *true*:

- If (group name **does not exist** in xMatters) AND (group meets batch qualification criteria) AND [(group name is not in excluded list) OR (group name is in included list)]:
    - New group is created in xMatters
    - Group attributes are added
    - Coverage is created
    - Team is created
- IF (group name **already exists** in xMatters):
    - No changes are made

If the GROUP_SEED_ONLY variable is set to *false*:

- If (group name **does not exist** in xMatters) AND (group meets batch qualification criteria) AND [(group name is not in excluded list) OR (group name is in included list)]:
    - New group is created in xMatters
    - Group attributes are added
    - Coverage is created
    - Team is created
- IF (group name **already exists** in xMatters):
    - Group attributes are updated
    - Team membership is updated (see "Team data load" on page 26)
    - Group coverage is **not** updated

Notes:

- Group updates may modify team memberships, but will maintain existing xMatters Team information, such as type and rotation settings, and the rotation order and delay settings for existing members.
- If a BMC Remedy Support group has no members at the time it is transferred to xMatters, a group will be created with a coverage and a team, but the team will have no members.
- Renaming groups via data load is not supported: if you change the name of a BMC Remedy group after the group has been transferred to xMatters, subsequent batch or dynamic synchronization will create a new group in xMatters matching the new name of the BMC Remedy group. The data load will not modify the original xMatters group, and the new group will not have any coverages that may have been added to the original group.

Dynamic group data load

The dynamic group data load follows the same behavior defined above for batch data loads, with the following additions:

If GROUP_SEED_ONLY is set to *false*:

- IF the request from BMC Remedy indicates that the group has been deleted:
  - The group is deleted from xMatters
- IF (the group is updated) AND (group name **already exists** in xMatters) AND (group currently does not meet batch qualification criteria:
  - The group will be updated in xMatters
- IF (the group is updated) AND (group name **does not exist** in xMatters) AND (group currently does not meet batch qualification criteria):
  - Nothing is changed or updated

Team data load

Team membership is updated in xMatters only as part of a batch or dynamic update of BMC Remedy Support groups; the following sections are included to provide detail on the process. Team data load behavior is the same for both batch and dynamic synchronizations.

Note: The "Escalation Types" field for a Rotation Team is overwritten whenever group or team members are updated. This is default xMatters web services behavior.

If the GROUP_SEED_ONLY variable is set to *true*:

- If (group name **does not exist** in xMatters):
  - New team will be created in xMatters with the name "<GroupName> - Default Team"
  - The team is associated with a default 24x7 coverage
  - New team will comprise only those users in xMatters who are members of the group in BMC Remedy AND for whom "Assignment Availability" equals "Yes"
- IF (Group name **already exists** in xMatters):
  - No changes are made

If the GROUP_SEED_ONLY variable is set to *false*:

- If (group name **does not exist** in xMatters):
  - New team will be created in xMatters with the name "<GroupName> - Default Team"
  - The team is associated with a default 24x7 Coverage
  - New team will comprise only those users in xMatters who are members of the group in BMC Remedy AND for whom "Assignment Availability" equals "Yes"
- IF (group name **already exists** in xMatters) AND ("<GroupName> - Default Team" **already exists** in xMatters):
  - Any users in xMatters who are associated with this BMC Remedy group AND for whom "Assignment Availability" equals Yes AND who are not already in the team are added to the default team in the last position. Team type, member order, and escalations are preserved.
- IF (group name **already exists** in xMatters) AND ("<GroupName> - Default Team" **does not exist** in xMatters):
  - New team will be created in xMatters with the name "<GroupName> - Default Team"
  - The team is **not** associated with any coverage
  - New Team will comprise only those users in xMatters who are members of the group in BMC Remedy AND for whom "Assignment Availability" equals "Yes"

2.3.4 Data load notification and logging

Following each data load operation, a summary of successful, successful with warning, and failed actions is written to the Integration Agent logs. You can also use the XMATTERS_ADMINISTRATOR and SEND_SYNC_SUMMARY variables in

the configuration.js file to send a notification containing the summary to a user or group within xMatters.

Note that the summary notification is FYI-only. No user responses to the notification are supported and the integration does not support any annotations from the recipients of the notification or from xMatters concerning the delivery of the notification.

Chapter 3: Integration validation

After configuring xMatters and BMC Remedy, you can validate that communication is properly configured. Verify that the following components are running:

- BMC Remedy Incident Management
- xMatters On-Demand
- 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.

