xMatters On-Demand

FOR CA SPECTRUM INFRASTRUCTURE 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.

Wednesday, July 08, 2015

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
Facsimile: 925-226-0310

Client Assistance:

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: http://support.xmatters.com

This integration was designed and tested on an unmodified version of CA Spectrum Infrastructure 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 Spectrum, 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 Client Assistance, but can be performed through the xMatters Client Success department. For more information, contact your xMatters Sales representative.

Table of contents

Introduction

Welcome to xMatters for CA Spectrum Infrastructure Management. This document describes how to install and configure the xMatters for CA Spectrum software integration. The intended audience for this document is experienced consultants, system administrators and other technical readers.

Summary

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 On-Demand and CA Spectrum 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 (the management system, such as CA Spectrum). When CA Spectrum 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 CA Spectrum. Responses are executed immediately on CA Spectrum, enabling remote resolution of the event.

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

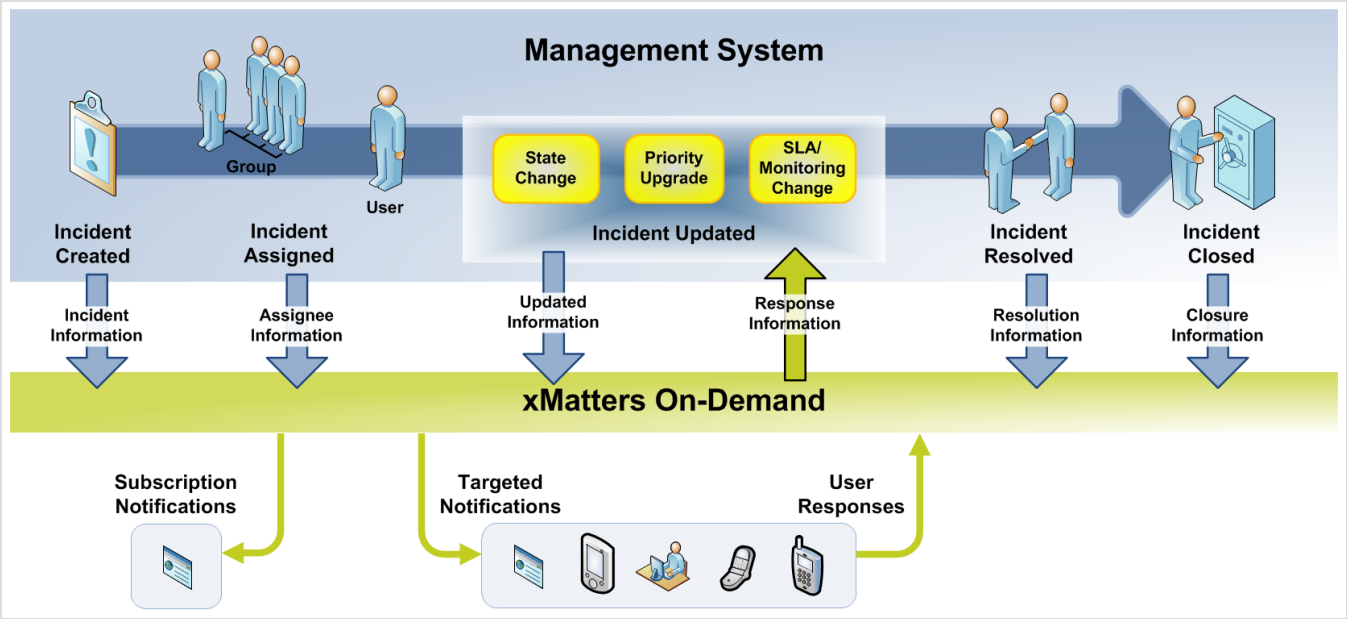
Features

This integration supports event notifications (from CA Spectrum to xMatters) by adding functionality to the CA Spectrum Alarm Notifier scripts which communicate via the xMatters integration agent. It also supports inbound actions (from xMatters to CA Spectrum), through the use of the Command Line Interface (CLI) tool, allowing users to own, acknowledge, and clear events.

Note that you may need to modify this configuration for 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 that indicate each stage of delivery. In a high-volume production system, this constant stream of communications from xMatters to CA Spectrum may result in a significant amount of network traffic that can affect overall system performance. Consider your expected volume of injected events and your server capacity when designing your own integration with xMatters.

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:

