# CA Automation Point

## Product Guide

Release 11.4

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

# CA Technologies Product References

This document references the following CA Technologies products:

- CA Automation Point
- CA Remote Console™
- CA OPS/MVS® Event Management and Automation
- CA Network and Systems Management (CA NSM)
- CA Software Delivery (USD)

# Contact CA Technologies

**Contact CA Support**

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

**Providing Feedback About Product Documentation**

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

# Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Added the AP Web Service Components (see page 45) section.
- Added the Export AP Rules To Local Components (see page 47) section.

# Contents

## Chapter 1: Introduction 9

## Chapter 2: How You Monitor Enterprise Systems 19

## Chapter 3: Event Management 31

## Chapter 4: Notification Overview 49

## Chapter 5: Notification Strategy 59

# Chapter 1: Introduction

This guide introduces you to CA Automation Point. By the time you have finished reading this guide, you will know how to install the product and have an overview of how it works. It is important to us that you feel comfortable with CA Automation Point before you begin to use it.

## Overview

CA Automation Point lets you perform a variety of essential tasks in various management areas, which are discussed in the following sections.

### Event Monitoring and Automation

In the areas of event monitoring and automation, you can do the following:

- Manage events from multiple platforms and devices
- Consolidate management of all host consoles from different systems, platforms, and devices into a central point
- Increase system availability by automating systems management and problem detection, notification, and resolution
- Initiate and automate the entire IPL/IML process.
- Simultaneously view and automate the following:
  - z/OS MCS consoles
  - JES3 console sessions
  - VTAM and CA Remote Console sessions
  - VM and VSE console sessions
  - TPF sessions
  - iSeries (AS/S400) sessions
  - Telnet, SSH, UNIX, LINUX, OpenVMS sessions
- Remotely view managed secured sessions from a Windows workstation through the Remote Viewer and the Web Message Viewer
- Capture messages and events from the Windows Event log
- Handle automation requirements using rules. Rules can be message-, time-, or command-based

- Handle the management of complex automation applications using REXX programming
- Export a message during rules processing to a customer-written function using a rules keyword
- Enable session-level and user-level security by leveraging Windows file security

## Notification and Escalation

In the areas of notification and escalation, you can do the following:

- Sound audible alarms when critical messages arise
- Automatically contact personnel over the telephone through sophisticated inbound and outbound voice communications, by playing either pre-recorded or dynamically defined messages for notification or escalation of critical events
- Send notifications to numeric and alphanumeric paging devices
- Send messages to and receive replies from two-way paging devices
- Send notifications using the following methods:
  - Email
  - Text-to-speech technology to remote workstations with sound cards
  - Implementation of notification policies through a secure notification website, excluding the need for REXX programming
- Provide corporate-wide access through a secure notification website for maintaining personal notification data

## Interface with Other CA Products

Through an interface with CA NSM, you can do the following:

- Create, manipulate, and delete objects in the CA NSM Common Object Repository
- Enable the communication of messages, commands, SNMP traps, and notification requests to and from the CA NSM Event Management component
- Automatically populate icons on the CA NSM WorldView map that represent the CA Automation Point server and its selected sessions
- Directly interface with the CA OPS/MVS Multiple-System Facility (MSF) using TCP/IP communication technology

# Console Consolidation

Today, many companies find that their mission-critical computer systems are spread over several locations. Even if your company is not particularly large, and has not grown by acquisition or merger, you may have several data centers that are physically separated from each other and possibly distant from some of the people who need to operate them.

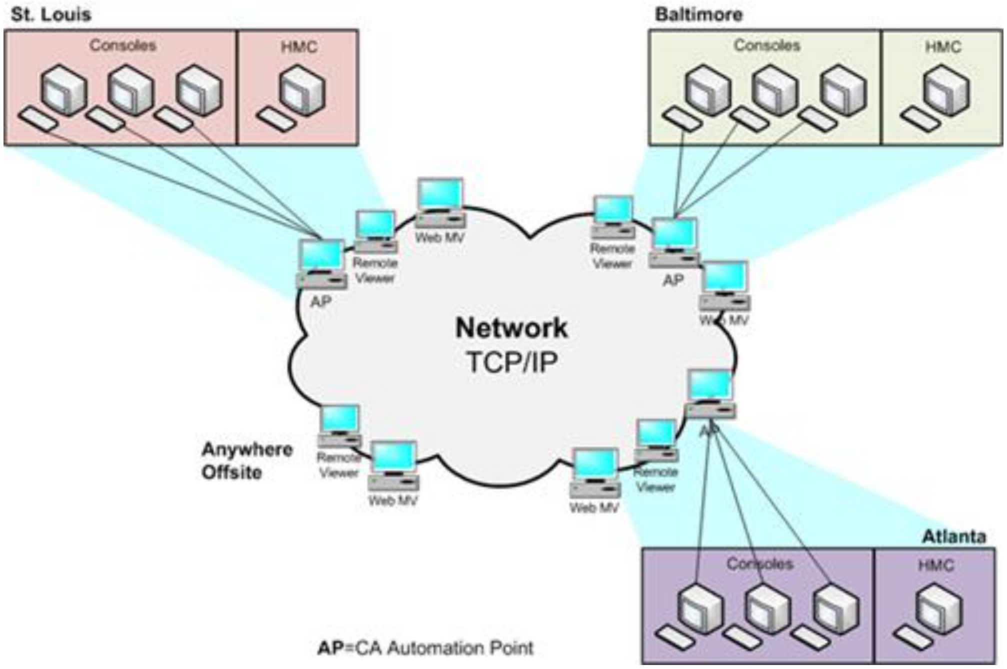
With CA Automation Point, operators can monitor messages across multiple heterogeneous host systems and display them in a single focal point window for easy operator viewing. Operators are alerted to problems quickly, and actions can be taken to reduce impact on affected systems before the problems escalate, saving both time and money.

## How Console Consolidation Works

Using CA Automation Point, you could respond to the problem of multiple sites as follows:

- **Consolidate alerts.** Since you typically want to interact with a system in response to a problem, it is inefficient to have to inspect each system for those problems. Collecting the alerts provides a starting point for managing your various systems on a priority basis.
- **Coordinate activity across systems.** Your order entry system may be tightly tied to your distribution system. Responding to a problem may require interacting quickly with more than one system to address the real problem plaguing your enterprise.
- **Use a centrlized notification application.** When you need some outside expertise, you typically use your telecommunication facilities to contact an expert - phone, pager, and so on. You should feed problems from all systems into such a notification mechanism, not through a data center that happens to have the connection to your paging service provider.
- **Group systems by function or type.** Once you have access to all of your enterprise, you can group systems in a fashion meaningful to your site. You can group by a system type (such as z/OS, VAX, or UNIX), or you can group by the function performed (such as all systems involved in your payroll system, or your billing system).

The following illustration shows a sample end result of this console consolidation. (We will revisit this illustration later.)



## Multiple Monitored Systems

CA Automation Point can collect and consolidate messages from multiple software consoles. After you designate which console sessions CA Automation Point controls, the product collects highlighted and non-highlighted messages from each controlled session, displays each type of message in a separate window, and combines both types of messages in a single Merged Msg window. Operators can be alerted to problems or changing conditions as follows:

- Displaying important messages in a variety of colors
- Sounding audible alarms when critical messages appear
- Printing selected messages on the workstation printer to create a hardcopy log
- Preserving selected messages in log files
- Displaying selected system data graphically in real time through dedicated plot windows

Operators can issue commands directly to any connected host system. Because the product can be simultaneously connected to multiple host systems, you can also coordinate activities among the systems or pass messages between them.

## Graphical User Interface for Configuration

Using a graphical user interface tool, you can do the following:

- Specify session and communications settings
- Set customizable options for each component of CA Automation Point
- Obtain directed help through use of online guides and help systems provided in specific easy-to-use formats
- Use a directory structure that separates site-created or site-edited files from the files that are distributed with the product

# CA Automation Point Environment

CA Automation Point provides event monitoring and automation to help you manage systems and operations at your data center.

## Primary Monitoring Capabilities

The primary monitoring capabilities provided by CA Automation Point include:

- Watching for organized data streams of information referred to as *messages*
- Processing messages through user-specified predefined rules
- Sending commands to platforms under the product's control (often in response to the processed messages' need to initiate an action)

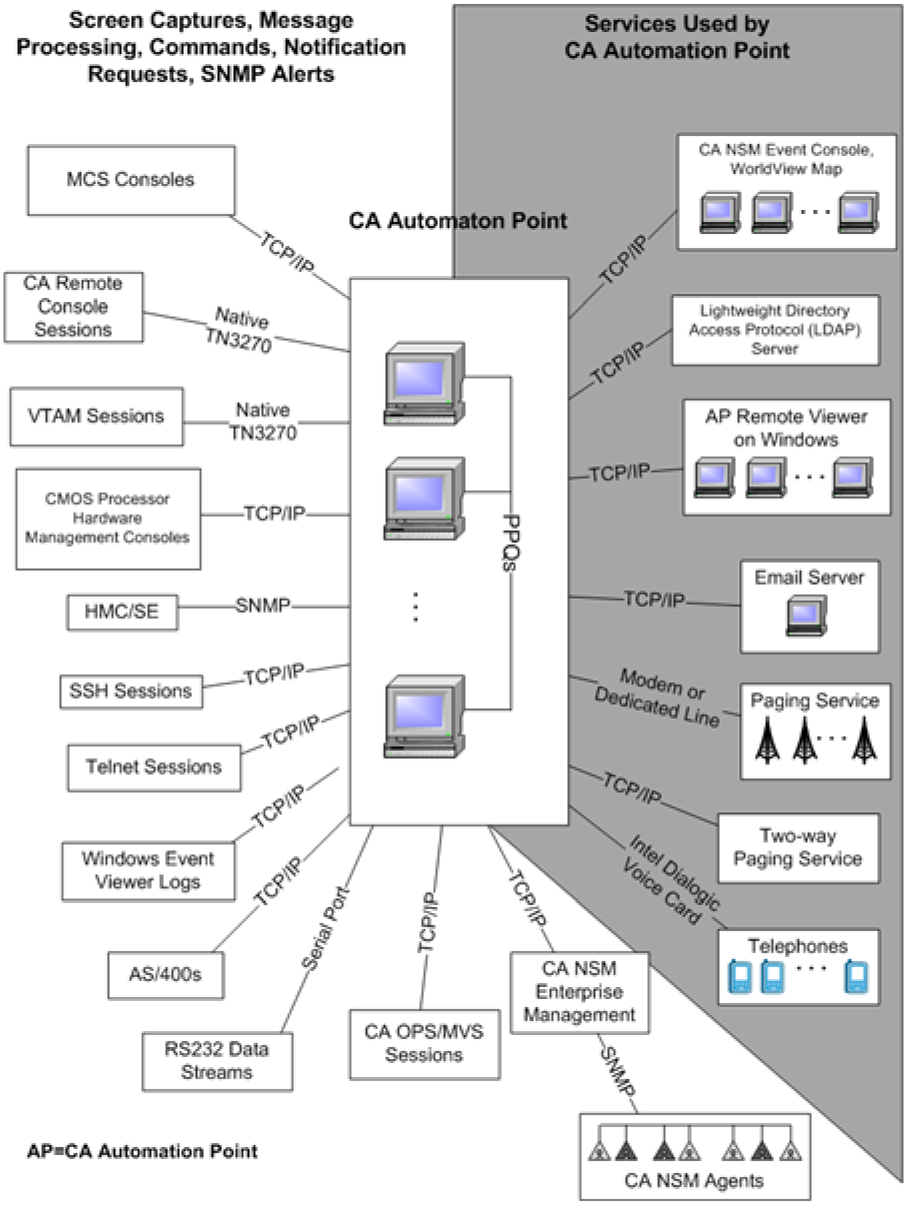
## CA Automation Point Servers

The number of CA Automation Point servers you choose to run depends on the following:

- The location of the monitored platforms
- The number of platforms monitored
- The quantity of message or data stream activity
- The extent you use the product's notification capabilities
- Your need for backups to the CA Automation Point servers
- The processor speed and size of RAM on each workstation

## Common Platforms

The following illustration shows the common platforms (and other externally generated data streams) that CA Automation Point is capable of monitoring. It also shows the various services used by the product for notifying data center personnel of problems, securing product functions, or remotely accessing the CA Automation Point servers.