3.1 Validating data load communication

The following validates that communication from BMC Remedy to xMatters is properly configured for data loading.

To test the data load configuration:

1. Review the `dataSyncList.js`, and ensure that the values of the SYNC_ACTION and syncList variables will allow a new BMC Remedy user to be added to xMatters.
2. In BMC Remedy, create a new user and assign them an email address to use as a device. The user must also have their support staff property set to "Yes", and they must belong to at least one support group.
3. Log in to the xMatters web user interface, and confirm that a new user has been added, and has an email device with the expected address.

If the new user does not exist in xMatters, check the Integration Agent logs for a summary detailing any warnings or failures.

Note:	*After the user has been synchronized, it is recommended that you set the email device's user service provider to use virtual email. (The default synchronization process sets the email service provider to "SMTP Email".) Using the Virtual Email service provider may help when troubleshooting problems in later testing.*

3.2 Triggering a notification

To trigger a notification, create a new incident with a priority of High or Critical in BMC Remedy, and assign it to a user or group that exists in both BMC Remedy and xMatters:

Quick Action

- Assign to Me
- Auto Assign
- Broadcast Incident
- Create Relationship to ▼
- Create Related Request ▼
- 2 Customer's Incidents
- Incident Matching
- Process Overview
- Select Operational
- Select Product

▼ Functions

- Search Knowledge Base
- Decision Tree
- Initiator Script
- Impacted Areas
- Assignment Script
- Email System
- ▶ **more**

Field	Value
Incident ID*+	INC000000000236
Company*+	Calbro Services
Customer*+	Baxter, Bob
Contact+	<Search using Corporate ID>

Field	Value
Notes	
Template+	
Summary*	Exchange Server is down

Field	Value
Service*+	
CI+	
Target Date	
Impact*	1-Extensive/Widespread
Urgency*	1-Critical
Priority*	Critical
Incident Type*	User Service Restoration
Reported Source	

Field	Value
Assigned Group*+	Frontoffice Support
Assignee+	
Vendor Group+	
Vendor Ticket Number	
Status*	New
Status Reason	
Resolution	

3.3 Responding to a notification

This section describes how to respond to a notification from xMatters. In the following example, the notification is received on an Android 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 notifications:
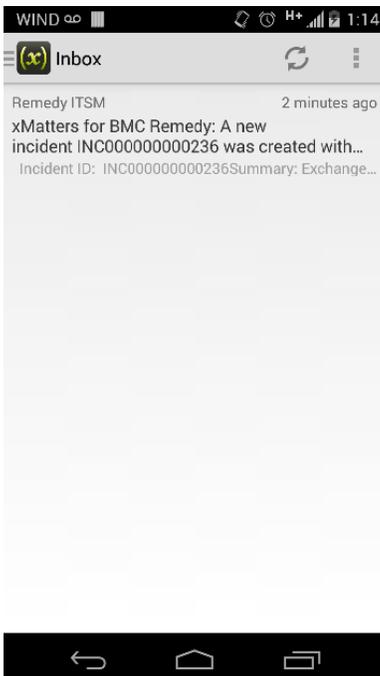
2. Opening the notification displays its details:
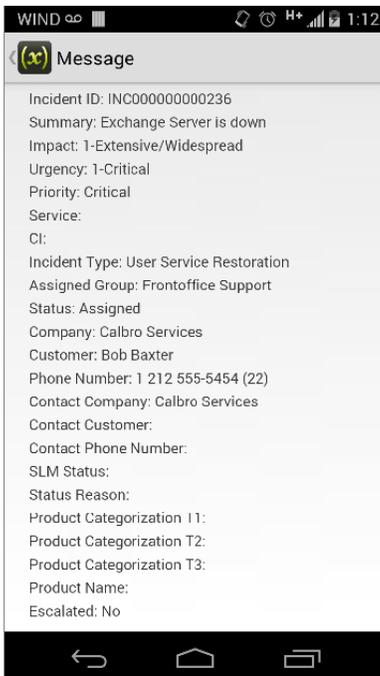
3. Scrolling down will display the remainder of the details, and the list of possible replies:
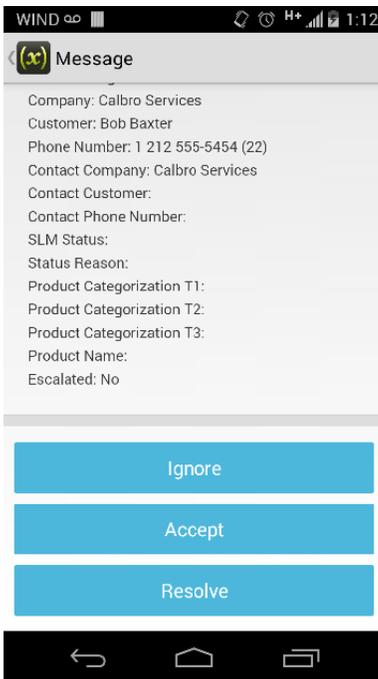
4. To respond to the notification, the user taps on a response choice, and xMatters updates the event in BMC Remedy.
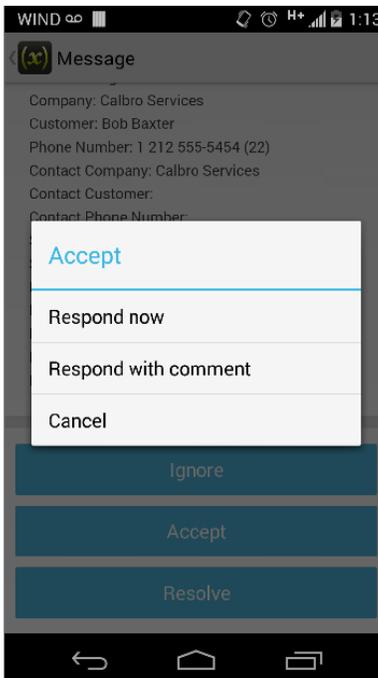
For more information about response choices, and changing the options available to users, see "Response choices" on page 40.

