

AlarmPoint Express for HP NNMi

Integration Guide



Licensing AlarmPoint Express

After installing AlarmPoint, you must apply the AlarmPoint Express license file, which will enable all of the AlarmPoint Express features, and remove the 30 day trial time limitation.

To receive your AlarmPoint Express license file, visit:
<http://express.alarmpoint.com/hp>

Save the license file to your hard drive, and then use the following instructions to install it.

To install the license file:

1. Log in to AlarmPoint:
 - a. Login ID: **root**
 - b. Password: **tree**
2. Click the Admin tab.
3. In the Administration menu, under Permissions, click Active Licenses.
4. On the Active Licenses page, click the From File link.
5. On the Add License page, click Browse.
6. In the File Upload dialog box, select the AlarmPoint Express license file, and then click Upload.

AlarmPoint then displays the updated Active License.

AlarmPoint Java Client

As part of the installation, you will install the AlarmPoint Java Client on the NNM system for communications to the AlarmPoint server. The Java Client installation requires a keycode during the install, please use the following:

APJCCCS3BYLZCX8ZA72

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

January 24, 2008

Copyright © 1994-2008. All rights reserved.

AlarmPoint Systems™, AlarmPoint®, AlarmPoint® Java Client, AlarmPoint® Mobile Gateway, AlarmPoint® Integration Agent, AlarmPoint® Express, AlarmPoint® Standard, AlarmPoint® Professional, AlarmPoint® Enterprise, and AlarmPoint® Notification Server are trademarks of AlarmPoint Systems, Inc.

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

Contacting AlarmPoint Systems, Inc.

You can visit the AlarmPoint Systems Web site at: <http://www.alarmpoint.com>

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

AlarmPoint Systems, Inc.
Corporate Headquarters
4457 Willow Road, Suite 220
Pleasanton, CA 94588

Sales and Technical Support:

Telephone: 925-226-0300

Facsimile: 925-226-0310

support@alarmpoint.com

sales@alarmpoint.com

<https://support.alarmpoint.com>

Contents

CHAPTER 1: INTRODUCTION	3
INTRODUCTION TO ALARMPPOINT EXPRESS	3
How the AlarmPoint System Works.....	3
ABOUT THIS DOCUMENT	6
Important AlarmPoint Terms.....	6
CHAPTER 2: INSTALLING AND CONFIGURING	8
Assumptions.....	8
System Requirements	8
INSTALLATION OVERVIEW	8
INSTALLING THE ALARMPPOINT JAVA CLIENT	9
INSTALLING ALARMPPOINT	10
STARTING ALARMPPOINT	12
Licensing AlarmPoint Express	14
CONFIGURING ALARMPPOINT	15
Configuring the Web Services Connection	15
Further Configuration Options.....	17
CONFIGURING HP NNMI	23
Create a Web Services Client	23
Configuring NNMI Incident Types for Automatic AlarmPoint Notifications	24
TRIGGERING A NOTIFICATION	28
Increase the Polling Frequency	28
Disconnect a Computer from the LAN.....	28
Responding to a Notification	29
Viewing Notification Results.....	31
CHAPTER 3: MANAGING USERS AND DEVICES	32
ADDING USERS	32
ADDING DEVICES	33
Validating Devices.....	34
CHAPTER 4: MANAGING GROUPS	36
IMPORTANT TERMS FOR GROUPS	36
CREATING GROUPS	37
MANAGING ESCALATIONS	38
Other escalation options.....	39
CHAPTER 5: MESSAGING.....	41
SENDING A MESSAGE	41

CHAPTER 6: MANAGING SYSTEM DATA	43
GENERATING REPORTS	43
Accessing Reports.....	43
IMPORTING DATA	45
Importing spreadsheets	45
CHAPTER 7: SUBSCRIBING TO ALERTS	47
Important Terms	47
CONFIGURING SUBSCRIPTIONS	47
Adding a Custom Subscription Panel	48
Configuring a Subscription	48
ASSIGNING SUBSCRIPTIONS	51
CHAPTER 8: SCRIPTING IN ALARMPPOINT.....	54
INTRODUCTION TO SCRIPTING	54
Important Terms	54
Concepts.....	55
Event Processing Overview	56
EDITING ACTION SCRIPTS	57
Installing the AlarmPoint Developer IDE	57
Using the AlarmPoint Developer IDE	58
Scripting example	59
CONFIGURATION VARIABLE REFERENCE	60
Local Configuration Variables.....	60
Global Configuration Variables.....	62
CHAPTER 9: OPTIMIZING THE INTEGRATION.....	65
CONFIGURING THE SUBSCRIPTION JSP	65
ADDING DATA ELEMENTS	66
RESPONSE CHOICES	67
Changing response choices	67
ALTERING THE DURATION OF EVENTS	69
FYI NOTIFICATIONS	69
Generating FYI notifications for specific incidents.....	69
Generating FYI notifications for Subscriptions.....	70
CONSTRUCTING HTML EMAIL NOTIFICATIONS	70
CHAPTER 10: CONTACTING ALARMPPOINT	72
CUSTOMER SUPPORT FOR ALARMPPOINT EXPRESS USERS	72

Chapter 1: Introduction

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.

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 Network Node Manager i-series). When NNMi detects an event 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 event. Once contacted, the AlarmPoint System gives the notified person instant two-way communication with NNMi. Responses are executed immediately on NNMi, enabling remote resolution of the event.

Introduction to AlarmPoint Express

AlarmPoint Express is designed for small groups that do not require voice or distributed load capability (AlarmPoint Express installs on a single computer). However, AlarmPoint Express is a great way to get started with the AlarmPoint product family and includes many sophisticated notification options and a web user interface for the system administrator.

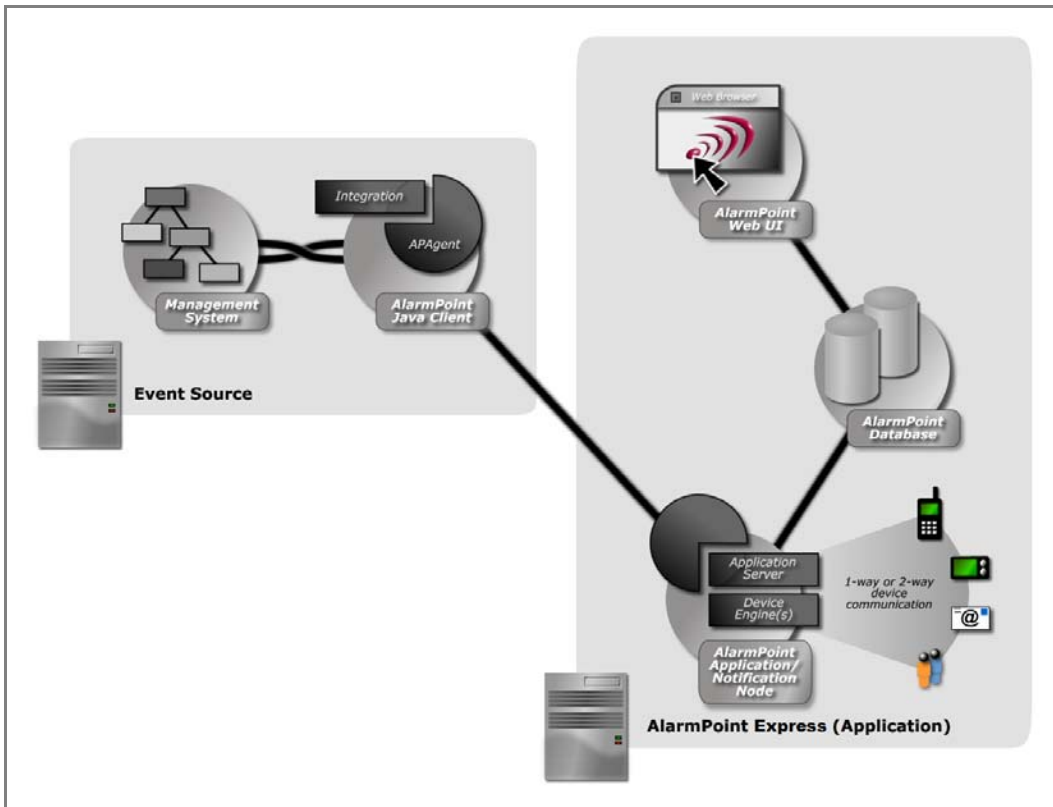
AlarmPoint Express has no voice communication capability, but is well-suited for a production environment in which few Users and Groups are required.

This version of AlarmPoint Express has been specially configured to work with HP Network Node Manager i-series 8.01.

How the AlarmPoint System Works

The AlarmPoint System can be thought of as an employee trained to notify people when problems arise. NNMi can inform the AlarmPoint System about situations in an organization that will trigger notifications to people based on predefined steps.

The following diagram shows an example AlarmPoint Express deployment:



The example deployment shows the interrelationship between the key AlarmPoint components, with the AlarmPoint Java Client acting as a bridge between AlarmPoint and the external Management System.

In this all-in-one deployment, the AlarmPoint Application/Notification Server Node routes and sends notifications through the configured Device Engines. Virtually all system configuration is done through the AlarmPoint Web User Interface, and the AlarmPoint Database acts as a central repository of all configuration, notification, component availability, and audit information. The database can be an internal Microsoft SQL Server or Oracle database on the AlarmPoint System, or it can be located on another system.

The following table summarizes the key components of an AlarmPoint deployment:

Component	Notes
AlarmPoint Application Server (Node)	The AlarmPoint Application Server (Node) is the central AlarmPoint component, running the business processes that instruct other components in the system.
Notification Server (Node)	An AlarmPoint deployment can have one or many Notification Servers that communicate with the Application Server and AlarmPoint Database to queue, route, and send notifications and their responses. Note that AlarmPoint Express does not have a separate Notification Server Node.
Device Engines	A sub-component of Notification Servers, Device Engines send notifications to various Devices (phones, pagers, email, etc.). A Notification Server may have several Device Engines; for example, a Notification Server can have an Email and a Paging Engine. Note that due to thread availability, it is strongly recommended that a Notification Server does not have more than one Device Engine of the same type.
AlarmPoint Database	The AlarmPoint Database is the central storehouse of User, Device, Group, logging and auditing information for the AlarmPoint System.
AlarmPoint Java Client	The AlarmPoint Java Client acts as a two-way bridge, translator, filter, and message enhancer between NNMi and AlarmPoint. The Java Client formats messages into AlarmPoint XML messages before being transmitted to AlarmPoint.

AlarmPoint dynamically selects and runs the script – called an Action Script – appropriate for an incoming event. Scripts can contact one person, a group, or even a specific communication device. Some scripts establish contact with people or services, while others provide a choice of actions specific to the situation. AlarmPoint constantly updates the Management System on what is happening, including replies from real-time two-way telephones, messaging devices, two-way pagers, or email.

An application called the AlarmPoint Java Client allows NNMi to communicate with AlarmPoint. The Java Client is like a bridge, translator, and message enhancer between NNMi and AlarmPoint. If NNMi wants to start or stop a situation, it uses the AlarmPoint Java Client to send a message. To respond, AlarmPoint returns a message to the Java Client, which can log the information, run a command on NNMi, and so on.

The AlarmPoint Java Client running on NNMi sends messages to AlarmPoint on behalf of NNMi. AlarmPoint splits the notification process into several basic components, which allows the administrator to reuse several scripts, making Action Scripting more like piecing modules together than programming.

Note: *For more details and information about Action Scripting, see the AlarmPoint Developer's Guide & Scripting Reference.*

AlarmPoint's main processing component is called an Application Server. The Application Server communicates with one or many AlarmPoint Notification Servers to manage sending and receiving of notifications. Notification Servers contain Device Engines (e.g., Email Engine, Phone Engine). In AlarmPoint Express, the Application Server and Notification Server are combined into an all-in-one deployment.

About this document

The *AlarmPoint Express for HP NNMi Integration Guide* is intended to help AlarmPoint Express users install, configure, and maintain an AlarmPoint Express installation on an HP NNMi deployment.

This guide is not intended to be a complete guide to all of AlarmPoint's features and capabilities, but rather to provide an introduction to and basic usage instructions for AlarmPoint Express for HP NNMi.

The primary documentation resource for AlarmPoint includes the following:

- *AlarmPoint Installation and Administration Guide*: this guide is intended to help AlarmPoint Administrators install, configure, and maintain an AlarmPoint installation. The *Administration Guide* also introduces key concepts, including the role of AlarmPoint within an organization, and provides an overview of the main modules and processes.
- *AlarmPoint User Guide*: intended for end users, this guide explains the basics of the AlarmPoint Web User Interface, and how to accomplish common tasks. The *User Guide* also includes a section for supervisors about more advanced tasks, such as Group creation and management.
- *AlarmPoint Developer's Guide & Scripting Reference*: this guide is intended for developers and administrators, and contains instructions on using the scripting tools and integration components of AlarmPoint.
- *AlarmPoint Java Client Guide*: this guide explains how to configure and use the custom features of the AlarmPoint Java Client.

AlarmPoint Administrators may also refer to some of the advanced features described in the *AlarmPoint User Guide*.

Important AlarmPoint Terms

This manual uses the following terms to refer to specific components within AlarmPoint. These terms are capitalized to help identify them as AlarmPoint terminology, and are used throughout the AlarmPoint documentation.

Event

An Event is any kind of message generated by an external source (in this case, HP NNMi) that enters AlarmPoint and describes a situation that requires a notification. Each Event requires at least one Alert.

Alert

An Alert is any message or notification sent by the system to a Device, in order to inform a User of an Event that requires attention. The Alert contains information about the Event, such as the time and location, and may ask Users to respond, acknowledging that they have received the notification.

Users

In AlarmPoint, people who can receive notifications are called “Users”. Every person in the AlarmPoint system is a User defined by a set of details, including ID number, user name, login password, and so on. In AlarmPoint Express, you are limited to a maximum of ten Users.

Devices

A Device in AlarmPoint is any means of receiving a notification message. Devices can include physical items like a telephone or a BlackBerry, or intangible items such as email accounts. In AlarmPoint Express, each User can have a maximum of three Devices.

Groups

In AlarmPoint, Groups are used for collecting Users and Devices and organizing them into notification schedules. For a complete definition of Groups, including the terms used to define Group components, see “Creating Groups” on page 37. In AlarmPoint Express, you are limited to a maximum of five Groups.

Chapter 2: Installing and Configuring

The following sections describe how to install, start, and configure an example AlarmPoint Express deployment.

Assumptions

To simplify the installation and configuration process described in this document, the instructions assume the following conditions:

- AlarmPoint Express and the AlarmPoint Java Client will be installed on the same computer as HP NNMi 8.01.
- The HP NNMi deployment is already installed and fully operational.

In addition, some instructions in this section are geared towards a Windows installation. For Unix or Solaris installations, some of the paths and instructions represented must be modified for the appropriate operating system.

If you require that AlarmPoint Express be installed on a separate machine from the HP NNMi application, see “Optimizing the Integration” on page 65 for information about the required changes.

