AlarmPoint Systems

AlarmPoint for HP Service Manager Incident Management

This integration was designed and tested on an unmodified version of HP Service Manager Incident Managment, and this document describes how to configure AlarmPoint to integrate with the default installation. If you have customized or altered your instance of Service Manager, 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 Professional Services department. For more information, contact your xMatters Sales representative.

Validation Date
December 15, 2010
Version 2.2.1

Contents

1. Introduction

Welcome to the AlarmPoint for HP Service Manager integration. This document describes how to install and configure the AlarmPoint for HP Service Manager software integration. The intended audience for this document is experienced HP consultants, system administrators, and other technical readers.

1.1 Summary

AlarmPoint 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.

AlarmPoint 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, the AlarmPoint System can become the voice and interface of an automation engine or intelligent application (the Management System, such as HP Service Manager). When Service Manager detects an incident that requires attention, AlarmPoint places phone calls, sends pages, messages, or emails to the appropriate personnel, vendors or customers.

The AlarmPoint System is also persistent, escalating through multiple devices and personnel until someone accepts responsibility or resolves the incident. Once contacted, AlarmPoint gives the notified person instant two-way communication with HP Service Manager. Responses are executed immediately on Service Manager, enabling remote resolution of the incident.

This integration supports event notifications (from Service Manager to AlarmPoint) through the use of Javascript triggers and web service calls. It also supports inbound actions (from AlarmPoint to Service Manager) to own the original incident, reject it, resolve it, and add informational annotations.

You will need to modify this configuration to suit your particular business requirements and adjust it to suit your expected loads. The default integration features automatic status annotations on the Service Manager incident; 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 AlarmPoint.

1.1.1 Benefits

With the AlarmPoint 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, AlarmPoint will update the Service Manager incident in real-time. The benefit is that this process is immediate – significantly faster than the time required for Operations 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 AlarmPoint. In addition, AlarmPoint automatically annotates the original Service Manager incident with status information.

The AlarmPoint product features a self-service web user interface to allow accurate assignment of responsible personnel for each job. AlarmPoint also includes an optional enhanced Subscription panel that allows both managed and self-subscription to Service Manager incidents. This Subscription panel queries the Service Manager Server directly in real time to retrieve lists of categories, subcategories, product types and problem types removing the need to create and maintain these lists.

1.1.2 AlarmPoint Mobile Gateway

This version of AlarmPoint also includes the AlarmPoint Mobile Gateway application. With the AlarmPoint Mobile Gateway, the appropriate technician can create, view, and update Service Manager messages directly via a mobile device's web browser. Information about Service Manager messages 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 Service Manager issues or change requests from any mobile device. In addition, the Service Manager integration can be updated to notify AlarmPoint Users on their mobile device with a link to the mobile view of the message, allowing the user to update the message remotely.

1.2 Overview

The following is an overview of the integration steps for the AlarmPoint for Service Manager integration:

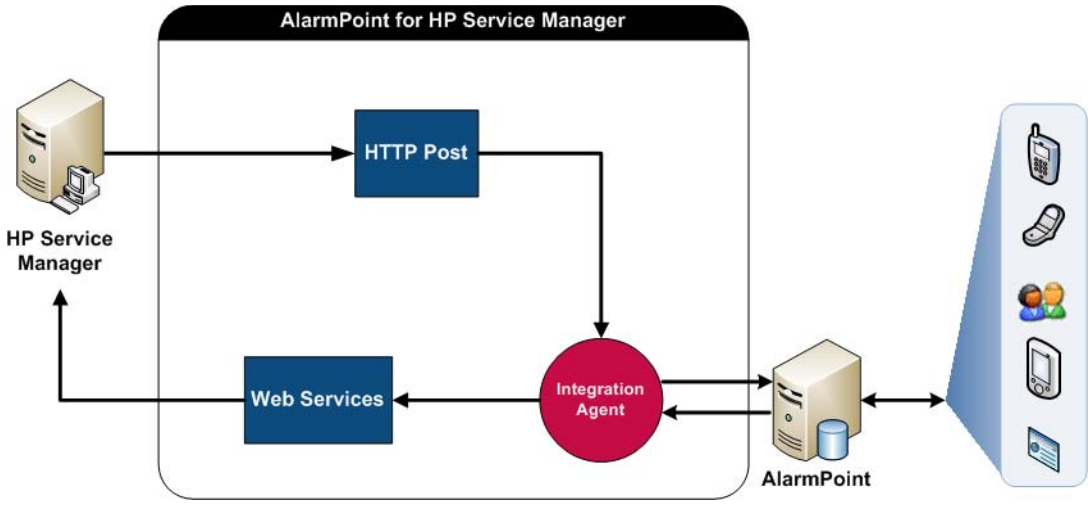
- Install the Web Services Library on the AlarmPoint Webservers and Application server.
- Install the AlarmPoint Subscription panel for Service Manager on the AlarmPoint Webservers. (Optional)
- Install the AlarmPoint Integration Service (and the optional AlarmPoint Mobile Gateway files).
- Install the integration voice files for the AlarmPoint Application server.
- Install the Synchronization configuration files.
- Import the AlarmPoint tables and records.
- Modify the Service Manager triggers and the AlarmPointConfig script.
- Add the SOAP API and AlarmPoint capabilities to Service Manager User for AlarmPoint Web Service Calls.
- Update the IM.template.update and IM.update.incident forms to allow Web Service Calls to update incidents.
- Expose the problem.type and product.type tables for Web Service Calls.
- Remove the invalid data from Service Manager Categories.
- Add the syncContact call to the createUser 2 Wizard.
- Enable Resolve for Web Services.
- Install the AlarmPoint Action Scripts for Service Manager using the AlarmPoint Developer IDE.
- Configure an Event Domain and an Integration Service in AlarmPoint, and define Custom Fields.
- Configure a default User with a two-way Device and Mobile Gateway access.
- Add the AlarmPoint Web Service User.
- Configure the Subscription Panel (optional).
- Create a Service Manager Admin Group.
- Configure synchronization of Service Manager Users and Groups into AlarmPoint.
- Test the Subscription Panel. (Optional)
- Validate User and Group Synchronization.
- Validate that the integration can inject Service Manager incident parameters for AlarmPoint notifications, and that AlarmPoint responses properly update the Service Manager incident.
- Optimize and extend the functionality of the integration by adding custom data elements, responses and Service Manager screens, and configuring integration variables.

1.2.1 Integration Architecture

The software components in the architecture include:

- **Service Manager**: HP Service Manager software.
- **AlarmPoint**: the AlarmPoint Application Server Node.

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

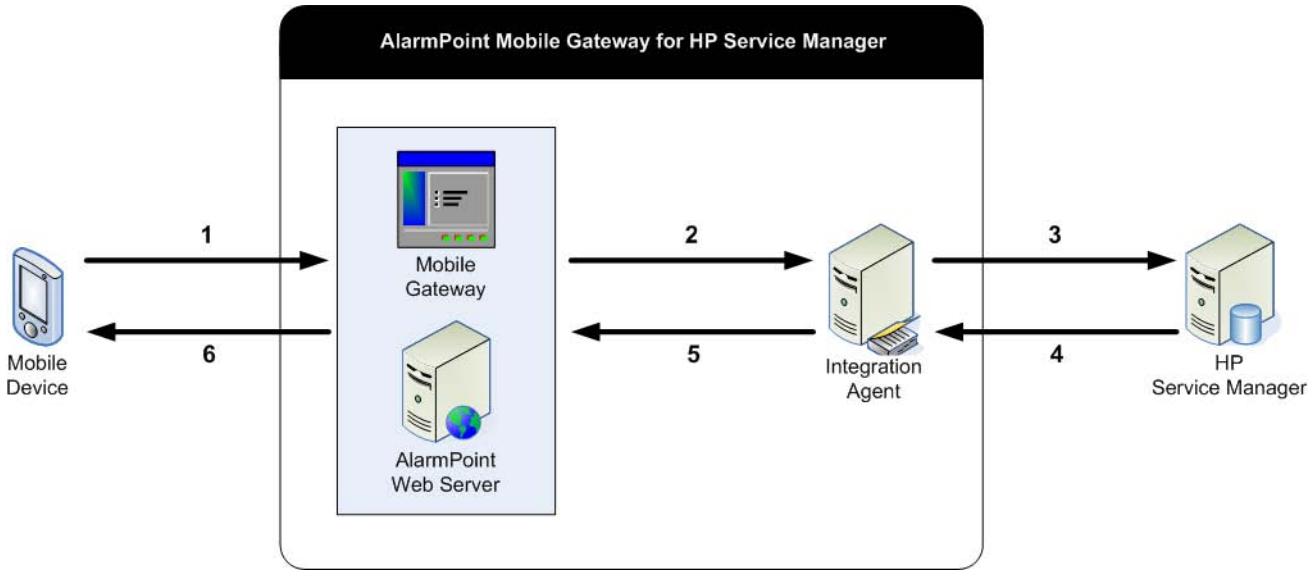


Whenever Service Manager detects a problem, it triggers the following steps:

1. Service Manager sends the event details to the AlarmPoint Integration Agent via HTTP POST.
2. The Integration Agent forwards the event details to AlarmPoint via webservices.
3. The response returns to Integration Agent
4. The Integration Agent sends the response to Service Manager via webservices.

1.2.1.1 Mobile Gateway Integration Architecture

The following diagram illustrates the software processes used by the Mobile Gateway integration:



The following steps occur for each action initiated by a mobile user (the steps correspond to the numbers in the above diagram):

1. A User sends a request from a mobile Device to the AlarmPoint Mobile Gateway.
2. The Mobile Gateway processes the request and relays instructions to the AlarmPoint Integration Agent.
3. The Integration Agent communicates with HP Service Manager via the Service Manager web services API.
4. The response is sent back to the Integration Agent via web services.
5. The Integration Agent processes the response and sends it to the Mobile Gateway.
6. Rendered results are sent back to the mobile device.

1.3 System Requirements

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

- AlarmPoint 4.0 (patch 009 or later) with a valid Mobile Gateway license
- AlarmPoint Integration Agent 4.0 (patch 002 or later)
- AlarmPoint Developer IDE 4.0
- HP Service Manager software, version 7.11

1.3.1 Operating Systems

The following operating systems are supported by this integration:

- Microsoft Windows 2003 (validated)

1.4 Conventions & Terminology

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

1.4.1 Conventions

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

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

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

1.4.1.1 Directory paths

Except where explicitly stated, the directory paths in this document are listed in Windows format.

The AlarmPoint installation folder is referred to throughout the documentation as `<APHOME>`.

- The default is `C:\Program Files\AlarmPointSystems\AlarmPoint\`

The AlarmPoint Integration Agent installation folder is referred to throughout the documentation as `<IAHOME>`.

- The default is `C:\Program Files\AlarmPointSystems\IntegrationAgent\`

1.4.2 Terminology

With respect to the AlarmPoint System, the following definitions apply:

Term	Meaning
AlarmPoint Application Server Node	The core AlarmPoint application, consisting of various components that process events and perform notifications
AlarmPoint Notification Server Node	Delivers notifications to a person in a variety of ways (pager, phone, e-mail, etc.)
AlarmPoint System	Umbrella term for all AlarmPoint software components
AlarmPoint Web User Interface	Browser-accessible interface for controlling AlarmPoint components and information
Management System	A synonym for HP Service Manager
Event	Item of interest that typically generates a notification for a person or group
Device	Medium through which a recipient is contacted (e-mail, phone, pager, etc.)
Recipient	User or Group who should be notified of the event
User Guides	The AlarmPoint documentation suite, which includes the *AlarmPoint Installation and Administration Guide*, the *AlarmPoint Online Developer's Guide*, the *AlarmPoint User Guide*, and the *AlarmPoint Java Client User Guide*.

2. Installation

This chapter provides information about installing the core components for the AlarmPoint for HP Service Manager Software Integration. Components may be installed in any order.

2.1 AlarmPoint System

This integration requires the following AlarmPoint applications:

- AlarmPoint 4.0 (patch 008 or later) with a valid Mobile Gateway license
- AlarmPoint Integration Agent 4.0 (patch 002 or later)
- AlarmPoint Developer IDE

Note: *When installing AlarmPoint, you must select the option to install the AlarmPoint Webserver.*

Consult the AlarmPoint user guides for installation instructions and details.

2.2 HP Service Manager Software

Consult the HP Service Manager User Guides for installation details.

Make a note of your Service Manager installation directory, which is referred to throughout this document as `<SMHOME>`. The default installation location for Windows is `C:\Program Files\HP\Service Manager 7.11\Server\`.

`<SMHOME>` represents the parent directory of the HP Service Manager's `RUN` directory.

2.3 Integration

This section describes the installation processes required for the integration components.

2.3.1 Integration Archive File

Extract the AP-HP-ServiceManager archive to access the integration components. The following shows the notable files and folders (in bold) in the archive:

```
|-- components
| |-- alarmpoint
| | |-- lib
| | | '-- com.alarmpoint.servicemanager.jar
| | |-- mobilegateway
| | | '-- hpsmim
| | |-- scripts
| | | '-- AP-HP-ServiceManager-IM.aps
| | |-- sub_panel
| | | '-- hpsmim
| | |   '-- SMIMSubscriptionForm.jsp
| | '-- vox
| |   '-- english
| |-- alarmpoint-integration-agent
| | '-- hpsmim
| |   |-- hpsmim.js
| |   |-- hpsmim.xml
```

```
| |   '-- lib
| |     '-- com.alarmpoint.servicemanager.jar
| '-- servicemanager
|   |-- config
|   | |-- AlarmPointSyncConfig.xml
|   | '-- AlarmPointSyncList.xml
|   '-- imports
|     |-- AlarmPointCapability.sc
|     |-- AlarmPointForms.sc
|     |-- AlarmPointIDTable.sc
|     |-- AlarmPointScriptLibrary.sc
|     |-- AlarmPointTriggers.sc
|     |-- AlarmPointUnload.sc
|     '-- AlarmPointWebService.sc
'-- documentation
  '-- AP40-HP-ServiceManager_2.2.pdf
```

2.3.2 Component Description

The following table describes some of the notable integration components:

Component Name	Description
com.alarmpoint.servicemanager.jar	Contains the Web Services Library, which is used in the AlarmPoint Action Scripts to inject responses back to Service Manager, and used by the Subscription Panel to retrieve the available Categories, Subcategories, Problem Types and Product Types.
SMIMSubscriptionForm.jsp	Custom Subscription JSP that allows users to subscribe to Events associated with specific criteria (CATEGORY, SEVERITY, etc.).
AlarmPointSyncConfig.xml	Contains all the Groups, Teams, Users, Devices and Coverage value mappings used when synchronizing Service Manager operators and assignments with AlarmPoint Users and Groups.
AlarmPointSyncList.xml	Contains a list of all of the Service Manager operators and assignments to either include or exclude from synchronization with AlarmPoint.
AlarmPointCapability.sc **AlarmPointForms.sc** **AlarmPointIDTable.sc** **AlarmPointScriptLibrary.sc** **AlarmPointTriggers.sc** **AlarmPointUnload.sc** **AlarmPointWebService.sc**	Service Manager unload files used to import all the custom AlarmPoint records and tables into Service Manager.
AP-HP-ServiceManager-IM.aps	Contains the AlarmPoint Action Scripts required for the Service Manager integration.
hpsmim.js	Contains the Javascript code to support the calls from Service Manager to the Integration Agent when injecting events into AlarmPoint.
hpsmim.xml	Contains the configuration information for the Integration Agent.