Screen Captures, Message Processing, Commands, Notification Requests, SNMP Alerts
Services Used by CA Automation Point
CA Automaton Point
MCS Consoles
TCP/IP
CA Remote Console Sessions
Native TN3270
VTAM Sessions
Native TN3270
CMOS Processor Hardware Management Consoles
TCP/IP
HMC/SE
SNMP
SSH Sessions
TCP/IP
Telnet Sessions
TCP/IP
Windows Event Viewer Logs
TCP/IP
AS/400s
TCP/IP
RS232 Data Streams
Serial Port
CA OPS/MVS Sessions
TCP/IP
CA NSM Enterprise Management
TCP/IP
SNMP
CA NSM Agents
PPQs
CA NSM Event Console, WorldView Map
TCP/IP
Lightweight Directory Access Protocol (LDAP) Server
TCP/IP
AP Remote Viewer on Windows
TCP/IP
Email Server
TCP/IP
Paging Service
Modem or Dedicated Line
Two-way Paging Service
TCP/IP
Telephones
Intel Dialogic Voice Card
AP=CA Automation Point

# Components

The following CA Automation Point components work together to provide automation, event monitoring, and notification capabilities.

**CA Automation Point Desktop**

Displays and manages CA Automation Point sessions using your workstation's graphical user interface

**Configuration Manager**

Enables you to configure various CA Automation Point functions and services. It is composed of two interfaces:

- The Wizard Interface, which you can use to initially set up your site configuration
- The Expert Interface, which you can use to fine tune CA Automation Point

**Notification Server**

Services all notification requests from the VOX client command environment, manages the interaction of the VOX environment with the workstation's notification facilities (voice card, paging services, and email), and returns result information to the VOX client command environment.

**VOX Client**

Provides remote connectivity from one CA Automation Point Server to the Notification Server component running on another remote CA Automation Point server machine.

**Notification Manager**

Helps you implement automated notification policies in your operations. Notification methods can include paging, email, text-to-speech, voice notification, solicitation of input through DTMF tones, pre-recorded messages, message forwarding, and combinations of these functions.

**PPQs**

Provides a means for REXX programs to communicate with each other even if they are running on different computers.

**Notification Website**

Lets you to manage (create, edit, view, and delete) the methods, contacts, schedules, and login names used with Notification Manager.

**Web Message Viewer**

Provides a common, remotely accessible message window from which you can view all of the messages received and processed through rules by CA Automation Point in as close to real time as possible.

**Remote Viewer**

Provides access to sessions that are managed by CA Automation Point from a remote workstation.

**Speech Notification Client**

Receives text-to-speech notification requests that are sent from the CA Automation Point server machine.

# Interfaces to Companion Products

The following interfaces to companion CA products can be installed with CA Automation Point.

## CA OPS/MVS Interface

The CA OPS/MVS Interface supplies a direct interface to the CA OPS/MVS Multiple-System Facility (MSF) using TCP/IP communication technology. MSF can be used to interface with multiple copies of the product running on different z/OS images (such as z/OS and z/OS.e), and offers two-way communication using CAICCI services.

## CA NSM WorldView Map Interface

Through its WorldView Map, CA NSM provides ways to manage complex enterprise environments on a high level. Using the ADDRESS TNG environment, you can access the objects contained in the Common Object Repository for CA NSM and perform various management tasks.

## CA NSM Event Manager Interface

The Event Traffic Controller provides an interface between CA Automation Point and the Event Manager component of CA NSM, letting you control the flow of event traffic between the two products.

**Note:** These interfaces do not need to be installed on the CA Automation Point server machine if CA NSM is already installed on the machine.

# Product Documentation

The CA Automation Point manuals are provided in portable document format (PDF) and in HTML format accessible from the CA Automation Point Bookshelf provided on the product DVD. This bookshelf is also available at CA Support Online (http://www.ca.com/support).

# Chapter 2: How You Monitor Enterprise Systems

Today's eBusiness applications are often complex and deployed in multi-tier, multiplatform configurations. Due to mergers and acquisitions, independent business units, and the heterogeneous nature of a corporation's computer platforms, today's businesses often find that their mission critical computer systems are spread over several locations. In addition, business transactions are increasingly initiated through the Internet. All of this creates the need for an efficient, simplified approach to enterprise management. CA Automation Point provides a response to that need with intelligent, single-point monitoring of disparate platforms and application servers, along with outstanding notification capabilities.

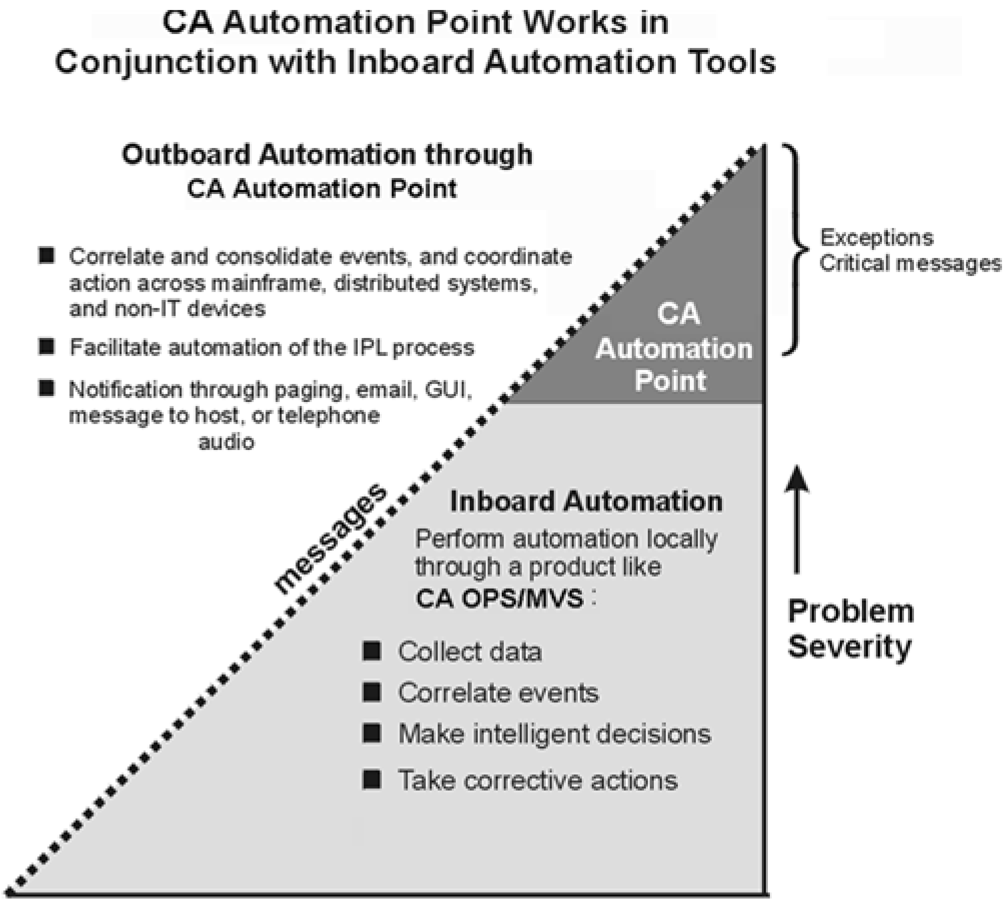
CA Automation Point provides this solution by supporting connections to a variety of host systems and consolidates them to a single workstation desktop. It simplifies your complex environment by focusing on your specific monitoring needs through the flexibility provided by its outboard automation feature.

In addition to its automation features, CA Automation Point has a suite of notification capabilities, including paging, telephone, email, and text-to-speech, as well as network message pop-ups. For more information on notification and Notification Manager aspects of CA Automation Point, see the chapters on these topics later on in this guide. This chapter focuses on outboard automation, which is the basis for the complete solution that CA Automation Point offers.

# Outboard Automation

Two types of automation-inboard and outboard-must be implemented to monitor systems most efficiently. Inboard automation is performed locally and involves actions on the local platform. Outboard automation provides a much more comprehensive type of automation that targets exceptions and the most critical problems. Outboard automation does not replace inboard automation, but complements it. Inboard automation products such as CA OPS/MVS on the z/OS platform can manage 90% or more of all messages, leaving exceptions and critical messages that require further analysis and action for outboard automation. Outboard automation is a primary feature of CA Automation Point.

The following illustration depicts the inboard/outboard automation concept:


CA Automation Point Works in Conjunction with Inboard Automation Tools
Outboard Automation through CA Automation Point
■ Correlate and consolidate events, and coordinate action across mainframe, distributed systems, and non-IT devices
■ Facilitate automation of the IPL process
■ Notification through paging, email, GUI, message to host, or telephone audio
CA Automation Point
Exceptions
Critical messages
messages
Inboard Automation
Perform automation locally through a product like CA OPS/MVS :
■ Collect data
■ Correlate events
■ Make intelligent decisions
■ Take corrective actions
Problem Severity

As you read the following sections and view the illustrations, keep in mind the following questions concerning CA Automation Point and its outboard automation capabilities.

- Can CA Automation Point connect to all of the platforms that need to be monitored? How do you make these connections?
- Can CA Automation Point control mainframe HMC (processor) consoles as well as operator consoles?
- Can CA Automation Point manage non-CPU devices such as computer room environmental systems through RS232 connections?
- How are host console images displayed and controlled by CA Automation Point?
- Can you use CA Automation Point to replace and consolidate existing consoles?
- Can CA Automation Point analyze and respond to events that occur on the hosts it is connected to?
- Can CA Automation Point read console messages, run them though automation for possible action, and issue commands to the various host systems where necessary? If so, how does it do this?
- Does CA Automation Point allow remote access so that you can monitor the various hosts from a dial-up connection or web browser?
- Can you issue remote commands to control the hosts?
- What kind of authentication is required before permitting remote access, and how is that security administered?

When you have finished reading this chapter, you not only will have learned the answers to these specific questions, but you also will be aware of a solution to the broader problem of how to simplify the complexity of your enterprise environment and meet your monitoring needs.

## Connections Under CA Automation Point

CA Automation Point correlates and consolidates events and coordinates actions across mainframe systems, distributed systems, and non-IT devices. You can connect the workstation on which CA Automation Point runs to a system almost anywhere that you would connect a terminal as a processor console, software console, VTAM terminal, or workstation. CA Automation Point monitors systems through remote connections to those systems. The remote connection to the monitored system is normally through a bisynchronous or asynchronous physical connection or a LAN connection. Once connected, CA Automation Point can be set up to monitor the system data stream, or it can function solely as a terminal emulator. These connections are referred to as sessions.

# Session Types

A session is a link to a host console or to a CA Automation Point function. CA Automation Point displays each session in its own window. There are two types of sessions.

- Terminal emulator sessions
- CA Automation Point function windows

**Note:** The session window is for the convenience of the operator. CA Automation Point can automate the session without a window.

## Terminal Emulator Sessions

Using terminal emulator sessions, you can view various host console screens from windows on your workstation. You can configure CA Automation Point sessions in multiple ways, so your session configurations can reflect the tasks an operator currently needs to perform. A CA Automation Point workstation can have multiple terminal emulator sessions running on it concurrently. You can define these sessions for your site, and then monitor and control them from CA Automation Point windows.