System Requirements

The following table outlines the general hardware requirements for an AlarmPoint Express deployment (the processors are assumed to be Pentium 4 or equivalent):

Requirement	Minimum	Recommended
CPU	1 x CPU 2.8 GHz	2 x CPU 3.6 GHz
Memory	4 GB	4 GB (8GB for high-volume systems)
Disk Space	15 GB	30 - 60 GB

Installation Overview

Installing AlarmPoint Express requires the following components:

AlarmPoint Database

The AlarmPoint installer requires that you enter parameters related to the database installation. For this reason, install the database you plan to use with AlarmPoint before installing the AlarmPoint application. (If you are using the included Microsoft SQL Server database, it is installed during the installation of the AlarmPoint application.)

Note: *This document includes instructions on how to configure AlarmPoint for the included Microsoft SQL Server 2005 Express database. For instructions on how to configure AlarmPoint for other databases, including Oracle installations, refer to the AlarmPoint Installation and Administration Guide.*

AlarmPoint Java Client

The AlarmPoint Java Client has its own installer, and the procedure for installing the AlarmPoint Java Client is outlined in the following section.

AlarmPoint Express application

The AlarmPoint Express application install includes the AlarmPoint database components, Web Server, and Application Server Node. The AlarmPoint Express licensing requires that it be installed on a single computer; other versions of AlarmPoint may be distributed across multiple computers and different physical locations.

This version of AlarmPoint Express includes the integration components for HP NNMi.

Installing the AlarmPoint Java Client

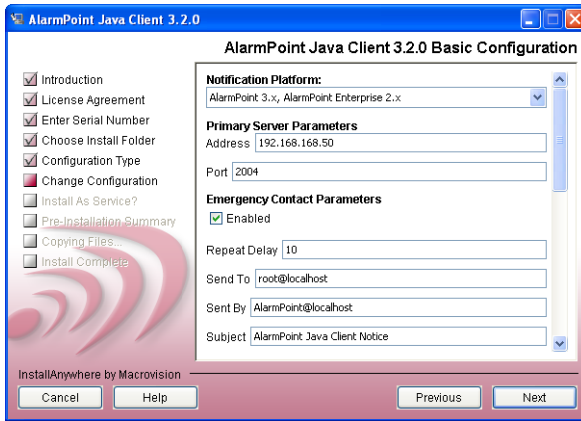
The AlarmPoint Java Client (APJC) is a remote agent used to forward Events from HP NNMi to the application server. It is contained in a separate installation file and requires a separate license key. All AlarmPoint Express for HP NNMi deployments may use the following license key for their APJC installation:

APJCCCS3BYLZCX8ZA72

To install the AlarmPoint Java Client, run the appropriate executable file for your operating system. The following table lists each file and its location on the HP NNMi CD:

O/S	File Location
Windows	\\JavaClient\windows\apjc_321.exe
Solaris	\\JavaClient\solaris\apjc_321.bin
Linux	\\JavaClient\linux\apjc_321.bin
HP Itanium	\\JavaClient\hpux\apjc_321.bin

The following section identifies items of specific interest for the APJC installation, or settings that should be changed from the default.



- In the Primary Server Parameters area, the installer automatically inserts the current IP address in the **Address** field. It is recommended that you accept this value as some operating systems may not resolve “localhost” properly.
- The Emergency Contact Parameters allow you to specify an email account and SMTP server to use if the Java Client detects issues with contacting the application server. These are optional.

Windows installations:

- When prompted whether you want to install the Java Client as a Windows service, select **Yes**.

When the installation is complete, the Java Client should automatically begin running as a service, visible in the Windows Services panel.

Note: *For complete APJC installation instructions and more information about APJC features and capabilities, see the AlarmPoint Java Client Guide.*

Installing AlarmPoint

To install AlarmPoint, run the appropriate executable file for your operating system. The following table lists each file and its location on the HP NNMi CD:

O/S	File Location
Windows	\AlarmPoint\windows\ap321_install.exe
Solaris	\AlarmPoint\solaris\ap321_install.bin
Linux	\AlarmPoint\linux64\ap321_install.bin
HP Itanium	\AlarmPoint\HPItanium\ap321_install.bin

The initial installation of AlarmPoint provides several options, such as the installation folder, component features, etc. This section describes the recommended choices for various stages of the installation process.

Follow the on-screen instructions to install AlarmPoint, using the settings explained below.

Installation folder

Unless your company requirements do not allow the installation of any application software under the default folders (C:\Program Files\AlarmPoint Systems or /opt/alarmpoint), accept the default settings. Otherwise, specify the folder in which you want to install AlarmPoint, and note its location.

Database Installation Query

If you are installing AlarmPoint Express for HP NNMi for evaluation purposes, it is recommended that you install and use the Microsoft SQL Server 2005 Express database.

1. On the installer's AlarmPoint 3 Database Installation Query page, select the **Install Microsoft SQL Server 2005 Express** option, and supply an "sa" (Super Administrator) password. (Note that the password must satisfy Microsoft SQL Server's "strong password" guidelines or the installation will fail. It is recommended that you specify a password consisting of a combination of eight letters and digits.)
2. Click **Next**.
3. Once the SQL Server 2005 installer has completed, select **Allow installer to automatically create**, and then click **Next** to create the database.
 - Make a note of the passwords as they are required when installing other AlarmPoint components.

Note: *If you want to use an existing database, refer to the AlarmPoint Installation and Administration Guide for instructions.*

Merging Accounts

When asked whether to merge the AlarmPoint Administrator accounts, select **Yes**. This merges the separate Company Administrator and Super Administrator accounts into a single account using `root` as the Login ID, and `tree` as the password.

AlarmPoint Components

On the Select Components page of the installer, select the following options:

- **Install AlarmPoint Web Server**
- **Install AlarmPoint Node**
 - **Create New Node**

You do not need to configure the settings on the Health Monitor tab at this point. If required, you can configure the Health Monitor (an AlarmPoint utility for monitoring the community of Nodes) using the Global Configuration page of the AlarmPoint Web User Interface.

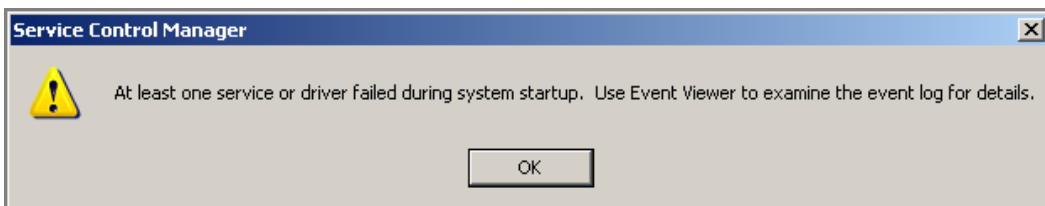
Virtual Devices

The main AlarmPoint installer includes Virtual Devices (Email, Pager, Text Phone) that can be used for training, testing, and troubleshooting without having to configure phone lines, email servers, pagers, modems, etc. The Virtual Devices are automatically configured during the installation process.

Starting AlarmPoint

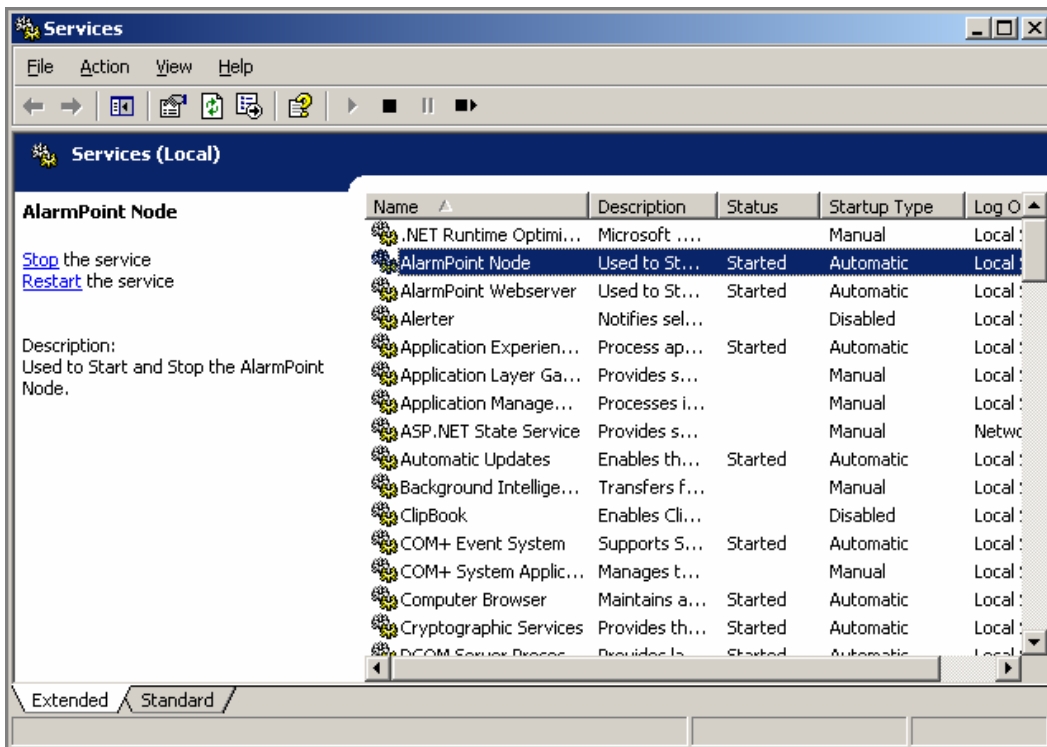
When the installation is complete, restart the computer.

On less-powerful machines, the startup of the AlarmPoint services can exceed Windows thresholds. If this occurs, Windows displays the following error message:



Note that a failure may not necessarily have occurred; the AlarmPoint services may have started more slowly than Windows tolerance.

If AlarmPoint starts up successfully, the Virtual Phone appears and the AlarmPoint Node service will be marked as Started, as shown in the following figure:



To verify that the web server components are correctly installed, open a web browser and navigate to <http://localhost:8888/alarmpoint> (or double-click the AlarmPoint icon on your desktop).

- AlarmPoint displays the login page:



Licensing AlarmPoint Express

The default installation of AlarmPoint Express is a 30-day trial version. To remove the 30-day trial time limitation, you can register at <http://express.alarmpoint.com/hp> and download an AlarmPoint Express license file. Copy the license file to your hard drive, and then use the following instructions to install it.

To install the license file:

1. Log in to AlarmPoint:
 - **Login ID:** root
 - **Password:** tree
2. Click the **Admin** tab.
3. In the Administration menu, under Permissions, click **Active Licenses**.
4. On the Active Licenses page, click the **From File** link.
5. On the Add License page, click **Browse**.
6. In the File Upload dialog box, select the AlarmPoint Express license file, and then click **Upload**.
 - AlarmPoint displays the updated Active Licenses page:

AlarmPoint EXPRESS

About AlarmPoint | Sign Out

Reports Messaging Admin

Administration

Super Admin

Admin > Active Licenses > Active Licenses

Active Licenses

Add New From File

Name	Value	Expiry Date
Has Alerts	1	Never
Has Apic Standard	1	Never
Has Gen Messaging	1	Never
Has Language English	1	Never
Has Lookup Assignments	1	Never
Has Reports Activity	1	Never
Has Reports Administration	1	Never
Has Role Company Admin	1	Never
Has Role No Access	1	Never
Has Role System Admin	1	Never
Has Role Web Service User	1	Never
Has Subscriptions	1	Never
Has Web Services Standard	1	Never
Number Of Application Server Nodes	1	Never
Number Of Devices Per User	3	Never
Number Of Event Domains	1	Never
Number Of Groups	5	Never
Number Of Java Client Connections	1	Never
Number Of Orgs	1	Never
Number Of Seconds Per Event	4	Never
Number Of Subscription Panels	1	Never
Number Of Text Engines	15	Never
Number Of Threads Per Text Engine	1	Never
Number Of Total Text Engine Threads	15	Never
Number Of Users	10	Never

Logged in as Super Administrator
AlarmPoint Systems, Inc. All Rights Reserved.

Configuring AlarmPoint

AlarmPoint Express for HP NNMi has been specifically configured to integrate with HP Network Node Manager i-series version 8.01.

Among the changes made to this version are the following configuration items:

- The AP-HP-NNMi.aps script package is automatically imported into the AlarmPoint Action Scripts.
- Scripts are automatically modified to allow Web Services to annotate tickets within HP NNMi.
- The hp_nnm Event Domain is included in the AlarmPoint settings.
- The AlarmPoint Node is pre-configured to initialize the Web Services library.
- The APJC configuration file includes the HP NNMi client ID.

Configuring the Web Services Connection

AlarmPoint Express for HP NNMi uses the following default settings to connect to NNMi via Web Services:

NNMi Web Services NodeBean (initial PROCESS script):

```
http://localhost:8004/IncidentBeanService/IncidentBean
```

NNMi Web Services NodeBean (Subscription Panel):

```
http://localhost:8004/NodeBeanService/NodeBean
```

Web Services User:

```
webservices
```

Web Services Password:

```
nnm
```

If your NNMi deployment is running on a port other than 8004 (or if you require a different URL or User/Password combination), you must change the settings in the custom Subscription panel and in the initial PROCESS script.

Identifying your NNMi port

You can determine whether the default port setting of 8004 is correct for your NNMi installation by checking the port information contained in the NNMi port configuration file, located in the following folder:

```
${NNM_DATA_DIR}\shared\nnm\conf\nnm.ports.properties"
```

Note: *The default NNM_DATA_DIR folder (for Windows installations) is C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software.*

Changing the Web Services Port

If your installation is running on a port other than 8004, use the following steps to change the port number.

To change the Web Services port in the custom Subscription panel:

1. Open the following file:

```
$(AlarmPoint)\webservers\webapps\cocoon\alarmpoint\jsp\subscription\nnmi\NNMiSubscriptionForm.jsp
```

2. Within the Subscription JSP, locate the following section:

```
final String NNM_NODE_SERVICE_WS_URL = "http://localhost:8004/NodeBeanService/NodeBean";
```

3. Edit the port number specified to match the port on which NNMi is running.
4. Save and close the JSP file.

Note: *For more information about the settings in the custom Subscription panel, see “Configuring the Subscription JSP” on page 65.*

To change the Web Services port in the initial PROCESS script:

1. Launch the AlarmPoint Developer IDE.
 - For installation and database configuration instructions, see “Editing Action Scripts” on page 57.
2. Check out the **HP Network Node Manager i-series (Business)** script package.
3. In the initial PROCESS script, locate the following line (to locate the variable quickly, press **Ctrl-F** and search for 8004):

```
$main.nnmi_incident_url = "http://localhost:8004/IncidentBeanService/IncidentBean"
```

4. Edit the port setting to the correct value and save your changes.
5. Check in the script package and close the Developer IDE.

Note: *For more information about the settings in the initial PROCESS script, see “Global Configuration Variables” on page 62.*

Further Configuration Options

You can further configure your installation by using the AlarmPoint Web User Interface to set up Device Engines, Protocol Providers, and User Service Providers. The following sections provide an example of the configuration process by explaining how to create an SMTP protocol to send email notifications to a real-life recipient.