3.4 Viewing response results

In BMC Remedy, the results of the notification are displayed on the incident's Work Detail tab:

Work Detail	Categorization	Tasks	Relationships	Date/System

8 entries returned - 8 entries matched | Preferences ▼ | Refresh

Type	Notes	Submit Date ▼	Submitter
Working Log	[xMatters] - Incident status changed to 'In Progress'.	20/01/2015 13:16:59	xmatters
Working Log	[xMatters] - Response Accept received from Ian.	20/01/2015 13:16:58	xmatters
Working Log	[xMatters] - Notification delivered successfully to Ian	SMS Phone.	20/01/2015 13:12:04	xmatters
Working Log	[xMatters] - Notification delivered successfully to Mary	Android Phone.	20/01/2015 13:12:01	xmatters
Working Log	[xMatters] - Notification delivered successfully to Ian	Android Phone.	20/01/2015 13:11:58	xmatters
Working Log	[xMatters] - Notification delivered successfully to Ian	Home Email.	20/01/2015 13:11:46	xmatters
Working Log	[xMatters] - Event 858009 successfully created in xMatters.	20/01/2015 13:11:43	xmatters
Working Log	[xMatters] - Notification will be sent to [Calbro Services*IT Support*Frontoffice Support].	20/01/2015 13:11:32	xmatters

Chapter 4: Optimizing and extending the integration

This section describes some of the ways you can optimize or extend the integration.

4.1 Customizing communication plans

This integration includes an exported version of the xMatters communication plan that includes forms and properties. The following sections describe the imported components that you can customize to suit your needs.

4.1.1 Configuring communication plan forms

The BMC Remedy Incident Management integration provides 5 form templates:

- Incident Priority Upgrade Alerts
- New Incident Alerts
- Reopened Incident Alerts
- Reassigned Incident Alerts
- SLM Alerts

These forms are used for creating content for xMatters notifications triggered by various BMC Remedy XM:Incident filters. Out of the box, the content of these notification messages is similar, except for the subject lines of email or push messages. However, these subject lines can be customized using the xMatters user interface.