## Function Windows

CA Automation Point function windows let you view different types of information from windows. You use these windows to monitor and control CA Automation Point processing. For example, you can use a window to view and act upon highlighted messages displayed by the host console.

## Connection Types

CA Automation Point supports a wide variety of simultaneous connections to both mainframe systems and asynchronous-type host systems without requiring any software to be installed on the host system.

The following list shows the connections available with CA Automation Point. Note that the connection type affects how CA Automation Point communicates to the monitored host and how it detects messages.

**3270**

- **TN3270 session** - TCP/IP connection to a TN3270 server

**Asynchronous**

- **RS-232 Session** - cable connection, through serial (com) port
- **Telnet session** - TCP/IP connection
- **SSH session** - TCP/IP connection

**Windows Command Prompt**

- **VIO session** - Virtual I/O connection

If your system can communicate through one of the connections that are illustrated above, CA Automation Point can communicate with your system. For example, suppose that you want to know if CA Automation Point can connect to an AIX system. Or you have a system with an HP2625 terminal on its console, and you want to know if CA Automation Point can automate that system. Look at the connections in the illustration; if the particular system that you want to connect to CA Automation Point can communicate using one of the methods listed, then your answer is yes.

The following sections provide quick reference lists of console types and terminal types that CA Automation Point supports.

### Console Types

CA Automation Point can control the following types of consoles:

- Asynchronous consoles, including VAX, Tandem, and DataFrame consoles
- MCS consoles
- JES3 consoles
- Sessions for CA Remote Console
- Sysplex consoles
- TPF consoles - 3270 and asynchronous
- VM consoles
- VSE consoles

## Terminal Types

The following lists describe the kinds of terminal emulation that you can use for your sessions.

**3270 Sessions**

- 3278 Model 2 (24x80
- 3278 Model 3 (32x80)
- 3278 Model 4 (43x80)
- 3278 Model 5 (27x132)
- 3279 Model 2 (24x80)
- 3279 Model 3 (32x80)
- 3279 Model 4 (43x80)
- 3279 Model 5 (27x132)

**Asynchronous Sessions**

- Tandem 6530 (conversational or block mode)
- VT52 terminal emulation
- VT100 terminal emulation
- VT320 terminal emulation
- An asynchronous (ASCII TTY) terminal

**Windows Command Prompt Sessions**

- VIO

### TN3270E Connection Support

One of the principle functions of CA Automation Point is to provide outboard monitoring and automation of mainframe systems. This is done by establishing 3270 connections to the mainframe host.

To meet connectivity requirements for currently supported 3270 console controllers, CA Automation Point provides native support for TN3270E connections.

## Session Configuration

You can easily configure your sessions using the Session Definition Sets dialog in the Configuration Manager graphical user interface. Defaults are incorporated into the dialogs, and if you omit a value for an option that is required, you are reminded before you leave the dialog. What's This? help is available for fields to help you choose among optional values.

# Remote Access

Remote access capabilities are of great value to your data center, particularly at these times:

- When the proximity of the CA Automation Point Server to monitored systems (when direct connections are used) or to telephony equipment makes human access inconvenient
- When an operator control room is geographically separated from the enterprise servers, including CA Automation Point servers

CA Automation Point supports secured remote access to any of the systems to which it is connected-even across multiple CA Automation Point servers-providing geographic and off-hours flexibility for operator access to systems.

CA Automation Point provides two tools for remote access:

- The Remote Viewer
- The Web Message Viewer (Web MV)

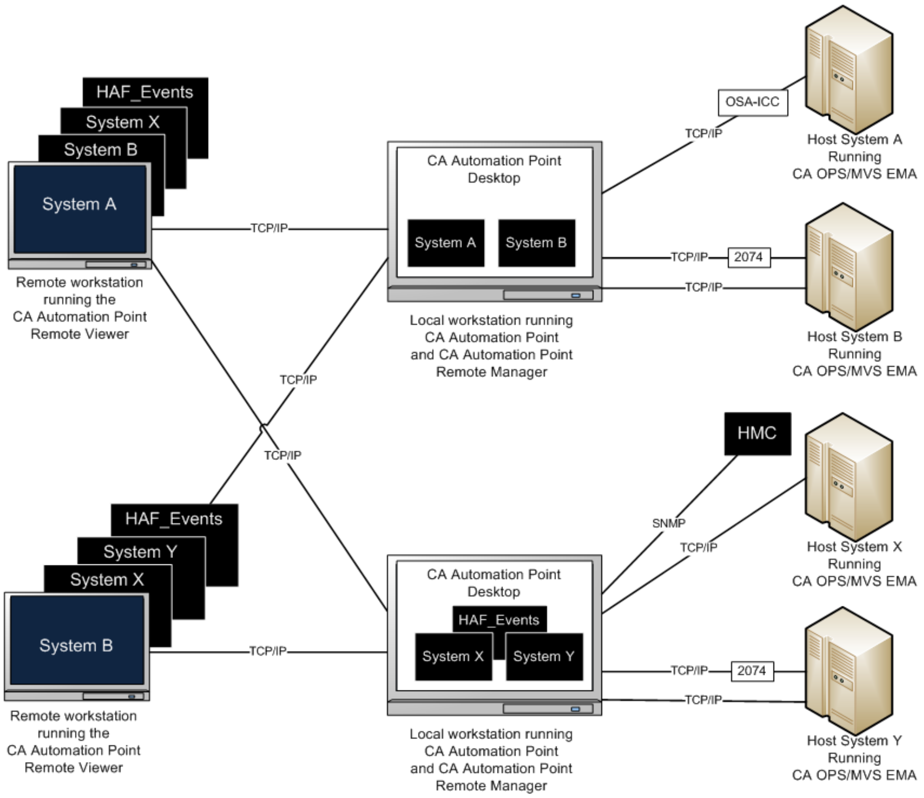
## Remote Viewer

The CA Automation Point Remote Viewer lets you access and control sessions that are running on CA Automation Point workstations at remote sites. Through a TCP/IP connection, the Remote Viewer enables one or more users to simultaneously connect up to 200 sessions from any number of CA Automation Point engines connected to the network. The Remote Viewer is a separately installable client component. It provides session-level security, logon, and auditing capabilities by mapping sessions to Windows file security.

You can perform the following actions with the Remote Viewer:

- Remotely view CA Automation Point host sessions
- Send commands to monitored CA Automation Point sessions
- Shut down and restart CA Automation Point remotely
- Submit REXX programs for execution on the CA Automation Point server machine

The following diagram shows how each remote viewer simultaneously displays sessions from each host.


HAF_Events
System X
System B
System A
Remote workstation running the CA Automation Point Remote Viewer
TCP/IP
CA Automation Point Desktop
System A
System B
Local workstation running CA Automation Point and CA Automation Point Remote Manager
OSA-ICC
TCP/IP
Host System A Running CA OPS/MVS EMA
TCP/IP
2074
TCP/IP
Host System B Running CA OPS/MVS EMA
TCP/IP
TCP/IP
HMC
SNMP
TCP/IP
Host System X Running CA OPS/MVS EMA
HAF_Events
System Y
System X
System B
Remote workstation running the CA Automation Point Remote Viewer
TCP/IP
CA Automation Point Desktop
HAF_Events
System X
System Y
Local workstation running CA Automation Point and CA Automation Point Remote Manager
TCP/IP
2074
TCP/IP
Host System Y Running CA OPS/MVS EMA

After you are connected to the CA Automation Point Server, you can choose any session or window to view. You can display multiple windows on your remote PC all at one time. Essentially, you can recreate the CA Automation Point server windows that are on a remote machine.

## Web Message Viewer

The Web Message Viewer (Web MV) is a web-based message-oriented application for viewing managed CA Automation Point sessions. It uses TCP/IP to connect to the CA Automation Point server, and is accessible from any machine running a Java-enabled Web browser. Since the applet runs in a web browser, there is no need for CA Automation Point software on your machine.

You can use the Web MV application to select which CA Automation Point sessions to monitor.

Web MV provides a common, remotely accessible message window that lets you view all of the messages received by CA Automation Point in as close to real time as possible. These include not only the messages received from CA Automation Point-managed sessions, but also messages generated by CA Automation Point.

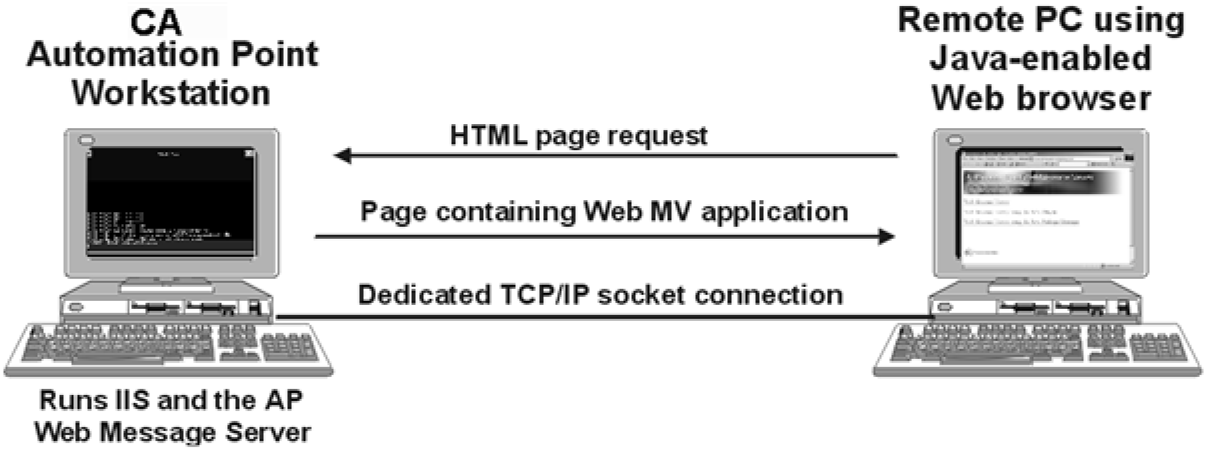
In addition to viewing CA Automation Point messages, you can also use Web MV to access detailed information about each message, separated into logical columns and displayed according to your specification. You can also specify the number of messages you want to store in a database, and scroll back as far as you need to view previous messages.

With Web MV, you can also:

- Set the visual attributes of messages (including color and font)
- Set the visual attributes of session windows (including background color, columns, and size)
- Send commands to monitored sessions
- Issue CA Automation Point DOM requests for action messages

## How Web MV Works

The following illustration shows how Web MV works:



1. You request the Web MV HTML page through the client Web browser.
2. From this page, you download and launch the Web MV application.
3. The Web MV application uses TCP/IP to connect to the CA Automation Point server from which it was launched.

4. You select which CA Automation Point sessions to monitor.
5. TCP/IP is used to transport both HTML page requests and messages captured from web-enabled CA Automation Point sessions.