This section is optional; if you would prefer to use only the AlarmPoint Virtual Devices, continue to “Managing Users and Devices” on page 32.

Configuring a Protocol Provider

The first step in configuring SMTP is to set the Protocol Provider details. Protocol Providers define how AlarmPoint accesses servers for outgoing notifications.

To configure the SMTP Protocol Provider:

1. Log in to AlarmPoint as an Administrator and click the **Admin** tab.
2. In the Administration menu, click **Protocol Providers**.
 - AlarmPoint displays the list of available Protocol Providers:

The screenshot shows the AlarmPoint Express Administration interface. The left sidebar contains a navigation menu with categories like Administration, Configuration, and Providers. The main content area displays the 'Protocol Providers' page, which includes a table of existing providers and an 'Add New' link.

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Airtouch Email	Airtouch Email Service Provider
<input type="checkbox"/>	Airtouch SNPP	Airtouch SNPP Service Provider
<input type="checkbox"/>	Airtouch TAP	Airtouch TAP Service Provider
<input type="checkbox"/>	Alltel Email	Alltel Email Service Provider
<input type="checkbox"/>	Alltel SNPP	Alltel SNPP Service Provider
<input type="checkbox"/>	Alltel TAP	Alltel TAP Service Provider
<input type="checkbox"/>	American Messaging EMAIL	American Messaging Email Service Provider
<input type="checkbox"/>	American Messaging WCTP	American Messaging WCTP Service Provider
<input type="checkbox"/>	Arch/USA Mobility EMAIL	Arch/USA Mobility Email Service Provider
<input type="checkbox"/>	Arch/USA Mobility TAP	Arch/USA Mobility TAP Service Provider
<input type="checkbox"/>	Arch/USA Mobility WCTP	Arch/USA Mobility WCTP Service Provider
<input type="checkbox"/>	Bell Mobility Canada Email	Bell Mobility Canada Email Service Provider
<input type="checkbox"/>	Bell Mobility Canada TAP	Bell Mobility Canada TAP Service Provider
<input type="checkbox"/>	Bell South Email	Bell South Email Service Provider
<input type="checkbox"/>	Bell South TAP	Bell South TAP Service Provider
<input type="checkbox"/>	Blackberry TAP	Blackberry TAP Service Provider
<input type="checkbox"/>	Cingular Email	Cingular Email Service Provider
<input type="checkbox"/>	Cingular TAP	Cingular TAP Service Provider
<input type="checkbox"/>	Fido Email	Fido Email Service Provider

3. Click the **Add New** link.
4. In the **Provider Type** drop-down list, select **SMTP**, and then click **Continue**.

5. On the SMTP Provider Details page, specify the following settings:

- **Name:** Type a name for the new Protocol Provider.
- **Email Sender:** Type the email address from which the notifications will be sent. It is strongly recommended that you do not use your personal or company email address, as there is a chance that the contents of the account's Inbox will be deleted.
- **Server Address:** Type the URL or IP address of the email server.

AlarmPoint EXPRESS

About AlarmPoint | Sign Out

Reports Messaging Admin

Administration

Super Admin Admin > Protocol Providers > Add New Protocol Provider > Provider Details

SMTP Provider Details

Details

Name: Internal Company Email *

Description:

Maximum retries: 3 *

Retry Interval: 10 *

Maximum session size: 20 *

Split long message:

Split size: 160 blank = unlimited

Maximum message length: blank = unlimited

Maximum PIN length: 100 blank = unlimited

Authenticate:

Account:

Password:

Email Sender: network@admins.com *

Reply To:

Server Address: 198.198.198.2 *

Server Port: 25 *

Domain Name:

Use SSL:

Save

6. Accept the default settings for the remainder of the protocol provider details, unless your server or email settings require specific ports or other changes.

Note: For more information about the individual settings, refer to the AlarmPoint Installation and Administration Guide.

7. Click **Save** to create the new Protocol Provider.

Configuring a User Service Provider

Once you have created a Protocol Provider, you can add a User Service Provider, which determines how AlarmPoint communicates with Users' Devices.

1. On the Admin tab, in the Administration menu, click **User Service Providers**.

- AlarmPoint displays the list of available User Service Providers:

AlarmPoint EXPRESS

About AlarmPoint | Sign Out

Reports Messaging Admin

Administration

Super Admin

Admin > User Service Providers

Super Admin Details

Company

User Service Providers

User Service Providers for "Default Company" [Add New](#)

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Airtouch	Airtouch Service Provider
<input type="checkbox"/>	Alltel	Alltel Service Provider
<input type="checkbox"/>	American Messaging	American Messaging Service Provider
<input type="checkbox"/>	Arch/USA Mobility	Arch/USA Mobility Service Provider
<input type="checkbox"/>	Bell Mobility Canada	Bell Mobility Canada Service Provider
<input type="checkbox"/>	Bell South	Bell South Service Provider
<input type="checkbox"/>	BES	BES Service Provider
<input type="checkbox"/>	Blackberry	Blackberry Service Provider
<input type="checkbox"/>	Cingular	Cingular Service Provider
<input type="checkbox"/>	Fido	Fido Service Provider
<input type="checkbox"/>	GSM modem 1-way	GSM Service Provider
<input type="checkbox"/>	GSM modem 2-way	GSM Service Provider
<input type="checkbox"/>	Jabber COM	Jabber COM Service Provider
<input type="checkbox"/>	Jabber ORG	Jabber ORG Service Provider
<input type="checkbox"/>	MAPI Email	Service Provider for MAPI e-mail
<input type="checkbox"/>	mBlox Pager	mBlox Service Provider
<input type="checkbox"/>	Metro PCS	Metro PCS Email Service Provider
<input type="checkbox"/>	Metrocall/USA Mobility	Metrocall/USA Mobility Service Provider
<input type="checkbox"/>	MobileCom	MobileCom Service Provider

Location

Sites

Countries

Time Zones

Calendars

Custom Holidays

Company Holidays

Permissions

Active Licenses

Configuration

Global Configuration

Nodes and Device Engines

Device Types

LDAP Servers

Password Policy

Schedule Jobs

Clear Runtime / History

Providers

User Service Providers

Protocol Providers

2. Click the **Add New** link.
3. On the User Service Provider Details page, specify the following settings:
 - **Name:** Type a name for the new User Service Provider.
 - **Description:** Type a short description of the User Service Provider, such as “Express Email”.
 - **Device Types:** Select **Email Device**.
4. Click **Continue**.
5. In the Protocol Providers area, click the **Add New** link.
6. On the Select Your Protocol Providers page, click the Protocol Provider you created in the previous section, and then click **Add**.
7. Click **Save** to add the Protocol Provider and return to the User Service Provider Details page:

The screenshot shows the AlarmPoint Express Admin interface. The left sidebar contains a navigation menu with categories like Administration, Super Admin, Company, Location, Calendars, Permissions, Configuration, and Providers. The main content area is titled 'User Service Provider Details' and shows configuration fields for Name (Internal), Description (Express Email), Device Types (Email Device), and PIN mask. Below these fields is a table for 'Protocol Providers for: Internal' with columns for Order, Name, Description, Category, and Enabled. The table contains one entry: 'Internal Company Email' with Category 'SMTP' and Enabled checked. A 'Common Tasks' box on the right contains a 'Return to User Service Providers' link. The bottom right corner shows the user is logged in as 'Super Administrator'.

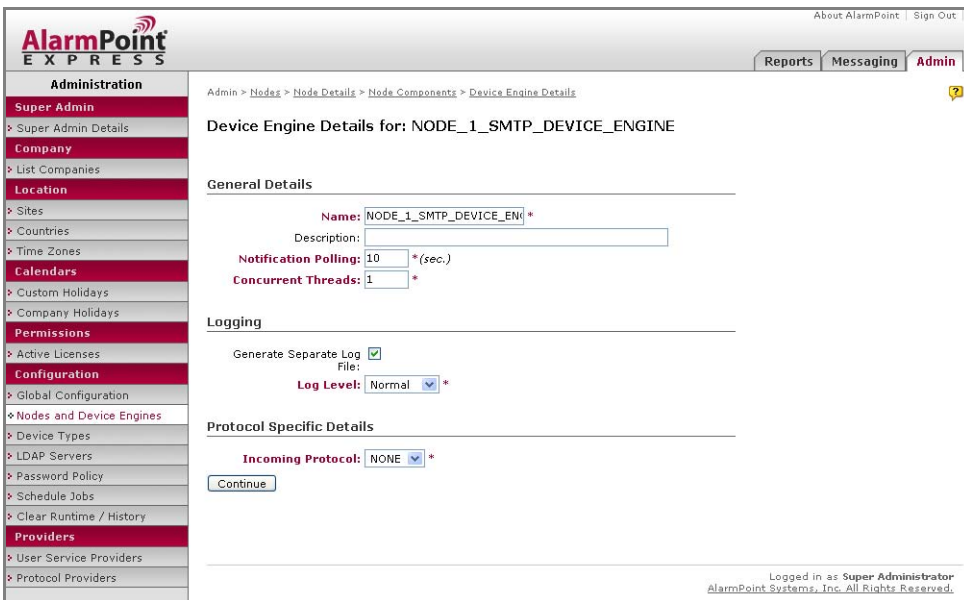
Configuring Nodes and Device Engines

The last step required when configuring the SMTP protocol is to create a Device Engine.

1. On the Admin tab, in the Administration menu, click **Nodes and Device Engines**.
2. On the Nodes page, in the All Nodes table, click the **Device Engines** link.
 - AlarmPoint displays the Node Components page:

The screenshot shows the 'Node Components' page in AlarmPoint Express. The left sidebar is the same as in the previous screenshot. The main content area is titled 'All Components for Node NODE_1' and features a table with columns: Name, Description, Type, Status, and Activity State. The table lists three device engines: 'SNPP Device Engine', 'Virtual Device Engine', and 'WCTP Device Engine', all with a status of 'Running'. Below the table are buttons for 'Start Selected', 'Stop Selected', and 'Remove Selected'. A 'Common Tasks' box on the right contains a 'Configure Node Resources' link. The bottom right corner shows the user is logged in as 'Super Administrator'.

3. Click the **Add New** link, select **SMTP Device Engine** from the drop-down list, and then click **Continue**.
 - AlarmPoint displays the SMTP Device Engine Details page:



AlarmPoint
EXPRESS

About AlarmPoint | Sign Out

Reports | Messaging | Admin

Admin > Nodes > Node Details > Node Components > Device Engine Details

Device Engine Details for: NODE_1_SMTP_DEVICE_ENGINE

General Details

Name: NODE_1_SMTP_DEVICE_EN| *

Description:

Notification Polling: 10 * (sec.)

Concurrent Threads: 1 *

Logging

Generate Separate Log File:

Log Level: Normal *

Protocol Specific Details

Incoming Protocol: NONE *

Logged in as Super Administrator
AlarmPoint Systems, Inc. All Rights Reserved.

4. Specify the following settings:

- **Description:** Type a brief description to help identify the new Device Engine.
- **Log Level:** Select **Detailed**; this will assist you with any future troubleshooting.
- **Incoming Protocol:** Select the protocol used by the company's email server; this is usually POP.

5. Accept the remaining default settings and click **Continue**.

- AlarmPoint displays the Protocol Specific Details page:

AlarmPoint EXPRESS

About AlarmPoint | Sign Out

Reports Messaging Admin

Administration

Admin > Nodes > Node Details > Node Components

Protocol Details for Device Engine NODE_1_SMTP_DEVICE_ENGINE

Protocol Specific Details

Email Account: *

Email Format: user@domain *

Password: *

Incoming Email Server: *

Incoming Server Port: 110 *

SSL Flag: DISABLED

Mailbox Polling Interval (sec): 30 *

Notification Key: Please make sure to include the original message in your reply. The following is used by the server to identify the email %Notification Key%.

Response Key: RESPONSE

Choice Message: Your response choices are %Response Choices%

Response Message: If you would like to reply to this e-mail, simply reply with the word "%Response Key%" followed by your choice in the subject line.

Save

Logged in as: Super Administrator
AlarmPoint Systems, Inc. All Rights Reserved.

6. Specify the following settings:

- **Email Account:** Type the email address used to send notifications. It is strongly recommended that you do not use your personal or corporate account for this setting; have your system administrator create a dedicated AlarmPoint evaluation account.
- **Password:** Type the password used to access the IMAP or POP server.
- **Incoming Email Server:** Type the address of the email server AlarmPoint should poll for responses to notifications.
- **Incoming Server Port:** Type the number of the server port to use for incoming responses.

Note: *If you are not sure about any of the required settings, contact your system administrator.*

7. Accept the remaining default settings and click **Save** to return to the Node Components page.

Configuring HP NNMi

The following section describes how to configure HP Network Node Manager to work with AlarmPoint Express for HP NNMi. This requires the following steps:

- Create a Web Services Client
- Configure NNMi Incident Types for automatic AlarmPoint notifications

Create a Web Services Client

Configuring a Web Services Client allows notification responses to update the NNMi incidents appropriately.

To create a Web Services Client:

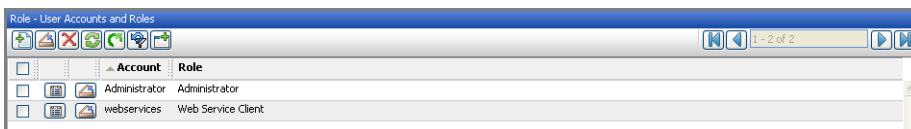
1. Launch the NNMi Web Console, and log in as an Administrator.
2. Under the Configuration Workspace, click **User Accounts and Roles**.
3. On the Role – User Accounts and Roles page, click **New**.
4. On the Role page, under Basics, select **New** in the **Account** drop-down list.
5. On the User Account page, specify the **Name** and **Password** for the Web Services Client User:



The screenshot shows a web interface for configuring a user account. At the top, there are navigation buttons: 'Save and Close', 'Delete User Account', and a refresh icon. The title bar reads 'User Account'. Below this is a 'Basics' section with two input fields: 'Name' containing 'webservices' and 'Password' containing 'nnmi'.

Note: *By default, the user name and password configured within the AlarmPoint Action Scripts is webservices/nnmi. If you want to use a different name or password, you must update the Configuration Variables in the initial PROCESS Action Script. For more information, see “Configuration Variable Reference” on page 36.*

6. Click **Save and Close**.
 - The “webservices” user is now specified in the Account field on the Role page.
7. In the **Role** drop-down list, select Web Service Client.
8. Click **Save and Close**.
 - The Web Service Client will now allow AlarmPoint responses to update NNMi incidents using Web Service Calls. The webservices user is listed on the User Accounts and Roles page:



The screenshot shows the 'Role - User Accounts and Roles' page. It features a table with columns for 'Account' and 'Role'. The table lists three entries: 'Administrator' (Administrator), 'Administrator' (Administrator), and 'webservices' (Web Service Client). The 'webservices' entry is highlighted. The page also includes navigation buttons and a page indicator '1 - 2 of 2'.