Note: *The names of the properties and values of list properties are expected to match the names of the XML elements and values returned by the BMC Remedy web service.*

The forms come pre-configured to support the following properties returned by the BMC Remedy web service:

Name	Type	Values
Status	List	New
		Assigned
		In Progress
		Pending
		Resolved
		Closed
		Cancelled
Product_Categorization_Tier_1	String	
Product_Categorization_Tier_2	String	
Product_Categorization_Tier_3	String	
Department	String	
Site_Group	String	
Region	String	

Name	Type	Values
Product_Name	String	
Manufacturer	String	
Product_Model_Version	String	
Site	String	
ServiceCI	String	
HPD_CI	String	
Company	List	Calbro Services Invention, Inc.
Country	String	
City	String	
Assigned_Support_Organization	String	
Last_Name	String	
First_Name	String	
Middle_Initial	String	
VIP	List	No Yes
Contact_Sensitivity	List	Standard Sensitive
Phone_Number	String	
Categorization_Tier_1	String	
Categorization_Tier_2	String	
Categorization_Tier_3	String	
Contact_Company	String	
Service_Type	List	User Service Restoration User Service Request Infrastructure Restoration Infrastructure Event

Name	Type	Values
Status_Reason	List	Automated Resolution
		Reported
		Client Action Required
		Client Hold
		Customer Follow-Up Required
		Future Enhancement
		Infrastructure Change
		Infrastructure Change Created
		Local Site Action Required
		Monitoring Incident
		No Further Action Required
		No Longer a Causal CI
		Purchase Order Approval
		Registration Approval
		Request
		Supplier Delivery
		Support Contact Hold
		Temporary Corrective Action
		Third Party Vendor Action Required
Resolution	String	
Urgency	List	1-Critical
		2-High
		3-Medium
		4-Low
Impact	List	1-Extensive/Widespread
		2-Significant/Large
		3-Moderate/Limited
		4-Minor/Localized
Priority	List	Critical
		High
		Medium
		Low
Priority_Weight	String	

Name	Type	Values
Reported_Source	List	Direct Input
		Email
		External Escalation
		Fax
		Self Service
		Systems Management
		Phone
		Voice Mail
		Walk In
		Web
		Other
		BMC Impact Manager Event
Assigned_Group	String	
Assignee	String	
Assigned_Support_Company	String	
Assigned_Group_Shift_Name	String	
Reported_Date	String	
Resolution_Method	String	
Resolution_Category	String	
Resolution_Category_Tier_2	String	
Resolution_Category_Tier_3	String	
Closure_Product_Category_Tier1	String	
Closure_Product_Category_Tier2	String	
Closure_Product_Category_Tier3	String	
Closure_Product_Name	String	
Closure_Product_Model_Version	String	
Closure_Manufacturer	String	
Assignee_Login_ID	String	
Incident_Number	String	
Summary	String	
Notes	String	

Name	Type	Values
Direct_Contact_First_Name	String	
Direct_Contact_Last_Name	String	
Direct_Contact_Phone_Number	String	
SLM_Status	List	No Service Target Assigned
		Within the Service Target
		Service Target Warning
		Service Targets Breached
		All Service Targets Breached
Escalated	List	Yes
		No
Contact_Organization	String	

4.1.2 Defining form properties

The default plan provided with the integration includes a number of properties that contain information about the incoming event. These properties are created when you import the communication plan definition file, and assigned common values as defaults. You will need to modify or remove the default values of list properties to match your deployment.

This integration is preconfigured to support the properties defined in "Configuring communication plan forms" on page 33

For more information about form properties, including the available types, refer to the xMatters On-Demand Online help at help.xmatters.com.

4.1 Configuring integrated properties

This version of the integration supports integrated properties and includes a sample communication plan you can use to demonstrate and test this feature.

This plan is not required for the feature to work and is provided only as an example; to add integrated properties to an existing communication plan skip to Step 2.

Step 1: Import the sample plan

This integration includes a sample plan containing a simple form that you can use to manually create notifications with a custom "escalation message" property and incident data retrieved from BMC Remedy.

To import the sample communication plan:

1. Log in to xMatters, and click the **Developer** tab.
2. On the Communication Plans page, click **Import Plan**.
3. In the Import Communication Plan File dialog box, click **Choose File**, and then locate the `\components\xmatters\plans\BMCRemedyITSMIntegratedProperties.zip` file extracted from the integration archive.
4. Click **Open**, and then click **Import Plan**.
5. Click **Plan Disabled** to enable the plan.

6. In the **Edit** drop-down list, select **Forms**.
7. In the Incident with Integrated Properties form, in the **Not Deployed** drop-down list, click **Form**.
   - After you deploy the form, the drop-down list label will change to "Form Only".
8. In the **Form Only** drop-down list, click **Permissions**.
9. Enter the REST API user you created in "Adding the web service and REST API users" on page 9, and then click **Save Changes**.

Step 2: Defining the integration service

For the installation to be successful, the integration service names must match the names specified in the `bmcremedyincident.xml` file installed on the Integration Agent.