2.3.3 Installing the Web Services Library

To enable Web Service calls between the AlarmPoint and Service Manager servers, you must copy the JAR file into the AlarmPoint Node, and the AlarmPoint Web Server library folders. If you have installed more than one web server; install the JAR file into the library folder for each one.

Note: *The AlarmPointWebService Java Script, imported as part of the AlarmPointScriptLibrary.sc, is a generated file with customized modifications. Do not attempt to regenerate this file, and do not alter it in any way.*

Source File:

```
AP-HP-ServiceManager\components\alarmpoint\lib\com.alarmpoint.servicemanager.jar
```

Web Server Destination Directory:

```
<APHOME>\webserver\webapps\cocoon\WEB-INF\lib
```

Mobile Gateway Destination Directory:

```
<APHOME>\webserver\webapps\mobilegateway\WEB-INF\lib
```

2.3.4 Installing the Subscription File

To use the optional Subscription Panel, you must copy the JSP file into the AlarmPoint installation folder. If you have more than one web server, repeat the following steps for each one.

To install the JSP file:

1. Copy the `AP-HP-ServiceManager\components\alarmpoint\sub_panel\hpsmim` folder from the extracted integration archive into the `<APHOME>\webserver\webapps\cocoon\alarmpoint\jsp\subscription` directory.
2. Restart the AlarmPoint Webserver.

Note: *On Windows, the AlarmPoint Webserver runs as a Windows Service.*

2.3.5 Installing the Integration Service

To enable the Service Manager integration service, you must copy the folder containing the Integration Agent files into the AlarmPoint Integration Services folder and modify the `hpsmim.js` and `IAConfig.xml` files. If you have more than one Integration Agent providing the servicemanager service, repeat the following steps for each one.

To install the integration service:

1. Copy the `AP-HP-ServiceManager-IM\components\alarmpoint-integration-agent\hpsmim` folder from the extracted integration archive into the `<IAHOME>\integrationservices` directory.
2. Open the `<IAHOME>\conf\IAConfig.xml` file add the following line to the “service-configs” section:

   ```
   <path>hpsmim/hpsmim.xml</path>
   ```

3. Open the hpsmim.js file (now located in <IAInstall_Dir>/integrationservices/hpsmim/) and modify the following fields:
   - **smUrl**: replace “localhost” with your Service Manager server’s IP Address.

- **closureCode**: (optional) replace this value with the default closure code that will appear in the ticket when selecting the Resolve response to an event.
- **calloutAnnotateUser** and **calloutAnnotatePassword**: replace with user credentials for a Service Manager user with SOAP API, AlarmPoint and Incident Management Administration capabilities/permissions. This user will be used to update the Journal Activities with phone callout annotations.

4. Restart the Integration Agent.
   - On Windows, the Integration Agent runs as a Windows Service.

2.3.6 Installing the Mobile Gateway Files

If you are using the Mobile Gateway feature, you must copy the Mobile Gateway files to the appropriate location on the AlarmPoint server.

To install the Mobile Gateway files:

1. Copy the `AP-HP-ServiceManager-IM\components\alarmpoint\mobilegateway\hpsmim` folder from the extracted integration archive to the `<APHOME>\webserver\webapps\mobilegateway\jsp` folder on the AlarmPoint server.

2.3.7 Installing the Voice Files

These files must be installed into an AlarmPoint deployment running a Voice Device Engine. For more information, refer to the *AlarmPoint Installation and Administration Guide*.

To install the voice files:

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

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

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

2.3.8 Installing Synchronization Configuration Files

The `AlarmPointSyncConfig.xml` and `AlarmPointSyncList.xml` files contain the configuration information for synchronizing Users, Groups, Devices and Coverages from Service Manager into AlarmPoint. Note that the synchronization process and all its files are identical for both Service Manager integrations (Incident Management and Change Management) integrations; if you have already installed the AlarmPoint for HP Service Manager Change Management integration (version 2.2), you can skip this step.

To install the synchronization configuration files:

1. Copy the files in the `AP-HP-ServiceManager\components\servicemanager\config\` folder from the extracted integration archive to `<SMHOME>`.

Note: *If these files are installed to a different location, you must modify the AlarmPointConfig script library within Service Manager.*

---

3. Configuration

Before you can begin using the integration, you must configure HP Service Manager and AlarmPoint. This chapter explains the configuration processes required for each product and the configuration processes for the optional User Synchronization and Custom Service Manager Forms components.

Note that in HP Service Manager, Login IDs are case sensitive; for example, “FALCON” and “falcon” represent two separate users in Service Manager. In AlarmPoint, Users IDs (the equivalent to Login IDs in Service Manager) are case insensitive: AlarmPoint would not recognize “FALCON” and “falcon” as belonging to different Users.

3.1 HP Service Manager

Configuring HP Service Manager for the integration requires the following steps:

- Import the AlarmPoint tables and records.
- Modify the Service Manager triggers.
- Modify the AlarmPointConfig script.
- Add the SOAP API and AlarmPoint capabilities to Service Manager User for AlarmPoint Web Service Calls.
- Update the IM.template.update and IM.update.incident forms to allow Web Service Calls to update incidents.
- Expose the problem.type and product.type tables for Web Service Calls.
- Remove the invalid data from Service Manager Categories.
- Add the syncContact call to the createUser 2 Wizard.
- Enable Resolve for Web Services.

3.1.1 Importing the AlarmPoint Tables, Records, and Web Services

The AlarmPoint tables, records, and web services are used to inject change requests to AlarmPoint for notification, and required by the Service Manager database for the integration.

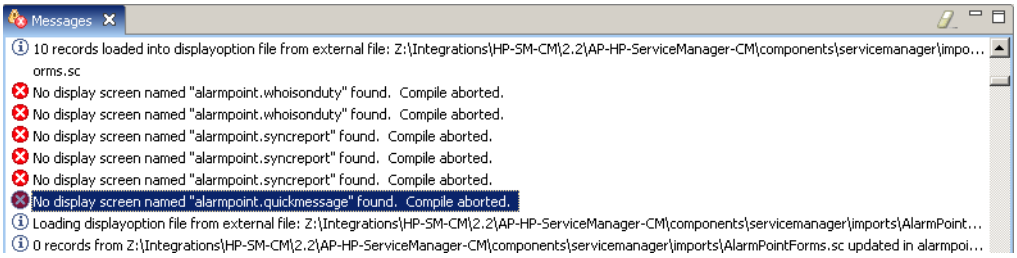
Note: *The* `.sc` *files described in this section are shared between both Service Manager integrations (Incident Management and Change Management); if you have already installed the AlarmPoint for HP Service Manager Change Management integration (version 2.2), you can skip this step.*

To import the AlarmPoint tables, records, and web services into Service Manager:

1. Log in to the Service Manager Client Console.
2. Click **Menu Navigation > Tailoring > Database Manager**.
3. In the drop-down list, select **Import/Load**.
4. Click the folder icon beside the **File Name** field.
5. Select the first `.sc` file in the `AP-HP-ServiceManager\components\servicemanager\imports\` directory.
6. Click **Open**.
7. Click **Load FG**.

Repeat the above steps for each of the remaining `.sc` files in the `imports` directory.

Note that when importing `AlarmPointForms.sc`, the error illustrated in the following figure may occur:



You can safely ignore this error message.

3.1.1.1 Service Manager Unload scripts

This integration includes a set of Service Manager unload scripts intended to help with the maintenance of the integration. The unload scripts are:

- **AlarmPoint Forms**: This script unloads all the capability words, dbdict definitions, displayoptions, displayscreens, formats, globallists, menus and scripts associated with the integration.
- **AlarmPoint Integration**: This unload script is a combination of AlarmPoint Forms, AlarmPoint ScriptLibrary, AlarmPoint Triggers, AlarmPoint Unload and AlarmPoint Web Services
- **AlarmPoint Purge**: This unload script is like AlarmPoint Integration but instead of an unload this script performs a purge
- **AlarmPoint ScriptLibrary**: This unload script unloads the AlarmPoint JavaScripts found in Script Library
- **AlarmPoint Triggers**: This unload script unloads the AlarmPoint triggers associated with the integration.
- **AlarmPoint Unload**: This unload script unloads the AlarmPoint unload scripts.
- **AlarmPoint Web Services**: This unload script unloads the External Access Definitions needed as part of the integration. Note that this does not unload a comprehensive list of the External Access Definitions that are required; it is an unload of the definitions which are unique to the integration and created to support the integration. Definitions such as IncidentManagement, which are updated to support the integration, must be managed manually.

3.1.2 Modifying the Service Manager Triggers

Importing the `AlarmPointTriggers.sc` file loads all of the triggers for both of the AlarmPoint for HP Service Manager integrations (Incident Management and Change Management). If you want the Incident Management integration only, you should delete the triggers specific to the Change Management integration.

To delete the Change Management triggers:

1. Log in to the Service Manager Client Console.
2. Click **Menu Navigation > Tailoring > Database Manager**.
3. In the **Form** field, type `triggers` and then press **Enter**.
4. In the **Trigger Name** field, type `alarmpoint` and then press **Enter**.
5. Locate and delete the following triggers:
   - alarmpoint.after.add.change
   - alarmpoint.after.update.change

3.1.3 Modifying the AlarmPointConfig Script

The AlarmPointConfig script contains configuration information for Web Services and Synchronization, and other parameters described in the table below.

Note: *The configuration files described in this section are shared between both Service Manager integrations (Incident Management and Change Management); if you have already installed the AlarmPoint for HP Service Manager Change Management integration (version 2.2), you can skip this step.*

To modify the AlarmPointConfig script:

1. In Service Manager, click **Menu Navigation > Tailoring > Script Library**.
2. In the **Name** field type **AlarmPointConfig**, click **Search**.
3. Modify the variables in the following table to suit the configuration of your integration.

Variable Name	Value
web_service_url	The URL of the AlarmPoint Web Service; for example: `"http://localhost:8888/api/services/AlarmPointWebService";`
web_service_user	The user name of the AlarmPoint Web Service User.
web_service_password	The password of the AlarmPoint Web Service User.
alarmpoint_servicemanager_domain	The name of the AlarmPoint Event Domain for notifications.
default_alarmpoint_admin_group	The target name of the AlarmPoint default Service Manager administration group.
send_sync_error_notifications	If *true*, sends notifications to the default AlarmPoint Service Manager administration group when a record fails to synchronize with AlarmPoint.
alarmpoint_servicemanager_sync_domain	The AlarmPoint Event Domain for Service Manager. The value initializes the variable using an existing variable value, and should not include quotes. **Note**: If you are installing ONLY the AlarmPoint for HP Service Manager Change Management integration, change the variable name to alarmpoint_servicemanager_cm_domain
config_file	The location of the `AlarmPointSyncConfig.xml`; for example: `"C:\\Program Files\\HP\\Service Manager 7.11\\Server\\AlarmPointSyncConfig.xml"`
synclist_file	The location of the `AlarmPointSyncList.xml`; for example: `"C:\\Program Files\\HP\\Service Manager 7.11\\Server\\AlarmPointSyncList.xml"`
ia_url	The URL of the Integration Agent HTTP listener; for example, `http://localhost:2010/agent`. If the Integration Agent is installed on the same computer as Service Manager, you do not need to modify this parameter.

Variable Name	Value
alarmpoint_company	Name of the Company within AlarmPoint; the default value is “Default Company”.
sync_voice	If *true*, voice Devices will be synchronized; the default is *true*.
detailedSyncLogging	If *true*, displays filtering information when performing a synchronization; default is *true*.
detailsEventLogging	If *true*, displays the APXML being sent to AlarmPoint; default is *false*.
sync_cm3groups	If *true*, synchronize Service Manager Change groups when performing a synchronization; default is *true*.
sync_assignmentGroups	If true, synchronize Service Manager Assignment groups; default is *true*.
assignmentGroupSuffix	Specifies the string to add to the end of Service Manager Assignment group names when synchronizing. **NOTE**: This suffix prevents possible name collisions between Assignment and Change groups, which can have the same name in Service Manager, but must have unique names in AlarmPoint.
changeGroupSuffix	Specifies the string to add to the end of Service Manager Change group names when synchronizing. (See note above for more information)

4. Click **Save**, **Compile**, and then **Execute**.

Note: *If Service Manager returns any errors after you click Compile, ensure that you have updated the file correctly.*

The Integration will now be configured to allow Service Manager to inject incidents to AlarmPoint through web services.

3.1.4 Add SOAP API and AlarmPoint Capabilities to Service Manager User

The integration requires all users who are going to respond to notifications through AlarmPoint to have both the SOAP API and AlarmPoint capabilities. These users can update and annotate Service Manager change requests from AlarmPoint through web service calls.

To add the AlarmPoint and SOAP API Capabilities to a Service Manager User:

1. In the Service Manager System Navigator pane, click **Menu Navigation > System Administration > Ongoing Maintenance** and then double-click the **Operators** item.
2. In the **Login Name** field type the login name of the user you want to give response capabilities to, and then click **Search**.

Note: *The default configuration of the AlarmPoint Action Scripts uses the default Service Manager user “falcon” to make web service calls; if you want to use a different user, you must update the Action Scripts accordingly. For more information, see “Configuration Variable Reference” on page 54.*

3. Select the **Startup** tab.
4. Under Execute Capabilities, if not already listed, add **SOAP API** and **AlarmPoint**.
5. Click **Save**.

AlarmPoint may now use web service calls to connect to this Service Manager User.

3.1.5 Updating the Incident Manager forms

The IM.template.update and IM.update.incident forms must be modified to allow web service calls to update Service Manager incidents.