Configuring NNMi Incident Types for Automatic AlarmPoint Notifications

To trigger notifications within AlarmPoint, NNMi must be configured to make a command line call passing the incident parameters into AlarmPoint through the APClient utility. For specific NNMi incident types to trigger Notifications within AlarmPoint, their Action Configuration must be enabled to make a command line call to the APClient utility.

The APClient call must have the desired Incident Parameters passed through the command line for them to be available within AlarmPoint.

The default incident types that require configuration are:

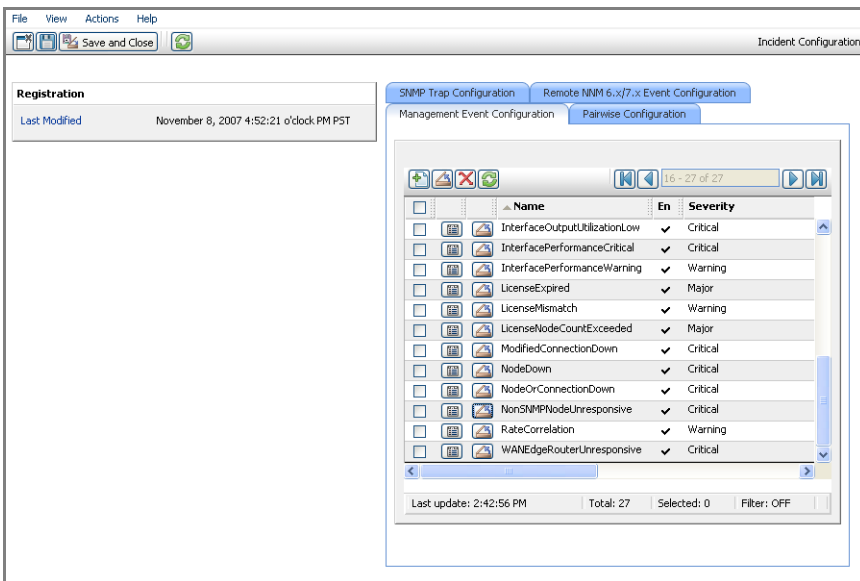
- AddressNotResponding
- ConnectionDown
- ConnectionPartiallyUnresponsive
- ImportantNodeOrConnectionDown
- InterfaceDown
- ModifiedConnectionDown
- NodeDown
- NodeOrConnectionDown
- NonSNMPNodeUnresponsive
- ImportantNodeUnmanageable
- InterfaceDisabled

Depending on the business behavior desired, use the following steps to configure each type of Event requiring AlarmPoint notifications. It is recommended that you forward only Critical Events to AlarmPoint for notification.

The following steps use the **NonSNMPNodeUnresponsive** Management Event as an example of the configuration process.

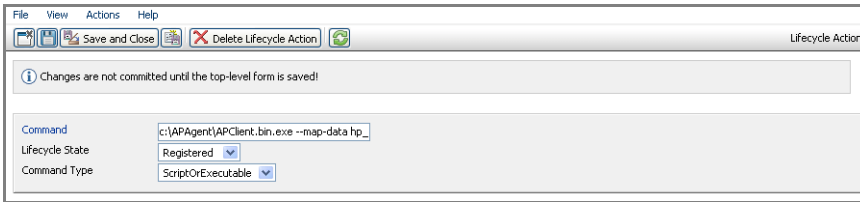
To configure an Incident Type for automatic notification:

1. Launch the NNMi Web Console, and log in as an Administrator.
2. Under the Configuration Workspace, select **Incident Configuration**.
 - The Incident Configuration page appears, displaying several types of events:



3. Open the Event Type you want to configure.
 - To open the NonSNMPNodeUnresponsive Event Type, click the **Management Event Configuration** tab, and then click the **Open** icon beside the NonSNMPNodeUnresponsive Event Type.
4. On the Events Configuration page, ensure the **Enable** check box is selected, and then click the **Action Configuration** tab.
5. On the Action Configuration tab, select the **Enable** check box.
6. Within the Lifecycle Actions table, click the **New** button to add a new Lifecycle Action.
7. On the LifeCycle Action page, enter the following information into the fields:

Field	Detail
Command	<p>Windows:</p> <pre>c:\APAgent\APClient.bin.exe --map-data hp_nnmi bsmith \$category \$severity \$family \$lifecycleState \$name \$nature \$priority \$sourceNodeName \$sourceObjectName \$uuid no</pre> <p>Unix:</p> <pre>/opt/alarmpointsystems/APAgent/APClient.bin --map-data hp_nnmi bsmith \$category \$severity \$family \$lifecycleState \$name \$nature \$priority \$sourceNodeName \$sourceObjectName \$uuid no</pre>
Lifecycle State	Registered
Command Type	ScriptOrExecutable

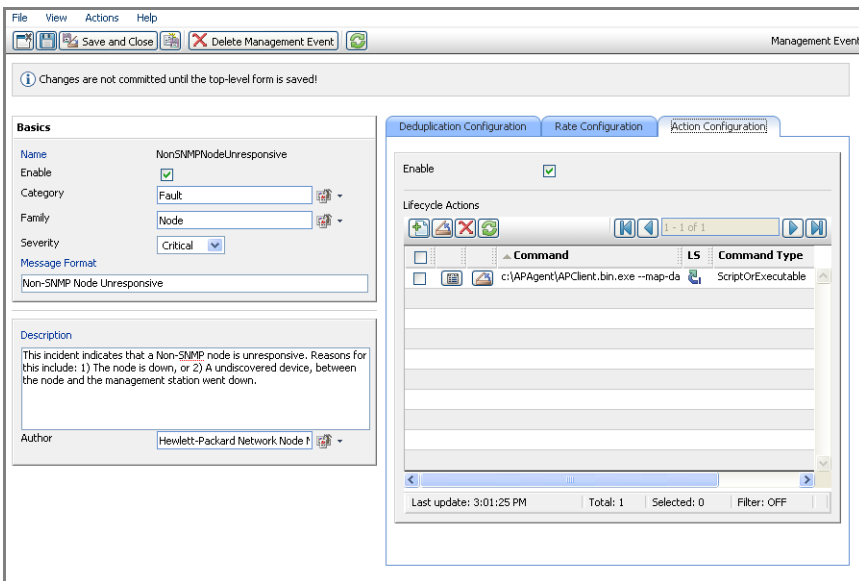


- You can customize the command to inject different event parameters. The following table identifies the default values suggested above:

Variable	Description
bsmith	Identifies the User or Group in AlarmPoint to which notifications for this incident type should be sent. For more information about creating Users and Groups, see “Managing Users and Devices” on page 32 and “Managing Groups” on page 36.
\$category	Describes the type of incident
\$severity	Importance of the incident as specified by NNMi
\$family	Type of object that created the incident
\$lifecycleState	Current Lifecycle State of the incident
\$name	Name of the incident
\$nature	Describes how NNMi views the incident
\$priority	Importance of fixing the incident as specified by users
\$sourceNodeName	Name of the node where the incident originated
\$sourceObjectName	Name of the object that generated the incident
\$uuid	Unique identifier of the incident, used by AlarmPoint as the Incident ID
no	Indicates if the event should be informational-only, or allow for response updates (<i>yes</i> = FYI and <i>no</i> = two-way)

8. Click **Save and Close**.

- NNMi displays the Action Configuration for the Management Event:



- Click **Save and Close** on the selected Event Type page, and then click **Save and Close** again on the Incident Configuration page to commit your changes.

The selected Event Type will now trigger incidents within NNMi and will inject a message through the command line for automatic AlarmPoint notification for each incident triggered. The following is an example of the injected command:

```
APClient --map-data hp_nnmi bsmith com.nms.incident.category.Fault
Critical com.hp.nms.incident.family.Address Registered
NonSNMPNodeUnresponsive ROOTCAUSE
com.hp.nms.incident.priority.None 192.168.168.40 192.168.168.40
a1810618-8308-42e9-8f2d-6758d739c2fd no
```

Note that the configuration of the alerts in NNMi is the responsibility of the system integrator. The recommended implementation pattern is to send in alerts only on items that are marked as “Critical”, and to target a group that is responsible for addressing the problem. Membership of the group can then be maintained in AlarmPoint. Individuals that want to receive information about the alert can create a Subscription.

Note: *The recipient ID specified in the "Command" (bsmith) is not automatically mapped within AlarmPoint. Ensure that the recipient target specified in NNMi matches a Group or User ID within AlarmPoint.*

Triggering a Notification

The following example shows resolution of a network outage on a monitored LAN.

Increase the Polling Frequency

The following section describes how the fault polling interval can be decreased to speed up the demonstration.

To adjust the fault polling interval:

1. If it is not already running, launch HP Network Node Manager i-series.
2. Log in to the NNMi Web Console as an Administrator.
3. Select the **Configuration Workspace**.
4. Open **Monitoring Configuration**.
5. In the Fault Monitoring dialog box, set the **Fault Polling Interval** to **15 seconds**:

Fault Monitoring

Determines the frequency at which NNMi polls SNMP Agents, Addresses, and Interfaces. See Help
→ Using the Monitoring Configuration Form.

Fault Polling Interval: 0 Days 0 Hours
0 Minutes 15 Seconds

ICMP Address Monitoring

Enable ICMP Polling

SNMP Interface Monitoring

Enable SNMP Polling

Poll Unconnected Interfaces

Poll Interfaces

Polling IP Addresses

6. Click the **Save and Close** button.

Disconnect a Computer from the LAN

If NNMi is monitoring a LAN, one of the easiest ways to trigger a notification is to interrupt the communication between NNMi and one of the computers on the LAN. The following steps describe how to do this and what to expect.

1. Physically disconnect a computer from the local area network (using a computer other than the AlarmPoint or NNMi servers).
2. When the computer goes offline, an incident will be triggered within NNMi and can be viewed in the Incidents workspace under Root Cause Incidents (or another incident category depending on the trigger).
 - The Notes entry for the open incident indicates that this event has successfully notified an AlarmPoint User:

Se	Pr	LS	Last Occur	AT	Source Node	Source Object	Ca	Fa	Or	Message	Notes
	5		10/12/07 8:06 PM		192.168.168.40	192.168.168.40				Non-SNMP Node Unresponsive	Mon Dec 10 20:03:45 PST 2007 AlarmPoint:Successful C
	5		10/12/07 7:47 PM		192.168.168.40	192.168.168.40				Non-SNMP Node Unresponsive	Mon Dec 10 19:44:44 PST 2007 AlarmPoint:Successful C
	1		10/12/07 5:56 PM		192.168.168.40	192.168.168.40				Non-SNMP Node Unresponsive	Mon Dec 10 18:00:44 PST 2007 AlarmPoint:Successful C

- To display the full Notes for an incident, click the **Open Incident** button to open the incident, and view the Notes area:

Notes
<p>Notes</p> <p>Mon Dec 10 20:03:45 PST 2007 AlarmPoint:Successful Delivery for bsmith@BlackBerry</p> <p>Mon Dec 10 20:03:46 PST 2007 AlarmPoint:Successful Delivery for bsmith@SMS Phone</p> <p>Mon Dec 10 20:03:47 PST 2007 AlarmPoint:Successful Delivery for bsmith@Work Email</p> <p>Mon Dec 10 20:03:48 PST 2007 AlarmPoint:Successful Delivery for bsmith@Work Email</p>

- The target's specified contact type will receive a message corresponding to the notification, as shown in the following section.

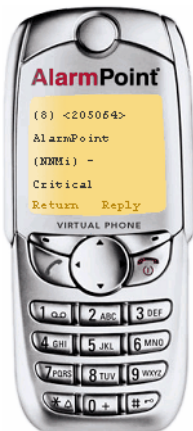
Responding to a Notification

This section describes how to respond to a notification using the default User's virtual text phone.

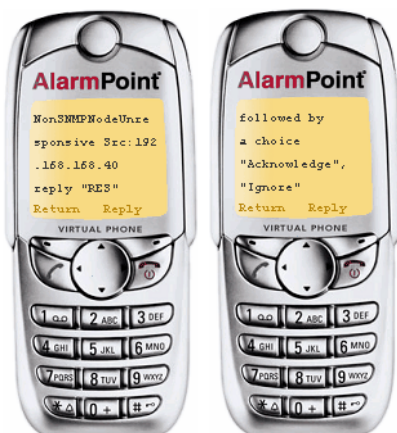
- When a notification arrives for the default user, the virtual text phone appears and indicates the number of notifications that have been received:



- To see the first notification, click **Select**:



3. Scroll down using the arrow buttons to view the details and the list of possible responses:



4. Click **Reply**, and then type **RES Acknowledge**:



5. Click **Send**, and AlarmPoint will send the acknowledgement of the Event to NNMi.

Note: For more about using or changing the available response choices, see “Changing response choices” on page 67.

Viewing Notification Results

In the Root Cause Incidents table, the In Progress arrow indicates that the incident has been acknowledged, and a message will be logged within the Notes field indicating who took responsibility.

To view the notification results:

1. Open the NNMi Web Console.
2. In the Incident Workspace, under Root Cause Incidents, locate the incident used for testing notifications..
 - The Incidents Life Cycle State has changed to **In Progress**, indicating that the incident was acknowledged from AlarmPoint:

	Se	Pr	LS	Last Occur	AT	Source Node	Source Object	Ca	Fa	Or	Message	Notes
<input type="checkbox"/>				10/12/07 8:06 PM		192.168.168.40	192.168.168.40				Non-SNMP Node Unresponsive	Mon Dec 10 20:03:45 PST 2007 AlarmPoint:Successful T
<input type="checkbox"/>				10/12/07 7:47 PM		192.168.168.40	192.168.168.40				Non-SNMP Node Unresponsive	Mon Dec 10 19:44:44 PST 2007 AlarmPoint:Successful T
<input type="checkbox"/>				10/12/07 5:56 PM		192.168.168.40	192.168.168.40				Non-SNMP Node Unresponsive	Mon Dec 10 18:00:44 PST 2007 AlarmPoint:Successful T

3. To display the acknowledged incident’s details, click the **Open** button.

- The Notes field indicates that the incident was acknowledged by bsmith:

Basics

Message
Non-SNMP Node Unresponsive

Severity: Critical
Priority: None
Lifecycle State: In Progress

Source Node: 192.168.168.40
Source Object: 192.168.168.40

Assigned To: [Empty]

Notes

Mon Dec 10 20:03:45 PST 2007 AlarmPoint:Successful Delivery for bsmith|Pager
Mon Dec 10 20:03:48 PST 2007 AlarmPoint:Successful Delivery for bsmith|Home Email
Mon Dec 10 20:10:20 PST 2007 AlarmPoint:Delivery Failure for bsmith|Work Phone
Mon Dec 10 20:20:32 PST 2007 AlarmPoint:Acknowledged by bsmith|

Details

Name: NonSNMPNodeUnresponsive
Category: Fault
Family: Node
Origin: Management Software
Correlation Nature: Root Cause

Duplicate Count: 0
RCA Active:

Correlation Notes

First Occurrence Time: December 10, 2007 8:06:59 o'clock PM PST
Last Occurrence Time: December 10, 2007 8:06:59 o'clock PM PST
Origin Occurrence Time: December 10, 2007 8:06:59 o'clock PM PST

Chapter 3: Managing Users and Devices

This chapter explains how to add Users to AlarmPoint, and configure the Devices used to contact them. You can add up to ten Users in AlarmPoint Express, and up to three Devices for each User.

