xMatters *(alarmpoint)* for CA

Service Desk Manager

(x) matters®
The relevance engine company.

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

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

Thursday, October 27, 2011

Copyright © 1994-2010. All rights reserved.

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

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

Contacting xMatters

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

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

xMatters, inc.
Corporate Headquarters
12647 Alcosta Blvd., #425
San Ramon, CA 94583

Sales and Technical Support:

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

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

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

Proprietary and Confidential © 2010 xMatters, inc

Table of Contents

Chapter 1: Introduction

Welcome to xMatters (alarmpoint) for CA Service Desk Manager. This document describes how to install and configure the xMatters (alarmpoint) for CA Service Desk Manager software integration. The intended audience for this document is experienced consultants, system administrators and other technical readers.

1.1 Summary

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

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

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

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

This integration supports ticket notifications (from CA SDM to xMatters) through an included shell script. It also supports inbound actions (from xMatters to CA SDM).

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

1.1.1 Benefits

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

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

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

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

1.1.2 xMatters mobile access

This version of xMatters also includes the xMatters mobile access application. With the mobile access component, the appropriate technician can create, view, and update CA SDM messages directly via a mobile device’s web browser. Information about CA SDM events can be displayed on the mobile device and updated in real-time.

The benefit is that this process is immediate and may be done remotely – providing users with an efficient method of handling CA SDM tickets from any mobile device. In addition, the CA SDM integration can be updated to notify xMatters Users on their mobile device with a link to the mobile view of the event, allowing the user to update the event remotely.

1.1.3 Integration Architecture

Events injected into xMatters from CA SDM are based on notifications that would have been sent from CA SDM through other methods. As part of our integration we require that a custom Notification Method be created in CA SDM. This Notification Method runs a wrapper shell script that executes APClient.bin. When the APXML messages reaches the xMatters integration agent, the integration agent parses a notification file that is created as part of the Notification Method to extract NX_NTF fields which are sent as event tokens to xMatters. A CA SDM administrator or contact can then select the "xMatters Notification Method" as the notification method for Low, Medium, High, or Emergency notifications.

This integration is tied to CA SDM sending notifications; this means that notifications are now sent for Incident, Request, Problem, Issue, and Change ticket types. But this also means that configuration of notifications are now done in CA SDM.

If CA SDM is going to send a notification, xMatters will send a notification. The setup is not different, nor is any setup added, to the normal configuration of CA SDM notifications. It is just important to note that xMatters will be sending CA SDM notifications. CA SDM allows users to define HTML content, we will send that content instead of creating our own. We just add an xMatters banner to the top of the content.

Responses for the integration are dynamic, and based on a query back to CA SDM when the APXML messages reach the integration agent. A web service call (getValidTransitions) is made to look-up the configured Transitions based on the type and current status of the ticket for which this notification was generated. Response handling is also done via web service calls back to CA SDM. The integration updates the state of the ticket to the next transition state. Authentication can be done either through providing a username/password or through creating a managed session which requires a policy be configured in CA SDM (preferred method). Impersonation is also supported.

The integration also performs a batch data load. Contact records are extracted from CA SDM and then pushed to xMatters via the web service interface. This process is run by a script installed locally to CA SDM within the integration agent directory.

1.2 System Requirements

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

- xMatters (alarmpoint) engine 4.1 (patch 006 or later)with a valid xMatters mobile access license
- xMatters integration agent 4.1 (patch 004 or later)
- xMatters Developer IDE 4.0
- CA Service Desk Manager 12.5

1.2.1 Operating Systems

The following operating systems are supported by this integration:

- Microsoft Windows 2003 (validated)
- Sun Solaris 10
- HP-UX B.11.23
- AIX 5.3
- Linux Redhat AS/ES 5.2

1.3 Conventions and Terminology

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

1.3.1 Conventions

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

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

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

Directory paths

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

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

- On Windows systems, the default is C:\Program Files\AlarmPointSystems\AlarmPoint\
- On Unix systems, the default is /opt/alarmpointsystems/alarmpoint/

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

- On Windows systems, the default is C:\Program Files\AlarmPointSystems\IntegrationAgent\
- On Unix systems, the default is /opt/alarmpointsystems/integrationagent

1.3.2 Terminology

The following terms are used through the xMatters documentation.

Documentation terminology

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

Chapter 2: Installation and Configuration

This chapter provides information about installing the xMatters (alarmpoint) for CA Service Desk Manager integration. This chapter also contains complete instructions on how to configure xMatters, CA SDM, and the integration components.

2.1 Installing the integration

This section describes the installation process for the xMatters (alarmpoint) for CA Service Desk Manager integration.

2.1.1 Installing the integration service

To enable the CA SDM integration service, you must copy the folder containing the integration agent files into the xMatters integration services folder and modify the `configuration.js` and `IAConfig.xml` files. If you have more than one integration agent providing the CA SDM 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 the contents (including the subfolders) of the `xM-CA-ServiceDesk\components\alarmpoint-integration-agent\` folder from the extracted integration archive to the `<IAHOME>` folder.
2. If you backed up an existing deduplicator file as indicated in the note above, merge the contents of your back up with the newly installed `<IAHOME>\conf\deduplicator-filter.xml` file: open both files in a text editor, and then copy the <filter> node from the backup file into the new deduplicator file after the last </filter> node. Save and close the file.
3. Open the `IAConfig.xml` file found in `<IAHOME>\conf` and add the following line to the “service-configs” section:

```
<path>caservicedesk/caservicedesk.xml</path>
```

4. Open the `configuration.js` file (now located in `<IAHOME>\integrationservices\caservicedesk\` folder, and set the values for the following variables:

Variable	Description
SERVICE_DESK_URL	The URL to the CA SDM web services.
SERVICE_DESK_USER	The user name of the CA SDM web service user used to access the web services.
SERVICE_DESK_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.
SEND_SYNC_SUMMARY	Determines whether the data load summary should be sent to the xMatters Administrator.
XMATTERS_ADMINISTRATOR	The xMatters User to whom you want to send the data load summary.
DEDUPLICATOR_FILTER	The name of the filter used to suppress duplicate notifications for this integration. For more information, see "Filtering and suppression" on page 31.

5. Save and close the file.
6. 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 a encrypted file, located in the `<IAHOME>\conf` folder, that stores the password for the management system. You will need to update the file with the correct password for the SERVICE_DESK_USER specified in the `configuration.js` 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/caservicedesk.pwd
```

Installing the Windows batch file

The Windows batch file assumes that the integration agent has been installed to `<IAHOME>\bin`. This path should be updated to the installation path of your integration agent. To simplify the command path for the notification method on Windows deployments, copy the integration BAT file to the CA SDM server.

To install the BAT file:

1. Copy the `xM-CA-ServiceDesk\components\alarmpoint-integration-agent\caservicedesk\xmattersIntegration.bat` file from the extracted integration archive to the `<CA SDMInstallFolder>\Service Desk\bin` folder.

2.1.2 Installing voice files

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

To install the voice files:

1. Copy all of the files in the `xM-CA-ServiceDesk\components\alarmpoint\vox\english` folder from the extracted integration archive to the following node installs folder:

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

Note: *This integration provides a complete set of English voice files.*

2.1.3 Installing the mobile access component files

To enable the mobile access component, you must copy the folders containing the installation files into the xMatters mobile access folder on the xMatters web server. If you have more than one web server, copy the folders into the indicated folder on each web server.

Note that these steps also install the latest images, styles, and resources for the mobile access component; these changes require the xMatters (alarmpoint) engine version 4.1 (patch 006 or later) or version 4.0 (patch 014 or later).

To install the mobile access component files:

1. Copy the contents of the `xM-CA-ServiceDesk\components\alarmpoint\mobilegateway` folder from the extracted integration archive to the `<xMHOME>\webserver\webapps\mobilegateway` folder on the xMatters server.
    - Note that this change will overwrite several files and directories on the xMatters server; if you have made any changes to these files, ensure that you create backups before overwriting your existing files.
2. Restart the xMatters web server.

2.2 Configuring CA Service Desk Manager

Configuring CA SDM to combine with xMatters requires the following steps:

- Configure a new notification method to notify Users via xMatters.
- Optionally, configure CA SDM to use managed login and allow impersonations (recommended).

2.2.1 Configuring a notification method

To configure a notification method for this integration, create a new notification for xMatters, and then set CA SDM to use the new notification method.

To configure a notification method:

1. In the CA Service Desk Manager Web Client interface, click the **Administration** tab, expand **Notifications**, and then click **Notification Methods**.
2. Click **Create New**.
3. In the Create New Notification Method dialog box, enter the following information:
    - **Symbol**: xMatters
    - **Write to File**: Yes
    - **Supports SMTP**: No
    - **Record Status**: Active
    - **Description**: Notify via xMatters
4. In the **Notification method** field, type the command appropriate for your operating system:

Windows:

```
launchit.exe -b xmattersIntegration.bat
```

Unix:

```
launchit -b xmattersIntegration
```

5. Set the xMatters notification method for contacts.
    - CA SDM will now use the xMatters (alarmpoint) engine to notify users.
6. Configure the notification rules in CA SDM.

For more information on how to automatically notify key personnel about ticket activities and events, refer to the *CA Service Desk Manager Administration Guide*.

2.2.2 Configuring CA SDM to use managed login

It is recommended that you configure CA Service Desk Manager to support managed login so that interactions from xMatters to CA SDM can be executed by impersonating the user responding to the notification.

Note: *Note that this requires each CA SDM user who you want to receive notifications from xMatters to have the* ***Impersonate*** *check box selected.*

The Managed Login functionality in CA SDM performs the user authentication by locating the defined security policy through the plain text policy code, finding the policyholder's public key associated with the policy, decrypting the encrypted policy code, matching decrypted content with the policy code, and finally, opening a session with a back-end server.

To configure Managed Login on CA SDM, please refer to the *CA Service Desk Manager Technical Reference Guide* on how to create the Manager Certificate for use in this process.

Note: *Ensure that you create a copy of the Manager Certificate file and store it in a location outside the CA SDM sub-directory. Upgrading CA Service Desk Manager will overwrite the Manager Certificate.*

Once the Manager Certificate has been created, open the `configuration.js` file and ensure that the ACCESS_POLICY_FILE_PATH matches the location of the Manager Certificate (ending in a forward slash) and the ACCESS_POLICY matches the name of the Manager Certificate (with no file extension). The values in the `configuration.js` file are the default values that are applicable if you are following the CA Service Desk Manager Technical Reference Guide.

If the integration is not being configured to use managed login, the MANAGED_LOGIN and ENABLE_IMPERSONATE variables should be set to false. In this case, the SERVICE_DESK_USER will be used to update the tickets from xMatters responses.

2.3 Configuring xMatters

Configuring xMatters to combine with CA Service Desk Manager requires the following steps:

- Import the script package
- Configure the Event Domain, including Integration Service and Event Domain Constants
- Configure the default User
- Add or configure a Web Services User
- Configure the batch data load component

2.3.1 Importing the script package

This integration includes a script package specific to CA SDM. To install the script package, you need to import it into the database, and configure the xMatters scripts to enable callout annotations.

Note: *This step requires the xMatters Developer IDE. For installation instructions, refer to the xMatters Online Developer's Guide.*

To import and configure the script package:

1. Launch the IDE, and then configure the database connection.
2. Click **Workspace > Import**.
3. Select the `xM-CA-ServiceDesk\components\alarmpoint\scripts\xM-CA-ServiceDesk.aps` file extracted from the integration archive, click **Open**, and then click **OK**.
4. When the script has finished importing, click **OK**.
5. Click **Database > Check Out**.
6. In the Check Out dialog box, click **Check Out**.
7. In the Workspace pane, expand the **Default Company** folder, and then expand the **callout (CALLOUT)** folder.
8. Expand the **PRODUCTION** folder and then open the **CONTACT:callout** script.
9. Insert the following line at the top of the callout script:

```
import com.invoqsystems.apex.component.broker.process.scriptObjects.ScriptObjectLinkedHashMap
```

10. In the callout script, locate the following line:
    ```
    @initiatingEvent = @interaction::getInitiatingEvent()
    ```
11. Immediately after the initiaingEvent line, add the following:
    ```
    GOSUB configureAdditionalESMTokens
    ```
12. Add the following code to the end of the script:

```
# Add any additional tokens required for the callout annotate here
```

```
configureAdditionalESMTokens:
  @esmTokens = new ScriptObjectLinkedHashMap()
  @script::log("Agent Client ID: " & $initiatingEvent.agent_client_id)
   IF ($initiatingEvent.agent_client_id == "caservicedesk|caservicedesk")
    @esmTokens::put( "incident_id" , $initiatingEvent.nx_ntf_ref_num )
    @esmTokens::put( "object_handle" , $initiatingEvent.nx_ntf_persistent_id )
  ENDIF
RETURN
```

13. Locate each `::send()` call in the script (there should be eight instances), and add the following code immediately BEFORE each one:

```
$connectionEventMessage.additionalTokens = @esmTokens::getSerializedEntrySet()
```

14. Right-click the **CONTACT:callout** script and select **Save**.
15. Open the **INTERACTION:authenticate** script, and repeat step 12.
    - Note that there are two instances of the `::send()` call in the authenticate script.
16. Right-click the **INTERACTION:authenticate** script and select **Save**.
17. Right-click the **CA Service Desk (BUSINESS)** folder, and then select **Validate**.
18. Right-click the **CONTACT:callout** script, and then select **Validate**.
19. Right-click the **Default Company** folder, and then select **Check In**.
20. In the Create Script Package dialog box, click **Create**.
21. In the Check In dialog box, click **Close**.

2.3.2 Configuring the Event Domain

By default this integration is set up to use an Event Domain of "caservicedesk"; it is strongly recommended that you use this default Event Domain.

Note: *The xMatters web server must be running to perform this portion of the integration.*

To define an Event Domain:

1. Sign on to xMatters as a Company Administrator, and click the **Developer** tab.
2. In the Developer menu on the left side of the screen, click **Event Domains**.
3. On the Event Domains page, click **Add New**.
4. Enter the following information into the form:
    - **Name**: caservicedesk
    - **Description**: CA SDM Integration
    - **Script Package**: CA Service Desk
5. Click **Save**.

Defining an Integration Service

The mobile access component portion of this integration uses a default integration service of "caservicedesk"; it is strongly recommended that you use this default integration service. For the installation to be successful, the integration service name must match the service specified in the file installed on the Integration Agent.

To define an Integration Service:

1. In xMatters, on the Event Domains page, click the **caservicedesk** 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**: caservicedesk
    - **Description**: CA SDM Integration Service

   - **Path**: caservicedesk/menu.jsp
4. Click **Save**.

Defining Event Domain Constants

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

The integration script package uses the names of the constants defined in the table below to look up the values; it is strongly recommended that you use the names specified. Note that the values for the **alarmpointurl** and **bespushurl** constants should be modified to specify the address of the xMatters web server (to enable the HTML response options) and the BES device server.

To add an Event Domain Constant:

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

Constant Name	Default Value	Description
alarmpointurl	http://localhost:8888	Used to specify the address of the xMatters (alarmpoint) engine web server. The links provided in notification content use this constant value to locate the web server which would process the response. For these links to work, this address must be reachable from the Device where the User will receive the notification; normally, this is the IP address or fully-qualified host name of the xMatters web server.
bespushurl	http://localhost:8888/static	Used to specify the address of the BES device server. Populates the `$main.bes_pushurl` parameter.
forcefyi	disable	Force notifications to be informational only (FYI), rather than requiring responses; this overrides the fyi behaviour specified on the injected event. Possible values: • **disable**: Nothing is forced. • **on**: Notifications are forced to be FYI. • **off**: Notifications are forced not to be FYI. Populates the `$force_fyi` parameter.

Constant Name	Default Value	Description
failsafegroup	CA Service Desk FailSafe	The fail-safe recipient to notify, typically a Group. The failsafegroup identifies the recipient that will be notified if an event is injected to xMatters and no Subscriptions exist that match the event. Set this constant if you want to change the fail-safe Group from CA Service Desk FailSafe to another Group defined in xMatters.
failsafe	enabled	Controls fail-safe functionality, notifying the fail-safe recipient via EMAIL under certain circumstances; populates the `$fail_safe` parameter. Possible values: • **enabled**: Notify if no subscriptions match or no notifiable recipients. • **for-subscriptions**: Notify if subscription functionality is enabled AND no subscriptions match. • **for-recipients**: Notify if no notifiable recipients. • **disabled**: Disable fail-safe functionality.
overridetimeframes	false	Override recipients' Device timeframes. Populates the `$override_timeframes` parameter.
useemergencydevices	false	Force the use of emergency Devices. Populates the `$use_emergency_devices` parameter.
trackdelivery	true	Track when each Device is delivered to. Setting this to false may give a performance advantage, but you lose any information about whether a delivery was successful or not. Populates the `$track_delivery` parameter.
annotate	true	Enables submission of annotations back to the management system. Populates the `$main.annotate` parameter.
annotatedelivery	true	Annotate when a notification is delivered to each Device. Note that setting this to *false* may result in a performance advantage, but will also result in the loss of any information about whether a delivery was successful.
subscriptionannotate	true	Enables submission of Subscription annotations back to the management system. Populates the `$main.subscription_annotate` parameter.
tracksubscriptiondelivery	true	Track when each Device is delivered to for Subscriptions. Populates the `$track_subscriptionDelivery` parameter.
timeout	259200	Amount of time (in seconds) the Event is allowed to run before timing out. 259200 seconds = 72 hours. Populates the `$main.timeout` parameter.
maxinvalidresponses	3	Specifies the maximum number of invalid responses allowed before notification is no longer requeued. Populates the `$main.maxInvalidResponses` parameter.

Constant Name	Default Value	Description
enablehtmlemail	true	Enables HTML email functionality. Populates the `$main.enable_HTML_Email` parameter.
uselogo	true	Set this if you want the logo displayed within HTML email notifications. Populates the `$main.use_logo` parameter.

Note: *Event Domain Constant values are case-sensitive; Boolean values must be lowercase* true *or* false. *For more information about the parameters referenced in the Description column, see "Configuration Variable Reference" on page 35.*

2.3.3 Configuring the default User

By default, this integration uses a default demonstration User named “bsmith”. Follow the steps below to ensure that this User has a virtual two-way text phone Device and has access to the mobile access component.

Note that all Users you want to have access to the mobile access component must have the Has Mobile Access check box selected on their User Details page in the xMatters web user interface.

To configure the default User:

1. In xMatters, click the **Users** tab.
2. On the Find Users page, click **S**.
3. In the list of returned Users, click **Smith, Bob**.
4. On the Details for Bob Smith page, select the **Has Mobile Access** check box.
5. In the Common Tasks pane, click **User Devices**.
6. Verify that a virtual text phone Device exists.
7. Click **Reorder**, and set the virtual text phone to be the first Device in the list.
8. Click **Save**.

Note: *If this user is missing, create a User with the User ID “bsmith”, and add a virtual text phone Device. Ensure that the User also has access to the xMatters mobile access. For more information and instructions on how to perform these tasks, refer to the* xMatters (alarmpoint) engine user guide.

2.3.4 Adding the Web Service User

This integration requires a Web Service User for the CA SDM events to be injected to xMatters using web services. The following steps describe how to configure the default Web Service User, IAUser, for this integration.

To set up a Web Service User:

1. In xMatters, click the **Users** tab, and then click **Find Web Service Users**.
2. On the Find Web Service Users page, click **All**.
3. In the returned search results, click **IA_User**.
4. On the Details for IA_User page, confirm that the list of **Allowed Web Services** includes the following web services; if any of the following are not listed in the Allowed Web Services list, select them in the **Denied Web Services** list (Ctrl-click to select more than one), and then click **Add**:
    - Add Coverage
    - Add Device
    - Add Group
    - Add Team

- Add User
- Find Devices
- Query Group
- Query Incident
- Query User
- Update Coverage
- Update Device
- Update Group
- Update Team
- Update User

5. Click **Save**.

2.3.5 Subscribing to Alerts

You can use the Subscriptions feature in xMatters to subscribe to CA SDM tickets that match specific criteria. For example, you could configure a subscription that would send an informational notification to a specific User each time an event entered the system that was of "Immediate" urgency, or whenever an event's status was changed to "Resolved". These notifications, and their responses, do not affect the normal progression of an event through the system.