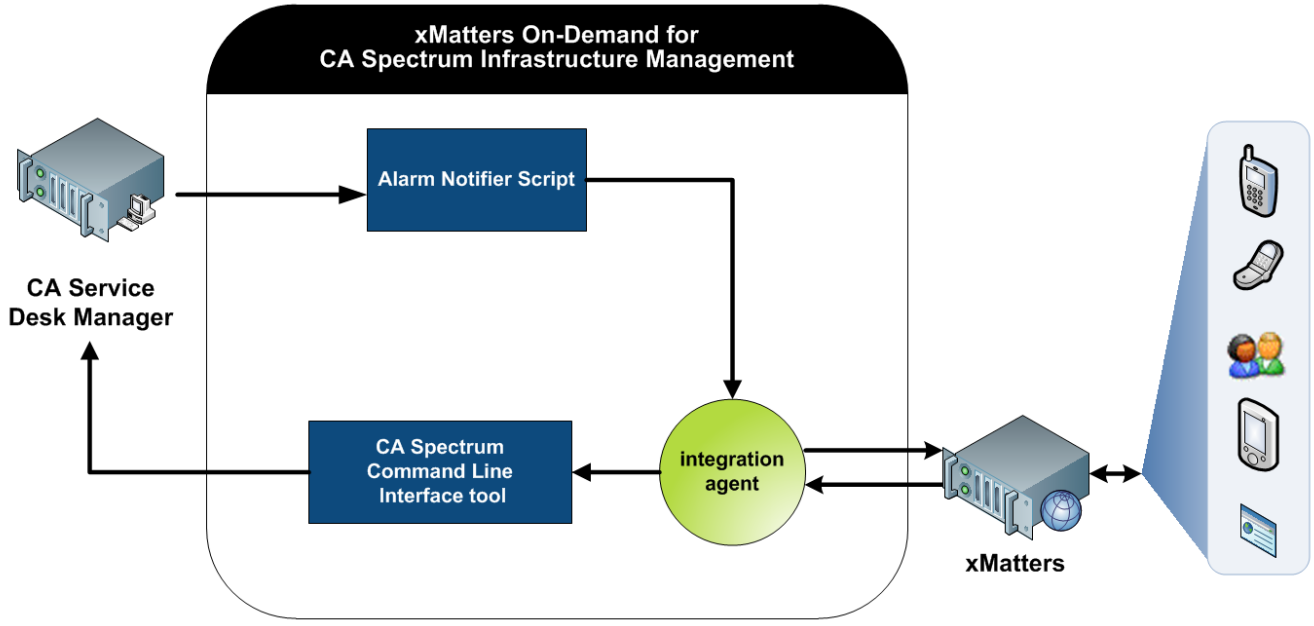


Integration architecture

The software components in this integration include:

- CA Spectrum Infrastructure Manager
- xMatters On-Demand
- xMatters integration agent

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



When a CA Spectrum event is detected, it triggers the following steps:

1. CA Spectrum injects the event to xMatters using a Command Line Interface (CLI) call to the integration agent via the Alarm Notifier script.
2. When the recipient responds to the notification, the response updates CA Spectrum using a CLI call via the integration agent.

System requirements

The following component versions are supported by this integration:

Integration Component	Version
xMatters On-Demand	5.5.75 (or later)
xMatters integration agent	5.1 (patch 005 or later)
CA Spectrum Infrastructure Manager	9.2.1

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

Conventions and terminology

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

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/integrationagent`

The CA Spectrum installation folder is referred to throughout the documentation as <CAS_HOME>.

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. Different management systems use different terminology (CA Spectrum uses the term "event"), but xMatters treats all of these items as 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 Spectrum.
device	A *device* is the medium through which a recipient is contacted by xMatters; i.e., email, 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 On-Demand online help.
communication plan	In xMatters, a *communication plan* is way of organizing information, notifications, options, and actions to selectively deliver relevant information to the right people at the right time. This integration includes a communication plan designed specifically for CA Spectrum.

Installation and configuration

This chapter provides information about installing the xMatters for CA Spectrum Infrastructure Management integration, and complete instructions on how to configure xMatters, CA Spectrum, and the integration components.

Configuring the xMatters integration agent permissions

The xMatters integration agent must be installed on the same machine as CA Spectrum Infrastructure Manager as the integration agent manages the communication between xMatters and CA Spectrum using locally-run CLI commands.

The integration agent service must be configured to log in as a user with sufficient permissions to update CA Spectrum events with notification responses using the CA Spectrum CLI. Typically, the user and credentials used to run the CA Spectrum Server is also used as the integration agent service user.

On Windows, configure the xMatters integration agent service using the following steps:

1. Open the Windows Services tool.
2. Right-click the **xMatters integration agent** service, and then select **Properties**.
3. Click the **Log On** tab, and then click **This account**.
4. Configure the user and password credentials with a Windows User with sufficient permissions to update CA Spectrum alerts (e.g. `.\Administrator`).
5. Click **OK** and restart the integration agent service.

Installing the integration

To install the integration, download and extract the integration package. Some of the following sections make reference to locations within the extracted integration archive.

Integration components

The following table describes some of the notable integration components:

Component Name	Description
com.alarmpoint.spectrum.jar	Contains the following libraries: • **CLI Manager**: Java code to communicate to CA Spectrum using the CLI, and to transform the responses into Java objects that can be processed by the scripts. • **Integration Agent Service Tag Library**: Java tag library and supporting code to allow the subscription panel to communicate to the integration agent. • **Subscription Panel Tag Library**: Java tag library to produce the subscription panel.
CASpectrum.zip	Contains a communication plan specifically designed to work with CA Spectrum.
caspectrum.xml, caspectrum.js, caspectrum-callbacks.js, caspectrum-event.js, xmrestapi.js	The JavaScript and XML service configuration files that define the service on the integration agent.

Configuring xMatters

The following sections describe how to configure xMatters for the integration.

Installing voice files

These files must be installed into any xMatters deployment that uses voice devices. For more information, refer to the *xMatters installation and administration guide*.

This integration provides a number of English voice files (.vox) customized for this integration and CA Spectrum. The files are located in the `/components/xmatters/vox` folder in the extracted integration archive.