Adding Users

After installing AlarmPoint, add and configure several sample Users. AlarmPoint Express allows you to add up to ten Users.

1. Log in to AlarmPoint as an Administrator.
 - **Login ID:** root
 - **Password:** tree
2. Click the **Users** tab.
3. In the Users menu on the left side of the browser, click **Add User**.
 - AlarmPoint displays the Add a User page:

The screenshot shows the AlarmPoint Express web interface. The top navigation bar includes 'Profile', 'Alerts', 'Users', 'Groups', 'Reports', 'Messaging', 'Admin', and 'Developer'. The left sidebar shows a tree view with 'Users' selected. The main content area is titled 'Add a User' and contains the following form fields:

- Active:
- User ID:
- First Name:
- Last Name:
- Site: Default Site (dropdown)
- Language: English (dropdown)
- Time Zone: US/Eastern (dropdown)

Below the form are two lists:

- Available Roles:** No Access User
- Selected Roles:** (empty)

Buttons for 'Add >' and '< Remove' are located between the lists. At the bottom of the form are 'Save' and 'Reset' buttons. The footer of the page reads: 'Logged in as: Company Administrator AlarmPoint Systems, Inc. All Rights Reserved.'

4. Specify the new User's **User ID**, **First Name**, and **Last Name**. Retain the other default settings, and assign the User to the Role of **No Access User**.
5. Click **Save** to add the User to AlarmPoint.
 - AlarmPoint displays the Details for User page:

The screenshot shows the AlarmPoint Express web interface. At the top right, there are links for 'About AlarmPoint' and 'Sign Out'. Below the logo, a navigation bar contains tabs for 'Profile', 'Alerts', 'Users', 'Groups', 'Reports', 'Messaging', 'Admin', and 'Developer'. The 'Users' tab is active. On the left, a sidebar menu shows 'Users' and 'Web Service Users' sections. The main content area displays 'Details for Mary McBride' with a message 'User has been saved.' and a form with the following fields: Active (checked), User ID (marym), First Name (Mary), Last Name (McBride), Site (Default Site), Language (English), and Time Zone (US/Eastern). At the bottom of the form are 'Save', 'Reset', and 'Delete User' buttons. On the right, a 'Common Tasks' menu lists 'View Supervisors', 'User Devices', 'Temporary Replacements', 'Groups User Belongs To', and 'View Roles'. At the bottom right, it says 'Logged in as: Company Administrator' and 'AlarmPoint Systems, Inc. All Rights Reserved.'

Note: For more information about adding Users and assigning Roles, refer to the AlarmPoint User Guide.

Adding Devices

Once you have added a User, you can specify the Devices AlarmPoint will use to notify the User. AlarmPoint Express allows you to add up to three Devices for each User.

1. On the Details for User page, in the Common Tasks menu, click **User Devices**.
2. On the Devices for User page, click **Add New**.
3. On the Add New Device page, in the **Select the Device Type** drop-down list, select **Email Device**.
4. Click **Continue**.
 - AlarmPoint displays the Email Device Details page:

AlarmPoint EXPRESS

Profile Alerts **Users** Groups Reports Messaging Admin Developer

Users > Find Users > Person Details > User Devices > Add Device > Email Device Details

Email Device Details for Mary McBride

Device Name: Home Email

Active:

Default Device:

Email Address: *

Provider: SMTP Email

Delay: 0 minutes

Priority Threshold: Use for All Events

Custom Timeframe?: default 24x7

Save Reset

Default Timeframe rule is 24 x 7

Logged in as Company Administrator
AlarmPoint Systems, Inc. All Rights Reserved.

5. In the **Provider** drop-down list, select **Virtual Email**.
6. In the **Email Address** field, type an email address for this User (the actual address is not relevant, but the field must have content).
7. Accept the remaining default settings, and click **Save**.
 - AlarmPoint returns you to the Devices for User page, and displays the new Device:

AlarmPoint EXPRESS

Profile Alerts **Users** Groups Reports Messaging Admin Developer

Users > Find Users > Person Details > Users Devices

Devices for Mary McBride

Existing Devices Add New

Order	Name	Type	Details	Valid	Status	Default	Timeframe	Delay
<input type="checkbox"/>	1	Work Email	Email marym@admins.com				24 x 7	0

Remove Selected Save

Common Tasks

- Validate User Devices
- Send a Message
- Home Page

Logged in as Company Administrator
AlarmPoint Systems, Inc. All Rights Reserved.

Continue to add up to ten Users, and add at least one Device for each User.

Note: *The Import Data feature provided in AlarmPoint allows you to add multiple Users, Devices, and Groups simultaneously by uploading a spreadsheet containing the necessary data. For more information, see “Importing Data” on page 45.*

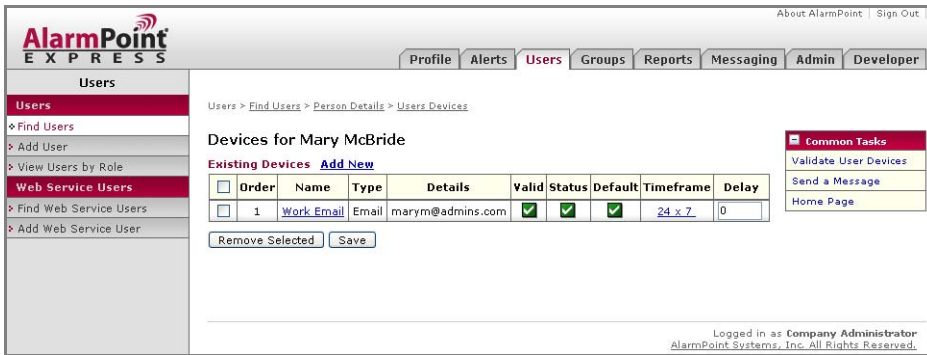
Validating Devices

AlarmPoint includes a testing and validation tool that allows you to ensure that each Device added is working properly and able to receive notifications.

The validation procedure is the same for all Device types; use the following steps to validate the User’s Virtual Email Device.

To validate a Device:

1. In the Existing Devices table, click the yellow triangle in the Valid column for the Virtual Email Device.
 - AlarmPoint prompts you to confirm the validation message.
2. Click **OK** to send the validation message.
 - After a few seconds, AlarmPoint will display the Virtual Email window containing the validation message.
3. In the Virtual Email window, double-click the email to reply to it.
4. In the **Subject** field, type `response validate`, and then click **Reply**.
5. Click **OK** to send the response.
6. Return to the Devices for User page.
 - If you successfully validated the Virtual Email Device, you will see a check mark next to it in the Valid column:



An hourglass icon indicates that a validation message has been sent to a Device, and AlarmPoint is awaiting a valid reply. You can use the same procedure to validate any User Device.

The following figure illustrates an example Existing Device table for a User with three Devices:

Users > Find Users > Person Details > Users Devices

Devices for Mary McBride

Existing Devices [Add New](#) [Reorder](#)

<input type="checkbox"/>	Order	Name	Type	Details	Valid	Status	Default	Timeframe	Delay
<input type="checkbox"/>	1	Work Email	Email	marym@admins.com				24 x 7	0
<input type="checkbox"/>	2	SMS Phone	Text Phone	5551234				09:00 - 17:00 MO TU WE TH FR	0
<input type="checkbox"/>	3	Numeric Pager	Numeric Pager	5555678				17:00 - 22:00 MO TU WE TH 17:00 Lasting 64:00 FR	0

[Remove Selected](#) [Save](#)

Note how each Device has a predefined Timeframe during which it is available to receive notifications. For more information about working with Devices and creating Timeframes, see the *AlarmPoint User Guide*.

Chapter 4: Managing Groups

The following sections describe how to add and configure Groups in AlarmPoint.

Important Terms for Groups

The following are some of the important terms used in relation to Groups:

Groups

Groups are a collection of Coverages (for details, see “Coverages”, below) relating to a specific task or responsibility. A Group might be created to meet a single, specific need, or it might serve as a duty roster or workgroup that relates to a similar function.

Each Group usually has a defined schedule that AlarmPoint uses to determine who to notify. When different company sites, time zones, work shifts, and business needs are involved, Group scheduling can quickly become complex – managing this complexity is one of the strengths of AlarmPoint.

For most AlarmPoint Users, it is sufficient to understand that Groups consist of Users, and that Users can be members of multiple Groups, depending on their responsibilities.

Coverages

Coverages are a combination of a Team and Schedule. AlarmPoint uses Coverages to identify the Users who are on duty at a particular time to receive notifications about events.

Schedules

In AlarmPoint, a Schedule is a specific period of time, such as a single day, a recurring span of several hours on certain days of the week, or 24/7 (every day, all day).

For example, a typical recurring Schedule is business hours, from 8:00 to 17:00, Monday through Friday. In turn, an ‘off-hour’ schedule could be from 17:01 to 7:59 Monday through Friday, and all day on Saturday and Sunday.

Schedules can also define rotations, such as 8:00 to 17:00 Monday through Friday every 3 weeks. This allows building sophisticated, automatic rotations with different Users and Groups.

Teams

A Team identifies who is available during specific Schedule times to receive notifications. Teams can consist of any combination of Users, Devices, Groups, or other Teams.

For example, a Team called “Shift 3” might include a User named “Terry Smith”, a Group named “Data Center Managers”, and a Device named “John’s Cell Phone”.

Creating Groups

This section demonstrates the escalation capabilities of AlarmPoint on a small scale by creating and configuring a simple Group. The following steps use the Operations Group, which is created during the AlarmPoint installation.

Note: *You can add up to five Groups in AlarmPoint Express.*

The default Operations Group has a single Team member assigned to a 24x7 Schedule. The first step in expanding the Group is to add more Users.

1. Log in as an Administrator, and click the **Groups** tab.
2. In the Groups I Supervise table, click **Operations**.
 - AlarmPoint displays the Group Details page:

AlarmPoint EXPRESS

About AlarmPoint | Sign Out

Profile Alerts Users **Groups** Reports Messaging Admin Developer

Groups > Groups I Supervise > Group Details

Group Details for: Operations

Show Details

Filter

Time Zone: US/Eastern

Filter By: -- None --

Apply

Existing Coverages for week of 07/15/2007

« Prev Next » Monthly View

	Complete	Coverage	Sun. Jul. 15		Mon. Jul. 16		Tue. Jul. 17		Wed. Jul. 18		Thu. Jul. 19		Fri. Jul. 20		Sat. Jul. 21	
			AM	PM	AM	PM	AM	PM	AM	PM	AM	PM	AM	PM	AM	PM
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Operations-24x7														

Remove Selected

Logged in as Company Administrator
AlarmPoint Systems, Inc. All Rights Reserved.

3. Move your mouse cursor over any of the light blue segments to see details of that shift; each shift in this Group has only one member, Bob Smith.
4. In the Coverage column, click **Operations-24x7**.
5. On the Schedule Details page, in the Team Members area, click the **Add Users** link.
 - AlarmPoint displays the Find Users page.
6. Click **All** to see a list of all the Users in AlarmPoint.
7. Select the check box next to four Users, and then click **Add**.
8. Click **Save** to add the Users to the Team, and return to the Schedule Details page.

Managing Escalations

After you have added Users to the Operations Group, you can define the escalation time for each Team member. If you do not specify a Delay between Team members, AlarmPoint attempts to notify all Team members at the same time, as soon as the Event occurs.

In an actual deployment situation, each User would require time to respond to a notification, but for demonstration purposes, you can minimize the delay.

1. On the Schedule Details page, type **1** in the **Delay** field for the second, third, and fifth Team members:

AlarmPoint EXPRESS

About AlarmPoint | Sign Out

Profile Alerts Users **Groups** Reports Messaging Admin Developer

Groups > Group I Supervise > Group Details > Recurring Coverage

Manage Groups

Groups I Supervise

Find Groups

View User Schedule

Who is On Duty?

Teams

My Team Templates

Schedule Details for: Operations

Show Details

Common Tasks

Change Existing Team

View Team Details

Back to Group Details

Team Members for: Operations-team

Recently Used: Smith, Bob (bsmith) Select

Add Users Add Groups Add Teams Add Devices Reorder

<input type="checkbox"/>	Delay (min)	Escalation	Name	Description	Type	Active
<input type="checkbox"/>	0	0	Smith, Bob (bsmith)		Person	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1	1	McBride, Mary (marym)		Person	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1	2	Oadry, Carol (carolo)		Person	<input checked="" type="checkbox"/>
<input type="checkbox"/>	0	2	Fuller, Will (willf)		Person	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1	3	Martin, Jim (jimm)		Person	<input checked="" type="checkbox"/>

Remove Selected Save Team

Logged in as Company Administrator
AlarmPoint Systems, Inc. All Rights Reserved.

- The Escalation column indicates how long, in minutes, AlarmPoint will wait after the Event occurs before it begins attempting to contact each Team member.

2. Click **Save Team**.

The escalation process for the Operations Group is now set to the following:

- The first Team member (in this case, Bob Smith) will be notified immediately when an Event occurs.
- One minute after beginning to notify Bob Smith, AlarmPoint will begin attempting to notify the second Team member.
- One minute after beginning to notify the second Team member, AlarmPoint will simultaneously begin attempting to notify the third and fourth Team members.
- One minute after beginning to notify the third and fourth Team members, AlarmPoint will begin attempting to notify the fifth Team member.

In the next chapter, you can test the escalation by sending a notification message to the Group.

Other escalation options

AlarmPoint includes a wide variety of options you can implement within Groups to create your ideal escalation schedule.

Team escalation options

You can create three different types of Teams, each of which affects the escalation order:

- **Basic:** Team members are notified in the order they are listed on the Team details page.
- **Event round robin:** After each Event, the first Team member will be moved to the last position on the Team list, and all other Team members will be moved up one position.

For example, assume an event round robin Team is made up of four members: A, B, C, and D. The first time AlarmPoint sends a notification to the Team, A is notified first, then B, and so on. After that Event, the list of members is reordered so that the order becomes B, C, D, and A. After the next Event, the list is changed again, to C, D, A, and B.

- **Rotation:** After a defined time period called the Rotation Interval, the first Team member will be moved to the last position on the Team list, and all other Team members will be moved up one position.

For example, assume a rotation Team is made up of four members: A, B, C, and D. Further assume that the Rotation Interval has been set to four days. In this case, for the first four days after the specified Start Date and Start Time, when AlarmPoint sends a notification to the Team, A is notified first, then B, and so on. After four days, the list of members is reordered so that the order becomes B, C, D, and A. After the next four days, the list is changed again, to C, D, A, and B.