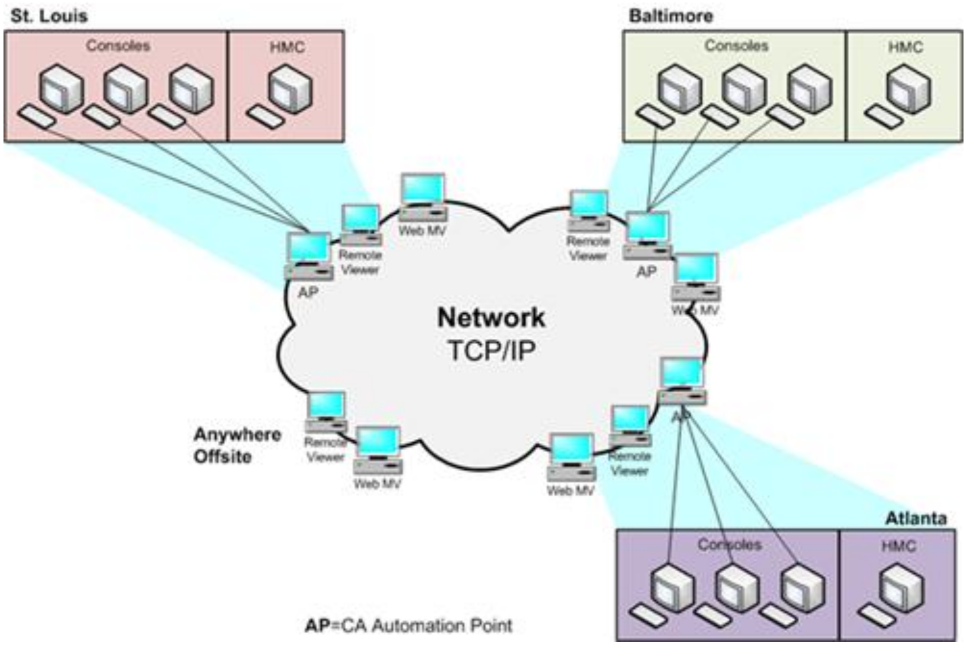
## The Web MV Interface

The main window of the Web MV interface has three separate areas:

- The Action Messages table, which displays DOMable action messages
- The Normal Messages table, which displays action and normal messages
- The Command area, which you can use to issue session commands or change the currently monitored session

## How Remote Access Provides Flexibility

The following graphic expands upon the preceding console consolidation illustration, showing you the flexibility achieved through remote access to any of the consoles on any of your data centers.



# Security

With the Remote Viewer and Web MV you have a great deal of concentrated power. To secure that power, CA Automation Point validates both the Remote Viewer and Web MV through the use of the Remote Manager service, which is a CA-provided service that runs on Windows. You can select your level of security, either by specifying a list of trusted hosts (including localhost for Web MV), or through user login security (either no user security or Windows security).

You select the level of security using the Remote Viewing dialog in Configuration Manager.

## User Login Security

CA Automation Point uses the following security levels for remote access.

- No User Security

  If you choose No User Security for login security, the user login (ID and password) is not verified. Session-level security is determined by the value set in the Permission Level field for your session.

- Windows Security

  Choosing Windows Security for login security means that you want to use the Windows security system to enforce user access privileges. The user login is verified on the host machine or domain, if specified. Session-level security is determined by the value set in the Permission Level field for your session. Session-level security by user is optionally determined by mapping session permissions to file permissions.

# How CA Automation Point Automates the IPL Process

A crucial capability related to outboard automation is the ability to automate the IPL process.

CA Automation Point can display and automate the startup process for mainframe or distributed systems. Inboard automation applications (like CA OPS/MVS on z/OS) cannot control these startup processes because their environment is not available until the operating system has completed its startup.

CA Automation Point can establish and control *software console* full-screen sessions with the mainframe. This capability lets CA Automation Point initiate and automate (from the software console) the IML/IPL process. For CMOS mainframe processors, CA Automation Point Point can initiate the IML/IPL process through a distributed REXX program. This program communicates, through SNMP, requested IML/IPL functions to the CMOS processors-just as the HMC (Hardware Management Console) GUI application does.

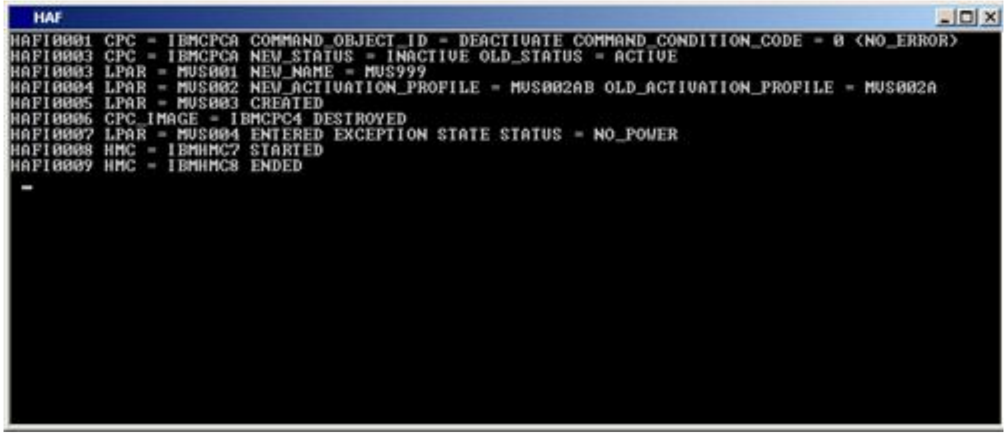
# How You Monitor HMC

You can monitor the Hardware Management Consoles (HMC) at your site through the CA Automation Point Hardware Automation Facility (HAF) feature. HAF extends CA Automation Point use of the HMC, moving in step with the IBM vision for the future of systems consoles. HAF collects all event and status, hardware-related messages sent to an IBM or Amdahl (Fujitsu IT Holdings) HMC from a CMOS processor.

Even though the HMC is intended to provide an easy-to-use GUI interface, an operator must still drive the process. HAF actively monitors the HMC at your site, and you can use an asynchronous/memory session to view the messages that CA Automation Point receives. In addition to monitoring these messages from the HMC, you can write rules against these messages and use a REXX program distributed with CA Automation Point to direct your HMC to take actions.

HAF is easily configurable, using the same Configuration Manager GUI available for configuration of other CA Automation Point interfaces.

The following is an illustration of a HAF window collecting consolidated hardware messages from your HMCs.



```
HAFI0001 CPC - IBMCPCA COMMAND_OBJECT_ID - DEACTIVATE COMMAND_CONDITION_CODE - 0 <NO_ERROR>
HAFI0003 CPC - IBMCPCA NEW_STATUS - INACTIVE OLD_STATUS - ACTIVE
HAFI0003 LPAR - MVS001 NEW_NAME - MVS999
HAFI0004 LPAR - MVS002 NEW_ACTIVATION_PROFILE - MVS002AB OLD_ACTIVATION_PROFILE - MVS002A
HAFI0005 LPAR - MVS003 CREATED
HAFI0006 CPC_IMAGE - IBMCPC4 DESTROYED
HAFI0007 LPAR - MVS004 ENTERED EXCEPTION STATE STATUS - NO_POWER
HAFI0008 HMC - IBMHMC7 STARTED
HAFI0009 HMC - IBMHMC8 ENDED
 _
```

# What's Next?

In this chapter you learned how, by outboard automation, CA Automation Point simplifies the management of your enterprise. The next chapter describes how, through event management, you can achieve the high level of availability that is critical to eBusiness success.

# Chapter 3: Event Management

Today's requirements for managing your enterprise include detecting and monitoring events, data, messages, and alerts across multiple systems; evaluating these events; and controlling and coordinating the states and actions of multiple hardware machines, software, and people across place and time. This sounds like a difficult objective to attain, but CA Automation Point can help you achieve a high level of system availability that is critical to eBusiness success.

## Availability Management

The term *availability* in this context means managing system events through a single point of control, suppressing non-essential events, and bringing disparate platforms together. It means increased productivity and reduced down-time, and systems running when and where they should, saving time and money. The term *availability management* is increasingly associated with event automation tools, especially when these tools improve uptime percentages for eBusiness and other traditional online applications.

## Automation

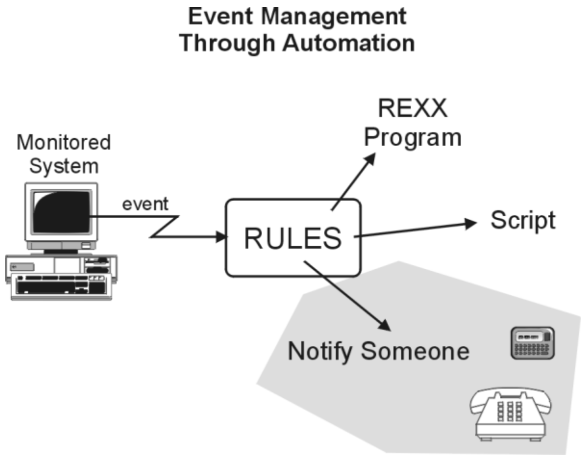
Event management through automation is the key to providing availability across systems. An event is an occurrence on your system at a particular place and time. Messages transmitted by an application, system, or device typify events in particular ways so that they can be managed. Through automation, you can suppress the non-essential messages, while at the same time act upon messages that require response. In addition, by using predefined corrective actions and notification techniques, you can respond proactively to problems and resolve them quickly.

CA Automation Point manages events by performing these operations:

- Detection-Monitors events, data, messages, and alerts
- Analysis-Evaluates and correlates the events it detects
- Action-Responds to events with predetermined actions such as:
  - Suppressing, highlighting, and rewording messages
  - Performing recovery procedures
  - Starting and stopping tasks of other resources
  - Restarting jobs, processes, or other resources

- Notification-Notifies personnel through various policies and procedures using the following:
  - Numeric and alphanumeric paging
  - Email
  - Text-to-speech audio messages
  - Windows popup messages
  - Voice:
    - Respond to queries through telephone keypad entries
    - Play prerecorded or dynamically built voice messages
    - Record and forward of voice messages

The following illustration shows how this process works:



The following sections describe how CA Automation Point manages events through rules, REXX programming, and integration with external event collection systems.

## How You Automate Using Rules

Through rules, CA Automation Point automates system tasks by managing messages and variables. Each rule specifies a message, group of messages, or time interval to which CA Automation Point responds. The CA Automation Point rules language allows CA Automation Point to detect and respond to system conditions automatically. Executing efficiently and using little system overhead, rules can handle about 80 percent of your automation needs, including automation for most time-sensitive operator tasks and for most message responses. Your rules can respond directly to system events or can invoke a CA Automation Point script or a REXX program to further automate tasks.

Through the CA Automation Point rules language, a variety of events can be specified for detection. When an event is detected, a rule can specify the action to be taken. This action can be as simple as issuing commands to the host system or displaying messages to an operator. An action can also include notifying someone to work on a problem by turning an icon red on the CA NSM WorldView Map or by calling, paging, or emailing someone. For more complex actions, you can specify a rule that initiates a REXX program.

**Note:** You can also send messages to the CA NSM Event Console to further consolidate information about critical events.

### Rule Types

CA Automation Point uses three types of rules:

- Message rules that tell CA Automation Point what action to take when a specified message appears on a console
- Time rules that tell CA Automation Point what action to take when a specified time or time interval occurs
- Command rules tell CA Automation Point what action to take when a user issues a specified command to a console

You can use the CA Automation Point rules action keywords to trigger a variety of actions. These actions occur in real time to control ongoing event management activity (such as logging and display). You can also use the REXX programming language and a rich set of command environments provided by CA Automation Point to perform a variety of complex tasks, including:

- Taking complex conditional actions with respect to event management
- Automatically issuing commands to connected systems
- Retrieving or storing data relevant to a REXX procedure
- Interfacing with the CA NSM WorldView Map and Event Console
- Interfacing with CA OPS/MVS
- Using the rich set of CA Automation Point notification services

## Rules Processing

Rules are loaded when CA Automation Point starts. Rules are then compiled for optimal runtime performance and checked for syntax errors. You can:

- Define rules for specific sessions.
- Write a rule or REXX program to reload rules dynamically without stopping and restarting CA Automation Point or disrupting monitoring activity. Loading an alternate set of rules from a different rules file may be useful as your workload changes from shift to shift.

For each automated session, CA Automation Point starts a rules processor to monitor the message stream for that session. Multiple, automated sessions are monitored concurrently by multiple rules processors. Each rules processor monitors the events defined in a common rules file.