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 CA SPECTRUM ALARM OCCURRED ON
   - **Event Domain:** applications
5. Click **Save**.
6. On the Edit Phone Recording Details page, click **Add New**.
7. On the Add Phone Recordings page, click **Choose File**.
8. Navigate to `\components\xmatters\vox`, and select `A CA SPECTRUM ALARM OCCURRED ON.vox`

Note: *The names of the recordings you type into the web user interface MUST match the names of the files; file names are case-sensitive, and spacing must be respected.*

9. Click **Open**.
10. Click **Save**.
11. Repeat steps 3-10 for each of the remaining .vox files in the `\components\xmatters\vox` folder.
    - Ensure that all files are added to the applications event domain.

Adding the web service and REST API users

This integration requires a dedicated web service user and a separate, specially-configured user with permission to access the xMatters REST API.

Adding the web service user

This integration requires an xMatters web service user with the "Receive APXML" permission 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. Log in to 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**.
    - If the IA_User does not exist, click the **Add New Web Service User** link to create a new web service 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**):
    - Query User
    - Receive APXML
    - Register Integration Agent
    - Submit 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 form 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 a user ID for the REST API user; the default is "caspectrum". (This value will also be configured as INITIATOR in the `configuration.js` file.)
    - **First Name**: CA
    - **Last Name**: Spectrum
4. Select **Full Access User** from the Available Roles list, 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**: Enter a web login ID for the REST API user; the default is "caspectrum". (This value will also be configured as INITIATOR in the `configuration.js` file.
    - **New Password** and **Verify New Password**: Type the web login password (this password will also be encoded in the `configuration.js` file).
7. Click **Save**.

Importing communication plan

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

To import the integration communication plan:

1. Log in to xMatters as a company administrator, and click the **Developer** tab.
2. In the Manage Communication Plans menu, click **Import Plan**.
3. In the Import Communication Plan File dialog box, click **Choose File**, and then locate the `\components\xmatters\plan\CASpectrum.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 **Spectrum Incidents** 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 you created in "Adding the web service and REST API users" on page 6.
10. Click **Save Changes**.
11. Repeat steps 7-10 for the remaining form.
12. When you have finished deploying and permissioning the forms, review the form properties to make sure the values match your CA Spectrum 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 may appear twice in the drop-down menu. Ensure that you click the option just below Create Event Web Service.*

Specifying a default recipient

Most events generated by this integration are designed to be subscription-only, meaning the recipients for each event are not specified in the event details. To ensure that the system does not attempt to generate any events without recipients, you should specify a default recipient for each form. This recipient will always be notified, even if your subscriptions do not target anyone.

To add a recipient, open each form's Layout tab and add at least one recipient (a user with a valid, active device, or a non-empty group) to the Recipients section.

Note: *The Error Alert, Change Approval Alert, and Sync Error Alert forms do not require default recipients.*

Configuring the default user

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.

To configure the default user:

1. In xMatters, click the **Users** tab.
2. On the Find Users page, click **S**.
3. In the returned list of users, click **Smith, Bob**.
4. In the Common Tasks pane, click **User Devices**.
5. Verify that a virtual text phone device exists.
6. Click **Reorder**, and set the virtual text phone to be the first device in the list.
7. Click **Save**.

Note: *If this user is missing, create a user with the User ID “bsmith”, and add a virtual text phone device. For more information and instructions on how to perform these tasks, refer to the* xMatters user guide.

Installing the integration service

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

- Copy the folder containing the integration components into the integration agent; this process is similar to patching the application, where instead of copying files and folders one by one, you copy the contents of a single folder directly into the integration agent folder (<IAHOME>). The folder structure is identical to the existing integration agent installation, so copying the folder's contents automatically installs the required files to their appropriate locations. Copying these files will not overwrite any existing integrations.
- Modify the integration agent's IAConfig.xml file to include the path for the new integration service.
- Modify the variables in the configuration.js files associated with the integration services.

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

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

To install the integration files:

1. Copy all of the contents of the \components\integration-agent folder from the extracted integration archive to the <IAHOME> folder.
2. Open the configuration.js file found in <IAHOME>\integrationservices\caspectrum-2-0 and modify the value of the CAS_HOME variable to match your CA Spectrum installation.
3. Open the IAConfig.xml file found in <IAHOME>\conf\ and add the following line to the "service-configs" section:

```
<path>caspectrum-2-0/caspectrum.xml</path>
```

4. To enable the logging of user annotations and notification delivery annotations to <IAHOME>\logs\AlarmPoint_Notification.txt, backup the <IAHOME>\conf\log4j.xml file and then replace it with the file provided with the integration.
5. 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.
6. Open the configuration.js file (now located in the <IAHOME>\integrationservices\caspectrum-2-0\ folder, and set the values for the following variables:

Variable	Description
CAS_HOME	The CA Spectrum installation folder.
XMATTERS_REB_FORM_ CASPECTRUM	The name of the communication plan form used to inject the events. **Note**: You will need a web service URL for each form used in the integration. For more information, see "Accessing web service URLs" on page 8.
RESPONSE_OPTIONS_WHEN_NOT_ CLEARABLE	Response options available to the user for events that are not clearable.