You can also ‘freeze’ a Team Member’s position in the rotation so that they no longer rotate, but instead remain in the same position on the Team list.

Allowing duplicate members in Groups

The Allow Duplicates check box on the Group details page specifies the following:

- whether the same Team member or members can appear more than once in the escalation rotation; and,
- whether the Group allows duplicate notifications for a single Event.

The Allow Duplicates setting applies to all Groups within a Group, even if the sub-Group is flagged differently.

For example, assume that User Bob Smith is a member of both the Operations Group, which allows duplicates, and the Support Group, which does not allow duplicates. If the Operations Group is added as a Team member to the Support Group, and a notification is sent to both Bob Smith and to the Operations Group, Bob would receive only one notification because the Support Group is not flagged to allow duplicates.

Note that if the Allow Duplicates check box is cleared, Users, Teams, and Groups already specified as Group members will not be displayed as part of any search results when adding members to the Group.

Schedule escalation options

When creating a new Group, AlarmPoint provides you with the opportunity to create a single Coverage consisting of one Schedule and one Team. Depending on your scheduling requirements, you might want to add more Coverages to your Group.

You can also add a One-time Coverage for unique scheduling situations, or add a Recurring Coverage for on-going and long-term scheduling. When adding a new Coverage to an existing Group, AlarmPoint prompts you to set the Schedule first, and then assign the Team.

Note: *For detailed information about Group escalations and Schedule options, see the AlarmPoint User Guide.*

Chapter 5: Messaging

This chapter explains how to send a message in AlarmPoint using the Quick Messaging panel. The messaging feature in AlarmPoint mimics the injection of an event from an outside source using the “messaging” Event Domain.

Sending a Message

The quickest way to verify a Group’s escalation process is to use the Quick Message feature to send a message to the Group.

1. Click the **Messaging** tab.
 - AlarmPoint displays the Send a Quick Message page.
2. Select an option from each of the **Event** and **Detail** drop-down lists.
3. Type the text for the message in the **Message Text** field.
4. In the Recipients area, click **Add Groups**.
 - Alarm displays the Find Group Recipients page:

Find Group Recipient(s)

Results per page: 10

Find Groups Where: Name Begins With

Selected groups must Any All
match:

Available Group Members	Current Group Members
-- None --	-- None --
<input type="button" value="Save"/>	

5. Click **Show All**, select the check box next to the **Operations Group**, and then click **Add**.
6. Click **Save** to close the window and return to the Quick Message page.
7. In the Delivery area, ensure that the **All Devices** check box is selected.
 - Your Quick Message page should resemble the following:

AlarmPoint EXPRESS

About AlarmPoint | Sign Out

Profile Alerts Users Groups Reports **Messaging** Admin Developer

Messaging

Quick Messages

- Send Message
- View Sent Messages
- View Scheduled Messages

Send a Quick Message (Incident ID: WEB_MESSAGE_1192734983593) ?

Message

Event: Flood

Detail: Main Computer Room

Message Text: Testing the Group Escalation.

(1000 char. max.)

Recipients

[Add Users](#) [Add Groups](#)

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	Operations	Group

[Remove Selected](#) [Refresh](#)

Delivery

All Devices Email Instant Message Text Devices

Scheduled Messaging

[Send Message](#)

Logged in as Super Administrator
AlarmPoint Systems, Inc. All Rights Reserved.

8. Click **Send Message**.

AlarmPoint will send a Message to the Group, which results in Bob Smith immediately receiving a notification. To test the escalation schedule, you can respond to Bob Smith's notification with "Acknowledge". This records the response, but does not clear the Event, and AlarmPoint will continue to notify Group members.

Note the delay between notifications sent to Group members, and wait until the third or fourth User has been notified before responding with "Clear". This will prevent AlarmPoint from sending more notifications based on the submitted message, and prevents the fifth Team member from receiving a notification.

Chapter 6: Managing System Data

This chapter explains the reporting features of AlarmPoint, and provides an introduction to the Import Data feature, which you can use to add multiple Users, Devices, Groups to AlarmPoint.

Generating Reports

AlarmPoint provides a number of web-viewable reports for system monitoring and troubleshooting. The reports include logs of incoming messages, actions taken within AlarmPoint, notification status messages, component status, and other interactions.

The following table summarizes some key terms used in AlarmPoint Reports:

Term	Description
Incident	Represents one or many Events. For example, a Management System can use a single Incident ID to span multiple Events.
Event	Events originate when the Management System sends a message to the AlarmPoint Java Client, or when the Event is generated from an AlarmPoint Messaging Panel. Events represent the starting point and highest level of AlarmPoint's internal tracking. The Event ID is assigned within AlarmPoint.
Notification	Generated based on Events, and can target one or many recipients (Users, Groups, and Devices). Notifications are delivered based on the Users' settings (schedules, escalations, overrides, and so on) and the business logic of the script used to process the Event.

Accessing Reports

To access AlarmPoint Reports, log in to the AlarmPoint Web User Interface and click the Reports tab. The left menu displays links to all available Reports.

Available Reports

AlarmPoint includes many predefined Reports with search criteria designed to help Administrators understand the application's runtime status, historical performance and auditing capabilities.

The following table summarizes the available reports and provides a brief description of each:

Category	Report	Description
Activity	Events Activity	Returns Events submitted to the system.
	Events for User	Returns Event details for a specific User based on a date and time range.
	Events for Group	Returns Event details for a specific Group based on a date and time range.
	Submitted Notifications	Returns all notifications sent within a specified date and time range.
	Live Notifications	Returns notifications that are currently live in the system, at a specified refresh rate (in seconds).
Company Reports	Message Throughput	This report returns all notifications the system has submitted, sent, and received based on a date and time range.
	Domain Summary	Returns all notifications the system has delivered based on a date and time range, and sorted by the specified Event Domain.
	Synchronization Report	Returns the results of data synchronizations based on a date and time range.
	Application Audit Report	Returns any additions, deletions, or changes to the specified system item, based on a date and time range.
System Reports	Component Status	Returns the status of all AlarmPoint components, at a specified refresh rate (in seconds). By default, this Report is available only to the AlarmPoint Super Administrator.
Audit	Security Audit Report	Returns login attempts (success/failure) by User ID and Web Login based on a date and time range.
	Web Service Audit Report	Returns AlarmPoint Web Services activity, including Audit Time, WS User, Status, Method Name, Client Timestamp, Client IP, and Client OS user, based on a date and time range.
Note: <i>For more information about working with AlarmPoint's Reports, see the AlarmPoint Installation and Administration Guide.</i>		

Importing Data

You can use the AlarmPoint Web User Interface to import XML spreadsheets of User information or other data directly into the AlarmPoint database. The Import Data feature provides a quick way to import large amounts of records without the need for significant resources, or having to enter data into the system manually, one record at a time.

While this feature is most useful in more robust installations, AlarmPoint Express users may find it useful if they are repeatedly seeding the installation for evaluation purposes.

You can use the Import Data feature to import the following information from the spreadsheet:

- User information: User ID, first and last name, Site, Role, Phone ID, and up to three Devices, including the Service Provider for each Device.
- Group information: Group names, descriptions, and default time zones.
- Group Member information: the Users to assign to each Group.

Note: *You can add a maximum of five Groups and ten Users in AlarmPoint Express.*

Spreadsheet template

AlarmPoint includes a pre-formatted Excel 2003 XML spreadsheet you can use as a template when entering your data. The template is named `DataImportTemplate.xml`, and is stored in the AlarmPoint installation folder.

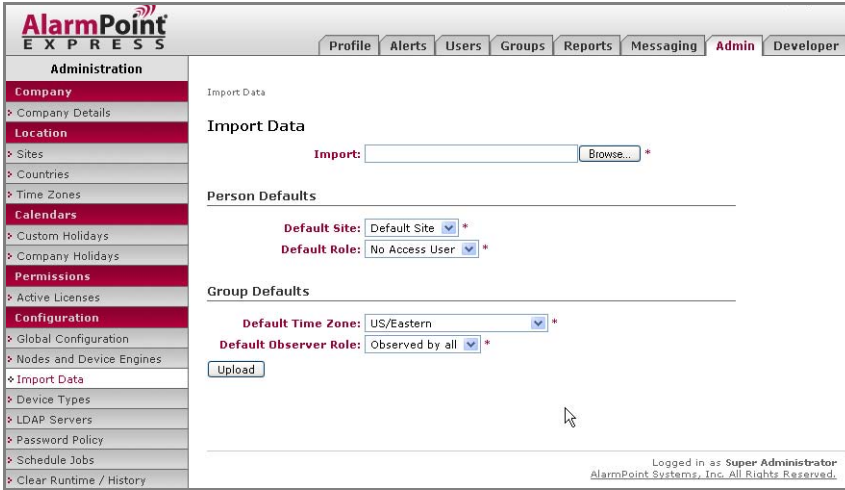
For complete instructions on how to use the sample spreadsheet with the AlarmPoint Import Data feature, see the *AlarmPoint Installation and Administration Guide*. Note that many of the fields included in the Import Data spreadsheet, such as Web and Phone Login IDs, are not required in AlarmPoint Express.

Importing spreadsheets

Once your data is formatted on the Excel 2003 XML spreadsheet, you can import it into the AlarmPoint database using the web interface.

To import a spreadsheet:

1. Click the **Admin** tab.
2. In the Configuration area of the Administration menu, click **Import Data**.
 - AlarmPoint displays the Import Data page:



3. On the Import Data page, enter the following information into the form:

Detail	Description
Import	Name and location of the Excel 2003 XML spreadsheet you want to import. Type a path and a file name into the field, or click Browse to locate a spreadsheet file on your system.
Default Site	Site to which all Users will be assigned, unless otherwise specified in the spreadsheet.
Default Role	Role to which all Users will be assigned, unless otherwise specified in the spreadsheet.
Default Time Zone	Time Zone to which all Groups will be assigned, unless otherwise specified in the spreadsheet.
Default Observer Role	Observer Role which will be assigned to all Groups, unless otherwise specified in the spreadsheet.

4. Click **Upload** to import the spreadsheet data into AlarmPoint.

- AlarmPoint attempts to upload the data and import it into the database. If the import process is successful, AlarmPoint displays a success message at the top of the Import Data page.
- If the import process failed for any reason, AlarmPoint displays a failure message. You can click the **Download Results** button to generate and view an Excel 2003 spreadsheet with more information about the errors.

Chapter 7: Subscribing to Alerts

With Subscriptions, AlarmPoint can automatically notify Users whenever an event matches a pre-defined set of criteria. For example, when a certain type of error occurs on a specific asset or service, AlarmPoint can notify a particular Group.

The following sections describe how to create Subscriptions in AlarmPoint Express for HP NNMi, including instructions on how to incorporate the included custom Subscription panel and assign Subscriptions to Users. Note that this feature is strictly optional; the ability to directly target Users, Devices, and Groups through integration or web messaging is sufficient for most deployments.

AlarmPoint Express for HP NNMi includes a pre-configured custom Subscription Panel, `NNMiSubscriptionForm.jsp`.

Important Terms

The following terms are used in relation to Subscriptions in AlarmPoint:

Event Domain

Each source of incoming Events, such as HP NNMi, requires a separate Event Domain in AlarmPoint. The Event Domain defines the name/value pairs that AlarmPoint uses to determine the nature of the Event. The information contained in the Event identifies its Event Domain, which in turn determines which Script Package AlarmPoint should use to handle the Event. AlarmPoint Express supports a maximum of one customer Event Domain.

Predicate

Each name/value pair within an Event Domain is referred to as a predicate.

Subscription Domain

A Subscription Domain defines a subset of the predicates within an Event Domain, and sends notifications to Subscribers based on those criteria. AlarmPoint Express supports a maximum of one Subscription Domain.

Configuring Subscriptions

Subscriptions can be used in one of two ways: self-subscriptions and managed subscriptions. With self-subscriptions, Users with proper permissions can create their own Subscriptions for informational types of Events and Alerts. With managed subscriptions, supervisors can define Subscriptions and assign them to Groups or Users, who can then see what has been assigned to them. You can also create Subscriptions that combine both approaches.

For AlarmPoint Express, it is recommended that you create “Managed” Subscriptions, as only the Administrator account has access to the AlarmPoint Web User Interface.

The instructions in the following sections describe how to work with the pre-configured “hp_nnmi” Event Domain and “AP-HP-NNMi.aps” script package in AlarmPoint Express for HP NNMi. Changes to other Event Domains may require changes to their associated script packages. For more information about Subscriptions, and instructions on how to create Event and Subscription Domains, see the *AlarmPoint Installation and Administration Guide*.

Adding a Custom Subscription Panel

AlarmPoint Express for HP NNMi comes equipped with a pre-built custom Subscription panel (and modified script package) that you can use to create Subscriptions in AlarmPoint. If you want to create your own Subscription panel, see the *AlarmPoint Developer’s Guide & Scripting Reference* for complete instructions; note that AlarmPoint Express supports only one custom Subscription Panel per installation, and that all custom Subscription panels must be in Java Server Pages (.jsp) format.

Note: *The custom Subscription panel included with AlarmPoint Express for HP NNMi, NNMiSubscriptionForm.jsp, is automatically installed to the correct location.*

Configuring a Subscription

The AlarmPoint Express for HP NNMi installer automatically creates and configures the “hp_nnmi” Event Domain and the “NNMi” Subscription Domain with the following predicates (case sensitive):

- SEVERITY
- CATEGORY
- NAME
- SOURCENODENAME
- SOURCEOBJECTNAME
- PRIORITY
- FAMILY
- NATURE

The following sections explain each predicate’s settings and its corresponding value in HP NNMi.

SEVERITY

Severity is a list predicate containing some or all of the following values (case sensitive):

- Critical
- Major
- Minor

- Normal
- Warning.

The items listed for Severity should be specifically chosen to match the severity of the Events forwarded from NNMi. Exclude any severities that will not be submitted for notification.

This predicate corresponds to the \$severity variable in NNMi.

CATEGORY

Category is a list predicate that describes the type of incident; allowed values are:

- com.hp.nms.incident.category.Fault
- com.hp.nms.incident.category.Status
- com.hp.nms.incident.category.Config
- com.hp.nms.incident.category.Accounting
- com.hp.nms.incident.category.Performance
- com.hp.nms.incident.category.Security
- com.hp.nms.incident.category.Alert

NNMi will generate only the values listed above. Exclude from your list any categories that will not be submitted for notification.

This predicate corresponds to the \$category variable in NNMi.

NAME

Name is a list predicate that identifies the incident type of the event. The values should be only those incident types you have configured to inject messages into AlarmPoint, as described in “Configuring NNMi Incident Types for Automatic AlarmPoint Notifications” on page 24.

The default available incident types are:

- AddressNotResponding
- ConnectionDown
- ConnectionPartiallyUnresponsive
- ImportantNodeOrConnectionDown
- InterfaceDown
- ModifiedConnectionDown
- NodeDown
- NodeOrConnectionDown
- NonSNMPNodeUnresponsive
- ImportantNodeUnmanageable
- InterfaceDisabled

This predicate corresponds to the \$name variable in NNMi.