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

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

Note: *The Subscription Panel file is copied to the correct directory during the integration installation, as described in .*

Defining Event Domain predicates

The default Subscription configured for this integration requires that you define the Event Domain predicates specified in this section.

Note: *You can also use the following steps to add other predicates that you consider important and which you plan to add to the integration.*

To define the Event Domain predicates:

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

Event Domain predicates

Predicate	Type	Important	Description
assignee_name	Text		Name of the User to which the event was assigned.

Predicate	Type	Important	Description
impact	List		The perceived impact of the event, as defined in CA SDM; default values are: • 1-Entire organization • 2-Multiple Groups • 3-Single Group • 4-Small Group • 5-One person
requestor_name	Text		Name of the User who submitted the request.
priority	List		The severity of the event as defined in CA SDM; default values are: • None • 1 • 2 • 3 • 4 • 5
status	List		The status of the event in CA SDM; default values are the same as those defined in "Response choices" on page 28.
urgency	List		The urgency assigned to the event in CA SDM; default values are: • 1-When Possible • 2-Soon • 3-Quickly • 4-Very Quickly • 5-Immediate
ticket_factory	List		The type of ticket created in CA SDM; default values are: • chg • iss • in • cr • pr

Note: *For more information about predicates and how they work in xMatters, see the* xMatters (alarmpoint) engine installation and administration guide.

Defining a Subscription Domain

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

To create a Subscription Domain:

1. On the Developer tab, in the Developer menu, click **Subscription Domains**.
2. On the Subscription Domains page, click **Add New**.
3. In the **Event Domain** drop-down list, select **caservicedesk**, and then click **Continue**.
4. On the Subscription Domain Details page, in the **Name** field, type `CA Service Desk`.
5. Select the **One-Way** check box.
    - For this integration, responses are dynamically created for each notification; this makes defining precise response choices very difficult. It is recommended that you create only One-Way Subscriptions for this integration.
6. Click **Continue**.
7. On the Select Appropriate Predicates page, add all of the predicates to the **Applied Predicates** list, and then click **Continue**.
8. On the Select Roles page, specify the Roles you want to be able to create Subscriptions on the Domain, and then click **Save**.

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

Creating a Subscription

You can use the Subscriptions feature in xMatters to subscribe to CA SDM events that match specific criteria. For example, you could configure a subscription that would send an informational notification to a specific User each time an event entered the system that was of "Immediate" urgency, or whenever an event's status was changed to "Resolved". These notifications, and their responses, do not affect the normal progression of an event through the system.

To create a Subscription:

1. On the Alerts tab, in the Alerts menu, click **My Subscribed Alerts**.
2. Select the CA Service Desk Subscription Domain, and click the **Add New** link.
3. On the Subscription Details page, specify a name for the Subscription, and set the Subscription criteria using the tabs.
4. When you are satisfied with the criteria, click **Save** to create the Subscription.

Creating a fail-safe Group

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

To create a fail-safe Group:

1. In xMatters, click the Groups tab.
2. Create a new Group named CA Service Desk FailSafe, with at least one User as a Team member to receive notifications.

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

Note: *If you want to use an existing Group or a different Group name, modify the value for the failsafegroup Event Domain Constant, as explained in "Configuring the Event Domain" on page 8.*

2.4 Configuring batch data load

This integration supports one-way batch loading (adding and updating only) of Groups, Users, and Devices from CA SDM into xMatters. To configure the data load according to your desired business behavior, modify the included configuration files; the following sections provide an overview of the configuration options.

2.4.1 Data load configuration files

The batch data load configuration files are located in `<IAHOME>\integrationservices\caservicedesk` and define the default values for Users, Groups, and Devices. The default values can be customized to use different values for a specific instance of an object.

Data load files

File name	Description
dataSyncUser.js	Defines the default User object details.
dataSyncDevice.js	Defines the default Device object details.
dataSyncGroup.js	Defines the default Group object details.
dataSyncTeam.js	Defines the default Team object details.
dataSyncCoverage.js	Defines the default Group member object details.
dataSyncList.js	Defines the action taken, whether the data load will update existing objects or only add new objects, and the list of included or excluded objects. For more information about these parameters, see the following sections.
caservisedeskws.js	Contains the business rules and processes required to perform the data load.

Data load settings

You can define the basic behavior of the data load process by modifying the parameters in the dataSyncList.js file. The file includes the following customizable parameters:

Data load settings

Setting	Description
SYNC_ACTION	Defines whether the Users and Groups specified in the list (the syncList parameter defined below) should be included or excluded in the data load. The possible values for this parameter are: • **include**: Users specified in the list will be added to xMatters; if the syncList parameter does not contain any Users, NO Users will be loaded. (This also applies to Groups.) • **exclude**: Users specified in the list will not be added to xMatters; if the syncList parameter does not contain any Users, all Users in CA SDM will be loaded into xMatters. (This also applies to Groups.)
USER_SEED_ONLY	The possible values for this parameter are *true* and *false*. If set to *true*, objects will be added to xMatters only when they are initially loaded, and will no longer be updated. If the seedOnly attribute is *false*, any modifications to the object in xMatters will be overwritten when that object is updated in CA SDM.

Setting	Description
GROUP_SEED_ONLY	The possible values for this parameter are *true* and *false*. If set to *true*, objects will be added to xMatters only when they are initially loaded, and will no longer be updated. If the seedOnly attribute is *false*, any modifications to the object in xMatters will be overwritten when that object is updated in CA SDM. Note that the update process will maintain existing xMatters Team information (type, rotation, rotation interval and rotation unit) and rotations and delays for existing members.
syncList	Identifies the Users and Groups that should be included or excluded during the data load.

Defining default values

The default values for loaded objects are defined in the files listed in the "Data load files" table, above. The default values are contained with the **init: function** section at the beginning of each file.

Defining Devices

The following table identifies which fields in the CA SDM User details map to which Device names and Device Types in xMatters.

Device Types

CA SDM Field	xMatters Device Name	DeviceType
Telephone Number	Work Phone	Voice
Fax Number	Other Phone	Voice
Pager Phone Number	Text Pager	Pager
Alternate Phone Number	Home Phone	Voice
Email Address	Work Email	Email
Pager Email Address	Pager Email	Email

For these Devices to be loaded, you must add the above Device Names into xMatters. For more information about adding Device Names and Device Types, see the *xMatters (alarmpoint) engine installation and administration guide*.

2.4.2 Batch data load process

For this integration, user and group data is sent from CA SDM to xMatters as a batch load process. This means that data will only be sent to xMatters when you run the `xmattersintegration.bat` file to initiate the load process.

Initiating the batch triggers the following events:

1. Retrieves user and device information from CA SDM (via web service call).
   - Note that due to the potential volume of data, this may require multiple calls to retrieve all of the users and devices to be processed.
2. Iterates the user/device information.

For each user:

1. Determines whether the user is to be processed; i.e., either explicitly included or not excluded in the syncList object.