To modify the forms:

1. In Service Manager, click **Menu Navigation** > **Tailoring** > **Format Control**.
2. In the **Name** field enter `IM.template.update`, and then click **Search**.
3. Click **Subroutines**.
4. Right-click on the page, and select **Show Expanded Form**.
5. Scroll down to the section with an Application Name of **script.execute**.
6. Modify the **Update** field to contain the following:

```
problem.status in $file="Reject" and index("AlarmPoint", $lo.ucapex)<=0
```

7. Click **Save**.
8. In the **Name** field enter `IM.update.incident`, and then click **Search**.
9. Click **Subroutines**.
10. Right-click on the page, and select **Show Expanded Form**.
11. Scroll down to the section with an Application Name of **script.execute**.
12. Modify the **Update** field to contain the following:

```
problem.status in $file="Rejected" and gui()=true
```

13. Click **Save**.

The AlarmPoint web service calls will now be able to update the Service Manager incidents.

3.1.6 Exposing Additional Fields for Existing Web Services

For the Mobile Gateway to access tables in Service Manager, you must expose the sub-tables in the extaccess table.

To expose a Service Manager table for Web Services:

1. In Service Manager, click **Menu Navigation** > **Tailoring** > **Web Services** > **WSDL Configuration**..
2. On the External Access Definitions form, enter the name of the table you want to expose within the **Name** field, and then click **Search**.
   - If the form is automatically populated, ensure the Object Name matches the name used to construct SOAP Actions. If the Object Name does not match, modify it, or change the AlarmPoint Configuration Rules.
   - Confirm that the automatically populated table contains the values described in “Mobile Gateway Exposed Table Details”, below.
   - If the form is not automatically populated, continue with the following steps to create the table.

3. Enter the following information into the form:

Field	Value
Service Name	Name of the service
Name	Name of the table you want to expose
Object Name	Name to use when constructing the SOAP Action

4. Click **Add**, and then click the **Data Policy** tab.
5. Modify the fields as follows:

Field	Value
Field	Name of the field in the table.
Caption	Name to use for the element in the Web Service instance element; if left blank, the Field Name is used by default.
Type	Used to convert the record value to or from an XML value. (This is not required for the Mobile Gateway.)

6. Click **Save**, and then click **OK**.

3.1.6.1 Mobile Gateway Exposed Table Details

The following sections list the tables and fields that must be exposed for the default Mobile Gateway integration.

Incident Management table

- **Service Name**: IncidentManagement
- **Name**: probsummary
- **Object Name**: Incident

Confirm that all of the following fields exist; note that all bolded items must be added to default (or out-of-box) deployments.

Field	Caption	Type
action	IncidentDescription	StringType
agreement.id	SLAAgreementID	DecimalType
alert.status	AlertStatus	StringType
assignee.name	AssigneeName	StringType
assignment	PrimaryAssignmentGroup	StringType
brief.description	BriefDescription	StringType
category	Category	StringType
close.time	ClosedTime	DateTimeType
closed.by	ClosedBy	StringType

Field	Caption	Type
company	Company	StringType
contact.name	Contact	StringType
contact.phone	**Phone**	**StringType**
downtime.start	**OutageStart**	**DateTimeType**
downtime.end	**OutageEnd**	**DateTimeType**
explanation	Solution	StringType
extension	**Ext**	**StringType**
first.name	ContactFirstName	StringType
fix.type	ResolutionFixType	StringType
initial.impact	InitialImpact	StringType
last.name	ContactLastName	StringType
location.full.name	Location	StringType
logical.name	ConfigurationItem	StringType
number	IncidentID	StringType
open.time	OpenTime	DateTimeType
opened.by	OpenedBy	StringType
priority.code	**Priority**	**StringType**
problem.status	IMTicketStatus	StringType
problem.type	ProblemType	StringType
product.type	ProductType	StringType
resolution	Resolution	StringType
resolution.code	ClosureCode	StringType
severity	severity	StringType
site.category	SiteCategory	StringType
site.visit.date	**SiteVisitDate**	**DateTimeType**
site.visit.technician	**SiteVisitTech**	**StringType**
subcategory	Subcategory	StringType
ticket.owner	TicketOwner	StringType
type	**Type**	**StringType**
update.action	JournalUpdates	StringType
update.time	UpdatedTime	DateTimeType

Field	Caption	Type
updated.by	UpdatedBy	StringType
user.priority	UserPriority	StringType

3.1.7 Add the syncContact call to the createUser 2 Wizard

The AlarmPointUser.syncContact call must be added to the createUser 2 Wizard to enable synchronization of users upon their creation.

Note that while HP Service Manager's User Quick Add Utility has space for both first and last names, the AlarmPoint synchronization parses the first word (up to the first space) within the Full Name field as the first name, and adds any remaining words to the last name. For example, if a user was added in HP Service Manager with a first name of "One Two" and a last name of "Three Four", AlarmPoint would parse the entry as first name "One" and last name "Two Three Four".

To add the syncContact call:

1. In Service Manager, click **Menu Navigation** > **Tailoring** > **Wizards**.
2. In the **Wizard Name** field, type `createUser 2` (case sensitive), and then click **Search**.
3. Click the **Actions** tab, and then click the **Javascript** tab.
4. Add the following line to the Javascript:

```
system.library.AlarmPointUser.syncContact(vars.$contactname);
```

5. Click **Save**.

Now when a user is created in Service Manager using the createUser 2 Wizard, they will be automatically synchronized with AlarmPoint.

Note that in HP Service Manager, Login IDs are case sensitive; for example, "FALCON" and "falcon" represent two separate users in Service Manager. In AlarmPoint, User IDs (the equivalent to Login IDs in Service Manager) are case insensitive: AlarmPoint would not recognize "FALCON" and "falcon" as belonging to different Users.

3.1.8 Adding the syncContact call to the Process record

For the contact.do.save call to properly synchronize user information with AlarmPoint, the AlarmPointUser.syncUser call must also be added to the Process record.

To add the syncContact call:

1. In Service Manager, click **Menu Navigation** > **Tailoring** > **Database Manager**.
2. In the **Table** field, type `Process`, and then click the **Search** button.
3. On the Process Definition form, in the **Process Name** field, type `contacts.do.save`, and then click the **Search** button.
4. Click the **Final JavaScript** tab.
5. Add the following line to the JavaScript:

```
system.library.AlarmPointUser.syncUser(record, oldrecord);
```

6. Click **Save**.

3.1.9 Enabling Resolve for Web Services

You must modify the environment to allow Resolve to work with web services.

To enable Resolve for web services:

1. In Service Manager, click **System Administration** > **Ongoing Maintenance** > **Environment Records** > **Incident Management Environment**.
2. In the Incident Management Environment details, select the **Use Resolved Status** check box.
3. Save your changes, and log out of Service Manager.

3.2 Configuring AlarmPoint

Configuring AlarmPoint requires the following steps:

- Import the AlarmPoint script package.
- Define the Event Domain and Integration Service.
- Define Custom Fields
- Configure a default User with a two-way Device and Mobile Gateway access.
- Add the AlarmPoint Web Service User.
- Configure the Subscription Panel (optional).
- Create a Service Manager Admin Group.

3.2.1 Importing the AlarmPoint script package

This step requires the AlarmPoint Developer IDE. For installation instructions, refer to the *AlarmPoint Developer's Guide & Scripting Reference*.

To import the AlarmPoint Script Package:

1. Launch the IDE, and then configure the database connection.
2. Click **Workspace** > **Import**.
3. Select the `AP-HP-ServiceManager-IM.aps` file extracted from the integration zip file into the following directory:

   `AP-HP-ServiceManager-IM\components\alarmpoint\scripts\`

4. In the File dialog box, click **OK**, and then click **OK** again.
5. Expand the **HP Service Manager Incident Management (BUSINESS)** folder and open the **PROCESS:initial** script.
6. In the PROCESS:initial script, configure the `$main.AlarmPoint_URL` variable to specify the address of the AlarmPoint Webserver.
   - This enables the HTML response options.

Note: *For more information, see “Global Configuration Variables” on page 55.*

---

7. Right-click the **PROCESS:initial** script and select **Save**.
8. Right-click the **HP Service Manager Incident Management (BUSINESS)** folder, and then select **Validate**.

9. Right-click the **HP Service Manager Incident Management (BUSINESS)** folder and select **Check In**.
10. In the Create Script Package dialog box, click **Create**.
11. In the Check In dialog box, click **Close**.

3.2.2 Defining an Event Domain

By default this integration is set up to use an Event Domain of "hp_sm_incident"; it is strongly recommended that you use this default Event Domain. For the integration to be successful, the Event Domain name must match the alarmpoint_servicemanager_domain variable specified in the AlarmPointConfig script in Service Manager.

Note: *The AlarmPoint Webserver must be running to perform this portion of the integration.*

To define an Event Domain:

1. Sign on to AlarmPoint 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**: hp_sm_incident
   - **Description**: HP Service Manager Integration
   - **Script Package**: HP Service Manager Incident Management
5. Click **Save**.

3.2.2.1 Defining an Integration Service

The Mobile Gateway portion of this integration uses a default integration service of "hpsmim"; 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 `hpsmim.xml` file installed on the Integration Agent.

To define an Integration Service:

1. In AlarmPoint, on the Event Domains page, click the **hp_sm_incident** 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**: hpsmim
   - **Description**: HP Service Manager Integration Service
   - **Path**: hpsmim/menu.jsp
4. Click **Save**.

3.2.3 Defining Custom Fields

The Advanced Integration uses custom fields defined in AlarmPoint to obtain authentication credentials for submitting notification responses and annotations to the incident Journal Activities log in HP Service Manager. These custom fields are required by the Advanced Integration to enable the response option list to be displayed on notifications.

The Mobile Gateway uses custom fields defined in AlarmPoint to obtain authentication credential for logging into Service Manager. These custom fields are optional for the Mobile Gateway as a login page will be displayed if the custom fields are not provided.

By default, the custom fields are “HP SM Login” and “HP SM Password”; it is strongly recommended that you use these default field names.

To define the custom fields:

1. In AlarmPoint, click the Admin tab, and then, in the Administration menu on the left side of the screen, click **Custom Fields**.
2. Click **Add New**, and then enter the following information into the form:
   - **Field Name**: HP SM Login
   - **Type**: Text
3. Click **Save**.
4. Click **Add New**, and then enter the following information into the form:
   - **Field Name**: HP SM Password
   - **Type**: Password
5. Click **Save**.

Note: *For more information about custom fields see the AlarmPoint Installation and Administration Guide.*

3.2.4 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 AlarmPoint Mobile Gateway.

To configure the default User:

1. In AlarmPoint, 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.
   - If you defined the custom fields, enter the **HP SM Login** and **HP SM Password** information into the custom fields.
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 Mobile Gateway. For more information and instructions on how to perform these tasks, refer to the* AlarmPoint User Guide.

3.2.5 Add the AlarmPoint Web Service User

This integration requires an AlarmPoint Web Service User for the Service Manager incidents to be injected to AlarmPoint using web services.

The AlarmPoint Web Service User must have the User ID and Password configured within the Service Manager AlarmPointConfig script; for more information, see “Modifying the AlarmPointConfig Script” on page 12.

To setup an AlarmPoint Web Service User:

1. In AlarmPoint, click the **Users** tab, and then click **Add Web Service User**.
2. Enter the following information into the form:
   - **User ID**: `APWSU`
   - **Description**: `AlarmPoint Web Service User`
   - **Password**: type the User’s password (default is `password`)
   - **Verify Password**: retype the password to verify it.
3. Set this User to have access to all of the available web services.
4. Click **Save**.

3.2.6 Configuring the Subscription Panel

This integration is packaged with an optional Subscription panel which reads Category, Subcategory, Problem Type and Product Type list values from Service Manager through web services. This feature allows Administrators to change the source of the content supplied for these lists from web service calls to predefined predicate value lists.

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

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

Note: *Before you can configure the optional Subscription panel, you must install the SMSubscriptionForm.jsp file, as described in “Installing the Subscription File” on page 8.*

3.2.6.1 Defining Event Domain predicates

The default Subscription panel provided with the integration requires the following Event Domain predicates:

- category
- subcategory
- product_type
- trigger_rule
- severity
- impact

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. For more information, see "Adding Custom Data Elements" on page 45.*

To define the Event Domain predicates:

1. In AlarmPoint, click the **Developer** tab.
2. On the Event Domains page, click **hp_sm_incident**.
3. On the Event Domain Details page, click **Add New**.
4. Add the following predicates to the Event Domain:

Predicate	Type	Important	Values	Description
category	List	Yes	Manually entered	A list of categories that are currently marked as active in Service Manager and may be listed on a ticket. By default, possible values are: • Incident
subcategory	List		Automatically generated	A list of subcategories that are currently marked as active in Service Manager and may be listed on a ticket.
product_type	List		Automatically generated	A list of product types that are currently marked as active in Service Manager and may be listed on a ticket.
trigger_rule	List		Manually entered	A list of reasons the event was triggered, defined in the AlarmPointEvent script library in Service Manager. If this list is updated in Service Manager, it must also be updated on the Event Domain. By default, the possible values are: • Priority Upgrade • Assignment • Ticket Resolved
severity	List	Yes	Manually entered	The severity of the incident. By default events are only injected if the incident severity is Critical or High. If this is changed, the new values must be added to the Event Domain. By default, the possible values are: • 1 - Critical • 2 - High

Predicate	Type	Important	Values	Description
impact	List		Manually entered	The value of the impact drop-down list on the incident. By default, the possible values are: • 1 - Enterprise • 2 - Site/Dept

Note: *For more information on the automatically generated list predicates, see "Configuring the Subscription JSP", below.*

3.2.6.2 Defining a Subscription Domain

The Subscription Domain is the reference point of the optional Subscription panel and provides a means to control certain aspects of it. 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 **Add Subscription Domain**.
2. In the Event Domain drop-down list, select **hp_sm_incident**, and then click **Continue**.
3. On the Subscription Domain Details page, in the **Name** field, type `Service Manager`.
   - By default, Subscriptions are non-FYI (i.e., they support response options). To disable two-way Subscription notifications, select the **One-Way** check box.
4. In the **Custom Page URL** field, enter the following path:

```
jsp\subscription\hpsmim\SMIMSubscriptionForm.jsp
```

5. Click **Continue**.
6. On the Select Appropriate Response Choices page, specify the available responses for this Subscription, and then click **Continue**.
   - By default, the scripts support the following response choices: "Own", "Ignore", "Reject" and "Resolve". To enable two-way communications for Subscriptions, define all four response choices on the Select Appropriate Response Choices page. If you require only one-way, informational notifications, do not specify any response choices.