SOURCENODENAME

Source Node Name is a list predicate that identifies the name of the Node that is the source of the incident. This list is populated through a Web Services Call to NNMi.

This predicate corresponds to the \$sourceNodeName variable in NNMi.

SOURCEOBJECTNAME

Source Object Name is a text predicate containing the name of the Object that generated the incident. The Object can be determined through a combination of the Object Name and Family.

As this is a text field, you can use any number of filters on the results.

PRIORITY

Priority is a list predicate that identifies how important fixing the incident is to Users. This is in contrast to Severity, the level of which is automatically determined by NNMi. Note that AlarmPoint allows the priority to be altered by notification recipients.

Valid values for Priority are:

- com.hp.nms.incident.priority.None
- com.hp.nms.incident.priority.Low
- com.hp.nms.incident.priority.Medium
- com.hp.nms.incident.priority.High
- com.hp.nms.incident.priority.Top.

This predicate corresponds to the \$priority variable in NNMi.

FAMILY

Family is a list predicate that identifies the type of object that generated the incident. Valid values for Family are:

- com.hp.nms.incident.family.Address
- com.hp.nms.incident.family.Interface
- com.hp.nms.incident.family.Node
- com.hp.nms.incident.family.OSPF,
- com.hp.nms.incident.family.HSRP
- com.hp.nms.incident.family.AggregatePort
- com.hp.nms.incident.family.Board
- com.hp.nms.incident.family.Connection
- com.hp.nms.incident.family.Correlation

This predicate corresponds to the \$family variable in NNMi.

NATURE

Nature is a list predicate that describes how NNMi views the incident. Valid values for Nature are:

- ROOTCAUSE
- SECONDARYROOTCAUSE
- SYMPTOM
- USERROOTCAUSE.

This predicate corresponds to the \$nature variable in NNMi.

Assigning Subscriptions

Once the Event and Subscription Domains are prepared, you can assign Subscriptions to Users, Groups, and Dynamic Teams, or even specific Devices. For example, you could use the Subscription panel to subscribe to NNMi Events of specific criteria, such as those of “Critical” Severity.

To create a Subscription:

1. Click the **Alerts** tab, and then click **My Subscribed Alerts**.
2. On the My Subscribed Alerts page, in the **Subscription Domain** drop-down list, select **NNMi**.
3. Click the **Add New** link above the Self-made Subscriptions table.
4. On the Subscription Details page, enter a name for the Subscription and specify the Subscription criteria using the Event Details and Preferences tabs.
 - The Event Details tab (Ctrl-click to select more than one value):

Event Details
Preferences

Category: -- ANY --
Accounting
Alert
Config
Fault

Family: -- ANY --
Address
AggregatePort
Board
Connection

Incident Name: -- ANY --
AddressNotResponding
ConnectionDown
InterfaceDown
NodeDown

Nature: -- ANY --
ROOTCAUSE
SECONDARYROOTCAUSE
SYMPTOM
USERROOTCAUSE

Priority: -- ANY --
High
Low
Medium
None

Severity: -- ANY --
Critical
Major
Minor
Normal

Source Node Name: -- ANY --
192.168.168.1
192.168.168.40
LAGAVULIN
LJ_PRINTER_VICT

Source Object Name: CONTAINS Empty Field = Any Value

Save

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

Event Details
Preferences

Timeframe

Start Time: hours minutes *

On the following days: Sun Mon Tue Wed Thu Fri Sat

Time Zone: US/Eastern

Overrides

Device Types: All Devices Email Instant Message Text Devices Voice Devices

Override User Device Timeframes:

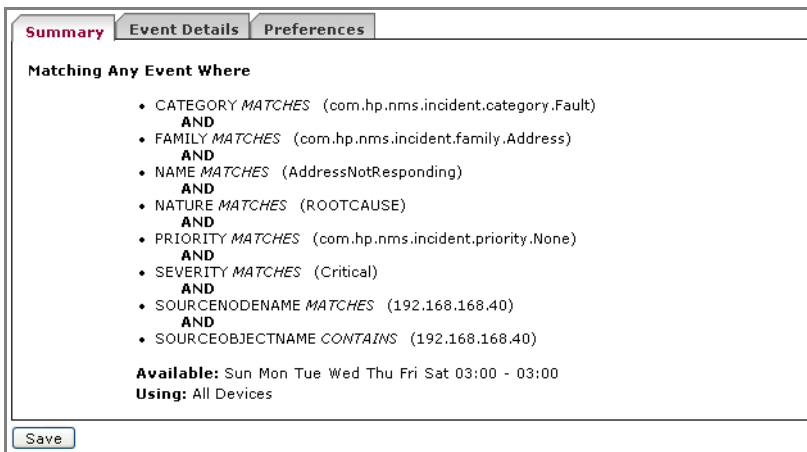
Ignore Device Delays:

Override Device Severities and Use All:

Notification Delay: min

Save

- 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:



The screenshot shows a web interface with three tabs: **Summary** (selected), **Event Details**, and **Preferences**. The main content area is titled **Matching Any Event Where** and contains a list of criteria:

- CATEGORY *MATCHES* (com.hp.nms.incident.category.Fault)
AND
- FAMILY *MATCHES* (com.hp.nms.incident.family.Address)
AND
- NAME *MATCHES* (AddressNotResponding)
AND
- NATURE *MATCHES* (ROOTCAUSE)
AND
- PRIORITY *MATCHES* (com.hp.nms.incident.priority.None)
AND
- SEVERITY *MATCHES* (Critical)
AND
- SOURCENODENAME *MATCHES* (192.168.168.40)
AND
- SOURCEOBJECTNAME *CONTAINS* (192.168.168.40)

Below the list, the following information is displayed:

Available: Sun Mon Tue Wed Thu Fri Sat 03:00 - 03:00
Using: All Devices

A **Save** button is located at the bottom left of the configuration area.

- On the Subscribers page, add any combination of Users, Groups, or Devices to create a list of subscribers.

Chapter 8: Scripting in AlarmPoint

The following sections provide a brief overview of scripting in AlarmPoint, including an introduction to Action Script, the terminology used when discussing AlarmPoint scripts, and how the included AlarmPoint Developer IDE works. This section also introduces the process required to create an integration.

AlarmPoint provides the ability for Administrators to edit scripts to enhance the notification business process. For example, you could:

- change the display content for a message; e.g., the default subject line for an email;
- change the job control when integrating with a management system; or,
- provide different response options for notification recipients.

Note that the sections included here are introductory in nature; for more complete information on these and other related topics, see the *AlarmPoint Developer's Guide & Scripting Reference*.

Note: *AlarmPoint-provided Integration Modules include the full Script Package required for integrations.*

Introduction to Scripting

Action Script, the scripting language used in AlarmPoint, has been designed to be lightweight and powerful, and to meet the unique requirements of AlarmPoint Systems software products and customers.

This introduction will focus on the basics of Action Script, and what is necessary for event resolution.

Important Terms

The following terms are used throughout this section to describe elements of the business process management system:

- A **business process** is a set of actions taken by the AlarmPoint runtime in response to an event from an event source.
- An **event** is an external occurrence that has been injected into the AlarmPoint system from another source, such a management system. The event contains data which determines how the associated business process will behave.
- Events are associated with **event domains** when they enter the AlarmPoint system. Event domains represent the event source and determine which scripts will be run for that event.
- A **script** is a user-modifiable part of the business process.

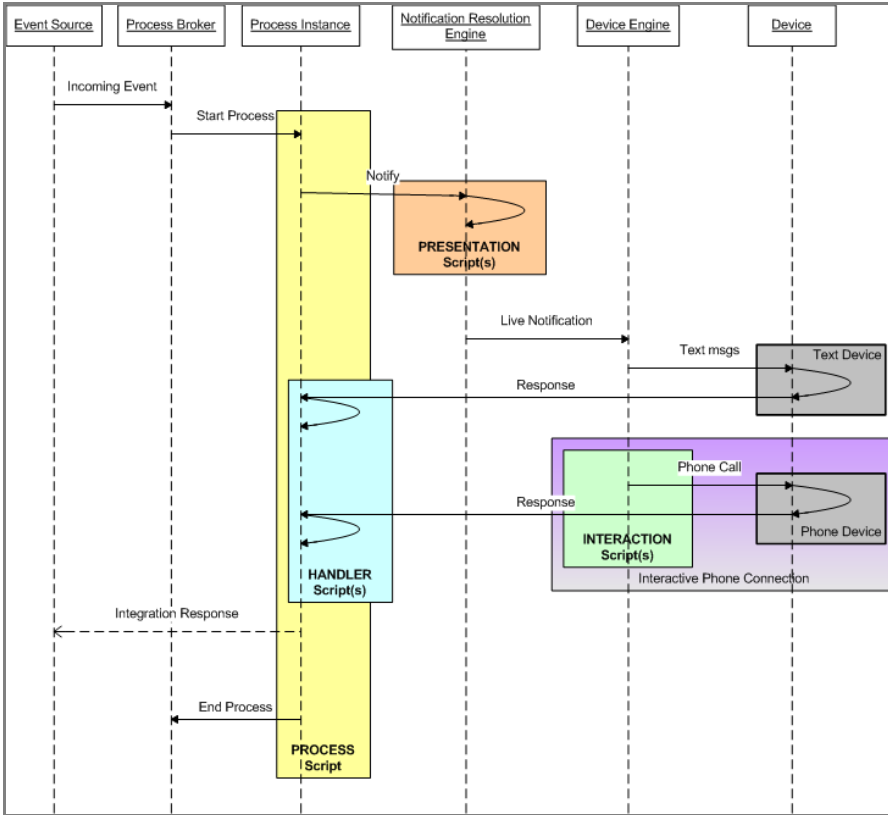
- A **script package** is a grouping mechanism for scripts and is associated with an event domain.
- A **script object** is a script element which functions as both a container for data (variables) and an interface from within a script to the AlarmPoint runtime (methods).
- A **notification** is a message from the AlarmPoint system to a User. Notifications have **content** which is presented to a User on a **Device**. Notifications are dispatched to Users by **Device Engines**.
- Users can send **responses** to the AlarmPoint system that typically consist of **response choices** and sometimes auxiliary data.

Much of the business process is managed by compiled code distributed with the AlarmPoint runtime. However, certain parts of the business process are “scriptable” so that users can customize behaviour according to their needs.

Concepts

The primary purpose of the runtime portion of an AlarmPoint deployment (the community of nodes) is to receive external events and manage business processes surrounding those events. This business process typically includes generating notifications, processing responses from notification recipients, and managing the lifecycle of the business process and its constituent parts.

AlarmPoint Scripting and Event Flow



Event Processing Overview

The following figure represents a typical set of steps taken by the AlarmPoint system in response to an external event:

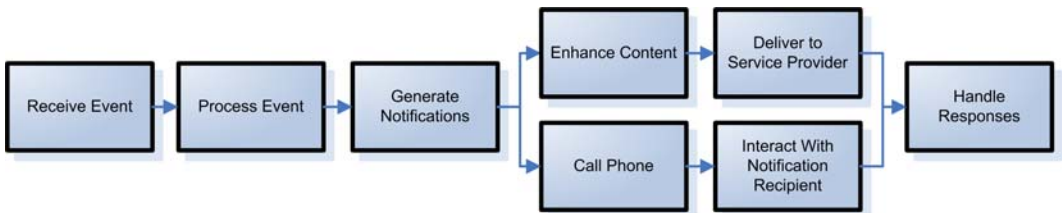


Figure 2.1: Typical Event Flow

Each of the steps is described as follows:

- **Receive Event:** an event is injected into AlarmPoint from an event source (through an integration or from the web interface).

- **Process Event:** a business process is created and started for the event.
- **Generate Notifications:** as part of the business process, notifications are generated.
- **Enhance Content:** content specific to the recipient is added.
- **Deliver to Service Provider:** the generated notifications are dispatched to User Service Providers.
- **Call Phone:** a conversation is established with the recipient.
- **Interact with Notification Recipient:** the notification is presented to the recipient.
- **Handle Responses:** responses are received for the generated notifications.

Note: *Scripting in AlarmPoint is extremely flexible; for illustration purposes, the workflow described in this section has been simplified. Actual scripting processes and data flow may vary.*

Editing Action Scripts

To create or edit an Action Script, you must install the AlarmPoint Developer IDE, and change the script based on the AlarmPoint Script Packages.

Installing the AlarmPoint Developer IDE

The AlarmPoint Developer IDE is an integrated development environment used to create, edit, and manage processes within AlarmPoint. You can also import the business processes provided by AlarmPoint for an integration to specific management systems.

The IDE has an automated installer (Windows wizard or console). The following sections describe the steps for installing the AlarmPoint Developer IDE.

To install the AlarmPoint Developer IDE:

1. On the HP NNMi CD, navigate to the appropriate folder for your operating system and double-click the installation file.
 - The following table lists each installation file and its location on the HP NNMi CD:

O/S	File Location
Windows	\AlarmPoint\windows\ap321_devide_install.exe
Solaris	\AlarmPoint\solaris\ap321_devide_install.bin
Linux	\AlarmPoint\linux64\ap321_devide_install.bin
HP Itanium	\AlarmPoint\HPItanium\ap321_devide_install.bin

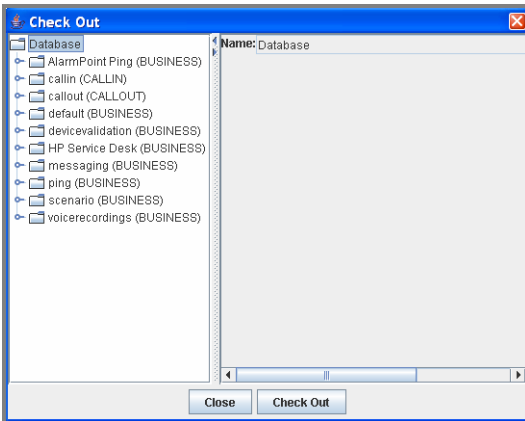
2. Read the text on the Introduction page, and then click **Next**.
3. Read the License Agreement, select **I accept the terms of the License Agreement**, and then click **Next**.
4. Specify the location to install the IDE or accept the default installation folder, and then click **Next**.
5. After the installation has completed, click **Done**.

Using the AlarmPoint Developer IDE

Once the AlarmPoint Developer IDE is installed, you can configure the connection to the AlarmPoint database.

To configure and use the AlarmPoint Developer IDE:

1. Once installation is complete, click **Start > Programs > AlarmPoint Systems > AlarmPoint Developer IDE**.
2. When the Developer IDE starts, click **Connection > SQL Server Example**.
3. Click **Connection > Edit Connection**.
4. In the JDBC Connection dialog box, specify the following settings:
 - **URL:** Type the URL to access the database; for example: `jdbc:jtds:sqlserver://<yourIPAddress>:1433`, where `<yourIPAddress>` is the URL.
 - **User:** Type the user name of the account to use when connecting to the database.
 - **Password:** Type the password for the account to use when connecting to the database.
5. Click **OK**.
6. Click **Database > Check Out**.
 - The Developer IDE connects to the database and presents a list of available scripts:



This indicates that the Developer IDE is properly configured. You can click **Close**, and then exit the Developer IDE.