To define an Integration Service:

1. In xMatters, on the Event Domains page, click the **applications** 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**: bmcremedyincident-5-1-2
   - **Description**: BMC Remedy ITSM Integration
   - **Path**: *Not required.*
4. Click **Save**.

Step 3: Configure the integrated properties

Once you have imported the sample plan and created the integration service, you can set up the integrated properties for your integration. (Integrated properties are not included in exported communication plans; they must be manually configured.)

Note:	*For more information about configuring integrated properties, click the Help button on the Integrated Properties tab in xMatters.*

To configure the integrated properties:

1. In xMatters, on the BMC Remedy ITSM - Integrated Properties plan, click the **Integrated Properties** tab, and then click **Create Integrated Properties**.
2. In the Create Integrated Properties dialog box, in the **Name** field, type `Incident Details`, and then click **Create Integrated Properties**.
3. Click **Edit** beside the new integrated properties.
4. On the Incident Details page, enter the following information:

5. Click the **Create a request property** button, and then select **Text** from the drop-down list.

6. In the Create a new Text property dialog box, in the **Name** field, type `Incident Number`, and then click **Create request property**.

7. Click the **Create a response property** button to add a response property; the section below describes the default properties supported by the integration.

   • You can create all of your response properties for the sample form as text properties, but make sure you modify the **Maximum Size** for each property to account for longer fields where required.

8. When you have finished adding properties, click **Save Changes**.

9. To check your configuration, click **Send Test Request** and inspect the returned data.

10. Once you are satisfied with your changes, click the Forms tab, and then click **Edit > Layout** for the Incident with Integrated Properties form.

11. On the Layout tab, drag the **Incident Details** section from the Integrated Properties section and drop it onto the form layout./

12. Click **Save Changes**.

Available properties

The names of the properties must match the names returned by the handleGetIncident() function defined in the integration's `bmcremedyincident-properties.js` file. By default, the integration returns all properties returned by the BMC Remedy web service, replacing the underscores in properties names with spaces. Properties without underscores in their names are returned as is.. You can edit the handleGetIncident() function to modify this behavior.

The default response properties are listed in "Configuring communication plan forms" on page 33. The properties returned can be different, however, particularly for those deployments where the database or web service have been customized. You can use the Send Test Request button to perform a query, and then investigate the XML data to see which properties are being returned.

You can also choose to include only a subset of properties; in this case, xMatters ignores the remaining properties returned by the integration and does not display them to users.

Step 4: Send a test message

You can now create the message content and send a test notification that includes the integrated properties.

To add the integrated properties to message content:

1. On your communication plan form, click the **Messages** tab.
2. Click **Edit** for each message type to which you want to add integrated properties.
3. In the message builder, drag the properties you want to include from the integrated properties section on the right and drop them into the message.pane.
   - Voice messages are constructed differently than email and text messages; for more information about working with voice messages, click the **Help** button at the top of the page on the Messages tab.
4. Click **Save Changes**.

You are now ready to send a test message containing the integrated properties.

To send a test message:

1. Click the **Messaging** tab, and click the name of the form with the integrated properties.
   - If you imported the sample communication plan, the form is named Incident with Integrated Properties.
2. On the form, in the Recipients section, specify a user (or device) whose notifications you can access.
3. Type a brief message in the **Escalation Message** field.
4. In the Integrated Properties section, in the **Incident Number** field, type the number for an active incident in your system, and then click **Search**.
   - xMatters will automatically populate the fields with the details of the specified incident. You can modify these details before sending the message, but your changes will not be reflected on the associated incident.
5. Click **Send Message** to send a test message to the specified recipient.

The test message will include both the escalation message and the incident details retrieved from BMC Remedy.

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 incident. Users notified on email devices also have the ability to respond with an extra annotation message which will be logged in the incident, 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 incident in BMC Remedy.

Response	BMC Remedy Update	xMatters Job Control
Accept (Acc)	Updates the owner of the incident to the responder, sets the Status to In Progress, and records the response in the incident log.	Assign to user
Ignore (Ign)	No status change; records the response in the incident log.	Escalate
Resolve (Res)	Updates the status of the incident to "Resolved", and records the response in the incident log.	End

Job control definitions

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

- **Assign to User:** xMatters stops notifying other recipients, but continues the process for this recipient.
- **Escalate:** xMatters stops notifying this user, but continues the process by immediately escalating the event to the next scheduled recipient.
- **End:** xMatters terminates this notification process for all recipients.