Note: *By default, Subscriptions are FYI (informational-only notifications). To enable two-way subscription notifications, set the $subscription_fyi variable to false in the configuration block of the initial PROCESS script.*

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* AlarmPoint Installation and Administration Guide.

3.2.6.3 Configuring the Subscription JSP

To configure the Subscription panel in a demo mode, using predefined predicate list values, you must modify the Subscription JSP.

To manually populate the predicate lists:

1. Open the `SMIMSubscriptionForm.jsp` found in `<APHOME>\webserver\webapps\cocoon\alarmpoint\jsp\subscription\hpsmim` folder on the AlarmPoint Webserver install.
2. Set the Boolean variable `QUERY_PREDICATE_VALUES` to *false*.
3. Save and close the `SMIMSubscriptionForm.jsp` file.
4. In AlarmPoint, click the **Developer** tab.
5. On the Event Domains page, click **hp_sm_incident**.
6. On the Event Domain Details page, click **subcategory** in the Predicates list.
7. Add to the predicate list values.
8. Repeat steps 6 and 7 for **product_type** in the predicates list.

The Subcategory and Product Type lists on the Subscription will now be populated with the predefined list values instead of the web service call results.

Note: *Changing Subscriptions by adding or removing Event Domain predicates may cause existing Subscriptions to fail. For more information about working with Event and Subscription Domains, see the* AlarmPoint Installation and Administration Guide.

If you want to populate the predicate values lists from Service Manager through web service calls rather than the predefined predicate list values, you must configure the connection properties within the JSP file.

To configure the Subscription JSP to connect to Service Manager through web services:

1. Open the `SMIMSubscriptionForm.jsp` found in `<APHOME>\webserver\webapps\cocoon\alarmpoint\jsp\subscription\hpsmim` folder on the AlarmPoint Webserver install.
2. Within the Subscription JSP, find the following section:

```
final String SERVICE_MANAGER_URL = "http://localhost:13080/sc62server/ws";
final String SERVICE_MANAGER_USER = "falcon";
final String SERVICE_MANAGER_PASSWORD = "";
```

3. Replace the value within quotes for each parameter as described in the following table:

Parameter	Value
SERVICE_MANAGER_URL	The URL for the Service Manager web services.
SERVICE_MANAGER_USER	User name of the Service Manager Web Services User.
SERVICE_MANAGER_PASSWORD	Password for the Service Manager Web Services User.

4. Save and close the JSP.

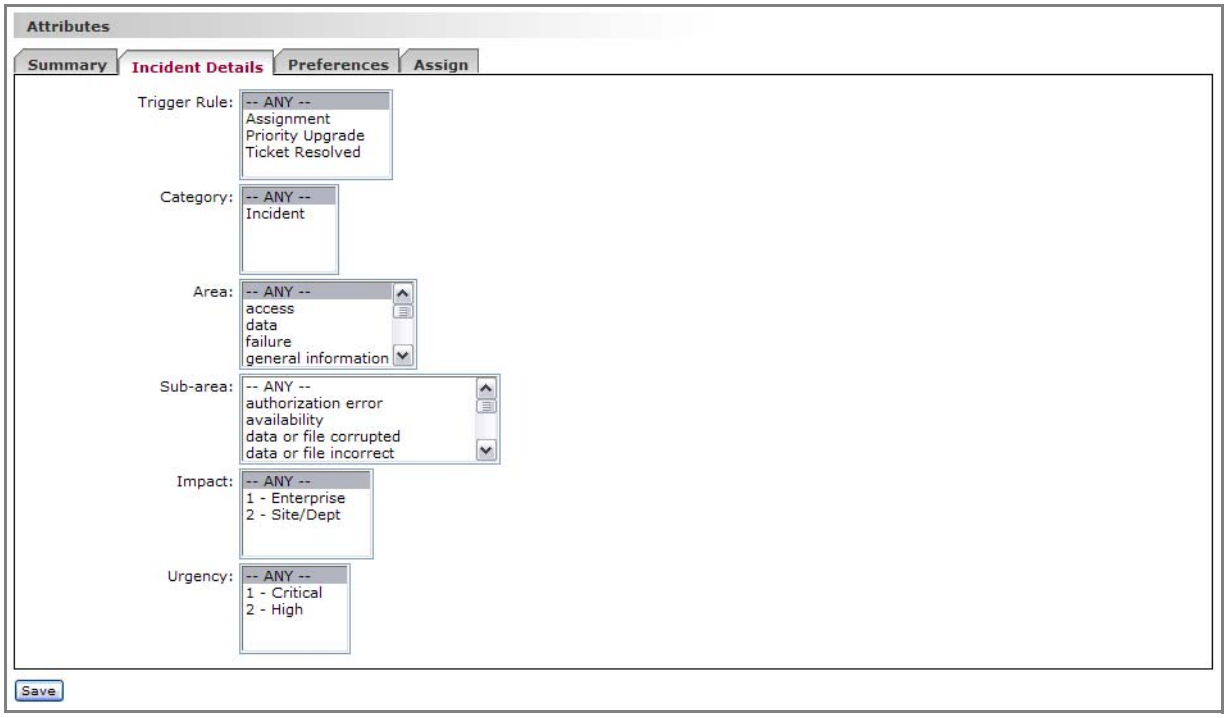
Note: *The SERVICE_MANAGER_USER and SERVICE_MANAGER_PASSWORD must match the User configured in "Add SOAP API and AlarmPoint Capabilities to Service Manager User" on page 13.*

3.2.6.4 Creating a Subscription

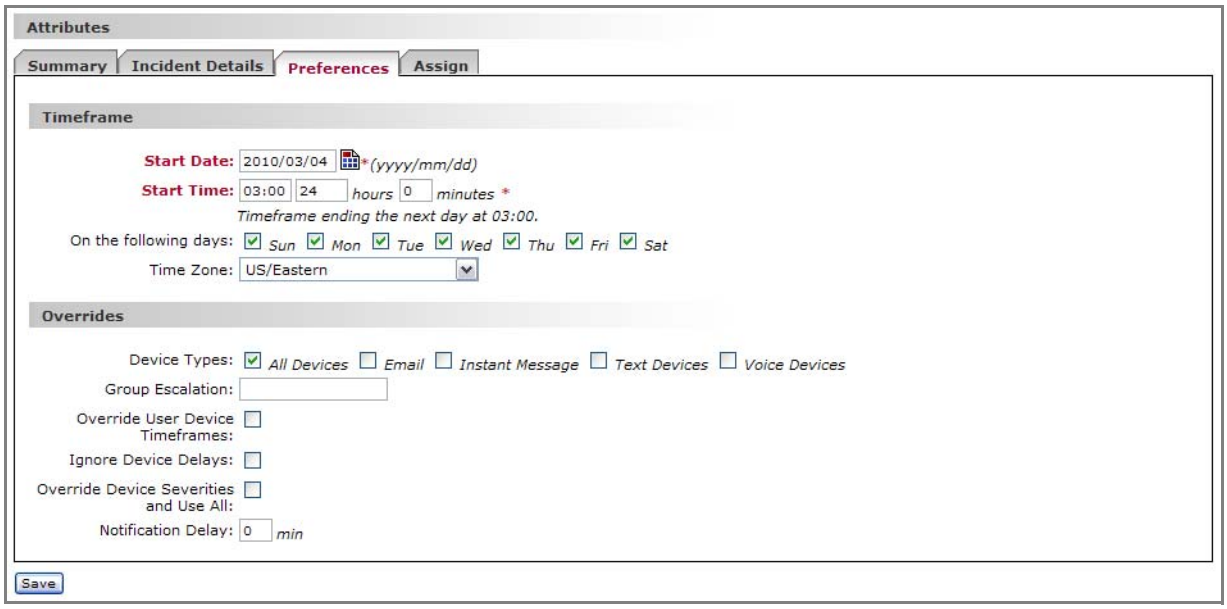
You can now use the custom Subscription panel to subscribe to Service Manager events of specific criteria, such as those of "Critical" Severity.

To create a Subscription:

1. On the Alerts tab, in the Alerts menu, click **My Subscribed Alerts**.
2. Select the Service Manager 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 Incident Details and Preferences tabs.
   - The Incident Details tab (Ctrl-click to select more than one value):



   - The Preferences tab (defines the Timeframe and Overrides applied to events for Subscription notifications):



4. When you are satisfied with the criteria, click **Save** to create the Subscription.
   - You can review the Subscription details at any time on the Summary tab:

3.2.6.5 Create a Fail-Safe Group

If a notification is submitted to AlarmPoint when the fail-safe functionality is enabled, and if it matches the necessary circumstances, AlarmPoint 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 AlarmPoint, click the **Groups** tab.
2. Create a new Group named **HP SM FailSafe**, with at least one User as a Team member to receive notifications.

For more information about creating Groups and Teams, see the *AlarmPoint User Guide*.

Note: *If you want to use an existing Group or a different Group name, modify the value for the $fail_safe_group variable defined in the initial PROCESS script in the AlarmPoint Action Scripts. You can also eliminate notifying any fail-safe group by setting $fail_safe to disabled.*

3.2.7 Creating a Service Manager Admin Group

If a synchronization error occurs and the send_sync_error_notification configuration variable is set to `true` in the AlarmPointConfig script, then a notification is sent out to the recipient defined in the default_alarmpoint_admin_group variable in the AlarmPointConfig script. The default value is set to "superadmin".

Note: *If AlarmPoint is installed with unmerged admin and root accounts, default_alarmpoint_admin_group should be changed to "companyadmin".*

To configure a Service Manager Admin Group, click the **Groups** tab in AlarmPoint, and create a new Group named **SM Admin**, with at least one User as a Team member to receive notifications. Update the default_alarmpoint_admin_group variable in the AlarmPointConfig script with the name of the new Group.

For more information about creating Groups and Teams, see the *AlarmPoint User Guide*.

Note: *If you do not want notifications to be sent out due to synchronization errors, set the send_sync_error_notification variable in the AlarmPointConfig script in Service Manager to* false.

3.3 Configure Synchronization

The AlarmPoint for HP Service Manager integration supports one-way synchronization of Groups (both Assignment and Change groups in Service Manager), Teams, Users, Devices and Coverages from Service Manager into AlarmPoint. To enable synchronization and customize it to your business behaviour, two configuration files are provided: `AlarmPointSyncConfig.xml` and `AlarmPointSyncList.xml`.

Modify these files according to your desired business behaviour; the following sections provide an overview of these files and their configurability.

Note: *When performing synchronizations, open the Service Manager messages panel. This allows you to see successful completion of synchronizations such as modifying Groups, Group memberships, Users, and User Devices. Alternatively, you can use the Sync Report under the Menu Navigation AlarmPoint entry to determine if any errors occurred after synchronization.*

3.3.1 AlarmPoint Synchronization Configuration File

The `AlarmPointSyncConfig.xml` file defines the synchronized values for Groups, Teams, Users, Devices and Coverages. The file included with the integration has default values to use for each object type, but can be customized to use different values for a specific instance of an object.

Note that in HP Service Manager, Login IDs are case sensitive; for example, “FALCON” and “falcon” represent two separate users in Service Manager. In AlarmPoint, User IDs (the equivalent to Login IDs in Service Manager) are case insensitive: AlarmPoint would not recognize “FALCON” and “falcon” as belonging to different Users.

3.3.1.1 Default Values

Each default element must specify a value for all possible fields (refer to the following section for a complete list of possible fields). Each default element must also specify the `seedOnly` and `deletable` attributes.

If the `seedOnly` attribute is true, then that object will only be added to AlarmPoint when it is initially synchronized and will no longer be updated. If the `seedOnly` attribute is `false`, any modifications to the object done in AlarmPoint will be overwritten when that object is updated in Service Manager.

If the `deletable` attribute is true, then that object will be removed from AlarmPoint when it is deleted from Service Manager; otherwise, it will remain in AlarmPoint indefinitely and must be deleted manually.

The following elements must exist in the `AlarmPointSyncConfig.xml` file:

- default-user
- default-email
- default-work-phone
- default-home-phone
- default-mobile-phone
- default-assignment-group
- default-change-group
- default-team
- default-coverage

By default, all objects are `deletable` and `seedOnly` except for email, work-phone, home-phone, and mobile-phone, which will always update in AlarmPoint.

There are three different ways that you can specify a default value to synchronize with AlarmPoint:

1. Set a default value for a field:
   - **default**: the value for this field

For example, the role for the following will be `standard user` unless it is overridden:

```
<role default="standard user"/>
```

2. Use a regular expression to extract a value from a field:
   - **default**: the default value for this field if the regular expression does not match
   - **field**: the column in this table to apply the regular expression
   - **regex**: the regular expression used to extract a value
   - **index**: when you use Groups, this is the index of the Group you want to use (where the first Group is 1)

For example, the area-code for the following will be the first submatch when the '\D*(\d{0,3})\D*([0-9]{1}[0-9., -]+)\D*' regular expression is applied to the contact_phone field

```
<area-code field="contact_phone" regex="\D*(\d{0,3})\D*([0-9]{1}[0-9., -]+)\D*"
index="1"/>
```

3. Map a field's value to a desired value:
   - **default**: the default value to use if there is no match
   - **map Element**: the field attribute specifies the column in the table to match; the value attribute specifies the value of the field to match on; and, the text of this field is the value to be saved

For example, the language for the following will be `English`, unless the value of the language column in the record is either `de` or `fr`:

```
<language default="English">
  <map field="language" value="de">German</map>
  <map field="language" value="fr">French</map>
</language>
```

3.3.1.2 Object Specific Values

All object-specific elements will override any default value element and can override the `seedOnly` and `deletable` attributes.