About the workspace

The workspace in the AlarmPoint Developer IDE is divided into two panes:

- **Workspace pane:** The area on the left side of your screen displays a list of your current Script Packages, and a collapsible view of each package's versions and scripts.
- **Scripting pane:** The area on the right side of your screen displays a separate pane for each script on which you are currently working. It is in these panes that you can add and edit the code for each script.

You can drag the border between the panes to resize them.

Saving your workspace

You can save your progress at any time by saving the state of your workspace. This does not save your scripts and Script Packages to the database, but allows you to restore your workspace at another time, or to revert to the current state.

To save your workspace:

1. In the Workspace pane, select the Workspace folder.
2. Click **File > Save All**.

Once you have saved your workspace, you can restore to the saved state at any time by clicking File > Revert. Note that this will discard any changes since the last time you saved your workspace.

Note: *For complete information about using the AlarmPoint Developer IDE, refer to the AlarmPoint Developer's Guide & Scripting Reference.*

Scripting example

The following code sample is taken from the “default” Script Package, and defines the subject line for all email notifications sent by AlarmPoint:

```
IF ($content.deviceclassification == "email")
    $content.subject = "AlarmPoint Message: " & $event.incident_id
```

In this case, once AlarmPoint determines that the notification is being sent to an Email Device, it sets the subject line to the default text for all AlarmPoint email notifications, which would resemble the following:

AlarmPoint Message: 3445

You can change the default subject line for email notifications by using the AlarmPoint Developer IDE to edit the Action Scripts. In the following example, the default script has been edited so that each email message subject line includes the severity of the event, in addition to the Incident ID:

```
IF ($content.deviceclassification == "email")
    $content.subject = "AlarmPoint Message: " & $event.incident_id &
    " Severity: " & $event.severity
```

The email message subject line for an AlarmPoint notification will now resemble the following:

AlarmPoint Message: 3445 Severity: CRITICAL

Configuration Variable Reference

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

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*

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 69.*

Variable	Description
<code>\$force_fyi = “disable”</code>	Forces notifications to be informational only rather than requiring responses. Possible values are: <ul style="list-style-type: none"> • disable: nothing is forced. • on: notifications are forced to be FYI. • off: notifications are forced not to be FYI.
<code>\$use_email_for_fyi = true</code>	Configure Device filters for informational-only (FYI) notifications. Setting these flags to <code>false</code> prevents that Device type from being notified with informational (FYI) messages.
<code>\$use_im_for_fyi = true</code>	
<code>\$use_text_phone_for_fyi = true</code>	
<code>\$use_text_pager_for_fyi = true</code>	
<code>\$use_numeric_pager_for_fyi = true</code>	
<code>\$use_generic_for_fyi = true</code>	

Variable	Description
<code>\$enable_subs = true</code>	Enables Subscription functionality. If set to <code>true</code> , Users subscribed to criteria matching the event will be notified. If set to <code>false</code> , no subscribed Users will be notified even if they match the criteria of the event.
<code>\$subscription_fyi = true</code>	<p>Forces Subscription notifications to be informational only; recipients of a Subscription notification will not be able to respond to the event.</p> <ul style="list-style-type: none"> • Note: If the <code>\$use_phone_for_fyi</code> flag is set to <code>true</code>, a User can respond with “delete”, which removes the notification from the phone queue, “save”, which moves to the next notification without deleting, or “repeat”, which replays the notification. <p>The <code>\$force_fyi</code> flag also forces subscriptions to be informational only. If both the <code>\$force_fyi</code> flag and the <code>\$subscription_fyi</code> flag are set to <code>false</code>, AlarmPoint will use the FYI flag submitted with the event from the Management System.</p>

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 “Creating a Fail-Safe Group” on page 18.*

Variable	Description
<code>\$fail_safe = “enabled”</code>	<p>Controls whether the fail-safe recipient is notified, and under which circumstances. Possible values are:</p> <ul style="list-style-type: none"> • 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.
<code>\$fail_safe_group = "NNMi FailSafe"</code>	Identifies the fail-safe recipient, which is typically a Group, but may be a User.

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.

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.
\$main.use_logFile = false	Specifies whether to use an alternate log file for debugging messages. This variable is ignored unless <code>\$main.debug</code> is also set to true.
\$main.logFile = “../logs/HP_NNMi_Script.log”	Defines the file used to log debugging information (only if <code>\$main.use_logfile</code> 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.

Variable	Description
\$main.annotate = true	<p>Enables submission of information back to the Management System.</p> <p>Information is logged throughout the script progress; if this variable is set to <code>true</code>, these logged messages will be annotated to the originating Event. Setting this variable to <code>false</code> may improve performance, but will make debugging difficult as some information may not be annotated to the originating event.</p>
\$main.subscription_annotate = false	<p>Enables submission of Subscription information back to the Management System. (As with <code>\$main.annotate</code>, but specifically for Subscription information.)</p> <p>Most Subscriptions are informational only; this variable can be enabled, for debugging and informational purposes but may reduce performance.</p>
\$main.enable_HTML_Email = true	<p>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.</p>
\$AlarmPoint_URL = "http://localhost:8888"	<p>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.</p>
\$main.HTML_form_url = \$AlarmPoint_URL & "/jsp/ProcessNotificationResponse.jsp"	<p>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.</p>
\$main.use_logo = true	<p>Specifies whether HTML email notifications will display the AlarmPoint (or custom) logo.</p>
\$main.logo = \$AlarmPoint_URL & "/static/images/logos/alarmpoint/UNKNOWN.gif"	<p>Specifies the path to the graphic displayed on HTML (email and BES) notifications.</p>

Variable	Description
\$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.]”	<p>The alternate text to display if the HTML email logo is unavailable.</p> <p>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).</p>
\$main.numeric_pager_number = “555-1212”	<p>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.</p>
\$main.nnmi_incident_url = "http://localhost:8004/IncidentBeanService/IncidentBean"	<p>Specifies the URL and port for the NNMi Incident Web Service Bean.</p> <p>Note: To determine the port used by your NNMi installation, see “Identifying your NNMi port” on page 15.</p>
\$main.nnmi_username = "webservices"	<p>Specifies the user name of the NNMi Web Service Client.</p>
\$main.nnmi_password = "nnm"	<p>Specifies the password of the NNMi Web Service Client.</p>

Chapter 9: Optimizing the Integration

This section describes some of the available methods you can use to optimize or extend AlarmPoint Express for HP NNMi. The instructions in this section are intended for more experienced AlarmPoint Administrators.

Configuring the Subscription JSP

The included custom Subscription panel reads the Source Node Name list values from NNMi 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 manually populate the predicate list values:

1. Open the `NNMiSubscriptionForm.jsp` found in the `\webservers\webapps\cocoon\alarmpoint\jsp\subscription\nnmi` folder on the AlarmPoint Webserver install.
2. Set the Boolean variable `QUERY_SOURCENODE_PREDICATE_VALUES` found on line 28 to `false`.
3. Save and close the `NNMiSubscriptionForm.jsp` file.
4. In AlarmPoint, click the **Developer** tab.
5. On the Event Domains page, click **hp_nnmi**.
6. On the Event Domain Details page, click **SOURCENODENAME** in the Predicates list.
7. Add to the predicate list values.

The `SOURCENODENAME` list 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 NNMi through Web Service Calls rather than the predefined predicate list values, you must configure the connection properties within the Subscription JSP.

To configure the Subscription JSP to connect to NNMi through Web Services:

1. Open the `NNMiSubscriptionForm.jsp` found in the `\webservers\webapps\cocoon\alarmpoint\jsp\subscription\nnmi` folder on the AlarmPoint Webserver install.
2. Within the Subscription JSP, locate the following section:

```
final String NNM_NODE_SERVICE_WS_URL = "http://localhost:8004/  
NodeBeanService/NodeBean";
```

```
final String NNM_WS_USER = "webservices";
final String NNM_WS_PASSWORD = "nnm";
```

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

Parameter	Value
NNM_NODE_SERVICE_WS_URL	The URL and port for the NNMi Web Services NodeBean. For information on how to determine the correct port setting, see “Identifying your NNMi port” on page 15.
NNM_WS_USER	User name of the NNMi Web Service Client.
NNM_WS_PASSWORD	Password of the NNMi Web Service Client.

4. Save and close the JSP.

Note: *The NNM_WS_USER and NNM_WS_PASSWORD must match the User configured in NNMi, as described in “Create a Web Services Client” on page 23.*

Adding data elements

Additional data elements can be forwarded to AlarmPoint by adding them to the command line call for a particular incident.

Any changes to the parameters passed with the execution of the Command for Automatic Action must be considered in the AlarmPoint Java Client parameter mapping and the Alarmpoint Action Scripts.

For each new parameter to be passed from NNMi to AlarmPoint, add a new line to the `hp_nnm.xml` mapping file similar to the following:

```
<parameter index="13" type="string">custom_parameter</parameter>
```

The new parameter may then be used within the AlarmPoint Action Scripts. A possible use for the variable would be to incorporate it in the notification content of a Device by adding the `$custom_parameter` to the presentation script within the Device’s content creation block:

```
$content.message = $content.message & "Custom Field : " &
$event.custom_parameter
```

Response choices

The following response choices are available in this integration:

Response	Description
Acknowledge	User takes ownership of the incident, preventing further notifications to other Users. (The exception is subscription FYI notifications, which are reporting on the service outage. These are not stopped until the problem has actually been solved.)
Ignore	Stops notifying the current User.
Set Priority Top	Sets the priority of the incident to Top. (Email and browser only)
Set Priority High	Sets the priority of the incident to High. (Email and browser only)
Set Priority Medium	Sets the priority of the incident to Medium. (Email and browser only)
Set Priority Low	Sets the priority of the incident to Low. (Email and browser only)
Annotate	Allows the User to append a message to the Notes field of the NNMI incident. (Non-HTML Email only)

Note: *Users responding with email Devices can add annotations to their responses, as described in “Adding Annotation Messages”, below.*

Adding Annotation Messages

Two-way email Device notifications (not FYI) can add extra annotations which will be appended to the NNMI Incidents Notes field. 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.

Changing response choices

Changes to the response choices and behavior can be changed in the response business script in the Action Script set. Actions available through Web Services Calls include acknowledging an incident, annotating it, and changing its priority. Any other response functionality for the integration must be configured within the response HANDLER script with NNMI-provided Web Services Calls.

As an example, the following code illustrates adding a response choice of "Be there in 10 minutes" to the integration:

AlarmPoint Action Scripts:

- Presentation script:

```
$content.choices::add( "be there in ten minutes" )
```

- Response script:

```
# Handle responses
$reply = $response.reply
$reply::toLowerCase()
$ten_minutes = $reply::startsWith( "be there in ten minutes" )
...
IF ( $ten_minutes )
    # Perform any changes to the AlarmPoint event and notifications
    here
    @event::delinkAll() # Consider the incident handled
    $main.continue = true
    ...
# Acknowledge Event on Management System
    GOSUB acknowledgeIncident
...

# Acknowledges the original NNM incident using a web service call,
changing the lifecycle state
acknowledgeIncident:
    @nnmiRequest = new NetworkNodeManagerScriptObject(
    $main.nnmi_incident_url,
        $main.nnmi_username, $main.nnmi_password )
    IF ( ! EXISTS($event.nnm_id) )
        $event.nnm_id =
    @nnmiRequest::getNNMIncidentId($event.incident_id)
    ENDIF
    $request_successful =
    @nnmiRequest::acknowledgeIncident($event.nnm_id)
    IF ($request_successful != true )
        $err_msg = "Failed to acknowledge NNMi incident: " &
    $event.incident_id
        IF ( $main.debug )
            @script::log( $main.log_prepend & $err_msg )
        ENDIF
        @event::report( $err_msg )
    ENDIF
RETURN
```

Note: *This is only 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.*

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
```

FYI notifications

You can make all notifications informational only, meaning that 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
```

Generating FYI notifications for specific incidents

The FYI parameter is an optional parameter added to the end of the command line that can be passed from NNMi into AlarmPoint. If it is set to “yes” in the NNMi Event Configuration, any notifications generated for the event will be informational-only, and have no response choices.

To use this feature, change the Command for Automatic Action field to the following:

Windows:

```
c:\APAgent\APClient.bin.exe --map-data hp_nnmi bsmith $category  
$severity $family $lifecycleState $name $nature $priority  
$sourceNodeName $sourceObjectName $uuid yes
```

Unix:

```
/opt/alarmpointsystems/alarmpoint/APClient.bin --map-data hp_nnmi  
bsmith $category $severity $family $lifecycleState $name $nature  
$priority $sourceNodeName $sourceObjectName $uuid yes
```


Note that 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.

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, ensure that the configuration section of the initial PROCESS script has the following:

```
$subscription_fyi = true
```

The `$enable_subs` variable must also be set to true. See the section on configuration variables in the initial PROCESS script for details.

Note: *For more information about the variables in this section, see “Configuration Variable Reference” on page 60.*

Constructing HTML email notifications

You can configure AlarmPoint Express for HP NNMi to create HTML email notifications.

This feature requires the AlarmPoint Developer IDE, described in “Installing the AlarmPoint Developer IDE” on page 57.

To enable HTML email, the HP Network Node Manager i-series (Business) script package set must be checked into the Developer IDE Database.

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 HTML email:

1. Launch the AlarmPoint Developer IDE.
2. Check out the HP Network Node Manager i-series (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 `$AlarmPoint_URL` to the base URL of your AlarmPoint web server. (The default is `localhost`.)
4. Optionally, you can also do any of the following
 - Change `$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 can not 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 web server 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 60.*

Chapter 10: Contacting AlarmPoint

You can access the AlarmPoint Systems Web Site at <http://www.alarmpoint.com>. From this site you can obtain information about the company, products, support and other helpful information. AlarmPoint Standard, Professional, and Enterprise customers may also access the Customer Support Site from the main web page. This protected site contains current product releases, helpful hints, patches, release notes, a product knowledge base, trouble ticket submission areas and other helpful tools provided by AlarmPoint Systems, Inc.

AlarmPoint Systems, Inc.

4457 Willow Road, Suite 220

Pleasanton, CA 94588

Phone: 925-226-0300

Fax: 925-226-0310

Email: support@alarmpoint.com

Website: <http://www.alarmpoint.com>

Customer Support for AlarmPoint Express Users

For AlarmPoint Express support and information, visit <http://express.alarmpoint.com>.

The AlarmPoint Express site contains links to helpful tools, documentation, and other assistance specific to AlarmPoint Express users.



4457 Willow Road, Suite 220, Pleasanton, CA 94588
Toll Free: 800.861.3916 | Fax: 925.251.5730

Unit 6, Woking 8, Forsyth Rd., Woking, GU21 5SB, UK
Tel: +44 (0)1483 722 001 | Fax: +44 (0)1483 723 181

www.alarmpoint.com