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, see xMatters On-Demand help at `https://help.xmatters.com/ondemand/index.htm`.

Adding annotation messages

Two-way email device notifications can add extra comments that will be added as a message on the incident 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.

Note:	*Responding with a comment is also supported by the xMatters mobile client application.*

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 DEDUPLICATOR_FILTER in the integration service configuration file;.this integration defines the variable within the `configuration.js` file as follows:

```
var DEDUPLICATOR_FILTER = "bmcremedyincident-5-1-2";
```

The value assigned to DEDUPLICATOR_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_number 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-5-1-2">
  <predicates>
    <predicate>incident_number</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.

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 `<IAHOME>\integrationservices\remedy81\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 `<IAHOME>\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 "bmcremedyincident-5-1-2".
- **<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 https://support.xmatters.com).

4.3.3 Updating HTTP to HTTPS

The next step is to update the PROTOCOL in the `<IAHOME>\integrationservices\remedy81\remedyincident-5-1-2\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 properties

Additional data elements can be forwarded to xMatters by adding them in BMC Remedy. The following steps explain how to add a new event property 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 `bmcremedyincident-event.js`. The tokens added to the APXML message are created in two ways:

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

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

- 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_HPD_HelpDesk_WS web service or the logic of makeApxmlFrom(), depending on the source of the information that defines the new token.

The XM_HPD_HelpDesk_WS web service is provided by the integration to directly obtain information from HPD:Help Desk. It is important to remember that this web service should only be used to obtain information from, and NOT push information to HPD:Help Desk. XM_HPD_IncidentInterface_WS 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 GetIncident 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 GetIncident operation.

4.4.1 Adding new properties to notification content

Once you have injected the new data elements, you must add them as properties to the relevance engine, then to individual form layouts and messages.

4.5 Changing and adding response choices

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

- Modify the choices in the relevance engine forms.
- Update the integration agent's configuration script to customize the response choices based on whether the incident is assigned to a group or a person.
- Update the Integration Agent to send the response choice into BMC Remedy to perform the desired action on the originating incident.

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:

1. Log in to xMatters.
2. Click on the **Developer** tab.
3. Locate the **BMC Remedy ITSM - Incident** relevance engine.
4. Click the **Edit** drop-down list, and then select **Forms**.
5. Click the **Edit** drop-down list on the **New Incident Alerts** form, and then select **Responses**.
6. Modify the choices by adding a new option "Be there in 10 minutes".
   - Set the appropriate Contribution and Action properties.
   - The response choices available to the user in the notifications depends on whether the incident is assigned to a user or a group. See "Step Two: Customizing the responses in the Integration Agent" on page 45

Step Two: Customizing the responses in the Integration Agent

The integration provides a way to configure which of the form's response choices will be available to users, depending on whether an incident is assigned to a particular person or a whole group.

It is possible that one or more response options configured in the form need to be excluded from one of the cases. If so, their identifiers need to be explicitly specified in the corresponding `RESPONSE_OPTIONS_WHEN` variable in the configuration.js. The value of the variable is an object that maps a form name to an array of string response identifiers.

Out-of-the-box, the Accept and Resolve are the only options available when the incident is assigned to a user, therefore the RESPONSE_OPTIONS_WHEN_ASSIGNED_TO_USER variable is expected to be configured with Accept and Resolve choices response identifiers for all forms used by the integration. If all response choices are to be available for a particular form, simply remove the mapping for this form.

By default, RESPONSE_OPTIONS_WHEN_ASSIGNED_TO_GROUP is empty and so all response options are available for all forms. When adding a new response choice to a form or forms, make sure to update these variables accordingly. In our example, you will need to add the response identifier of the response "Be there in 10 minutes" to RESPONSE_OPTIONS_WHEN_ASSIGNED_TO_USER map entries.