default-user Fields

Field	Description	Possible Values
active	Whether this User is active	true, false
first-name	User's first name	Any string
last-name	User's last name	Any string
has-mobile-access	Mobile access flag	true, false
site	User's Site	Valid AlarmPoint Site name
language	User's language	Valid AlarmPoint language
timezone	User's time zone	Valid AlarmPoint time zone
role	User's AlarmPoint Role	A comma-delimited list of valie AlarmPoint Roles.
supervisor	User's AlarmPoint supervisor	Valid AlarmPoint User target name. If the supervisor in Service Manager is not a valid User in AlarmPoint, the synchronization for the User/Group will fail.
has-phone-login	Phone login flag	true, false
phone-login	User's phone login	Unique string containing only digits
phone-password	User's phone password	String containing only digits
ldap-domain	User's web login LDAP domain	Valid AlarmPoint LDAP domain
web-login	User's web login	Unique web login
web-password	User's web login password	Any string
web-login-type	Defines whether the web login is a native AlarmPoint login or an LDAP authentication	NATIVE, LDAP
externally-owned	Indicates whether the User is externally-owned	true, false
custom-field-name	The name of the Custom Field in AlarmPoint that will contain the value of SM userId to be used by Mobile Gateway login and notification responses.	Any string. Default is "HP SM Login"
custom-field-value	The value to use in the Custom Field defined in the custom-field-name field.	Any string

default-email Fields

Field	Description	Possible Values
name	Device name (must match a Device name configured in AlarmPoint)	Valid AlarmPoint email Device name
active	Whether this Device is active	true, false
default	Whether this Device should be used as the User's default Device	true, false
delay	Device's delay setting	Integer value
externally-owned	Externally owned flag	true, false
priority-threshold	Device's priority threshold	LOW, MEDIUM, HIGH
user-service-provider-id	ID of the User Service Provider (is ignored if the name is present)	Long
user-service-provider-name	Name of the User Service Provider (takes priority over provider ID)	Valid AlarmPoint User Service Provider name
address	Device's email address	Valid email address

default-work-phone, default-home-phone, and default-mobile-phone Fields

Field	Description	Possible Values
name	Device name (must match a Device name configured in AlarmPoint)	Valid AlarmPoint email Device name
active	Whether this Device is active	true, false
default	Whether this Device should be used as the User's default Device	true, false
delay	Device's delay setting	Integer (time in minutes)
externally-owned	Externally owned flag	true, false
priority-threshold	Device's priority threshold	LOW, MEDIUM, HIGH
user-service-provider-id	ID of the User Service Provider (ignored if the name is present)	Long value
user-service-provider-name	Name of the User Service Provider (takes priority over provider ID)	Valid AlarmPoint User Service Provider name
area-code	Device's area code	String containing only digits
country-code-override	Device's county code	Valid two letter country code
extension	Device's extension	String containing only digits
number	Device's phone number	String matching [0-9]{1}[0-9., -]+

default-assignment-group and default-change-group Fields

Field	Description	Possible Values
description	Group's description	Any string
timezone	Group's time zone	Valid AlarmPoint time zone
site	Group's Site	Valid AlarmPoint Site
active	Whether this Group is active	true, false
allow-duplicates	Allow duplicates flag	true, false
externally-owned	Externally owned flag	true, false
observed-by-all	Observed by all flag	true, false
observer	Target name of a User to be the Group's observer	Valid AlarmPoint User target name
supervisor	Target name of a User to be the Group's supervisor	Valid AlarmPoint User target name
use-default-device	Use default Device flag	true, false

default-team Fields

Field	Description	Possible Values
suffix	Team name is generated by the Group name and the suffix	Any string not containing '|'
description	Description for the Team	Any string
externally-owned	Externally owned flag	true, false
reuse	Reuse Team flag	true, false
rotation-interval	Rotation interval (only used if type is ROTATION)	Integer value
rotation-start	Rotation start date (only used if type is ROTATION)	Date in the format 'dd/mm/yyyy h:mm:ss AM/PM'
rotation-unit	Rotation units (only used if type is ROTATION)	DAYS, MONTHS, WEEKS
type	Team type	BASIC, EVENT_ROUND_ROBIN, ROTATION
member-type	Team member type (should leave as PERSON for the integration)	PERSON, GROUP, TEAM, DEVICE
member-delay	Delay between Team members	Integer value
member-in-rotation	Are Group members in the rotation	true, false

default-coverage Fields

Field	Description	Possible Values
suffix	Coverage name is generated by the group name and the suffix	Any string not containing '|'
start-time	Start time for this shift	Time in the format "hh:mm"
duration-hours	Hours duration of the shift	Integer value 0 <= N <= 24
duration-minutes	Minutes duration of the shift	Integer value 0 <= N <= 60
exclude-holidays	Exclude holidays flag	true, false
sunday	Coverage on Sunday	true, false
monday	Coverage on Monday	true, false
tuesday	Coverage on Tuesday	true, false
wednesday	Coverage on Wednesday	true, false
thursday	Coverage on Thursday	true, false
friday	Coverage on Friday	true, false
saturday	Coverage on Saturday	true, false
recurrence-end-date	End date for the coverage	Time in the format `dd/mm/yyyy h:mm:ss AM/PM`
recurrence-frequency	Frequency of the recurrence	DAILY, WEEKLY, MONTHLY
recurrence-interval	Interval of the recurrence	Integer value
recurrence-no-end-date	No end date flag	true, false
recurrence-occurences	Number of recurrences for this coverage	Integer value
recurrence-start-date	Start date of the recurrence	Time in the format `dd/mm/yyyy h:mm:ss AM/PM`

Note: *See the* `AlarmPointSyncConfig.xml` *file for more examples.*

3.3.2 AlarmPoint Synchronization List File

The `AlarmPointSyncList.xml` file is used to define which operators and assignments should be synchronized with AlarmPoint. The XML file contains a list of user elements with a name attribute matching a Service Manager operator ID and a list of group elements containing a name attribute matching a Service Manager assignment name.

The user and group elements have an action attribute which tells the integration whether you want to include only the user and group in the list for synchronization and exclude all other users and groups, or whether you want to exclude the user and group in the list for synchronization and include everyone else. The following is an example of what the file would look like if you want to synchronize only the TELECOMS assignment and want to synchronize all the operators except for FALCON:

```
<synclist>
  <users action="exclude">
    <user name="FALCON"/>
```

```
    </users>
    <groups action="include">
      <group name="TELECOMS"/>
    </groups>
  </synclist>
```

3.4 Custom Service Manager Forms

The AlarmPoint integration is installed with the following Custom Service Manager Forms: Sync Report, Quick Message, and Who Is On Duty Report. These are used to synchronize Service Manager information with AlarmPoint, send messages to Groups and Users and determine who is on duty for a specific day.

3.4.1 Sync Report

The Sync Report can begin full system synchronization andview the last status of objects synchronized with AlarmPoint. The behavior of the page is as follows:

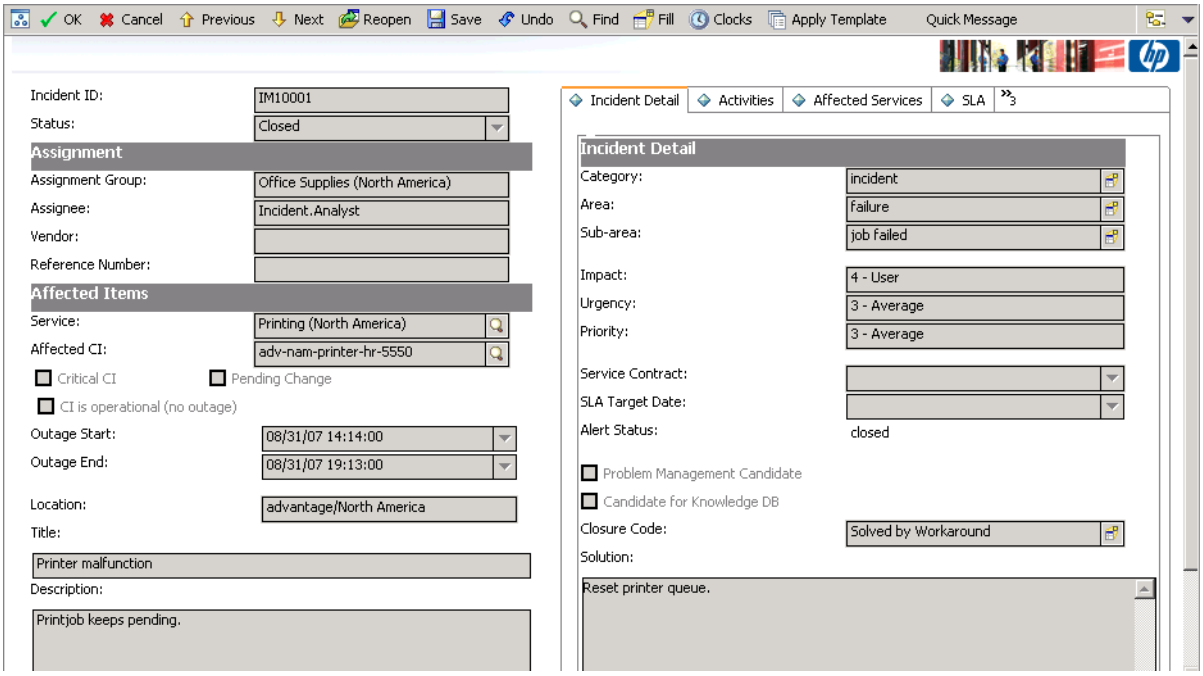
- Clicking **Show Errors** displays all synchronization records that are currently in an error state.
- Clicking **Show All** displays all synchronization records.
- Selecting **Sync Now** initiates an attempt to synchronize the entire system.
- Clicking **Filter** displays all synchronization records that match the specified filter criteria. These filter fields use the StartsWith operator.

3.4.2 Quick Message

The Quick Message page is used to send a quick message to a list of groups or operators. All messages from this screen will contain the following information:

- **Operator**: the user who initiated this message.
- **Reference ID**: a field that is meant to help associate this message with an incident. This is autofillable by setting the `$G.alarmpoint.quickmessage.incidentId` global variable.
- **Assignment and Change Groups**: a list of groups you want to target with this message.
- **Operators**: a list of operators you want to target with this message. This is autofillable by setting the `$G.alarmpoint.quickmessage.users` global variable.
- **Subject**: reserved for the subject of the message you want to send to the targeted groups and operators.
- **Message**: reserved for the message you want to send to the targeted groups and operators.

You should now be able to open the Update Incident form and see the Quick Message button. This allows you to send a quick message to a user with the incident ID auto-populated for the selected incident, as illustrated by the following figure:



3.4.3 Who Is On Duty Report

The Who Is On Duty Report is a method of determining who is on duty for a Group for a specified day. The behavior of this page is as follows:

- The **Assignment Group** and **Change Group** selector controls whether Assignment or Change Groups will be shown in the Group field.
- The **Group** field is used to select the Group for which you want to run the report. Based on the selected radio button, you can list Assignment Groups or Change Groups.
- The **Start Date** field is used to select the day on which you would like to run. This report always generates data for only a single day.
- Clicking **Check** makes the request to the server and displays the results in the HTML window at the bottom of the page.
- The **Recipients** list is automatically populated with the Group name, Group member names, and the Group Supervisor names. Clicking **Send Message** on this page will take you to the Quick Message page and auto-populate the Operators field with the selected Recipient.

Note: *The Who Is On Duty Report is available only to AlarmPoint Enterprise customers.*

3.4.4 Adding Buttons and Menus for the AlarmPoint Custom Forms

The `alarmpoint.syncreport`, `alarmpoint.quickmessage` and `alarmpoint.whoisonduty` scripts are provided with the integration and can be used with the `script.execute` RAD application. If you set the global variables `$G_alarmpoint_quickmessage_incidentId` or `$G_alarmpoint_quickmessage_users` before running the alarmpoint.quickmessage script, the incident ID and operators fields can be automatically populated with data.

To add Custom Form menu items to the System Navigator under the AlarmPoint group:

1. In Service Manager, open **Menu Navigation > Tailoring > Tailoring Tools > Menus**.

2. In the **Menu Name** field, type the name of the appropriate menu for your deployment (e.g., `HOME`), and then click **Search**.
3. Add the following values to the table:

Option Number	Description	Application	Parameter	Parameter Value	Condition
Next available number	AlarmPoint	menu.manager	name	AlarmPoint MAIN	index("AlarmPoint", $lo.ucapex)>0

Note: *Ensure that you record the Option Number assigned to each button and menu, as you will need to reference these numbers when adding the custom form buttons in the next section.*

4. Click **Save**, and then click **Save** again.
   - If you receive an error message after clicking Save the first time, you can safely ignore it.
5. Refresh the System Navigator.

You should now see a new AlarmPoint navigation group in the System Navigator with separate entries for each AlarmPoint Custom Form.

Note: *The Custom Form menu items and buttons will only be visible to users with the AlarmPoint Capability. For information about how to add the AlarmPoint Capability, refer to the "Add SOAP API and AlarmPoint Capabilities to Service Manager User" on page 13.*

The integration also installs a displayoption control, with a unique id of alarmpoint.apm.edit.problem.haltincident, labelled Halt AlarmPoint Notifications. Users should be able to open the Update Incident form and have the Halt AlarmPoint Notifications control available allowing you to halt all AlarmPoint notifications for that incident. Note that the default Balloon Help value for alarmpoint.apm.edit.problem.haltincident is 200, but this can be changed if your Service Manager installation already has a displayoption associated with apm.edit.problem that uses a value of 200.

4. Software Component Validation

It is recommended that the applications be run in the following order:

- HP Service Manager
- AlarmPoint Application and Notification Server Nodes

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

The following sections will test the integration for User and Group Synchronization, notification delivery and response, and the Subscription Panel functionality.

4.1 User and Group Synchronization

The following validates that one-way communication from Service Manager to AlarmPoint User and Group Synchronization 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 and Group Synchronization:

1. Edit the `AlarmPointSyncList.xml` file as follows:

```
<synclist>
  <users action="include">
  </users>
  <groups action="include">
  </groups>
</synclist>
```

2. Restart your Service Manager client.
3. Add a new Operator to Service Manager:
   - In Service Manager, open **Menu Navigation** > **System Administration** > **Ongoing Maintenance** > **User Quick Add Utility**.
   - Specify the required information.
   - Click **Next**, **Finish**, and then **OK**.
4. In Service Manager, open **Menu Navigation** > **System Administration** > **Ongoing Maintenance** > **Groups** > **Incident Management Assignment Groups**.
5. Type the name of the assignment group you want to use for testing purposes (eg. `TESTSYNC`).
6. Select the **Operators** tab, add the Operator you just created, click **Add**, and then click **OK**.
7. Edit the `AlarmPointSycnList.xml` file to look like the following (replace `operatorname` and `assignmentname` with the Operator and Assignment Group you just created):

```
<synclist>
  <users action="include">
    <user name="operatorname"/>
  </users>
  <groups action="include">
    <group name="assignmentname"/>
```

```
  </groups>
</synclist>
```

8. Restart the Service Manager client
9. Open the custom Sync Report form (see “Adding Buttons and Menus for the AlarmPoint Custom Forms” on page 34 for instructions how to add a menu item for this).
10. In the drop-down list in the upper right, select **Sync Now**.
    - This should synchronize the operator and assignment that you just added to Service Manager into AlarmPoint as a User and Group.
11. Log in to AlarmPoint to check that the User and Group was properly synchronized.