## Rules Actions

CA Automation Point provides various action capabilities that can be triggered by rules processing to control the following types of activity:

- Synchronous activity that occurs and must complete in real time with the processing of each message
- Asynchronous activities set up in real time, but which do not restrict ongoing message processing

The action capabilities can be grouped into the following categories:

- **Display actions** that control ongoing attributes of the CA Automation Point depiction of monitored systems. These include the coloring, highlighting or lowlighting, prefixing, and rewording of received messages and controlling whether the received message is displayed in theCA Automation Point Merged Msg window.
- **Logging actions** that control the logging and printing of received messages. These actions control whether the message is sent to the CA Automation Point message log file or whether the message is printed on the local printer.
- **Notification actions** that control the following:
  - Notifying local operators with auditory alarming when a given event occurs
  - Issuing messages to either an operator or the automation log
  - Notifying someone remotely through Notification Manager
  - Forwarding messages, session information, or other user-specified data to the CA NSM Event Console

- **Automation actions**, which act as triggers and constraints on the execution of rules. In addition to the primary rule types of message pattern matching and time-of-day, you can use actions to do the following:
  - Control time intervals for rule execution
  - Control the maximum number of times a rule may execute absolutely
  - Control the maximum number of times a rule may execute in a fixed time interval

  **Note:** Conditional rule activity can also be controlled by data comparison.

- **System event actions** that let you automatically issue commands to:
  - The operating system of monitored systems
  - Applications running on monitored systems
  - The operating system of the CA Automation Point workstation
  - Reply to WTORs on monitored systems
  - Dynamically write and read status variables
  - Run basic command sequences to configure the behavior of monitored systems
  - Run complex procedural activity
  - Write messages or other important data to a Program-to-Program Queue (PPQ) for processing by a REXX program on the same or another workstation

## Automating with REXX Programs

CA Automation Point supports automation procedures written in the SAA-compliant REXX programming language. When responding to a message or automating a task requires a complex series of operator actions, you can write a REXX program to manage the response. Then, you can write a CA Automation Point rule to invoke the REXX program at some specific time or whenever a specific message appears.

REXX programs can automate long, command-intensive procedures such as logically partitioning a mainframe processor and IPLing the partitions. REXX programs also excel at automating the following tasks:

- Performing complex procedures to determine the proper response to a message
- Retrieving all of the information needed for automation

Either the operator or a CA Automation Point rule can start a REXX program.

**Note:** For more information about REXX programs, see the *Administrator Guide*.

## Uses of REXX Procedures

Through CA Automation Point, either you or your rules can initiate REXX programs to:

- Execute more complex automation logic when an automation task is too big for rules alone to handle, or when the automation task must include a wait.
- Automate consoles that CA Automation Point does not directly support.
- Notify someone through voice, paging, or e-mail to resolve a problem or address an outstanding situation.

## Command Environments

To enhance the usefulness of REXX-and CA Automation Point connectivity to other hardware and software, CA Automation Point allows lets your REXX programs access special command environments, including the following:

**ADDRESS AXC**

Used to communicate within the CA Automation Point environment and the console windows. This is the default environment for issuing command processors specific to CA Automation Point.

**ADDRESS CMD**

Used to execute operating system commands.

**ADDRESS GLV (global variables)**

Lets you to store status values while CA Automation Point is running in order to maintain consistent data across restarts.

**ADDRESS OPS**

Involves interaction with the CA OPS/MVS interface.

**ADDRESS PPQ (Program-to-program queues)**

Used for queuing information between processes and remote systems. It can be used locally and over a network.

**ADDRESS TNG**

Involves interaction with CA NSM using the CA NSM WorldView and Event Management interfaces.

**ADDRESS VOX**

Involves inbound and outbound voice processing, paging, and email.

**Note:** For information about accessing various command environments from REXX programs, see the *Reference Guide*.

# Integration with External Event Collection Systems

This section describes how integrating with external event collection systems allows flexibility in your data center.

## CA OPS/MVS Interface

To simplify CA Automation Point message-handling, we recommend that you use a mainframe-based automation product, such as CA OPS/MVS, to perform the following tasks:

- Limit much of the message traffic to the master console by either suppressing a message entirely or using route codes to limit the number of consoles displaying the message. This is especially important for highlighted messages.
- Monitor the status of the WTO buffers and clear the buffers if they begin to fill up. Sample rules are available for CA OPS/MVS for this purpose. (This is not necessary for RCS sessions, because CA Remote Console does not allow the buffers to fill up.)

The CA Automation Point ADDRESS OPS command environment provides the outbound communication to CA OPS/MVS for the interface. The interface lets you perform the following outbound communication tasks:

- Send CA Automation Point messages to CA OPS/MVS
- Execute commands from CA OPS/MVS
- Execute REXX programs or TSO commands under an OSF TSO server on a CA OPS/MVS system
- Return a list of CA OPS/MVS systems currently defined to CA Automation Point with their current status

The CA Automation Point to CA OPS/MVS Interface also supports inbound communication from CA OPS/MVS. Using this interface, you can initiate the following tasks from CA OPS/MVS:

- Send WTO messages directly to CA Automation Point rules processing
- Invoke REXX programs on the CA Automation Point workstation
- Trigger NMFIND (notification) requests
- Issue PPQ WRITE commands from CA Automation Point

## How CA Automation Point Interfaces with CA NSM

Interfacing with CA NSM components is easier than ever. Even if you do not purchase CA NSM, CA Automation Point ships with CA Common Services (CCS), which provides components necessary to monitor particular types of events.

Through integration with CA Common Services, CA Automation Point offers you these additional benefits:

- The CA NSM command environment lets you store objects that represent the systems, and resources that are monitored by CA Automation Point, in the CA NSM Common Object Repository. It also enables you to display these objects and resources on the WorldView Map.
- The Remote Viewer lets you view and enter commands to CA Automation Point monitored sessions from a wide variety of remote Windows desktop or server operating systems. You can also launch the Remote Viewer from an icon that represents a system that is managed by CA Automation Point on the WorldView Map.
- The CA Automation Point Event Traffic Controller enables you to use messages, events, commands, and requests for actions to communicate between CA Automation Point and the CA NSM Event Manager component.

### How You Use the CA NSM Command Environment

Through its WorldView Map, CA NSM provides a new mechanism for the high-level management of complex enterprise environments. CA Automation Point can directly participate in this process from the interface through the methods described below.

The ADDRESS TNG environment provides a REXX-based programming interface to the objects contained in the Common Object Repository. This interface enables you to do the following:

- Create new objects
- Read and write values into properties of existing objects
- Set a color associated with an object based on the severity level of the problem
- List all objects that belong to a specific class
- Delete existing objects
- Place objects that represent resources monitored by CA Automation Point into the CA NSM Business Process Views

Using the ADDRESS TNG environment, you can graphically depict the activity that is being conducted by CA Automation Point on the WorldView Map. For example, you could create an object to represent each system that is being monitored by CA Automation Point and, using a combination of rules and REXX, turn an icon different colors based on various changes in the state of the managed session-such as a communication failure turning the icon red.

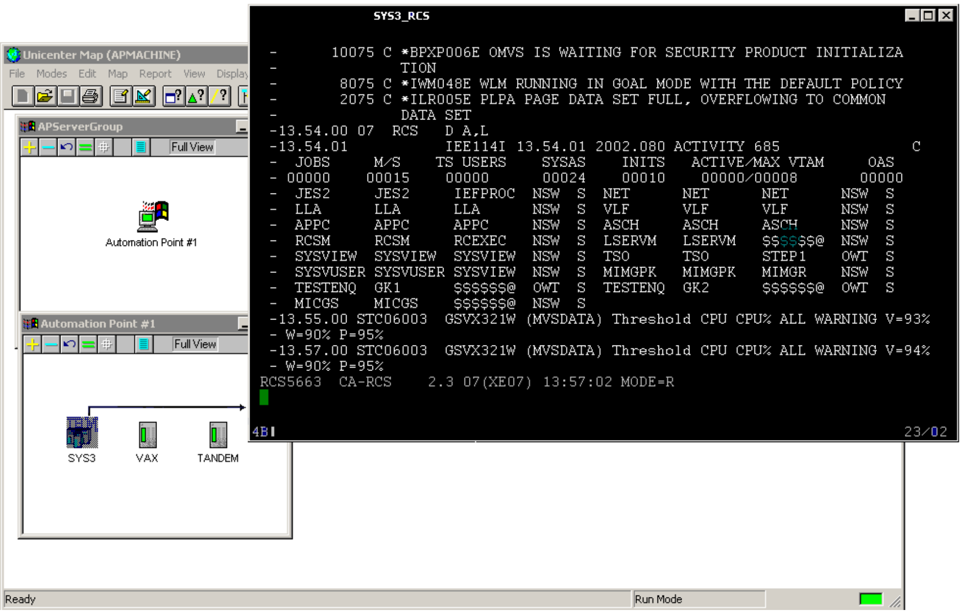
In this discussion, a system is referred to as both an object and an icon. When referred to as an *object*, the system relates to the Common Object Repository, or database. When referred to as an *icon*, the system relates to the WorldView Map.

New CA Automation Point users may want to use the ADDRESS TNG environment to place system icons on the WorldView Map and to update their statuses. When applications gain sophistication, CA Automation Point and CA NSM provide greater flexibility in the extent of monitoring and follow-up actions for items placed on the map.

## How You Launch the Remote Viewer

From the WorldView map, you can launch the CA Automation Point Remote Viewer (also known as APVIEW) to display the console of a system that is experiencing a problem. This capability is useful when you have an icon on the WorldView Map that represents a system and the color of the icon has turned yellow or red, indicating a warning or critical state. You can use the CA Automation Point ADDRESS TNG environment to set the severity level of the system object. The severity level determines the color of the icon.

The following illustration shows how you launch the Remote Viewer to display the console of a system:



```
-      10075 C *BPXP006E OMVS IS WAITING FOR SECURITY PRODUCT INITIALIZA
-              TION
-       8075 C *IWM048E WLM RUNNING IN GOAL MODE WITH THE DEFAULT POLICY
-       2075 C *ILR005E PLPA PAGE DATA SET FULL, OVERFLOWING TO COMMON
-              DATA SET
-13.54.00 07  RCS   D A,L
-13.54.01           IEE114I 13.54.01 2002.080 ACTIVITY 685              C
-  JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
- 00000    00015    00000      00024    00010    00000/00008       00000
-  JES2     JES2     IEFPROC  NSW  S  NET      NET      NET      NSW  S
-  LLA      LLA      LLA      NSW  S  VLF      VLF      VLF      NSW  S
-  APPC     APPC     APPC     NSW  S  ASCH     ASCH     ASCH     NSW  S
-  RCSM     RCSM     RCEXEC   NSW  S  LSERVM   LSERVM   $$$$$$@  NSW  S
-  SYSVIEW  SYSVIEW  SYSVIEW  NSW  S  TSO      TSO      STEP1    OWT  S
-  SYSVUSER SYSVUSER SYSVIEW  NSW  S  MIMGPK   MIMGPK   MIMGR    NSW  S
-  TESTENQ  GK1      $$$$$$@  OWT  S  TESTENQ  GK2      $$$$$$@  OWT  S
-  MICGS    MICGS    $$$$$$@  NSW  S
-13.55.00 STC06003  GSVX321W (MVSDATA) Threshold CPU CPU% ALL WARNING V=93%
 - W=90% P=95%
-13.57.00 STC06003  GSVX321W (MVSDATA) Threshold CPU CPU% ALL WARNING V=94%
 - W=90% P=95%
RCS5663  CA-RCS    2.3 07(XE07) 13:57:02 MODE=R

4B                                                                    23/02
```

**Note:** A significant benefit of the Remote Viewer is that you can customize the right-click menu for the system icons to launch the Remote Viewer to view the console for that system.