2. Checks to see if the user exists in xMatters; if it does, updates the User, otherwise adds as a new User.

3. For each identified device belonging to the current user, checks to see if the device exists in xMatters; if it does, updates the Device details, otherwise adds as a new Device.

The process then retrieves the GROUP information from CA SDM (another web service call).

For each group:

1. Retrieve the Users that have been assigned to the group in CA SDM.
2. For each group member:
    - If the user is to be processed (either explicitly included or not excluded in the syncList object), adds the user to the members collection in the group that is currently being processed.
3. If the group is to be processed (either explicitly included or not excluded in the syncList object), and the Group already exists in xMatters, and if the Team (collection of Group members) already exists, updates the Team. Otherwise, creates a new Team in that Group.
    - If multiple Teams exist in the Group in xMatters, the process will update the Team that matches the given Team name if it exists, otherwise a new team will be created.
    - Updating the Team will synchronize the members of the Team to match the group members in CA SDM. It will maintain existing xMatters team information (type, rotation, rotation interval and rotation unit) and rotations and delays for existing members. New members will be added to the end of the team with default values (as specified in the `dataSyncGroupMember.js` file).
    - Members that exist on the team in xMatters but not CA SDM will be removed from the team.
    - Coverages will NOT be updated.
4. If the group is to be processed (either explicitly included or not excluded in the syncList object), and the Group does not exist in xMatters:
    - Add the Group
    - Create a new Team in the Group with a name of "<Group Name> Team" (comprising of the group members)
    - Create a new default Coverage for the Team as specified in the `dataSyncCoverage.js` file.

Further process information:

- The data load will not delete Users or Groups from xMatters.
- If a user or group is loaded into xMatters and the specified supervisor is not valid (does not have the appropriate Role or does not yet exist in xMatters), the default supervisors (as specified in the dataSyncUser.js and dataSyncGroup.js files) will be used so that the Users and Groups will be created in xMatters for notifications.
- Following a data load, a User in xMatters can optionally be set to receive a notification of the results. This will be a summary of the successful, successful with warnings and failures. Full information is available in the integration agent logs where detailed information is provided at the User, Group, and Device level for more precise troubleshooting.

Chapter 3: Integration Validation

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

- CA SDM
- xMatters integration agent
- xMatters

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

The following sections will test the combination of xMatters and CA SDM for notification delivery and response, and data load configuration. This section also includes an explanation and demonstration of how to query CA SDM via the xMatters mobile access component using a BlackBerry.

3.1 Validating User and Group Data Load

The following tests the communication between CA SDM and xMatters to ensure that the data load is properly configured.

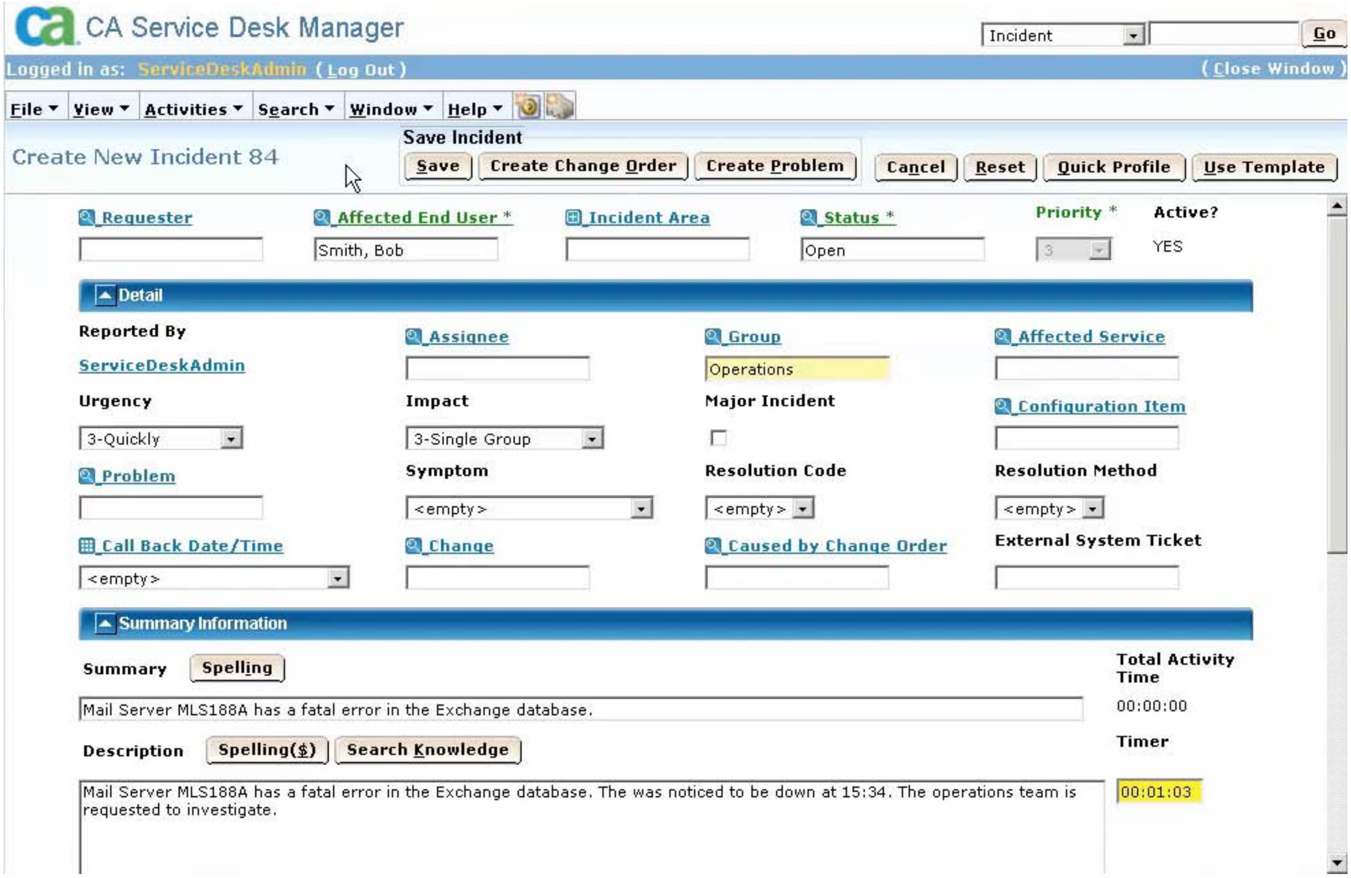
Note: *For this example, it is recommended that you set the Email Device's User Service Provider to use virtual email. This will help when troubleshooting problems in later testing.*

To test the User load:

1. In CA SDM, create a new user, and assign them an email address.
2. Navigate to the `<IAHOME>\integrationservices` folder, and launch the `xmattersIntegration.bat` file.
3. Log in to xMatters, and confirm that the user has been added, and has an Email Device with the correct address.
    - For additional information on the data load process, consult the integration agent's `AlarmPoint.txt` file, which includes a summary detailing any failures or warnings and their reasons.

3.2 Triggering a notification

To trigger a notification, create a new ticket or incident in CA SDM, and assign it to "Bob Smith", or a User that exists in both CA Service Desk Manager and xMatters.



Requester:
Affected End User *: Smith, Bob
Incident Area:
Status *: Open
Priority *: 3
Active?: YES

Reported By: ServiceDeskAdmin
Assignee:
Group: Operations
Affected Service:
Urgency: 3-Quickly
Impact: 3-Single Group
Major Incident: ☐
Configuration Item:
Problem:
Symptom: <empty>
Resolution Code: <empty>
Resolution Method: <empty>
Call Back Date/Time: <empty>
Change:
Caused by Change Order:
External System Ticket:

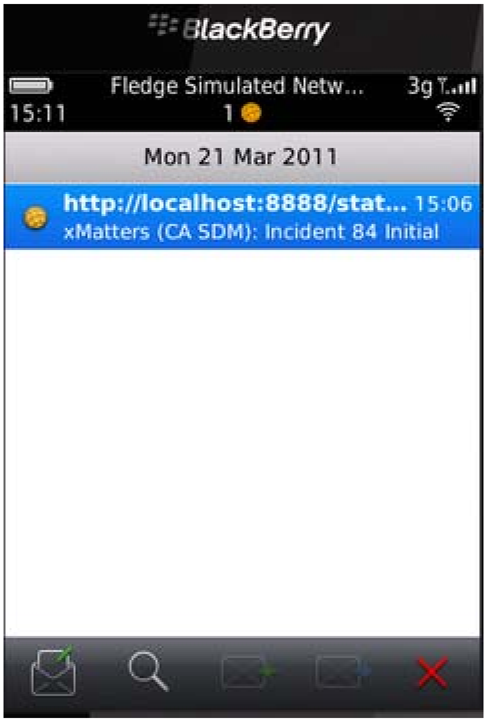
Summary: Mail Server MLS188A has a fatal error in the Exchange database.
Total Activity Time: 00:00:00
Description: Mail Server MLS188A has a fatal error in the Exchange database. The was noticed to be down at 15:34. The operations team is requested to investigate.
Timer: 00:01:03

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 a BlackBerry Device, but the process is similar for all Devices.

To respond to a notification:

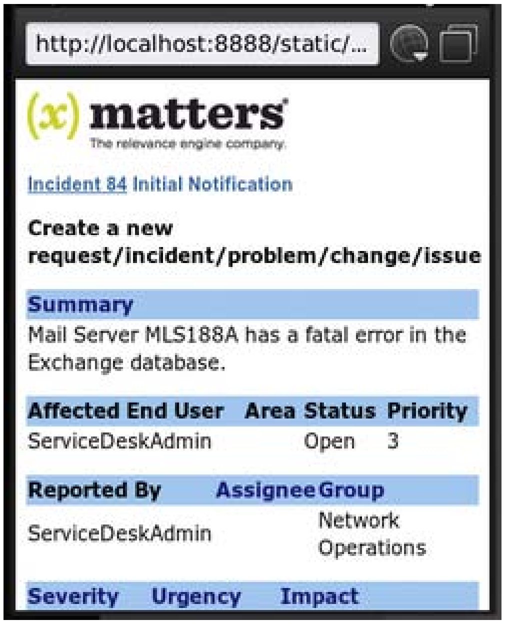
1. When a notification arrives for the User, the Device indicates the number of calls received:



Mon 21 Mar 2011

http://localhost:8888/stat... 15:06
xMatters (CA SDM): Incident 84 Initial

2. Opening the notification displays its details:


http://localhost:8888/static/...
(x) matters
The relevance engine company.

Incident 84 Initial Notification

Create a new request/incident/problem/change/issue

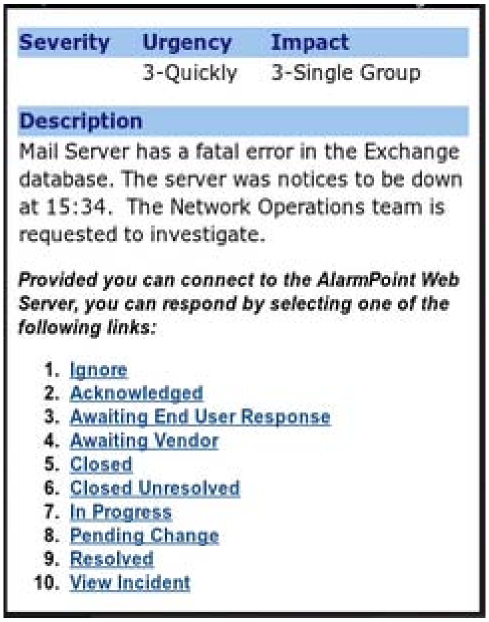
Summary
Mail Server MLS188A has a fatal error in the Exchange database.

Affected End User	Area	Status	Priority
ServiceDeskAdmin		Open	3

Reported By	Assignee	Group
ServiceDeskAdmin		Network Operations

Severity	Urgency	Impact

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



Severity	Urgency	Impact
	3-Quickly	3-Single Group

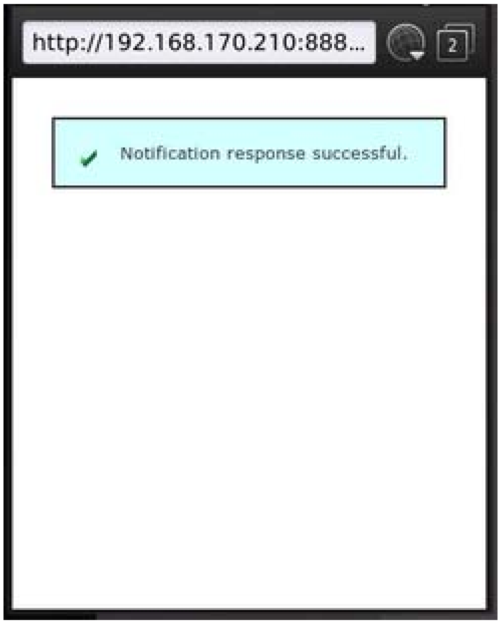
Description

Mail Server has a fatal error in the Exchange database. The server was notices to be down at 15:34. The Network Operations team is requested to investigate.

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

1. Ignore
2. Acknowledged
3. Awaiting End User Response
4. Awaiting Vendor
5. Closed
6. Closed Unresolved
7. In Progress
8. Pending Change
9. Resolved
10. View Incident

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

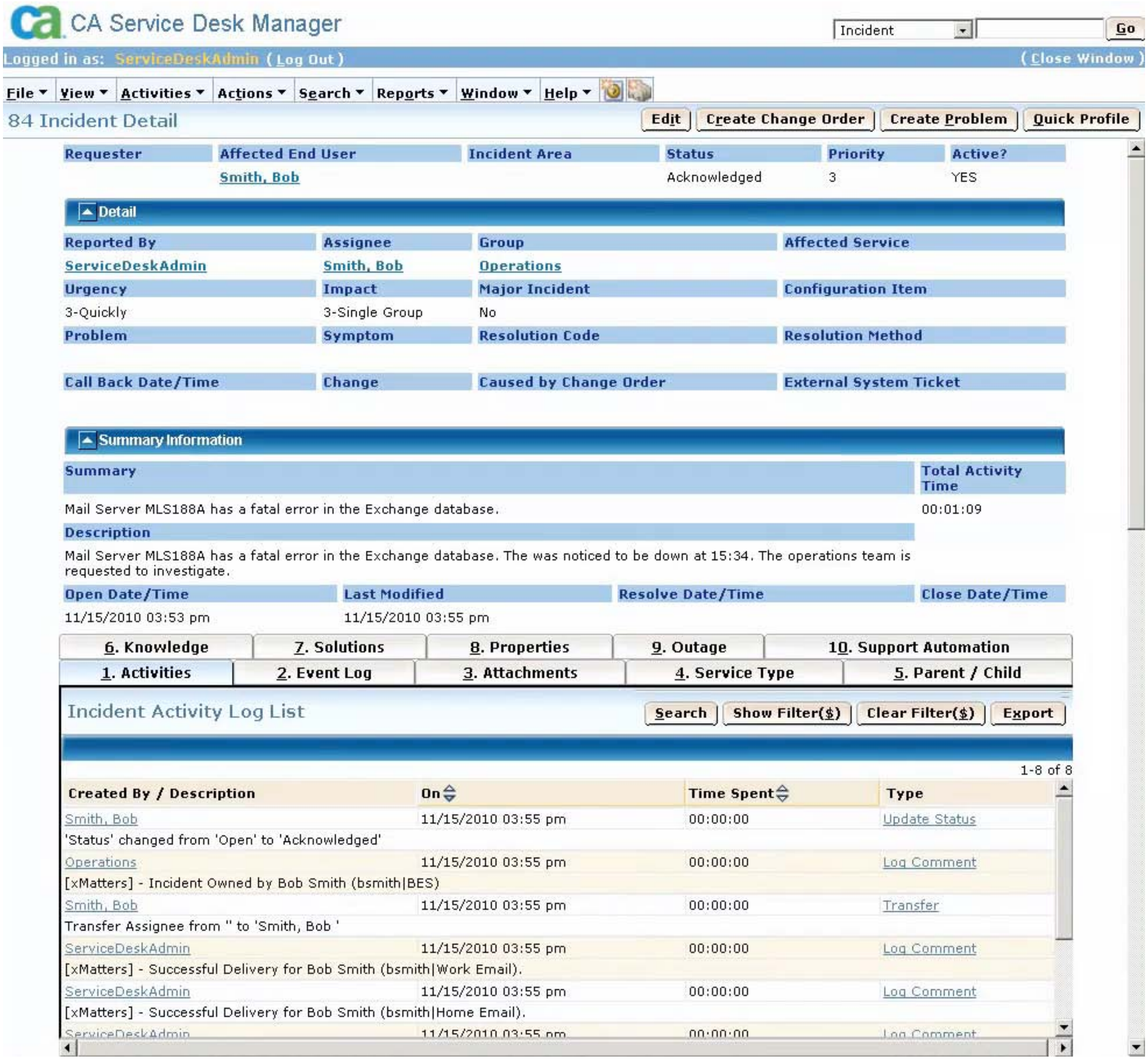


✔ Notification response successful.

3.4 Viewing response results

To view the results of the response, view the ticket in CA SDM.

In the following example, the "Assignee" field has been updated to the name of the responding User, the "Status" has been updated to "Acknowledged", and the "Incident Activity Log List" has been updated with additional entries to show the changes resulting from the User's response:



84 Incident Detail

Requester	Affected End User	Incident Area	Status	Priority	Active?
	Smith, Bob		Acknowledged	3	YES

Reported By	Assignee	Group	Affected Service
ServiceDeskAdmin	Smith, Bob	Operations	
Urgency	**Impact**	**Major Incident**	**Configuration Item**
3-Quickly	3-Single Group	No	
Problem	**Symptom**	**Resolution Code**	**Resolution Method**
Call Back Date/Time	**Change**	**Caused by Change Order**	**External System Ticket**

Summary: Mail Server MLS188A has a fatal error in the Exchange database.

Total Activity Time: 00:01:09

Description: Mail Server MLS188A has a fatal error in the Exchange database. The was noticed to be down at 15:34. The operations team is requested to investigate.

Open Date/Time	Last Modified	Resolve Date/Time	Close Date/Time
11/15/2010 03:53 pm	11/15/2010 03:55 pm		

Incident Activity Log List

1-8 of 8

Created By / Description	On	Time Spent	Type
Smith, Bob 'Status' changed from 'Open' to 'Acknowledged'	11/15/2010 03:55 pm	00:00:00	Update Status
Operations [xMatters] - Incident Owned by Bob Smith (bsmith|BES)	11/15/2010 03:55 pm	00:00:00	Log Comment
Smith, Bob Transfer Assignee from '' to 'Smith, Bob '	11/15/2010 03:55 pm	00:00:00	Transfer
ServiceDeskAdmin [xMatters] - Successful Delivery for Bob Smith (bsmith|Work Email).	11/15/2010 03:55 pm	00:00:00	Log Comment
ServiceDeskAdmin [xMatters] - Successful Delivery for Bob Smith (bsmith|Home Email).	11/15/2010 03:55 pm	00:00:00	Log Comment
ServiceDeskAdmin	11/15/2010 03:55 pm	00:00:00	Log Comment

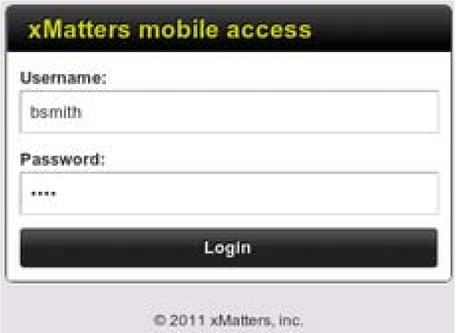
3.5 Creating an incident

This section describes how to use the mobile access component to create a new ticket in CA SDM. The preferred document set in the User's default role in CA SDM determines the type of ticket that you can create. The following example illustrates how to create an incident, but the process is the same for all ticket types.