Variable	Description
XMATTERS_REB_FORM_ CASPECTRUM_CONFERENCE	The name of the communication plan form used to create conferences.
XMATTERS_ENABLE_ CONFERENCES	When set to true, enables the creation of conferences for events with Critical and Major severity.
DEDUPLICATOR_FILTER	The name of the filter used to suppress duplicate notifications for this integration. For more information, see "Filtering and suppression" on page 18.
ANNOTATE_DELIVERY	Updates events in CA Spectrum with xMatters notification delivery status.
INITIATOR	Specifies the web login ID of a separate xMatters user for authenticating REST API requests. The user (or its role) must have permission to access the integration's forms via the REST API. For more information, see "Adding the web service and REST API users" on page 6.
PASSWORD	Specifies the location of the file containing the password of the xMatters initiator user. **Note**: This file must be created using the IAPassword utility as explained in "Setting password files", below.

7. Restart the integration agent service.

Setting password files

This integration includes encrypted files, located in the `<IAHOME>\conf` folder, that stores the passwords for the web services user required for the management system and the REST API user required by the xMatters REST API. You will need to update the files with the correct password for the HPSM_USER_NAME and INITIATOR variables specified in the `caspectrum-2-0\caspectrum.js` file.

Password file:

- `initiatorpasswd` stores the password for the INITIATOR variable, or xMatters REST API user.

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 `caspectrum.js` file, <old_password> is the existing password (the default value for a newly installed integration is "password"), and <filename> is the name of the password file (`caspectrum.pwd`):

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

Configuring CA Spectrum

Configuring CA Spectrum to combine with xMatters requires that you modify the CA Spectrum Alarm Notifier scripts.

Modifying the CA Spectrum Alarm Notifier scripts

To configure the Alarm Notifier scripts, you must add a reference to the APClient.bin.exe tool that injects the CA Spectrum events into the integration agent.

To modify the CA Spectrum Alarm Notifier scripts:

1. On the CA Spectrum server, navigate to the `<CAS_HOME>\Notifier\` directory.
2. Open the `ClearScript` file in a text editor.
3. Add the following code to the end of the file, replacing <IAHOME> with the installation folder of the integration agent:

```
#####################################################################
# xMatters
#####################################################################

if [ "$SEV" = "CRITICAL" -o "$SEV" = "MAJOR" ]
  then
    echo "Injecting xMatters event for cleared SPECTRUM AlarmID:" $AID
    "<IAHOME>/bin/APClient.bin.exe" \
    --map-data applications|caspectrum-2-0 "" "$AID" "$RAW_ALARM_TIME" "$DTYPE" "$MTYPE" "$MNAME" "$AID"
\
    "$SEV" "$CAUSE" "$REPAIRPERSON" "$STATUS" "$SERVER" "$LANDSCAPE" "$MHANDLE" "$MTHANDLE" \
    "$IPADDRESS" "$SECSTR" "$ALARMSTATE" "$ACKD" "$CLEARABLE" "$AGE" "Cleared Event" \
    "$EVENTMSG" "CLEARED EVENT" "CLEAR" "$CLEARED_BY_USER_NAME" "false"
  else
  echo "Not injecting AlarmPoint event for cleared SPECTRUM AlarmID:" $AID
fi
```

Note: *The default behavior for the integration is that when an event is cleared in CA Spectrum, the event is not deleted from xMatters. Instead, xMatters responds to the clear event by notifying Users that the event has been cleared. If you would rather have the event deleted from xMatters, change the value of the last parameter from* false *to* true.

4. Open the `<CAS_HOME>\Notifier\SetScript` file in a text editor.
5. Add the following code to the end of the file, replacing <IAHOME> with the installation folder of the integration agent:

```
#####################################################################
# xMatters
#####################################################################
# Parse Alarm Title info

if [ "$SEV" = "CRITICAL" -o "$SEV" = "MAJOR" ]
```

```
  then
    ALARMTITLE=`echo $PCAUSE | awk '{ print substr($0,1,index($0,"SYMPTOMS:") - 2) }'`
    echo "Injecting xMatters event for SPECTRUM AlarmID:" $AID
    "<IAHOME>/bin/APClient.bin.exe" \
    --map-data applications|caspectrum-2-0 "" "$AID" "$RAW_ALARM_TIME" "$DTYPE" "$MTYPE" "$MNAME" "$AID"
\
    "$SEV" "$CAUSE" "$REPAIRPERSON" "$STATUS" "$SERVER" "$LANDSCAPE" "$MHANDLE" "$MTHANDLE" \
    "$IPADDRESS" "$SECSTR" "$ALARMSTATE" "$ACKD" "$CLEARABLE" "$AGE" "$PCAUSE" "$EVENTMSG" \
    "$ALARMTITLE" "SET" ""
  else
  echo "Not injecting xMatters event for SPECTRUM AlarmID:" $AID
fi
```

6. Open the `<CAS_HOME>\Notifier\.alarmrc` file in a text editor.
7. Locate the GET_EXISTING_ALARMS parameter, and set its value to false.
    - If you do not change the GET_EXISTING_ALARMS parameter, CA Spectrum will attempt to notify any existing alarms in the system, regardless of whether they have already been notified, whenever you run the AlarmNotifier.exe command.
8. In the command prompt, run the `<CAS_HOME>\Notifier\AlarmNotifier.exe` command.