The Remote Viewer is distributed on the CA Automation Point DVD and can be installed separately from the rest of the product on any Windows workstation, including workstations that run the WorldView Map. (There are no licensing restrictions as to the number of workstations on which the Remote Viewer can be installed.)

The Remote Viewer also provides you with both logon and session-level security.

## Event Traffic Controller

The Event Traffic Controller provides an interface between CA Automation Point and the CA NSM Event Manager component, enabling you to control the flow of event traffic between the two products. It is a set of programs that gather events from and forward events to CA NSM Event Manager. It can be likened to an air traffic controller system, in that it obtains a list of events, like flights, and routes or reroutes them to their destinations. The Event Traffic Controller provides the following:

- Bidirectional message passing
- SNMP capabilities for CA Automation Point
- Notification capabilities for CA NSM Event Manager

Both CA Automation Point and CA NSM Event Manager enable you to monitor and process system events. Both products provide event capture and viewing capabilities, along with message matching and the ability to perform automated actions on selected system events. Both products also enable you to monitor the Windows event logs. However, each product has its own particular strengths regarding event processing, which are noted in the following sections.

## CA Automation Point Event Processing Strengths

- Enables the capture of z/OS console messages and the communication of commands back to z/OS
- Enables the automation of systems to which it is connected, eliminating the need to install the product on each system that is to be managed
- Provides automated *notification* policies and procedures through voice, paging, and email services
- Provides screen capture facilities that enable your custom automation applications to extract relevant events from arbitrary text streams

## CA NSM Event Manager Event Processing Strengths

- Enables events and actions to be defined using a graphical user interface (GUI)
- Enables message forwarding between multiple copies of Event Manager to be set up using a GUI, simplifying the process of defining a site policy for the management of numerous UNIX and Windows systems
- Provides the ability to capture, forward, and act upon SNMP traps
- Enables the viewing of all events across the enterprise through the Event Management Console

## How You Choose an Event Management Tool

Considering the strengths of CA Automation Point and CA NSM Event Manager, you must determine the following:

- Which product should capture a particular event?
- Which product can resolve the event most efficiently?
- Which product provides the interface that is best suited for the desired operator action?
- Where will an operator perform most of his or her system interactions (distributed system or mainframe system)?

The Event Traffic Controller leverages the strengths of each product, providing new and extended functionality for unparalleled enterprise-wide automation.

## How You Configure the Event Traffic Controller

You can easily configure the Event Traffic Controller using Configuration Manager. From the Event Traffic Configuration dialog, do the following:

- Enable or disable a given CA NSM event type.
- Specify the CA NSM hosts you want to process.
- Turn logging on or off for a given event type.
- Forward all CA Automation Point messages to CA NSM by default.
- Control performance metrics, including the frequency of event polling.
- Modify the session definition.
- Add rules for the session.

## How You Collect Information from the Windows Event Log

You can collect information from the Windows event log by enabling it to be monitored through Configuration Manager. Alternatively, you can use the Event Traffic Controller to remotely collect information from the Windows event log through CA NSM Event Manager.

**Note:** One key benefit of monitoring the Windows application event log is to obtain licensing messages into CA Automation Point. You can then take actions using rules and REXX.

As previously mentioned, both CA Automation Point and CA NSM Event Manager can be configured to monitor the Windows event logs. The following are considerations for deciding which of the two products best meets your needs:

- CA Automation Point understands more substitution parameters than CA NSM Event Manager does.
- CA Automation Point does not require you to install software on the monitored Windows system.
- CA Automation Point truncates log messages to 512 bytes.
- CA NSM Event Manager scales through the use of agents.

# How You Interface with Third-party Software Applications

## AP Web Services

Third-party products, like service desk or network monitoring applications, can remotely utilize the capabilities of CA Automation Point. CA Automation Point provides a web service API to enable such third-party applications to make requests of an AP server and receive data from an AP server. Such applications can be written in any programming language, can run under any operating system, and can reside on any computer in the corporate network.

Examples of operations that you can perform through the web service API are:

**Notifications**

- Request that AP send a notification.
- Get the status of a notification.
- Answer a notification

**Sessions**

- Get status
- Connect/disconnect
- Automate/pause
- Execute a command

**Messages**

- Get messages that are received and processed by rules in a selected AP session.
- Submit a message into an AP session to be processed by AP rules.

The following sources of documentation can assist you in using CA Automation Point web services.

***CA Automation Point Product Guide*** **(this document)**

- Why you want to use the AP web services.
- What types of things you can do with the AP web services.
- What programs work together to deliver the AP web services.

***CA Automation Point Administrator Guide***

- How you configure the AP web service listener on the AP server.
- How you deploy and configure the optional AP web service client on a remote computer.
- How you establish appropriate security.

***CA Automation Point Reference Guide***

- How you use the AP web service API to perform specific operations.

### XML Schema Definitions

- XML documents are used to transmit information to the AP web services. These XML documents are formally defined by XML schemas. The XML schemas for all AP web service XML documents are contained in:

  `%AP_HOME%\distrib\websvc\*.xsd`

- Schemas are exact specifications of particular types of XML documents. Schemas can also be used to programmatically validate an existing XML document. However, user-friendly documentation also exists, which describes the purpose and content of the AP XML documents. Documentation for all AP web service XML schemas is contained in:

  `%AP_HOME%\Doc\help\websvc\xmlSchemas\*.html`

### Java Client API

- You can choose to use the CA Automation Point client-side Java API to communicate to the AP web service. You can view that API documentation at:

  `%AP_HOME%\Doc\help\websvc\javaAPI\index.html`

### Command Line Client Options

- You can choose to use the CA Automation Point client-side command-line program (named 'RequestService') to communicate to the AP web service. You can view the documentation for using that program by running the program with no command-line parameters:

  `%AP_HOME%\bin\RequestService`

The AP web service API utilizes a REST (Representational State Transfer) architecture. A REST architecture uses the HTTP methods POST, GET, PUT, and DELETE against a well-defined URI hierarchy representing CA Automation Point objects. Use these HTTP methods to achieve required CRUD operations (create, read, update, delete).

Most of the AP RESTful HTTP operations include an attached XML payload containing parameters that are associated with the desired operation. Similarly, the replies that you receive and your error results are delivered in XML documents. By parsing the XML reply document, you can process detailed results from your request.

The design of our web service uses Java Servlet technology, so our web service must be deployed under a servlet-compliant application server. Since CA Automation Point already redistributes the Apache Tomcat application server for use with our Notification Website, we also utilize Tomcat to host the AP web service.

## AP Web Service Components

**AP Web Service Listener**

The AP Web Service Listener is a Java application that accepts web service requests from clients and returns replies to those clients. The Listener is bundled into a web application archive (or .WAR file) and deployed under Tomcat. The Listener must be running for the AP web services to be operational.

Once the AP Web Service Listener is deployed, you can write application software to issue HTTP methods to the appropriate URI. By sending HTTP methods with attached XML documents, applications can talk directly to the AP server from any computer in your corporate network.

The Listener dispatches the requests that it receives to the appropriate AP component to perform the desired operation for the calling program. The two AP components that perform the actual operations are the Automation Request Processor (AP Desktop) and the Notification Request Processor (Notification Server).

**Automation Request Processor**

This term represents the threads and logic within the AP Desktop application that perform the desired web service operations that are related to automation. This term includes, operations on messages and operations on sessions.

**Notification Request Processor**

This term represents the threads and logic within the Notification Server that perform the desired web service operations that are related to notifications. This term includes, send, answer, and query a notification.

**RequestService Java client API**

You are not required to use any CA client software to communicate to the AP web services. From many different programming languages, you can issue HTTP requests against specific URIs and can process their replies.

However, if you are the programmer of a Java application you likely already have the expertise to invoke Java methods. You may not have the expertise (or inclination) to perform web service communications. The RequestService Java API performs all of the communications necessary to transmit requests and receive replies from the AP web service. Use of the Java API can shorten the time that is required for you to integrate your Java application with CA Automation Point.

**RequestService command-line client application**

Engineering staff often perform their integration work using command line tools and scripting languages. The requirement to write a complete application program that correctly uses the HTTP protocol can sometimes be more time consuming than an organization can afford. We provide an optional command-line client application that is called RequestService to reduce programming effort and to reduce the requirement to understand fully the HTTP protocol.

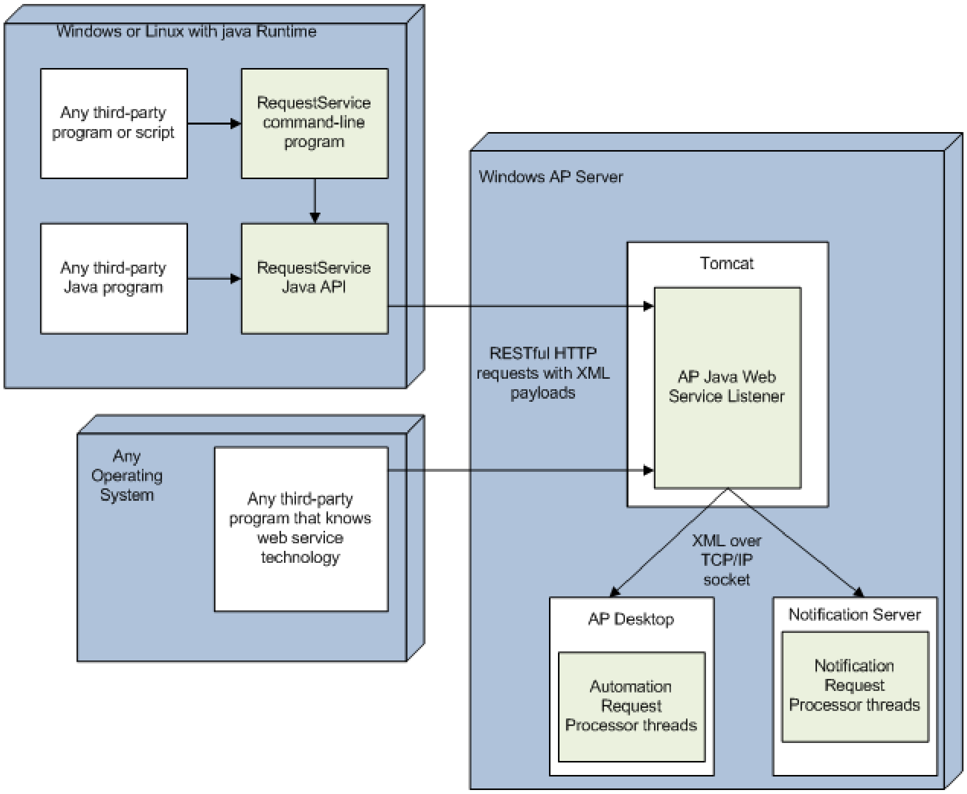
The RequestService application has the following capabilities:

- Accepts options from the command line and data from XML files
- Performs the client-side web service protocol that is required to send a request to a CA Automation Point server
- Produces XML reply data on standard output

Behind the scenes, the RequestService command-line application utilizes the RequestService Java API to perform most of its functionality. A Java Runtime Environment (JRE) must be installed before you can use the RequestService application.

The RequestService command-line application is less flexible in processing XML replies than the RequestService Java API. However, the RequestService command-line application provides an easy on-ramp for integrating a third-party application to CA Automation Point through web services with minimal programming.

The following diagram shows how the AP web service components are deployed.