Note: *The xMatters mobile access page has a default URL of* `http://<xMattersIP>:8888/mg`*, where <xMattersIP> is the IP address of the xMatters web server where the mobile access component is configured.*

To create a new ticket:

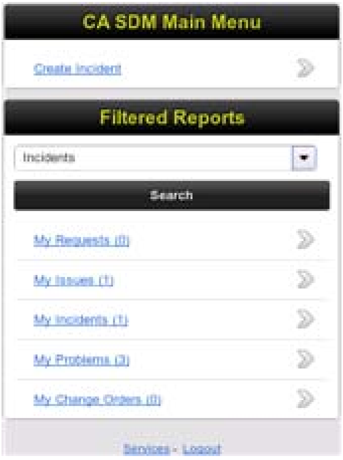
1. Using a browser-enabled smart phone (such as a BlackBerry), open a browser and navigate to the xMatters mobile access IP address.
2. Log in to the mobile access component:



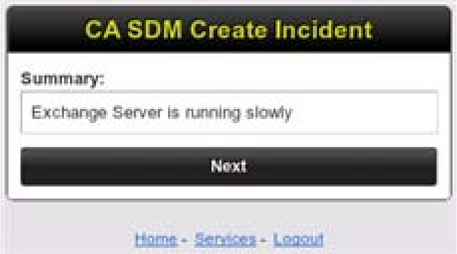
Username: bsmith

Password: ****

3. If more than one Integration Service is available, select the caservicedesk service.
   - The mobile access component displays the CA SDM menu:

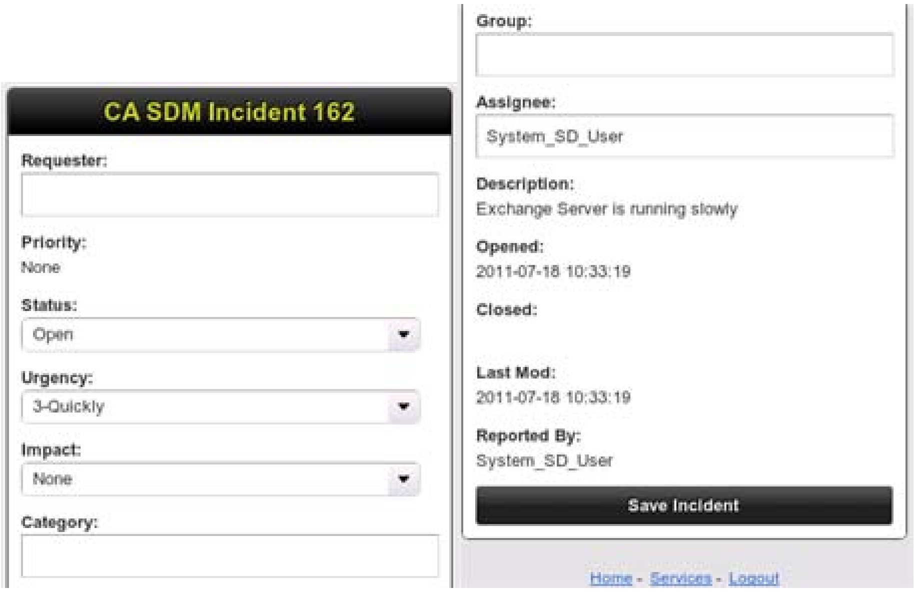


4. In the CA SDM Main Menu, click **Create Incident**; on the Create Incident page, type a description of the issue in the **Summary** field:



Summary: Exchange Server is running slowly

5. Click **Next**.
6. On the new incident form, enter the details for the new incident, and then click **Save Incident**:



Requester:

Priority: None

Status: Open

Urgency: 3-Quickly

Impact: None

Category:

Group:

Assignee: System_SD_User

Description: Exchange Server is running slowly

Opened: 2011-07-18 10:33:19

Closed:

Last Mod: 2011-07-18 10:33:19

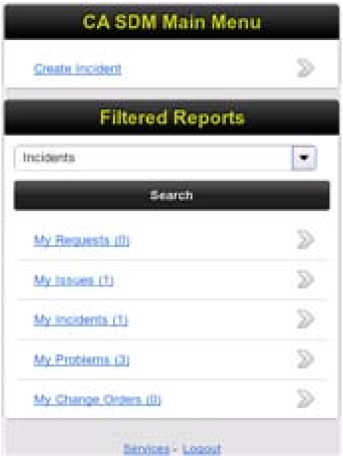
Reported By: System_SD_User

3.6 Querying for an event

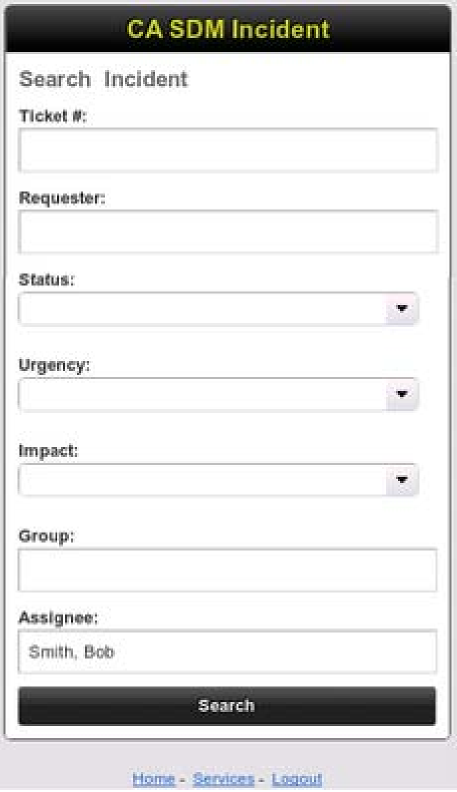
This section describes how to validate that the mobile access component, integration agent and CA SDM are properly configured by querying CA SDM for tickets.

To query for tickets:

1. In the CA SDM Main Menu, in the **Filtered Reports** drop-down list, select **Incidents**, and then click **Search**:



2. On the Search Incident form, enter your search criteria, and then click **Search**:



Ticket #:

Requester:

Status:

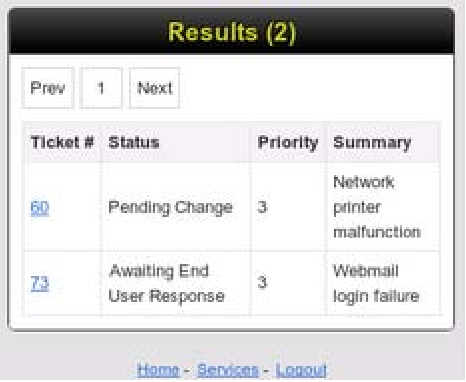
Urgency:

Impact:

Group:

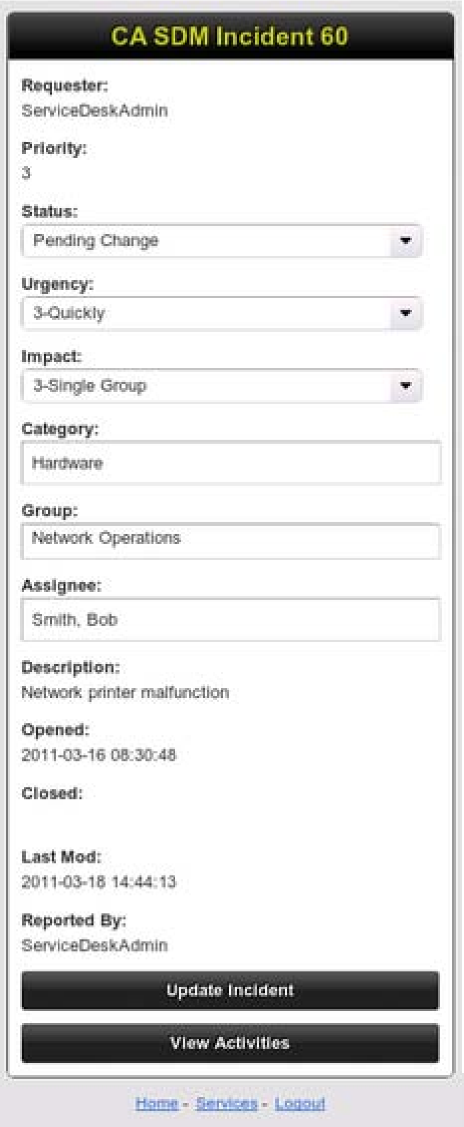
Assignee: Smith, Bob

3. The mobile access component displays the tickets that match your search criteria:



Ticket #	Status	Priority	Summary
60	Pending Change	3	Network printer malfunction
73	Awaiting End User Response	3	Webmail login failure

4. In the search results, click the ticket link to view its details:



CA SDM Incident 60

Requester:
ServiceDeskAdmin

Priority:
3

Status:
Pending Change

Urgency:
3-Quickly

Impact:
3-Single Group

Category:
Hardware

Group:
Network Operations

Assignee:
Smith, Bob

Description:
Network printer malfunction

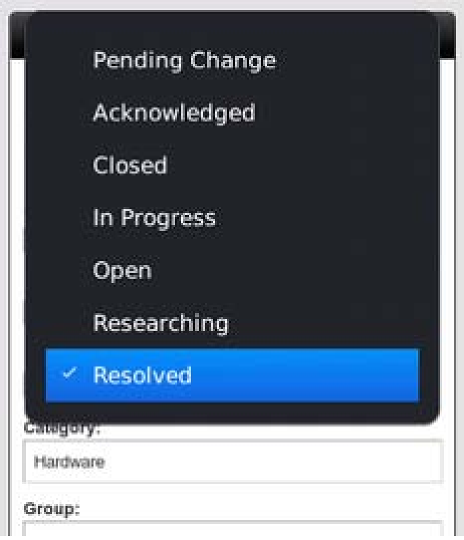
Opened:
2011-03-16 08:30:48

Closed:

Last Mod:
2011-03-18 14:44:13

Reported By:
ServiceDeskAdmin

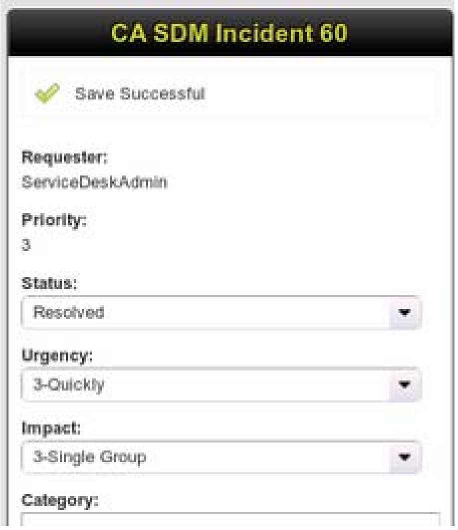
5. To view the available options for the ticket, click the drop-down list at the top of the screen:



Category:
Hardware

Group:

6. To resolve the ticket, select **Resolved** from the Status drop-down list, and then click **Update** (at the bottom of the Incident Details screen):



Requester: ServiceDeskAdmin

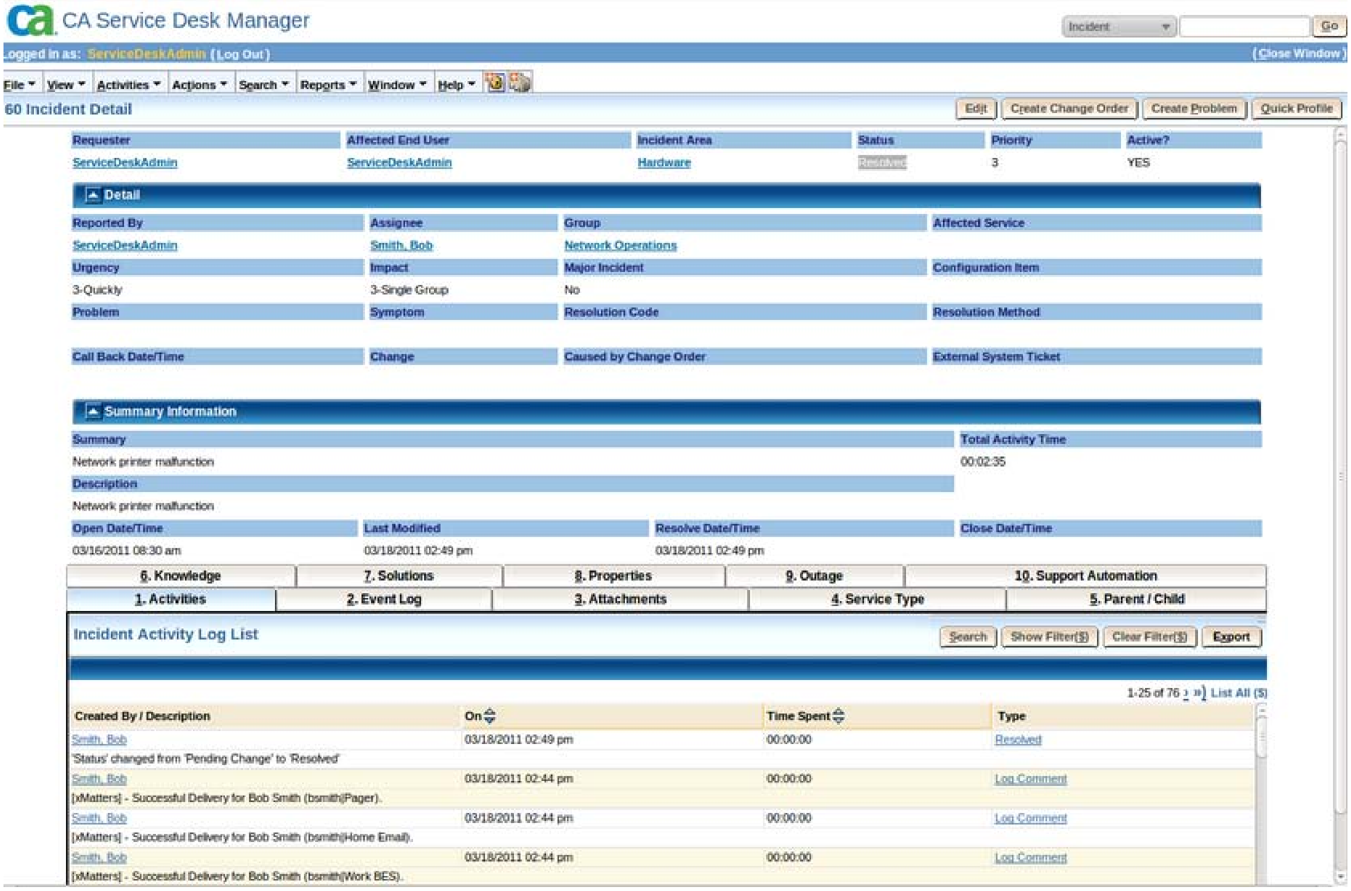
Priority: 3

Status: Resolved

Urgency: 3-Quickly

Impact: 3-Single Group

7. Log in to CA SDM and view the details for the ticket to confirm that its Status is now set to “Resolved”:



Requester: ServiceDeskAdmin
Affected End User: ServiceDeskAdmin
Incident Area: Hardware
Status: Resolved
Priority: 3
Active?: YES

Reported By: ServiceDeskAdmin
Assignee: Smith, Bob
Group: Network Operations
Affected Service:
Urgency: 3-Quickly
Impact: 3-Single Group
Major Incident: No
Configuration Item:
Problem:
Symptom:
Resolution Code:
Resolution Method:
Call Back Date/Time:
Change:
Caused by Change Order:
External System Ticket:

Summary: Network printer malfunction
Total Activity Time: 00:02:35
Description: Network printer malfunction
Open Date/Time: 03/16/2011 08:30 am
Last Modified: 03/18/2011 02:49 pm
Resolve Date/Time: 03/18/2011 02:49 pm
Close Date/Time:

Created By / Description	On	Time Spent	Type
Smith, Bob 'Status' changed from 'Pending Change' to 'Resolved'	03/18/2011 02:49 pm	00:00:00	Resolved
Smith, Bob [xMatters] - Successful Delivery for Bob Smith (bsmith|Pager).	03/18/2011 02:44 pm	00:00:00	Log Comment
Smith, Bob [xMatters] - Successful Delivery for Bob Smith (bsmith|Home Email).	03/18/2011 02:44 pm	00:00:00	Log Comment
Smith, Bob [xMatters] - Successful Delivery for Bob Smith (bsmith|Work BES).	03/18/2011 02:44 pm	00:00:00	Log Comment

Chapter 4: Optimizing and Extending the Integration

This section describes some of the available methods you can use to optimize or extend the xMatters (alarmpoint) for CA Service Desk Manager integration.

4.1 Response choices

This integration allows recipients to respond to notifications with several default choices, some of which are injected back to the CA SDM 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 original CA SDM incident.

The response choices presented on a notification will vary according to the ticket type that the notification represents, and the current status of the incident. xMatters presents the response choices that would be available in the ticket if the user were to perform the update directly in CA SDM.

Which the exception of "Ignore" and "Annotate", response choices are essentially ticket statuses and will update the status of the ticket to the specified response choice. CA SDM also adds an activity log entry to the ticket with details of who changed the status, and from which Device. "Ignore" and "Annotate" do not modify the ticket status; they only update the activity log.

For short text (SMS) and non-HTML email Devices, the responder must respond with the response code as spaces in the statuses would cause the response handler to take the text after the first word as annotation text.

Note: *To remove the "Ignore" option, edit the* `configuration.js` *file in a text editor, and set the* `ADD_IGNORE_RESPONSE` *option to* false.

The following is a list of the default response choices available with the integration and their associated actions on the xMatters event and the CA SDM incident. For a definition of the job control terms, see the list below the table.

Default response choices

Response	Response Code	Job Control
Ignore	IGN	Notify next, delink responder.
Acknowledge	ACK	Delink all except responder.
Analysis Complete	PRBANCOMP	Delivered
Approval In Progress	APP	Delink all except responder.
Approved (Request/Incident/Problem)	PRBAPP	Delink all except responder.
Approved (Change)	APR	Delink all except responder.
Avoided	AVOID	Notify next, delink responder.
Awaiting End User Response	AEUR	Delink all except responder.
Awaiting Vendor	AWTVNDR	Delink all except responder.
Backed Out	BACK	Delink all except responder.
Cancelled	CNCL	Delink all.
Close Requested	CLREQ	Delink all except responder.

Response	Response Code	Job Control
Closed	CL	Delink all.
Closed Unresolved	CLNRSLV	Delink all.
Customer Hold	CSTHLD	Delink all except responder.
Fix In Progress	FIP	Delink all except responder.
Fixed	FXD	Delink all except responder.
Hold	HLD	Delink all except responder.
Implementation in Progress	IMPL	Delink all except responder.
Implemented	IMPD	Delink all.
In Progress	WIP	Delink all except responder.
Known Error	KE	Delink all.
Not Approved	NOAP	Delink all.
Open	OP	Delink all except responder.
Pending Change	PNDCHG	Delink all except responder.
Problem Closed	PC	Delink all.
Problem Fixed	PF	Delink all except responder.
Problem Open	PO	Delink all except responder.
Reject Solution	REJSAP	Delink all except responder.
Rejected (Request/Incident/Problem)	PRBREJ	Delink all except responder.
Rejected (Change)	REJ	Delink all except responder.
Researching	RSCH	Delink all except responder.
Resolved	RE	Delink all except responder.
RFC	RFC	Delink all except responder.
SA-Abandon	SAABND	Delink all.
SA-Resolved	SARES	Delink all.
Scheduled	SCHDLD	Delink all except responder.
Suspended	SUSPEND	Delink all except responder.
Vendor Hold	VNDHLD	Delink all except responder.
Verification in Progress	VRFY	Delink all except responder.
Verify Solution	VERSOL	Delink all.

Job control definitions

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

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

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

4.1.1 Adding annotation messages

Two-way email Device notifications (not FYI) can add extra annotations that will be added to the CA SDM incident. 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.

4.1.2 Changing and adding response choices

You can change the response choices by adding new statuses and transitions in CA SDM. For each new status you add, you must update the Response Handler section in the Action Script to handle the new response choice.

A new ELSE-IF block must be inserted into the handler to capture the response code that will be returned by the notification response. If the status change is to be reflected in CA SDM, the first call must be to sendExternalServiceRequest. Subsequent calls are for job control and can be configured as required using the job control descriptions above.

Response script