Note: *The AlarmPoint User target name is the Service Manager contact's operator ID and the AlarmPoint Group name is the Service Manager assignments name.*

4.2 Trigger a Notification

In this example a Service Manager incident will be injected to AlarmPoint for notification for the Group configured in the User and Group Synchronization example.

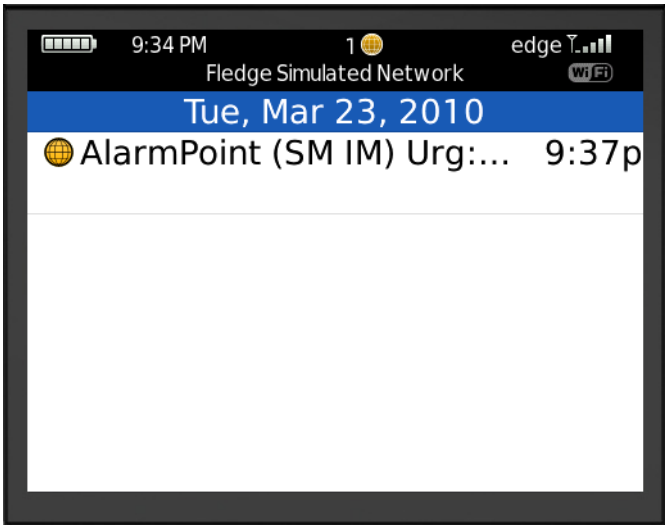
1. In Service Manager, open **Menu Navigation > Incident Management > Open New Incident**.
2. Specify the following values in the required fields:
   - **Primary Asgn Group**: the Assignment group you just synchronized with AlarmPoint.
   - **Urgency**: either 1 - Critical, or 2 - High.
3. Enter values for all other required fields.
4. Click **Submit**.

This should inject the incident parameters into AlarmPoint, triggering a new notification targeting the Assignment group you just synchronized with AlarmPoint in the User and Group Synchronization example.

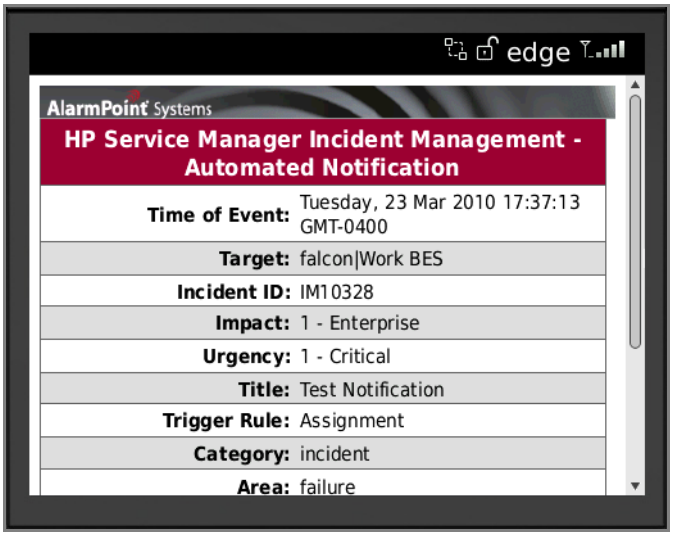
4.3 Responding to a Notification

This section describes how to respond to a notification using a virtual BlackBerry:

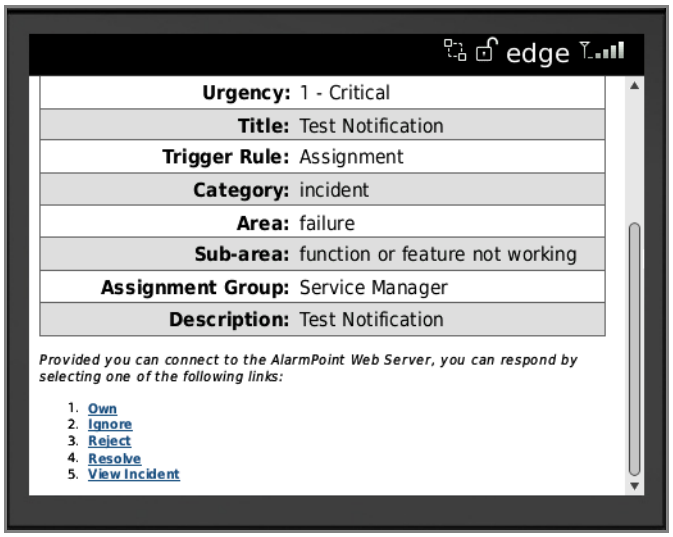
1. When a notification arrives for the User, the Device indicates the number of calls received:



2. Open the notification to view the incident details:



3. Scroll down to view the remainder of the details and the list of possible replies:



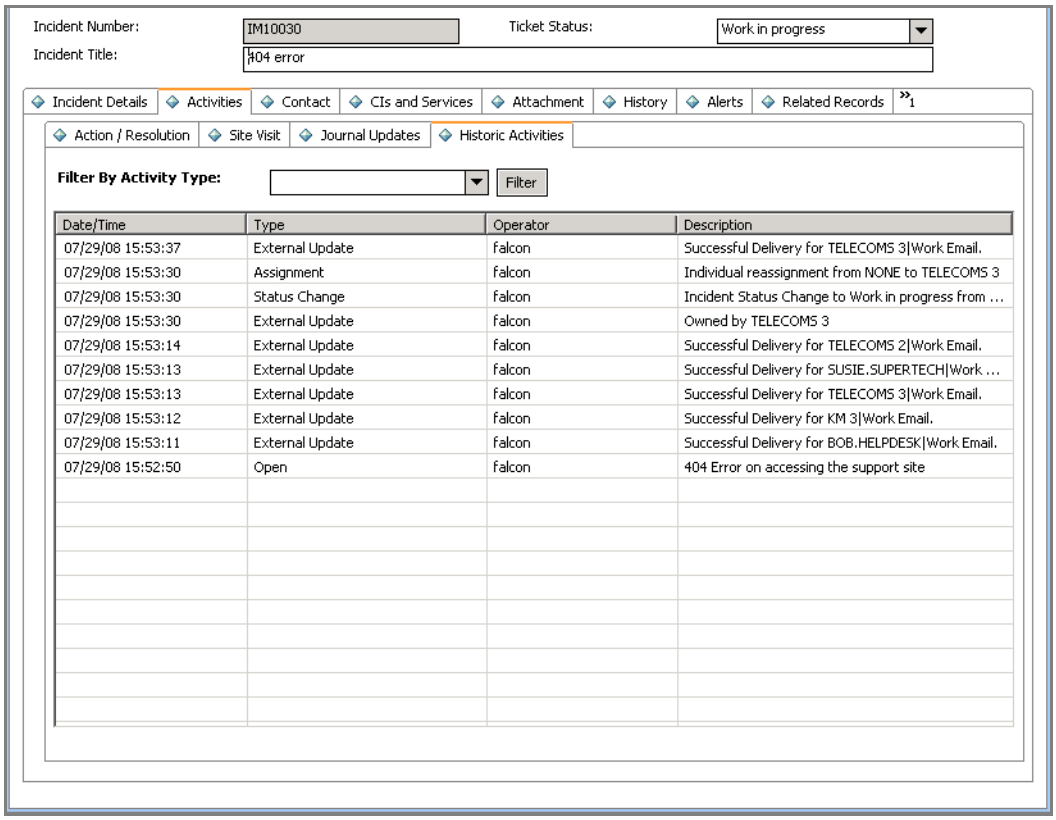
4. To respond to the notification, click your response choice, and AlarmPoint will update the Service Manager incident through Web Services.

4.4 View Response Results

When an action is taken on an AlarmPoint notification, that action is reflected in the Service Manager incident. When AlarmPoint makes changes to a ticket, it also updates the Historic Activities field on the Service Manager incident.

To view the updates:

1. In Service Manager, open **Menu Navigation > Incident Management > Search Incidents**.
2. In the **Number** field, type the incident ID of the ticket you want to view, and then click **Search**.
3. Click the **Activities** tab, and then click the **Historic Activities** tab to view the updates:



- The status of the Incident will be updated to “Work In Progress” (Own).

For each User Device notified during this process the Historic Activities log will be annotated with a message indicating “Successful Delivery for bsmith|Work Email” where “bsmith|Work Email” is the recipient (<User>|<Device>).

4.5 Testing the Subscription Panel

To test Subscriptions ensure that you have created a Subscription (for more information, see the “Configuring the Subscription Panel” on page 21). Trigger a Subscription Notification (see “Trigger a Notification” on page 37), specifying the criteria that you have configured your Subscription to match. You will receive an FYI Notification (informational only) similar to the one received in “Responding to a Notification” on page 37 which will not have any response choices available.

Note: *Ensure that Subscriptions are enabled in the Action Script Package with the $enable_subs variable. For more information on how to configure Subscriptions, see “Configuration Variable Reference” on page 54.*

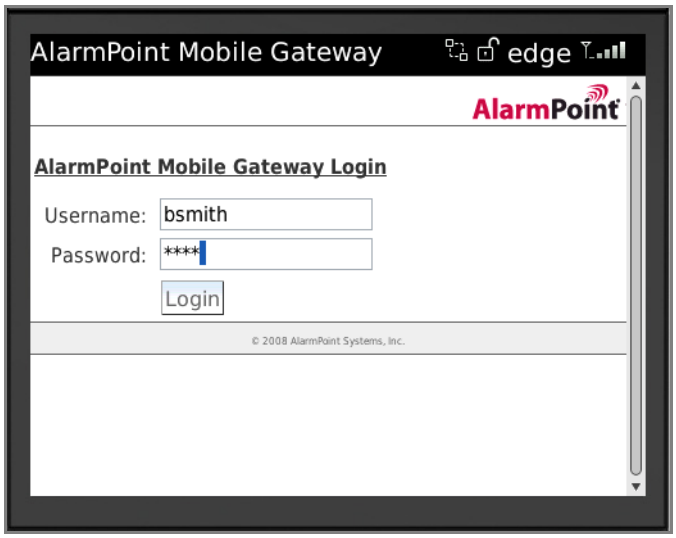
4.6 Query for an Incident

The following validates that the Mobile Gateway, Integration Agent and HP Service Manager are properly configured.

Note: *The Mobile Gateway page has a default URL of* `http://<AlarmPointIP>:8888/mg`, *where* `<AlarmPointIP>` *is the IP address of the AlarmPoint Webserver where the Mobile Gateway is configured.*

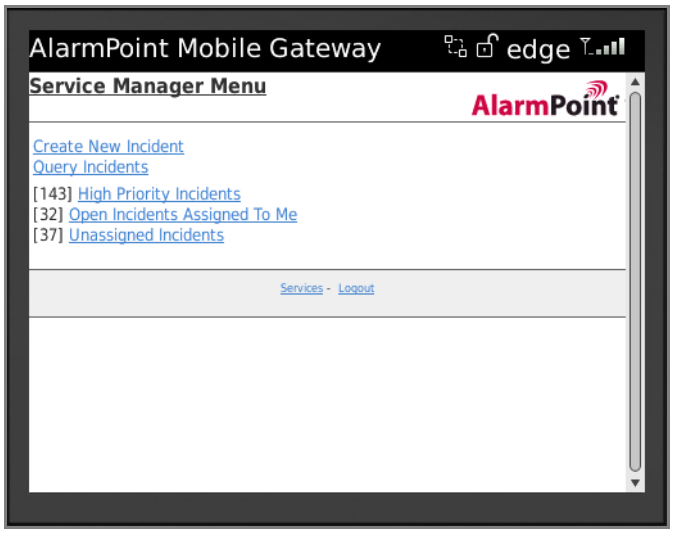
To query for an incident:

1. Log in to the Mobile Gateway as bsmith:

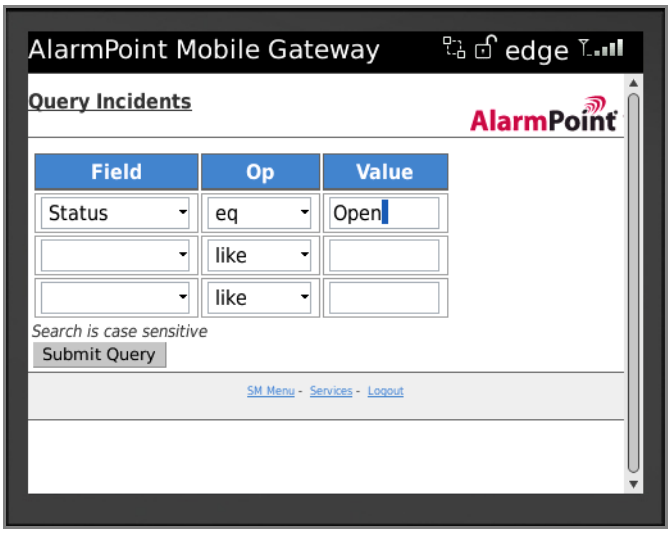


- If more than one Integration Service is available, select the **HPSMIM** service.