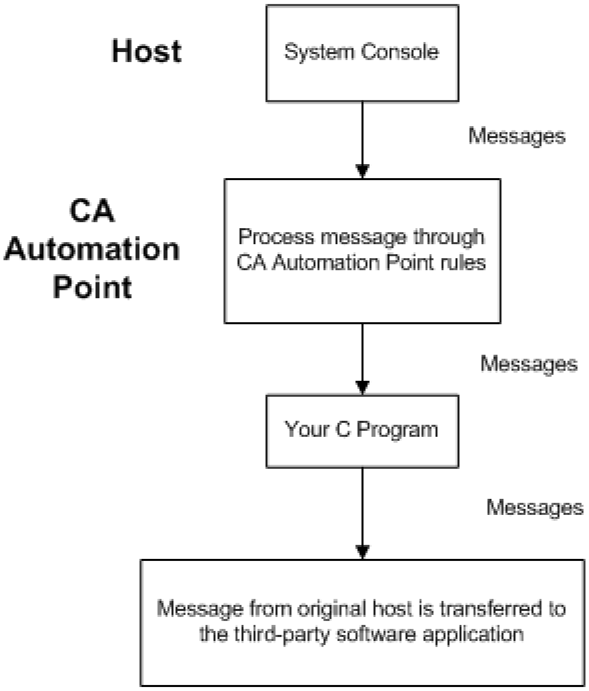

Windows or Linux with java Runtime
Any third-party program or script
RequestService command-line program
Any third-party Java program
RequestService Java API
Any Operating System
Any third-party program that knows web service technology
Windows AP Server
RESTful HTTP requests with XML payloads
Tomcat
AP Java Web Service Listener
XML over TCP/IP socket
AP Desktop
Automation Request Processor threads
Notification Server
Notification Request Processor threads

## Export From AP Rules To A Local C Program

Use EXPORTMSG to export a message that CA Automation Point has processed into another program residing on that same AP server. The EXPORTMSG keyword has a simpler working environment, but is less flexible than web services in the capabilities that it provides.

EXPORTMSG is a rules keyword. Using this keyword, an efficient, programmatic mechanism can be built for transmitting CA Automation Point messages to an API of any third-party software application. EXPORTMSG enables you to export any message that is processed through a rule into a C program that you create.

Example of how this export is done:


Host
System Console
Messages
CA Automation Point
Process message through CA Automation Point rules
Messages
Your C Program
Messages
Message from original host is transferred to the third-party software application

# What's Next?

In this chapter you learned how you can achieve a high level of system availability by using rules and REXX programs to monitor events across multiple systems, evaluate these events, and control and coordinate the states and actions of multiple hardware machines. The next chapter describes how CA Automation Point completes your automation solution by providing resolution of problems that require more than automation.

# Chapter 4: Notification Overview

This chapter describes how CA Automation Point can use notification to enhance your automation processes.

## Beyond Automation

There may be times when you need more than standard automation scripts to handle the complex problems that occur at your data center. Consider the following example.

You work for a bank that has systems that monitor the level of currency in all ATM machines across the city. One of your busiest ATMs is low on currency on a Friday night because of heavier than usual withdrawals. Your system puts out a message letting you know about this problem. Scripts and REXX programs cannot address this situation, as it is one that requires human intervention. This is a time when the notification capabilities of CA Automation Point could prove invaluable.

There are a number of such scenarios that require capabilities that are beyond the scope of automation. They fall into these categories:

- Your automated scripts are not complex enough to handle all of the possible events that occur in your data center.
- Some events are too unusual or complex for automated scripts to apply the kind of judgment required. Human awareness or intervention is required for decisions that must be made.
- Technical experts who could aid in solving a problem may not be readily available.

When automation is not enough to handle events, CA Automation Point provides you with the means to address those problems that require human attention, and possibly intervention. Your staff may need to become aware of these problems so they can make informed decisions about how to resolve them. Sometimes it is necessary to communicate the potential side effects of a problem or resolution to the appropriate people, or to require manual intervention from experts. CA Automation Point supplements inboard and outboard handling of events with notification and escalation policies that meet these needs.

## Whom Can You Notify and How?

Whom can you notify using CA Automation Point, and by what means? The following are a few of the answers to these questions:

- You can alert desktop staff over a network through TCP/IP, through speech over TCP/IP, and over public address speakers.
- You can notify mobile staff through email, one-way paging, two-way paging, and voice telephony.
- You can receive acknowledgements from notifications. For example, you can notify through two-way paging or through one-way paging with callback by telephone.

# How You Make Your Workstation into a Voice Server with Paging Capabilities

CA Automation Point provides a *VOX environment*, which consists of multichannel inbound and outbound voice processing software that transforms your workstation into a sophisticated voice server. Although a significant part of the function of the VOX environment is to provide voice processing services, paging and email services are also provided.

The VOX environment consists of the following components:

**notification server**

- Services all voice processing requests from the VOX client
- Manages interaction with the workstation voice card, with the workstation modem (for one-way paging), with Internet-accessible paging services (for two-way paging), and with the SMTP interface modules (for email)
- Returns resulting information to the VOX client

**VOX command environment**

Enables your REXX programs to request notification services from one or more notification servers and return the result to the calling REXX program

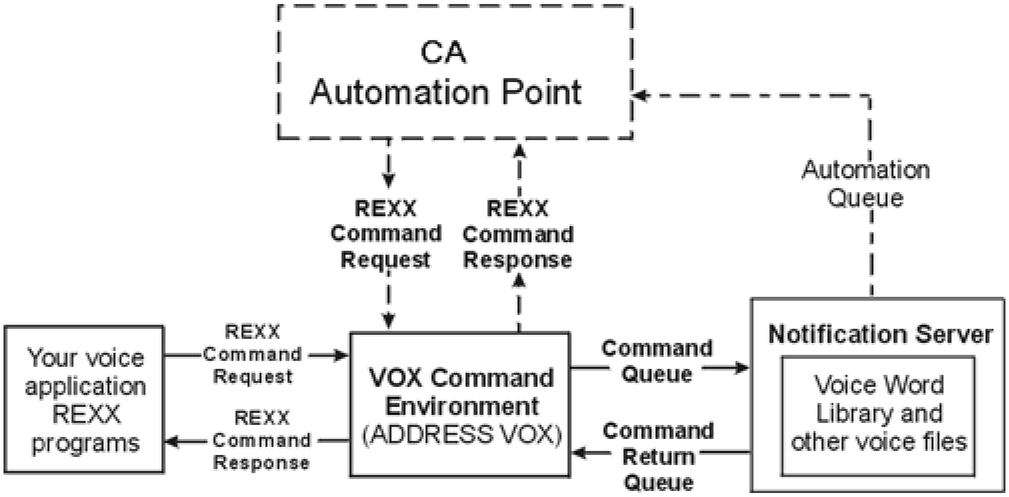
**voice word library**

Contains a voice index file and a voice data file

## Where Do These Components Reside?

The notification server component resides on a workstation of your choice. If you install more than one notification server, each one must reside on a separate workstation. The VOX command environment component can reside on a notification server workstation or on *any* network-connected workstation from which REXX-based VOX commands originate. The voice word library resides on a notification server workstation.

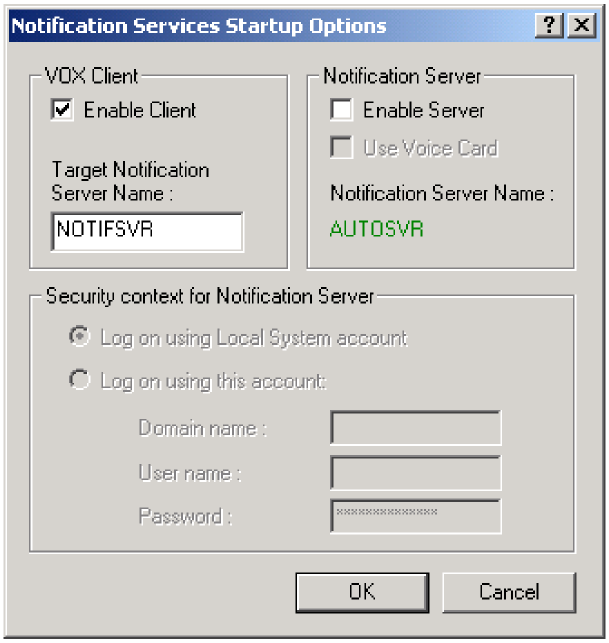
The following illustration shows how the Notification components work together:



## How You Use a Dedicated Notification Server

If you plan to use CA Automation Point to automate several systems and expect to use notification capabilities of CA Automation Point intensively, you have the option of using a dedicated notification server for performance optimization. To do so, you would install the CA Automation Point server on two machines, named, for example, AUTOSVR (for automation server) and NOTIFSVR (for notification server). On the automation server, you would configure the Notification Services startup options to disable the notification server, and use NOTIFSVR as the target notification server name for the VOX client.

The following dialog shows how you would do this.



Notification Services Startup Options

VOX Client

☑ Enable Client

Target Notification Server Name : NOTIFSVR

Notification Server

☐ Enable Server

☐ Use Voice Card

Notification Server Name : AUTOSVR

Security context for Notification Server

● Log on using Local System account

○ Log on using this account:

Domain name :

User name :

Password : **************

**Note:** Besides performance optimization, another reason for using a dedicated notification server is proximity to hardware and communication equipment.

# Notification Methods

CA Automation Point supports notification methods of varying complexity from alphanumeric paging, telephone, and email to two-way paging and text-to-speech notification.

The notification methods that are described in the sections that follow can be used in multiple ways to notify people and communicate problems, thereby leading to resolutions for those problems quickly and efficiently.

## One-way and Two-way Paging

You can notify a person at any time of day or night through a page that conveys the specifics of an event. If the pager supports two-way communication, you can use the paging device to respond directly to the event that triggered the notification. Two-way paging lets you take advantage of wireless technology to better track the status of a page request, and to retrieve a response from a person who has the wireless device. These paging requests are transmitted over the Internet, instead of using a modem, letting you avoid telephone dialing delays. You can also handle a greater number of different paging service providers concurrently without adding additional modems. You can use a two-way paging utility to display the status of an outstanding two-way page request in real time.

If a one-way pager is used, the incoming telephone answer capabilities provided by the Notification Server can be used to remotely respond to the event.

CA Automation Point supports paging providers who follow the standards outlined by the Telocator Alphanumeric Protocol (TAP). Support for additional protocols is available with NMTAP, which supports sending multiple pages to a paging service with a single phone call, and TAPPAGE, which enables you to issue a TAP page directly from the command prompt without going through the NMFIND command (or using the Notification Manager database). REXX programming is required for both these protocols.

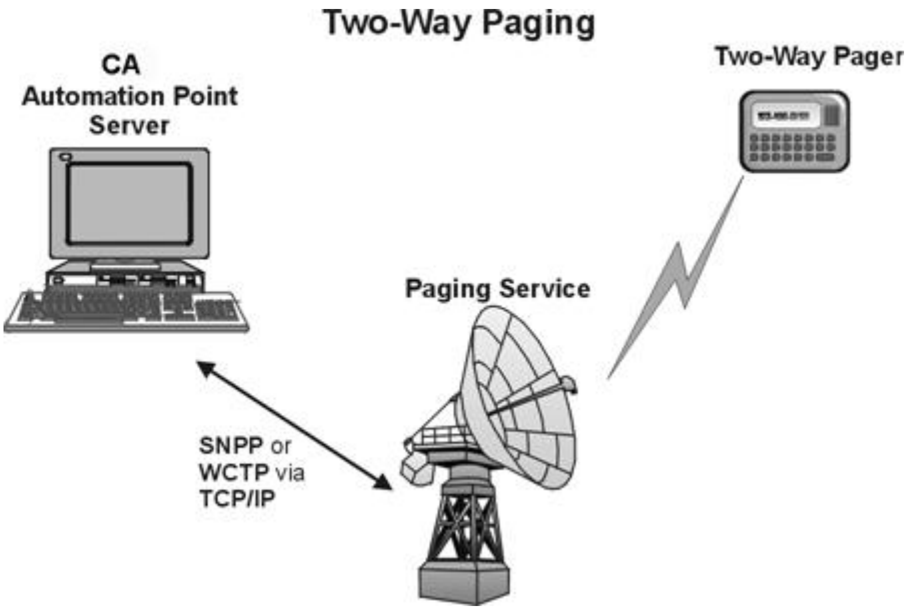
**Note:** For one-way paging, CA Automation Point supports controller-based hardware modems.