```
ELSE-IF ( $token == "newstatus" )       ### New Status
  CALL sendExternalServiceRequest
  CALL sendAPDelinkAllExceptResponderResponse
```

4.2 Delivery Annotations

This integration extensively annotates the originating CA SDM ticket for each Device to which a notification is delivered, but this may not be desirable in all environments. To prevent the delivery annotation of an incident, change the "annotatedelivery" Event Domain Constant to *false*. For more information, see "Defining Event Domain Constants" on page 9.

4.3 Altering the duration of events

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

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

For more information about working with Event Domain Constants, see "Configuring the Event Domain" on page 8.

4.4 FYI Notifications

You can make all notifications informational only (i.e., the user is not offered any response choices) by modifying the Event Domain Constants, as described in "Defining Event Domain Constants" on page 9. Setting the **forcefyi** Event Domain Constant to "on" makes all normal and Subscription notifications one-way (FYI).

4.5 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.

The `deduplicator-filter.xml` file is installed in the `<IAHOME>\conf` folder and is configured to suppress duplicate events for 30 minutes (up to a maximum of 100 events in that period).

This filter can be modified to extend the time period over which an event is considered to be a duplicate, the number of events in that period and the tokens that are used to determine what makes the event unique.

For example, to add REQUESTOR_NAME to the tokens, open the `deduplicator-filter.xml` file in a text editor and add the following line to the <predicates> collection:

```
<predicate>REQUESTOR_NAME</predicate>
```

Save the file and restart the integration agent for the changes to take effect.

Note: *To see a complete list of predicates available in the integration, reviewing the Event Data in the Event Summary Report in the xMatters web user interface.*

4.6 Configuring SSL

This integration supports SSL communication between the integration agent and CA SDM and between the integration agent and xMatters.

4.6.1 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\caservicedesk\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).

4.6.2 Importing certificates

The next step required to enable SSL support is to import the certificate used by the CA SDM 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 "caservicedesk".
- **<path>**: path to the certificate
- **<certificate>**: the certificate's file name
- **<dir>**: the directory in which the integration agent is installed.
- **<password>**: the password for the cacerts keystore; the default password is "changeit".

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

4.6.3 Updating HTTP to HTTPS

The next step is to update the SERVICE_DESK_URL in the `<IAHOME>\integrationservices\caservicedesk\configuration.js` file to use the HTTPS protocol instead of HTTP.

The modified value should resemble the following:

```
var SERVICE_DESK_URL = "https://localhost:8443/axis/services/USD_R11_WebService";
```

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 CA SDM.*

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.

4.6.4 Optional Configuration

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

Scenario 1

- CA SDM 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 CA SDM and the integration agent and xMatters uses the appropriate CA certified certificates

Scenario 2

- CA SDM 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 CA SDM.

Scenario 3

- CA SDM 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 CA SDM to use self-signed certificates while maintaining more complete security between the integration agent and xMatters.

Scenario 4

- CA SDM 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 CA SDM and between the integration agent and xMatters to use self-signed certificates.

4.7 Uninstalling

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

Chapter 5: Configuration Variable Reference

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

5.1 Global configuration variables

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

Note that many of the configuration variables are configurable using the Event Domain Constants described in "Defining Event Domain Constants" on page 9. Those variables are not listed here.

Gobal variables

$main.use_logFile = false	Specify whether to use an alternate log file for debugging messages. This variable is ignored unless $main.debug is also set to *true*.
$main.logFile = "../logs/"	Defines the file used to log debugging information (only if $main.use_logfile is set to *true*).
$main.HTML_form_url = $AlarmPoint_URL & "/jsp/ProcessNotificationResponse.jsp"	Specifies the URL of the xMatters web server’s Process Notification Response JSP form, used by HTML email and BES to inject responses through the system.
$main.logo = $AlarmPoint_URL & "/static/images/logos/alarmpoint/UNKNOWN.png"	Specifies the path to the graphic displayed on HTML (email and BES) notifications.
$main.logo_alt_text = “[If the logo does not appear you may be blocking images or you may be outside a firewall. If the latter, the links will not work for responding and you should respond by replying to this email as described below.]”	The alternate text to display if the HTML email logo is unavailable. **Note**: If the logo does not display, it is unlikely that the HTML_ form_url is valid and responses will not be injected from HTML Devices (email and BES).
$main.numeric_pager_number = “555-1212”	The phone number to display for calling in to retrieve event information. This variable has a non-existent number as a default value; a real call-in number must be supplied, or a message indicating that an xMatters event has occurred.

(x) matters

1 - 866 - xMattrs

12647 Alcosta Blvd.
Suite 425
San Ramon, CA 94583

Unit 6, Woking 8, Forsyth Rd.
Woking, GU21 5SB, UK
+44 (0) 1483 722 001

Copyright 2011 xMatters. All rights reserved. All other products and brand names are trademarks or registered trademarks of their respective holders.