Step Three: Sending the response into BMC Remedy

To send the response choice from the Integration Agent into BMC Remedy, open the bmcremedyincident-callbacks.js file, and add a new case block to the switch statement in the handleResponse function:

```
switch (String(msg.response).toUpperCase())
 {
  case RESPONSE_ACTION_ACCEPT:
    incident = getIncident(incidentId);
...
    break;
...
    case "BE THERE IN 10 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.

4.6 Annotations

This integration extensively annotates the originating BMC Remedy incident, but this may not be desirable in all environments. To reduce the number of annotations of incidents, change the ANNOTATE_DELIVERY variable in the configuration.js file to *false*. You can also modify the bodies of the handleEventStatus and handleDeliveryStatus functions in the bmcremedyincident-callbacks.js file.

Some devices, such as email and mobile devices, allow the user to enter comments when responding to a notification. These comments will be added to the originating BMC Remedy Incident Management's work log as annotations.

4.7 Optimizing the data load integration

The following sections identify some of the ways you can adjust or modify the behavior of the data load integration to best suit your deployment.

4.7.1 Mapping user roles

The default behavior of the data load integration is to assign the Role defined in the configuration.js file to all xMatters Users that it creates. For example, the default file uses the following code to assign the "Standard User" Role to all new xMatters Users:

```
var DEFAULT_XMATTERS_ROLES = ["Standard User"];
```

To assign a different Role, or to assign multiple Roles to all new or updated Users, you can modify the value of DEFAULT_XMATTERS_ROLES to include a comma-delimited list:

```
var DEFAULT_XMATTERS_ROLES = ["Role 1", "Role 2"];
```

The integration also supports the more flexible assignment of xMatters Roles based on the Support group functional roles associated with BMC Remedy users.

To map BMC Remedy roles to xMatters Roles:

1. In the configuration.js file, modify the value of the MAP_REMEDY_USER_ROLES variable to true; i.e.:

```
var MAP_REMEDY_USER_ROLES = true;
```

2. In the roleMap section, edit the roleMap lines to reflect the mapping you want to implement; e.g.:

```
1| var roleMap = [];
2| roleMap["Broadcast Submitter"] = ["Subscription Supervisor"];
3| roleMap["Support Group Admin"] = ["Group Supervisor"];
4| roleMap["Support Group Manager"] = ["Group Supervisor", "Person Supervisor"];
5| roleMap["Support Group Lead"] = ["Person Supervisor"];
```

Note how line 4, above, allows you to map a single BMC Remedy role to multiple Roles in xMatters. Any number of these one to many mappings can be specified, but the configuration does not allow you to assign multiple BMC Remedy roles to a single xMatters Role in a single roleMap entry.

Note: *Lines 2 through 5 can be modified, removed, or added to as needed, but do not remove or modify Line 1.*

4.7.2 Changing data load default values

The dataload integration service sets the values of some of the properties of xMatters Users, Groups, and Devices to hard-coded defaults. For example, Users are assigned by default to the "US/Pacific" time zone, and to the "Default Company".

While these defaults are set by code in library functions found in `<IAHOME>/integrationservices/lib/javascript/xmatters`, the recommended method of changing the default values is to use the property values available in the integration service files in `<IAHOME>/integrationservices/remedy81/remedyincident-5-1-2/`.

The following table lists the relevant files and functions; you can view the library javascript files to determine the names of the object properties.

Object	Library File	Integration Service File	Function	Details
User	dataSyncUser.js	processUsers.js	makeUserForAddUpdate()	Sets User properties after a new User objects is created by calling new User()
Device	dataSyncDevice.js	processUsers.js	makeUserForAddUpdate()	Sets property values for Devices other than Voice and Pager
		phonenumber.js	setVoicePhoneOrPager()	Sets property values for Voice and Pager Devices
Group	dataSyncGroup.js	processGroups.js	makeGroupForAddUpdate()	Sets Group properties after a new Group is created by calling new Group()
Team	dataSyncGroup.js	processGroups.js	makeGroupForAddUpdate()	Sets the property values for the Team created for Group objects
Team Member	dataSyncGroupMember.js	processGroups.js	makeGroupForAddUpdate()	Sets the properties for Team members after new GroupMember() is called

(x) matters ®

Online Support: http://support.xmatters.com

International: **+1 925.226.0300** and press **2**

US/CAN Toll Free: **+1 877.XMATTRS (962.8877)**

EMEA: **+44 (0) 20 3427 6333**

Australia/APJ Support: **+61-2-8038-5048** opt **2**

xMatters enables any business process or application to trigger two-way communications (voice, email, SMS, etc.) throughout the extended enterprise. The company's cloud-based solution allows for enterprise-grade scaling and delivery during time-sensitive events. More than 1,000 leading global firms use xMatters to ensure business operations run smoothly and effectively during incidents such as IT failures, product recalls, natural disasters, dynamic staffing, service outages, medical emergencies and supply-chain disruptions.