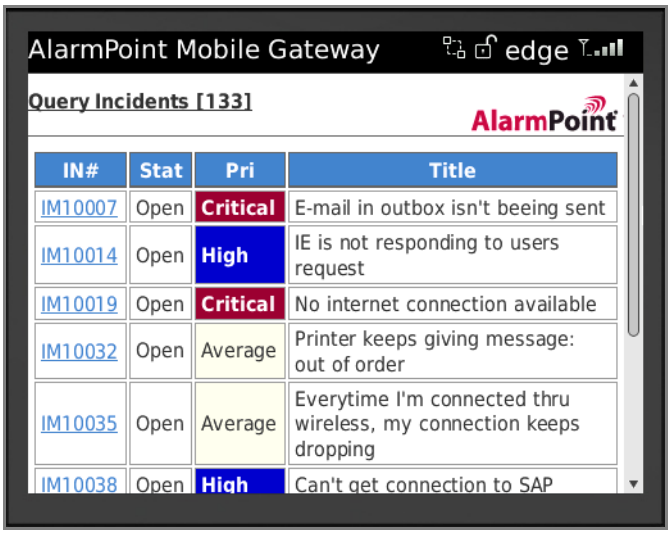
2. If prompted, enter the Service Manager login credentials, and then click the **Query Incidents** menu item:



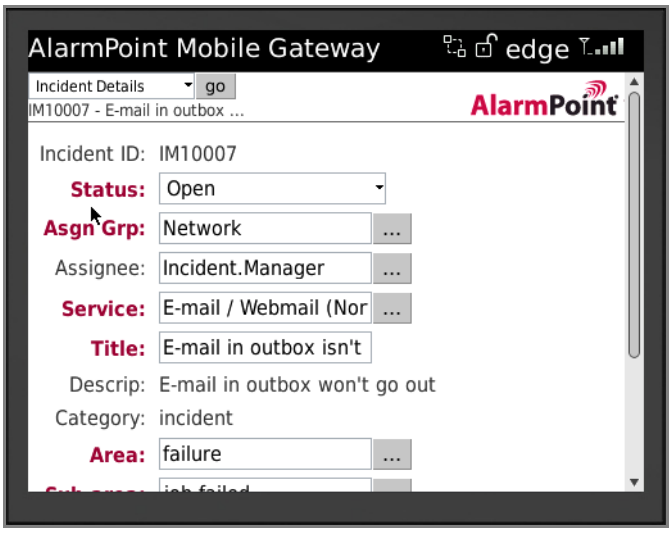
3. Enter `Status eq Open` in the fields provided:



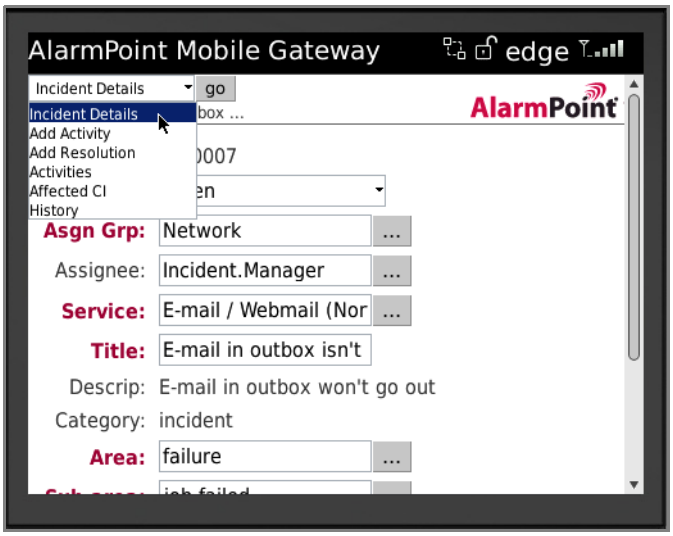
4. Click **Submit** to list all open incidents:



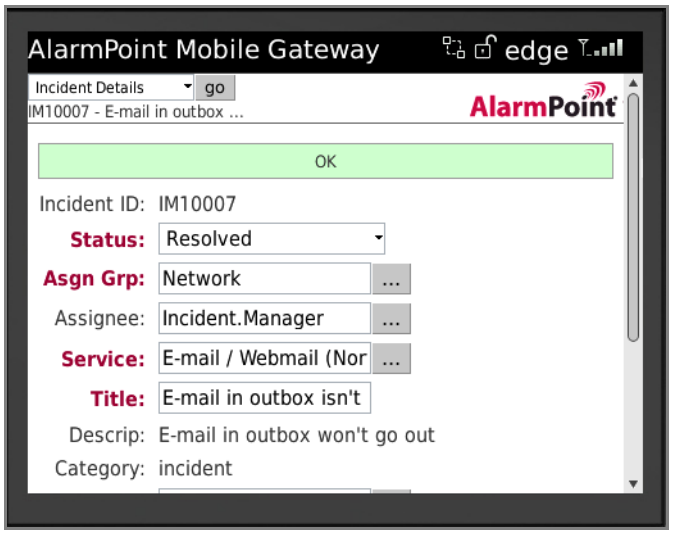
5. Click the **IN#** (Incident Number) for an incident to view its details:



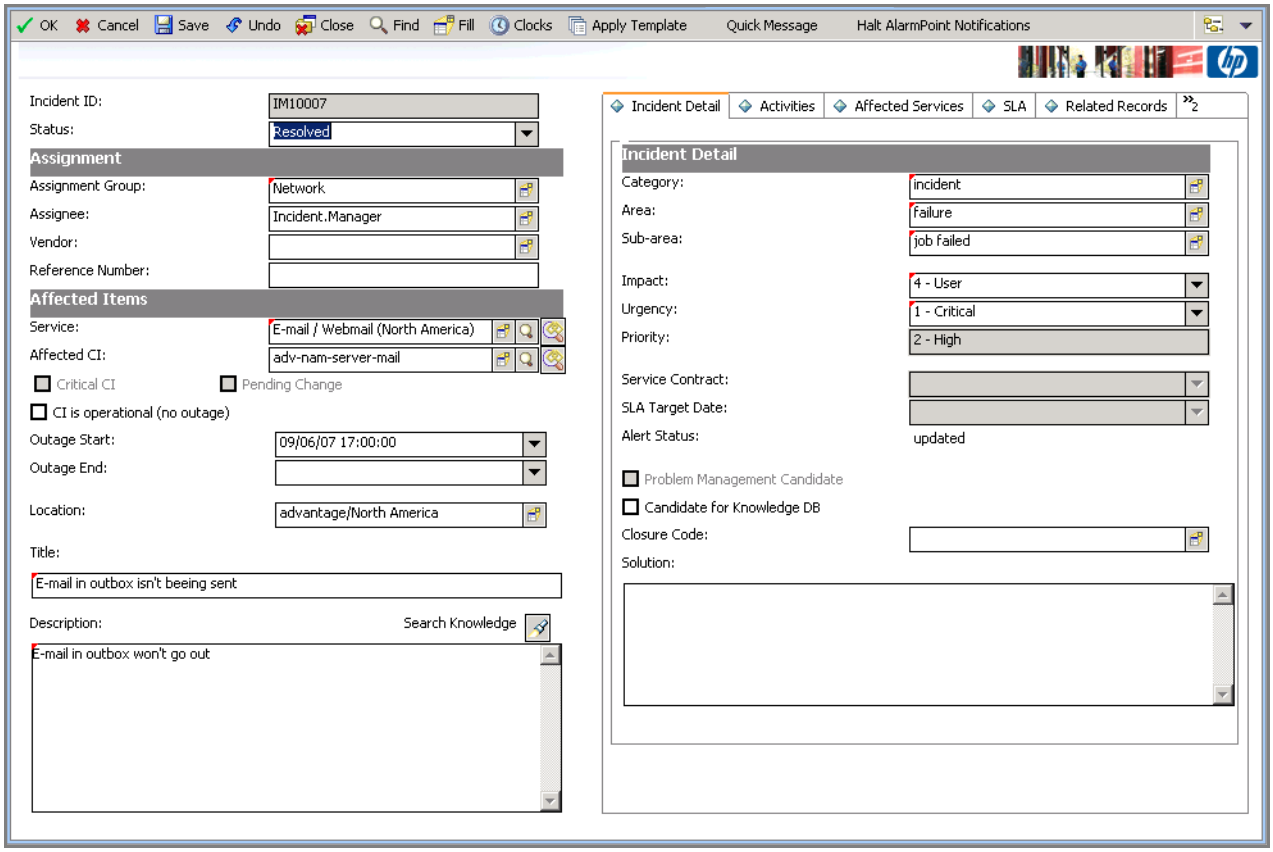
- You can view the available options for the incident in the drop-down list at the top of the screen:



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



7. Log in to HP Service Manager and view the details for the incident to confirm that its Status is now set to “Resolved”:



5. Optimizing and Extending the Integration

This section describes some of the available methods you can use to optimize or extend the AlarmPoint for HP Service Manager Integration.

5.1 Adding Custom Data Elements

Additional data elements can be forwarded to AlarmPoint by adding them to the AlarmPointEvent script in Service Manager. The following steps explain how to add a new event token to the event injected to AlarmPoint.

To add an Event Token:

1. In Service Manager, click **Menu Navigation > Tailoring > Script Library**.
2. In the **Name** field enter `AlarmPointEvent`, click **Search**.
3. Find the addEvent function.
4. After the other lines starting with addEventTokenToRequest, add the following:

```
addEventTokenToRequest(request, "TokenName", tokenvalue);
```

   - Where “TokenName” is the name of the token and “tokenvalue” is the value for the token.

5. Click **Save**.

5.2 Adding the custom parameter to notification content

Once you have injected the custom parameters, you can add the parameter to the notification content for Devices. The following steps explain how to add the custom parameter to email notifications; adding content for other Device types is similar and requires the presentation script to be modified for the specific Devices.

To add custom parameters to email notification content:

1. Open the AlarmPoint Developer IDE and check out the HP Service Manager Incident Management (BUSINESS) Script Package.
2. In the Presentation Action Script, add the following line to the email content creation section:

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

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

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

Your Custom Parameter should now appear in your Notification content for Email Devices.

5.3 Response Choices

The AlarmPoint integration allows recipients to respond to notifications with several default choices, some of which are injected back to the Service Manager 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 Service Manager incident.

The following is a list of the default response choices available with the AlarmPoint integration and their associated actions on the AlarmPoint event and the Service Manager incident:

Response Choice	AlarmPoint Action	Service Manager Update	Default Device Availability
Own	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 owns the event in AlarmPoint, and then closes the event. They may also annotate the owned event.	The ticket status for the incident is changed to Work In Progress and any additional notes added to the response are recorded on the incident's Journal Updates.	All non-FYI devices
Ignore	Signifies that the User ignores the notification.	The response is recorded on the incident's Journal Updates along with any additional notes.	Email, BES and Browser. For other non-FYI mobile Devices an Ignore is represented as "Ign".
Reject	Delinks all Users from the event, not allowing them to submit responses. An FYI notification is sent to the Service Manager incident owner.	The ticket status for the incident is changed to Rejected and any additional notes added to the response are recorded on the incident's Journal Updates.	Email, BES and Browser. For other non-FYI mobile Devices a Reject is represented as "Rej".
Resolve	Delinks all Users from the event, not allowing them to submit responses.	The ticket status is updated to Resolved and any additional notes added to the response are recorded on the incident's Journal Updates.	Email, BES and Browser. For other non-FYI mobile Devices a Resolve is represented as "Res".
Annotate	Halts delivery of notifications to any other Devices the responding User may have configured.	Any additional notes added to the response are recorded on the incident's Journal Updates.	This functionality is available for Email Devices only.

5.3.1 Responses for FYI Notifications

FYI notifications do not have any response choices available, except for FYI notifications sent to voice Devices. Voice FYI notifications offer the following response choices so that Users can navigate between multiple notifications. (This navigation is not required on other Devices.)

Response	Description
Delete	Removes the notification from the User's list.
Save	Saves the notification and stops attempting to deliver it to the User's other Devices. Users may select this option to delay listening to the notification when it is delivered, and access the details by calling in, or via the AlarmPoint Web User Interface, at a later time.
Repeat	Repeats the notification.

5.3.2 Adding Annotation Messages

Two-way email Device notifications (not FYI) can add extra annotations that will be added to the Service Manager incident as a message on the Journal Updates tab. 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.

5.3.3 Responses for Sync Errors and Quick Messages

Sync Error and Quick Message notifications are based on the hp_sm_incident Event Domain. These create an event within AlarmPoint and the available responses do not have any effect on the Service Manager system; the response choices are the same as those defined in "Responses for FYI Notifications", above.

5.4 Changing and Adding Response Choices

The response choices and behavior can be changed in the response script in the Action Script set (to change Subscription responses, update the subscriptionResponse script). Actions available through web service calls include owning, closing, rejecting and annotating an incident. Any other response functionality for the integration must be configured within the response HANDLER script with Service Manager provided web service calls.

For example, the following code illustrates the Own response and all its components:

AlarmPoint Action Scripts:

Presentation Script

```
$content.choices = "Own"
$content.choices::add( "Ignore" )
```

Response Script

```
# Handle responses
$reply = $response.reply
$reply::toLowerCase()
$own= $reply::startsWith( "own" )
...
IF ( $own )
```

```
...
$message_note = "Owned by " & $target_name
...
$service_manager_status = "Work in progress"
# If we fail to update the incidents status requeue the message
$requeue_on_failed_update = true
GOSUB updateIncident
...
IF($request_successful)
  @event::delinkAllExcept( $target_id )
ENDIF
```

Note: *The latter is intended only as a brief overview of the required components. For more information about AlarmPoint responses and scripting, refer to the AlarmPoint Action Scripts and the* AlarmPoint Developer's Guide & Scripting Reference.

5.5 Annotations

This integration extensively annotates the originating Service Manager incident, but this may not be desirable in all environments. To add or remove the annotations to the Service Manager incidents, edit the AlarmPoint Action Scripts.

All annotations are prefaced by a comment indicating that the following call is an annotation:

```
# Annotate SM Event
...
$service_manager_message = $message_note
...
GOSUB updateIncident
```

To prevent the annotation of a Service Manager incident replace `$service_manager_message = $message_note` with `$service_manager_message = ""`. For additional anotations add the following section of code where `$message_note` is the message to be annotated:

```
# Annotate SM Event
$service_manager_status = ""
$service_manager_message = $message_note
GOSUB updateIncident
```

5.6 Adding Custom Trigger Rules

To add a custom trigger rule that will trigger a notification to be injected into AlarmPoint:

1. Click **Menu Navigation** > **Tailoring** > **Script Library**.
2. Type **AlarmPointEvent** in the **Name** field
3. Click **Search**
4. Modify the following methods to suit your requirements:
   - **getTriggerRule()** - This method is used to determine whether a notification should be injected into AlarmPoint.
   - **getFYIFlag()** - This method is used to inform AlarmPoint whether this notification could be FYI.
   - **getDeviceFilter()** - This method is used to return a device filter string that will limit the Devices to which that notification will be sent.

- **getRecipients() -** This method returns a list of recipients that this notification should target in the format 'recipient1, recipient2, …'

For example, the default behavior is to inject a notification into AlarmPoint only upon incident creation when the urgency is either critical or high. To modify this to always inject a notification on creation, change the following lines:

```
else{
  if(record.severity <= 2)
     triggerRule = "Assignment";
}
To:
else{
   triggerRule = "Assignment";
}
```

5.7 Altering the duration of Events

You can modify the amount of time AlarmPoint will send out notifications for a particular event before it times out by changing the `$main.timeout` variable in the initial PROCESS script. This variable stores the number of seconds the notifications will be allowed to continue before timing out.

The default value is 86400, which is the number of seconds in a 24-hour period. You can change the delay to a two-hour timeout by changing the line to:

```
$main.timeout = 7200
```

5.8 FYI notifications

You can make all notifications informational only (i.e., the user is not offered any response choices). Setting the `$force_fyi` flag to "on" makes all normal and Subscription notifications one-way (FYI).

In the initial PROCESS script, locate the following line:

```
$force_fyi = disable
```

Change the line to:

```
$force_fyi = on
```

5.8.1 Generating FYI notifications for specific incidents

The FYI parameter is an optional parameter injected from Service Manager into AlarmPoint. If it is set to “yes” in the Service Manager `triggerRule`, any notifications generated for the event will be informational-only, and have no response choices.