Integration validation

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

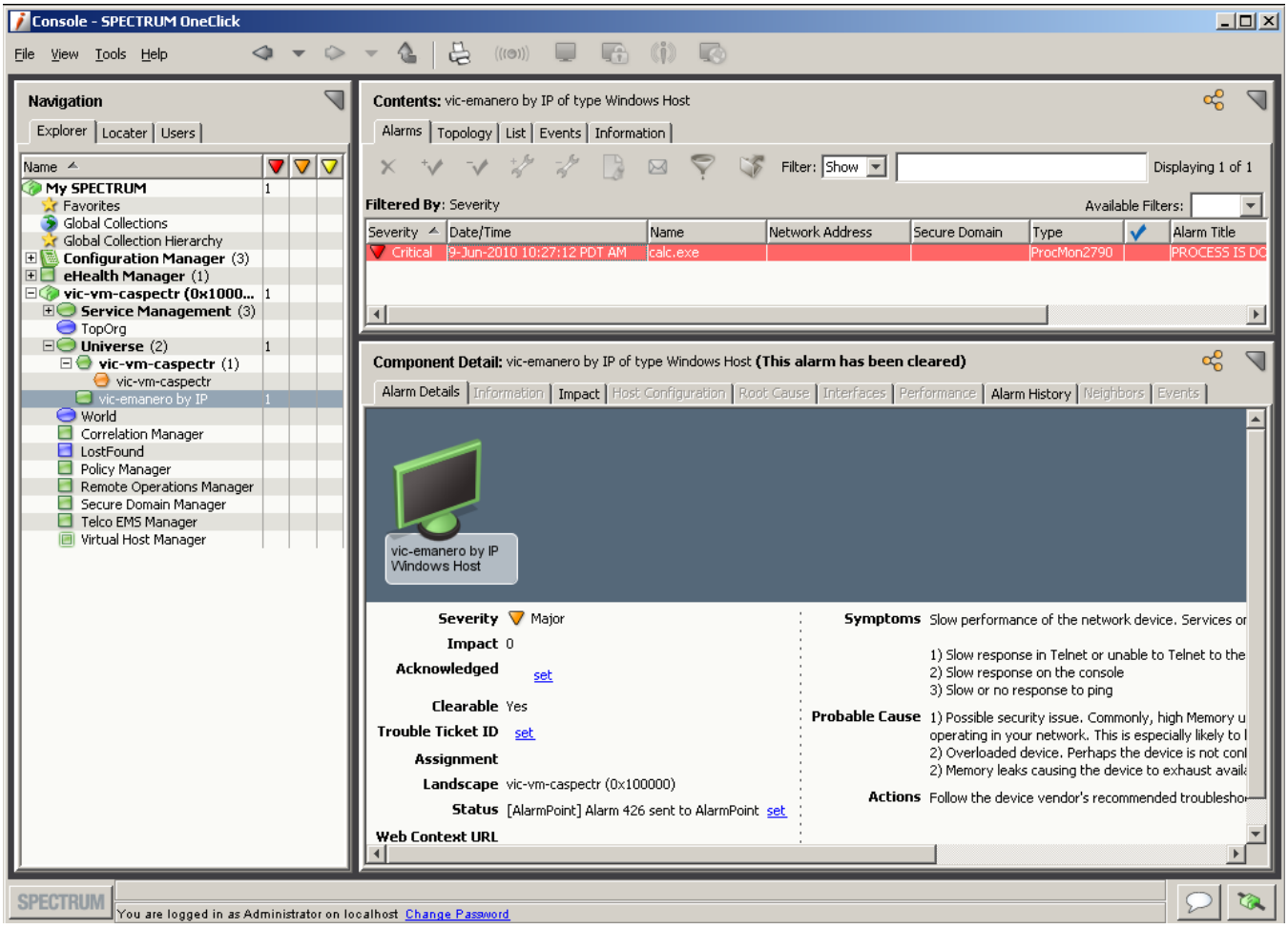
- CA Spectrum Infrastructure Manager
- CA Spectrum Alarm Notifier
- xMatters integration agent

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

The following sections will test the combination of xMatters and CA Spectrum for notification delivery and response.

Triggering a notification

To trigger a notification, create an alarm in CA Spectrum that matches the details of your subscription:

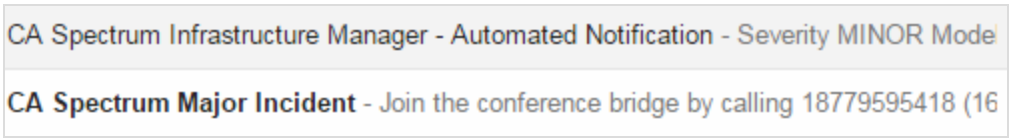


Responding to a notification

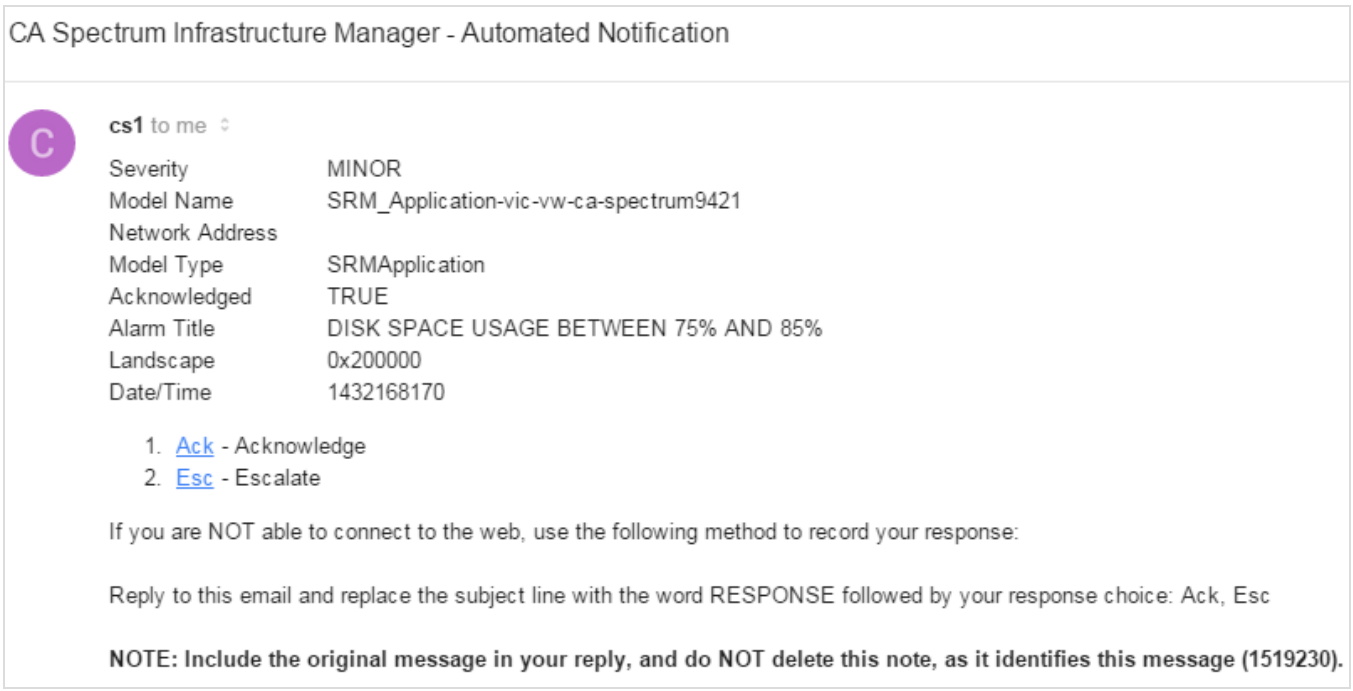
This section describes how to respond to a notification from xMatters. In the following example, the notification is received on a BlackBerry device, but the process is similar for all devices.

To respond to a notification:

1. When a notification arrives for the user, the device indicates the number of messages received:

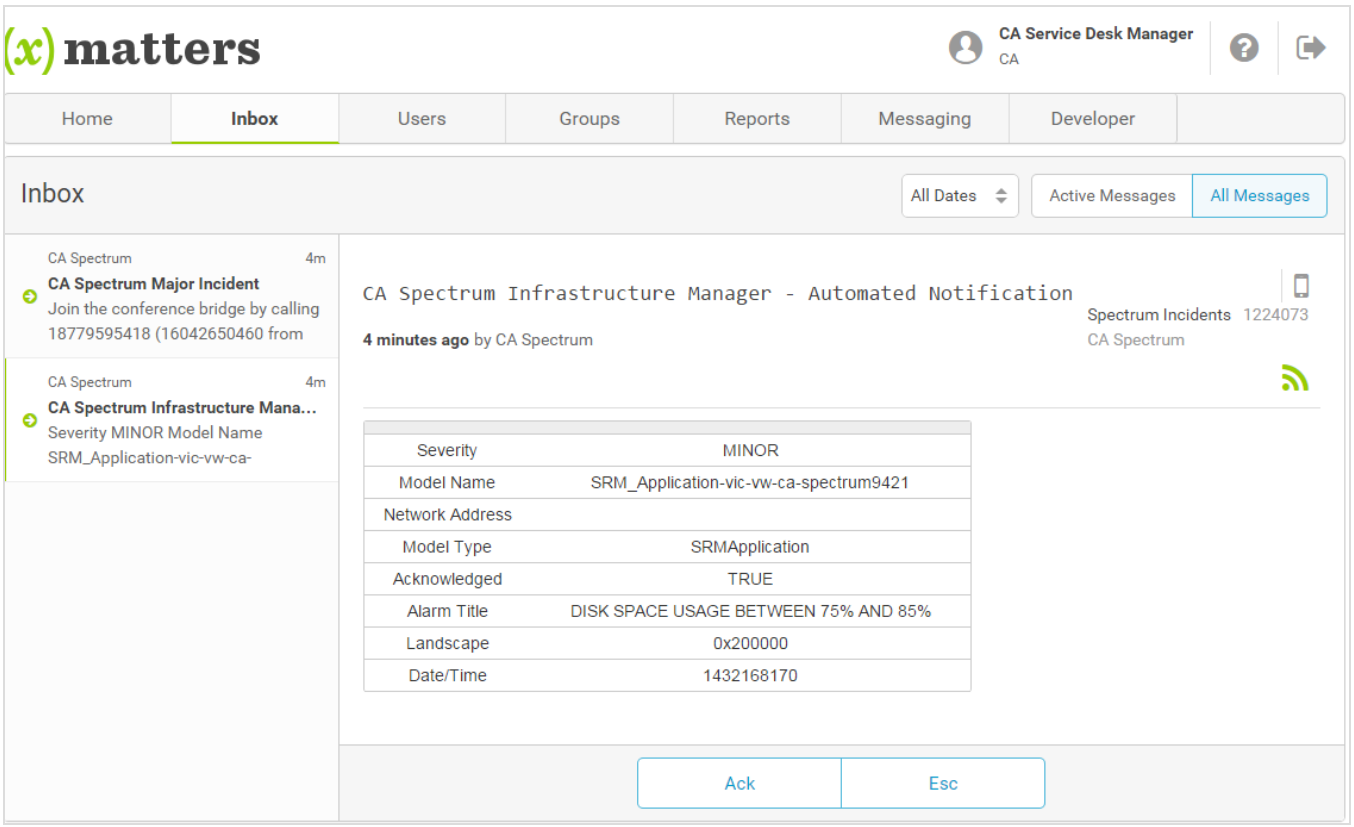


2. Opening the notification displays its details:



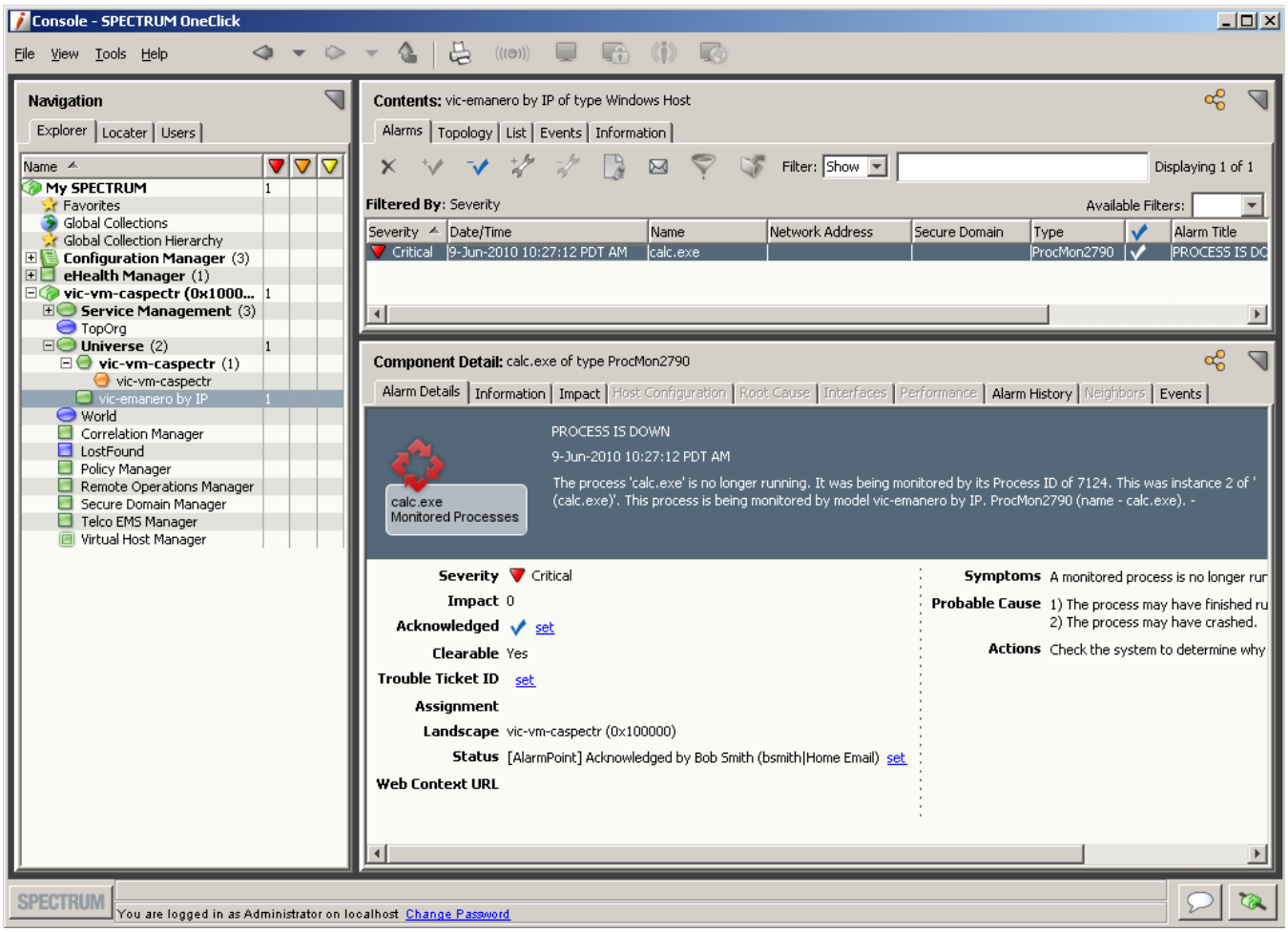
3. To respond to the notification, the user clicks a response choice, and the response is sent to CA Spectrum.