To use this feature, change the `triggerRule` to have the FYI Flag be `true`.

Within the script, you can choose to ignore the injected FYI variable to make an event informational-only by setting the `$force_fyi` variable to “off” in the configuration section of the initial PROCESS script. For more information, see “Configuration Variable Reference” on page 54.

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

5.8.2 Generating FYI notifications for Subscriptions

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

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

5.9 Optimizing the Mobile Gateway Integration

This section describes some of the ways you can optimize or extend the Mobile Gateway portion of the AlarmPoint for HP Service Manager integration.

5.9.1 Exposing a New Field

The following steps explain how to configure a new field that has been exposed in the Service Manager Incident Managment extaccess record to be displayed on the Mobile Gateway.

Note: *In the following steps, replace "Field Name" with the API caption name of the new field exposed in Service Manager.*

To expose a new field:

1. Expose the new field in the Service Manager extaccess record as descibed in “Exposing Additional Fields for Existing Web Services” on page 14.
2. In the `<APHOME>\webserver\webapps\mobilegateway\jsp\hpsmim\includes` folder, add the following line to the `initialize.jsp` and `initializeOldIncident.jsp` files:

```
newFields.put("Field Name", "");
```

3. To display the field on the New Incident screen, add the following to the `createFields.jsp` file; to display the field on the Update Incident screen, add the following to the `updateFields.jsp` file:

```
fields.put("Field Name", "Field Label");
fieldTypes.put("Field Name", "Field Type");
```

Field Name	The API caption name for the field exposed within Service Manager.
Field Label	The name that will appear within the Mobile Gateway representing the exposed Service Manager field.
Field Type	The type of field exposed (as defined in Table 5-1, below).

4. If the field is a required field, add the following:

```
requiredFields.add("Field Name");
```

Field Type	Description
Text	Displays the value of this field in an editable text input if there is a single value, or in a text area if there are multiple values.
ReadOnly	The value of this field will be displayed as plain text with no inputs
WriteOnly	The value of this field will not be displayed, but a text input will be displayed for a single value or a text area if there are multiple values, and both will allow input.

Field Type	Description
List	If a list is defined, a drop-down list will be displayed for this field; otherwise, a text input field will be displayed.

5.9.1.1 Defining List Field Values

To define the values for a list field you must add the following to the `<IAHOME>\integrationservices\hpsmim\hpsmim.js` file:

```
fields.put("Field Name", client.getSortedList("SoapAction", "Query", "Field"));
```

Where:

- **SoapAction** is the SOAP Action defined by the Service Manager web services; for example, “RetrieveCategoryListRequest”.
- **Query** is the query used to return a list of values.
- **Field** is the name of the API Caption defined in Service Manager.

5.9.1.2 Defining Static List Values

To define the values for a static list, you must add the following to the `<APHOME>\webserver\webapps\mobilegateway\jsp\hpsmim\includes\initialize.jsp` file:

```
incident.addList("Field Name", Arrays.asList(new String[]{ "Value 1",  "Value 2",
... }));
```

5.9.2 Add a Custom Query to the Home Page

To add a custom query and link to the home page, add the following to the `<APHOME>\webservices\webapps\mobilegateway\jsp\hpsmim\configuration.jsp` file installed on the Mobile Gateway:

```
MAIN_MENU_OPTIONS.put("Query Label", "Query");
```

For more information about constructing queries for Service Manager, consult the HP Service Manager documentation.

5.9.3 Creating a URL Alias

The `urlAlias.jsp` page in the Mobile Gateway is used to drive directly from an AlarmPoint notification to the Create Incident or Update Incident screens. It supports the following parameters:

Name	Description
newIncident	If this parameter is set, a new incident will be created and you will be taken to the Create Incident Mobile Gateway screen. If it is not set, you will be taken to the Update Incident Mobile Gateway screen for the specified incident.
IncidentID	The incident number of the incident to update. If the newIncident parameter is not set, this field must be set to a valid incident number.
Field Name	The name of an API Caption of a field for the incident. For each parameter set, it will update the field on the incident with that value

For more information about the urlAlias method in the AlarmPoint Action Script, refer to the AlarmPoint Online Developer's Guide.

5.10 Constructing BES and HTML email notifications

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

This feature requires the AlarmPoint Developer IDE. For installation instructions, refer to the *AlarmPoint Developer's Guide & Scripting Reference*.

To enable BES and HTML email, the HP Service Manager Incident Management (Business) script package set must be checked into the Developer IDE Database. If the script package has not been checked in already, see the instructions in "Importing the AlarmPoint script package" on page 18.

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

To enable BES and/or HTML email:

1. Launch the Developer IDE.
2. Check out the HP Service Manager Incident Management (Business) Production script package.
3. In the Global Configuration Variables section of the initial PROCESS script, do the following:
   - Set the `$main.enable_HTML_Email` variable to true.
   - Set `$main.use_logo` to true or false depending on whether you want your HTML email to show a logo.
   - Set `$AlarmPoint_URL` to the base URL of your AlarmPoint web server. (default is localhost).
4. Optionally, you can also do any of the following:
   - Change `$main.HTML_form_url` to point to a JSP page that you want to process any responses from the HTML email. (the default setting should work out-of-the-box).
   - Change `$main.logo` to a URL that holds the image you want to display at the top of HTML emails (by default, it points to the AlarmPoint logo).
   - Set `$main.logo_alt_text` to the text you wish to display when the logo cannot be fetched. This can be displayed if the email client is configured not to show images, or it could be displayed because the email client cannot access the AlarmPoint Webserver directly and thus cannot respond by using the links in the HTML.
   - If you are using BES and have access to a BES server, you can set the URL to the BES server in the `$main.bes_pushurl` variable.
5. Save and validate the script, and check in the script package.

Note: *For more information about these and other configuration variables, see "Configuration Variable Reference" on page 54.*

5.11 Service Manager Logging

All of the integration actions and errors are printed out to the messages panel and logged to the standard Service Manager log file specified in the `sm.ini` configuration file. These messages are defined in the AlarmPointUtil script library and are in the following format:

```
var RECIPIENT_UPDATE_FAIL = "Failed updating AlarmPoint %% %% - %%";
```

Messages are displayed using the following function:

```
logMessage(messageId, <args>)
```

where `messageId` matches the variable used to define the message and `<args>` is replaced by as many arguments as you want. These extra arguments are used in order to replace all occurrences of `%%` in the defined message.

For example, to log the message ‘Failed updating AlarmPoint Team TELECOMS-24x7 - UNKNOWN_GROUP’, you would use

```
logMessage("RECIPIENT_UPDATE_FAIL", "Team", "TELECOMS-24x7", "UNKNOWN_GROUP");
```

This would print in the Service Manager log file as:

3204(2656) 12/04/2007 11:15:26 JS I Failed updating AlarmPoint Team TELECOMS-24x7 - UNKNOWN_GROUP

5.12 Uninstalling

For instructions on removing an AlarmPoint deployment, refer to the *AlarmPoint Installation and Administration Guide*.

6. Configuration Variable Reference

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

6.1 Local Configuration Variables

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

6.1.1 FYI and Subscription Notification Variables

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

Note: *For more information on the behavior associated with informational-only notifications, see "FYI notifications" on page 49.*

Variable	Description
$force_fyi = "disable"	Forces notifications to be informational only rather than requiring responses. Possible values are: • **disable**: nothing is forced. • **on**: notifications are forced to be FYI. • **off**: notifications are forced not to be FYI.
# $use_email_for_fyi = true **# $use_phone_for_fyi = false** **# $use_im_for_fyi = true** **# $use_text_phone_for_fyi = true** **# $use_text_pager_for_fyi = true** **# $use_numeric_pager_for_fyi = true** **# $use_bes_for_fyi = true** **# $use_generic_for_fyi = true**	Configure Device filters for informational-only (FYI) notifications. Setting these flags to `false` prevents that Device type from being notified with informational (FYI) messages. **NOTE**: These variables are commented out in the integration script package. The preferred method for handling FYI notifications is to adjust User Device's to be used for only Medium and High priority alerts; see "Generating FYI notifications for specific incidents" on page 49

6.1.2 Fail-safe Configuration Variables

The following variables configure the fail-safe functionality, and specify when notifications will be sent to the fail-safe recipient. The value assigned to each variable is its default value within the script.

Note: *For instructions on how to set up a fail-safe recipient, see "Create a Fail-Safe Group" on page 26.*

Variable	Description
$fail_safe = "enabled"	Controls whether the fail-safe recipient is notified, and under which circumstances. Possible values are: • **enabled**: notify the fail-safe Group if no Subscriptions match and there are no notifiable recipients. • **for-subscriptions**: notify if the Subscription functionality is enabled and no Subscriptions match. • **for-recipients**: notify if there are no notifiable recipients. • **disabled**: disable the fail-safe functionality; no notifications will be sent to the fail-safe recipient.
$fail_safe_group = "HP SM FailSafe"	Identifies the fail-safe recipient, which is typically a Group, but may be a User.

6.1.3 Alert Configuration Variables

The following variables configure Alert behavior. The value assigned to each variable is its default value within the script.

Variable	Description
$override_timeframes = false	Overrides any Device Timeframes that have been configured for a User for this notification.
$use_emergency_devices = false	Forces the use of emergency Devices as part of the Device resolution processing.
$track_delivery = true	Configures the notification to run a response script when the delivery of a notification is successful. As this can limit Node performance, you can set this value to `false` if the custom behavior for successful delivery events is unnecessary, but you will lose any information about whether a delivery was successful.

6.2 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.

Variable	Description
$main.timeout = 86400	Amount of time (in seconds) the event is allowed to run before timing out. (86400 seconds = 24 hours.)
$main.debug = false	Indicates whether to log informational messages for debugging purposes. Disabling this variable may improve performance, but will provide less information.

Variable	Description
$main.use_logFile = false	Specify whether to use an alternate log file for debugging messages. This variable is ignored unless `$main.debug` is also set to true.
$main.logFile = "../logs/HP_SM_IM_Script.log"	Defines the file used to log debugging information (only if `$main.use_logfile` is set to `true`).
$main.maxInvalidResponses = 3	Specifies the maximum number of invalid responses allowed before the notification will no longer be requeued. If a recipient sends an invalid response and this number has not been exceeded, they will be renotified with the same content, prefixed with a message indicating that their response was invalid.
$main.annotate = true	Enables submission of information back to the Management System. Information is logged throughout the script progress; if this variable is set to `true`, these logged messages will be annotated to the originating event. Setting this variable to `false` may improve performance, but will make debugging difficult as some information may not be annotated to the originating event.
$main.subscription_annotate = false	Enables submission of Subscription information back to the Management System. (As with `$main.annotate`, but specifically for Subscription information.) Most Subscriptions are informational only; this variable can be enabled, for debugging and informational purposes but may reduce performance.
$main.enable_HTML_Email = true	Enables HTML Email functionality for email clients able to support HTML emails. If a client cannot support HTML than the plain text version will be passed.
$main.AlarmPoint_URL = "http://localhost:8888"	Identifies the AlarmPoint URL used for the HTML response form and AlarmPoint logo. If the specified URL cannot be reached, the logo will not appear, and the response links will not work.
$main.HTML_form_url = $AlarmPoint_URL & "/jsp/ProcessNotificationResponse.jsp"	Specifies the URL of the AlarmPoint Web Server's Process Notification Response JSP form, used by HTML email and BES to inject responses through the system.
$main.use_logo = true	Specifies whether HTML email notifications will display the AlarmPoint (or custom) logo.
$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).

Variable	Description
$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 AlarmPoint event has occurred.
$main.bes_pushurl = “http://localhost:8888/static”	Specifies the URL of the BES server. (Optional.)
$main.servicemanager_username_custom_field = "HP SM Login"** **$main.servicemanager_password_custom_field = "HP SM Password"	Specifies the names of the custom fields that store the user name and password for each user accessing HP Service Manager.

6.3 Mobile Gateway Configuration Variables

The `<APHOME>\webserver\webapps\mobilegateway\jsp\hpsmim\configuration.jsp` file installed on the Mobile Gateway contains the following configuration variables:

Variable	Type	Description	Default Value
MAIN_MENU_COUNTS	boolean	Enables the queries on the home page to be run	true
MAIN_MENU_OPTIONS	map	Defines what queries should be displayed on the homepage	High Priority Incidents Open Incidents Assigned To Me Hot Incidents Unassigned Incidents
PAGINATE_RESULTS	boolean	Enables pagination the incidents lists	true
RESULTS_PER_PAGE	int	Defines how many results should be displayed on each page of the incidents lists	10
SM_USER_NAME_FIELD	string	Defines the name of the custom field in AlarmPoint containing the Service Manager login user name	“HP SM Login”
SM_PASSWORD_FIELD	string	Defines the name of the custom field in AlarmPoint containing the Service Manager login user password	“HP SM Password”
VERIFY_SM_CREDS	boolean	Enables the validation of entered Service Manager login credentials when loading the Mobile Gateway homepageVar	true
SM_LISTS_EXPIRED	long	Defines how long to cache list values retrieved from Service Manager through Web Service Calls	3600000

6.4 Integration Agent Configuration Variables

The `<IAHOME>\integrationservices\hpsmim\hpsmim.js` file installed on the Integration Agent contains the following configuration variables:

Variable	Description
smUrl = “http://localhost:13080/sc62server/ws”	Defines the URL of the Service Manager web services
calloutAnnotateUser = "falcon"; **calloutAnnotatePass = "";**	These variables must be updated to specify a valid user name and password combination that has permissions to add journal entries to incident tickets. The values are only used for Callout Annotations from the CALLOUT APS script.

7. Contact Us

You can access the xMatters web site at http://www.xmatters.com. From this site you can obtain information about the Company, the Products, Support and other helpful information. You may also access the Customer Support Site from the main web page. In this protected site you will find current product releases, helpful hints, patches, release notes, a helpful product knowledge base, trouble ticket submission areas and other helpful tools provided by xMatters, inc.

xMatters, inc.

4457 Willow Road, Suite 220
Pleasanton, CA 94588

Phone: 925-226-0300

Fax: 925-226-0310

Email: support@xmatters.com

Website: http://www.xmatters.com

Hewlett-Packard Company

3000 Hanover Street
Palo Alto, CA 94304-1185 USA

Phone: 650-857-1501

Fax: 650-857-5518

Support: http://support.openview.hp.com

Website: http://www.openview.hp.com

8. Copyright

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 integration predates the change; for the sake of clarity, the old names of products have been maintained throughout the documentation.