The following image illustrates how the same notification appears in the xMatters web user interface:



Viewing response results

To view the results of the notification response, view the Status field on the Alarm Details tab in CA Spectrum:


Console - SPECTRUM OneClick
File View Tools Help
Navigation
Explorer Locater Users
Name
My SPECTRUM 1
Favorites
Global Collections
Global Collection Hierarchy
Configuration Manager (3)
eHealth Manager (1)
vic-vm-caspectr (0x1000... 1
Service Management (3)
TopOrg
Universe (2) 1
vic-vm-caspectr (1)
vic-vm-caspectr
vic-emanero by IP 1
World
Correlation Manager
LostFound
Policy Manager
Remote Operations Manager
Secure Domain Manager
Telco EMS Manager
Virtual Host Manager
Contents: vic-emanero by IP of type Windows Host
Alarms Topology List Events Information
Filter: Show
Displaying 1 of 1
Filtered By: Severity
Available Filters:
Severity Date/Time Name Network Address Secure Domain Type Alarm Title
Critical 9-Jun-2010 10:27:12 PDT AM calc.exe ProcMon2790 PROCESS IS DO
Component Detail: calc.exe of type ProcMon2790
Alarm Details Information Impact Host Configuration Root Cause Interfaces Performance Alarm History Neighbors Events
calc.exe
Monitored Processes
PROCESS IS DOWN
9-Jun-2010 10:27:12 PDT AM
The process 'calc.exe' is no longer running. It was being monitored by its Process ID of 7124. This was instance 2 of '(calc.exe)'. This process is being monitored by model vic-emanero by IP. ProcMon2790 (name - calc.exe). -
Severity Critical
Impact 0
Acknowledged set
Clearable Yes
Trouble Ticket ID set
Assignment
Landscape vic-vm-caspectr (0x100000)
Status [AlarmPoint] Acknowledged by Bob Smith (bsmith|Home Email) set
Web Context URL
Symptoms A monitored process is no longer run
Probable Cause 1) The process may have finished ru
2) The process may have crashed.
Actions Check the system to determine why
SPECTRUM
You are logged in as Administrator on localhost Change Password

Optimizing and extending the integration

This section describes some of the available methods you can use to optimize or extend the xMatters for CA Spectrum Infrastructure Management integration.

Modifying severity level

By default, the CA Spectrum Alarm Notifier only injects events of CRITICAL or MAJOR severity into xMatters On-Demand. To include other severity levels, modify the SetScript and ClearScript scripts.

To change the severity level of injected events:

1. Navigate to the `<CAS_HOME>\Notifier` directory, and open the SetScript and ClearScript scripts.
2. Locate the xMatters On-Demand section at the end of the scripts that were added during installation.
3. Modify the test condition on the line to specify the severity levels you want to inject:

```
if [ "$SEV" = "CRITICAL" -o "$SEV" = "MAJOR" ]
```

Possible severity levels include: CRITICAL, MAJOR, MINOR, MAINTENANCE, SUPPRESSED, and INITIAL.

Note: *Increasing the number of injected severity levels may impact system performance.*

Adding new parameters

You can choose additional data parameters (or alarm properties) to include in injected events. The following steps explain how to configure the integration components to include a new event token.

To add an event token:

1. Open the `<CAS_HOME>\Notifier\SetScript` file.
2. Add the parameter value, in quotes, to the end of the map-data line in the section added in "Modifying the CA Spectrum Alarm Notifier scripts" on page 11. Note that the maximum number of characters allowed in the map-data command is 255.
   - For more information about modifying these script files, refer to the CA Spectrum documentation.
3. Save and close the `SetScript` file.
4. Navigate to the `<IAHOME>\integrationservices\caspectrum-2-0\` folder and open the `caspectrum.xml` file in a text editor.
5. At the end of the list of parameters in the mapped-input node, add a new parameter using the same syntax as the other parameters in the list.

Note: *The parameters to APClient.bin.exe are positional so the parameter added in step 2 must be in the same position as the mapped-input element.*

6. The name of the parameter you add must match the name of the alarm property added to the `SetScript` file.
7. Save and close the `caspectrum.xml` file.

Adding new tokens to notification content

Once you have injected the new data elements, you can add the token as a property to the communication plan and the appropriate forms in xMatters. Once the property is added to the form's layout, you can add it to the message content for various devices. For more information about these processes, refer to the xMatters On-Demand help, accessible from within the web user interface.

Response choices

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

The following is a list of the default response choices available with the integration and their associated actions on the xMatters event and the CA Spectrum incident.

Default response choices

Response	xMatters Action	CA Spectrum Update	Availability
Acknowledge	Delinks all users other than the responder from the event, not allowing them to submit responses. The owner will not be notified further, but has the ability to affect the event by responding on one of their devices or from the browser. For example, a user acknowledges the event, and then later clears the event.	The status for the alert is changed to "Acknowledged by <User Name>". Any additional notes added to the Acknowledge response are logged to the `AlarmPoint_Notication.txt` file of the integration agent as an Annotate entry.	Email and browser; for other non-FYI mobile devices, an acknowledge is represented as "Ack".
Escalate	Signifies that the user ignores the notification. The event is escalated to the next recipient.	The user's response is logged to the `AlarmPoint_Notication.txt` file of the integration agent as "Ignored by <User Name>". Any additional notes added to the Ignore response are logged to the `AlarmPoint_Notication.txt` file of the integration agent as an Annotate entry.	Email and browser. For other non-FYI mobile devices an Ignore is represented as "Esc".
Clear	Delinks all users from the event, not allowing them to submit responses.	The status for the alert is changed to "Cleared by <User Name>", and the event is cleared. Any additional notes added to the Clear response are logged to the `AlarmPoint_Notication.txt` file of the integration agent as an Annotate entry.	Email and browser. For other non-FYI mobile devices a Clear is represented as "Clr".

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.

www.xmatters.com

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.