CA Automation Point supports two-way paging through both of the following protocols:

- Simple Network Paging Protocol (SNPP). This protocol uses TCP/IP sockets to connect to an SNPP server application maintained by the paging service. To use SNPP, you must be able to connect a socket to a host outside of your firewall.
- Wireless Communications Transfer Protocol (WCTP). This protocol uses XML over HTTP (or HTTPS) as its transport mechanism instead of using raw TCP/IP sockets. Because it uses HTTP (the same protocol as your web browsers) it can traverse proxy servers and firewalls.

If the WCTP protocol is used, the paging service must support version 1.1 of this protocol. The VOX command processor, PAGE2WAY, lets you submit two-way page requests.

The following illustration shows how two-way paging works.



## Telephone

To use telephone as a notification method, you must configure a Dialogic voice card.

The VOX environment supports up to 36 analog voice channels in a single workstation. These channels can be logically grouped so that you can control the available channels more easily.

The VOX environment accepts input from touch-tone and network devices. Touch tone telephones generate Dual Tone Multi-Frequency (DTMF) signals. Telephone network devices such as Central Office (CO) and Private Branch Exchange (PBX) switches generate Multi-frequency (MF) signals.

The following are some practical examples of how CA Automation Point provides telephone notification:

- **Help desk.** Through the Answer Tree application, the VOX environment waits for an incoming call, verifies the user ID and password of a caller, and presents the caller with a list of system incidents. When the caller selects an incident item, a voice file that details the status of the incident is played.
- **Problem escalation.** The VOX environment plays an announcement message over an intercom system one or more times, possibly increasing the volume and preamble each time. If an operator does not respond, the VOX environment dials the extension of each person on an internal notification list and plays the message. If there is no response, each person on an on-call list is called, and each person's beeper is activated in the order listed.

- **Auto-attendant.** One or more voice channels wait to answer an incoming telephone call. On the specified ring, the VOX environment answers the call and presents the caller with a menu of several options. Then depending on the menu selection, the VOX environment presents the caller with another menu, or transfers the caller.

## Email

The Notification server manages the interaction between the VOX environment and the supported SMTP email protocol. To use the SMTP protocol for transmitting email messages, you do not need to install any additional software.

You use the VOX SENDMAIL command to send email notifications.

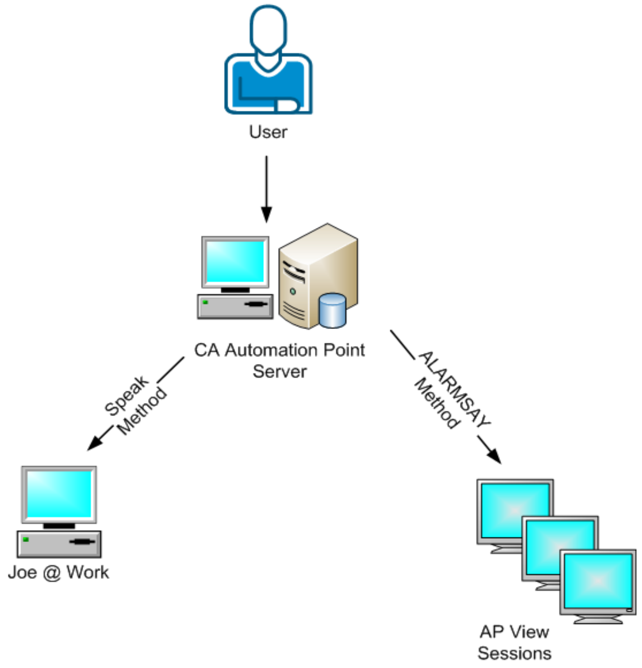
Whether you can use email paging depends on whether the feature is available through your paging service. If this feature is available, call costs can be significantly reduced by not requiring a modem or analog telephone lines.

## Text-to-Speech

The Text-to-Speech notification feature of CA Automation Point delivers spoken messages over your TCP/IP network. If the receiving PC is capable of using the Microsoft Agent technology (available on Microsoft Windows XP/Server 2003/Vista/Server 2008), the text message is spoken by an animated Microsoft Agent character.

If the platform is *not* capable of running the Microsoft Agent technology (Microsoft Windows 7/Server 2008 R2), a dialog box displays containing the message text, and this message text is sent through the Microsoft Speech API (SAPI) for text-to-speech processing.

The following illustration shows how text-to-speech notification works.



Two mechanisms are used to produce the text-to speech capability:

- The Notification Manager Speak method is used to notify a Notification Manager contact point-to-point.
- The ALARMSAY rules keyword uses the CA Automation Point alarm mechanism to send notifications to the local CA Automation Point server and to any Remote Viewer client currently monitoring the session.

The AP Listener icon is in the Status Tray Area of the receiving system. The appearance of the icon represents different states of the notification queue.

# How You Configure Notification Methods

In the preceding sections, you have learned about the various notification methods that CA Automation Point supports. This section discusses how you can easily configure two-way paging.

To both enable two-way paging support and to define the connection information for one or more paging services, you use the 2-Way Paging Setup dialog in Configuration Manager.

To define the connection settings, you use the fields in the Remote Connection Settings group box. You can further customize how the Notification Server interacts with each paging service using the fields in the Local Performance Settings group.

# ADDRESS VOX Environment

How do you use the VOX environment? You can quickly create elaborate voice applications using the voice processing (VOX) commands from the VOX environment in your REXX programs. ADDRESS VOX statements in your REXX programs enable you to access the VOX command environment.

## Outbound Recording with Voice Message Delivery

You are now aware of the wide variety of notification methods that CA Automation Point provides, and have seen how easy they are to configure. Perhaps you are now wondering how you use the VOX environment. This too is easy. Typically, an outbound recording with a voice message delivery application involves the VOX environment making a phone call and retrieving user security information before allowing a user to record a voice message. Depending on the application, voice messages can be deleted, recorded again, or forwarded to others.

For example, you might use this type of notification if you were maintaining system status on a daily basis, and an individual within a support group is responsible for updating the system status every hour.

# What's Next?

In this chapter you learned how the additional flexibility that CA Automation Point provides through notification and escalation techniques enhances your automation solution. The next chapter describes Notification Manager, which allows you to implement automated notification policies through its Notification Website, without the need for REXX programming.

# Chapter 5: Notification Strategy

This chapter tells you how to implement your notification strategy.

This section contains the following topics:

## Notification Manager Overview

You may find it necessary on occasion to hard-code a phone number, pager ID, or other information into a REXX program so that you can notify a particular person that a critical event has occurred. If you rely on this kind of hard-coded information, you can find yourself doing extra work in the long run. For example, suppose that a person leaves your company, and that person's telephone number is hard-coded in your program as the person to notify. You would have to change the program so that another person's telephone number could be used instead.

Notification Manager helps you avoid using hard-coded information in your programs altogether. It enables you to create a policy in which the telephone number of the person to be notified does not have to be hard-coded. It also enables you to expand upon that policy so that other people could be notified if the first person was unavailable. With Notification Manager, you can specify different ways of notifying different people in different locations and obtain responses from those people. The Notification Website lets you obtain the information characterizing the people you need to notify.

If you do not require ongoing, real-time queries to an external corporate data source in order to obtain information to notify someone, you can avoid the time and effort required to write the ADDRESS VOX programming described in the previous chapter on notifications. Instead, you can populate a database with the notification information, individual schedules, and escalation options collectively known as policies, and let Notification Manager do the rest.

Notification Manager offers the following advantages:

- Enables you to implement a sophisticated notification strategy without any REXX programming
- Lets you keep personal data such as name, pager number, and phone number out of rules

- Lets you keep time-specific information out of rules
- Handles escalation and forwarding
- Enables remote control of automation
- Enables confirmation of pages
- Provides store-and-forwarding of messages

# Notification Manager Structure

To meet your notification needs, Notification Manager provides a specialized database structured to support notification policies, a user interface for managing those policies, and the programmatic expertise to issue the underlying ADDRESS VOX calls to effectively notify a particular person at the time of the event.

## CA Automation Point DBMS

Notification Manager stores its data with the CA Automation Point DBMS (database management system). The CA Automation Point DBMS lets you access Notification Manager from your Web browser and lets you provide security restrictions for the operations that can be performed. Such security restrictions involve who can send a notification, who can modify his or her own schedule, who can modify schedules of other people, and who can modify notification methods.

The Web browser allows more platform independence; that is, it allows administration for an expanding number of client systems. This means you do not need to install software on PCs in every corporate department to send notifications or update notification policies.

# Notification Manager Policies

Notification Manager can help you implement automated notification policies and procedures in your operations without writing REXX programs. Notification procedures can include numeric paging, alphanumeric paging, email, voice notification, solicitation of input through DTMF (telephone keypad) tones, text-to-speech, Windows pop-ups, prerecorded or dynamically built messages, recording and forwarding of messages, or various combinations of these methods.

## Notification Manager Terminology

The basic purpose of Notification Manager is to find and contact someone using specified methods, tell them something, and optionally ask them something. It uses the following terminology:

**Login**

Identifies you to Notification Manager. It determines that you are who you claim to be before you can carry out any tasks.

**Contact**

Specifies a person or group you notify.

**Method**

Specifies a means by which you can notify a particular contact. Some people have numeric pagers, some alphanumeric pagers, and some no pager at all. Notification Manager lets you use different methods of notification depending on the person you are contacting and on the current time and day.

**Notification Schedule**

Defines time blocks that describe how to reach a contact during a particular block of time. For example, when a person is scheduled to be in the office you may want to send them a voice message, but when they are on the road, you may want to use a pager to contact them.

**Parameter**

Establishes and defines actions for a specified method. For example, when you use a pager, the phone number of the pager service, the pager number, and the maximum length this pager service allows for messages are all parameters.

## How You Implement Your Notification Strategy

With this terminology in mind, you can plan to implement your strategy by performing these actions:

- Choosing the method (for example, voice, or pager) used to contact people based on the time or day
- Choosing the behavior of the method (for example, number of times to let the phone ring, number of times to retry on busy) based on the individual being contacted or the time of day
- Providing multiple (backup) methods of contacting individuals
- Assigning responsibilities based on the time or day
- Assigning backup responsibilities based on the time or day
- Providing for temporary or periodic reassignment of responsibilities
- Grouping people by common job function or any other criteria
- Notifying just one or all of the people in a group about a situation
- Automatically escalating to the next contact when a person or group cannot be contacted

If you want to use Notification Manager to contact people by methods other than voice, paging, email, text-to-speech, or Netsend, you can easily integrate user-written REXX code into Notification Manager. Notification Manager treats your method exactly the same way it treats the methods provided with the product.

## How You Expand Upon Your Notification Strategy

CA Automation Point expands upon the strategy described above by offering you extra flexibility through the following features:

- **Clone a contact.** You can reduce the amount of data entry that you must perform when populating your database by cloning a contact. For example, suppose you want to notify a person named John, and John has a similar schedule and methods of notification as another person Tom, who is already in the database. When defining John as a person to notify, you can clone Tom's definition, and just make minor revisions to this definition to make it specific to John.
- **Mark a contact as unavailable.** You can use this feature like an out-of-office notice, telling Notification Manager to skip this contact even if there are active notification entries in that contact's schedule. This way, you can avoid delays that result from trying to notify a contact that is not available. It is much easier than requiring users to delete all their schedule entries when they go on vacation, and then recreate them when they return.
- **Use of method types.** All the Notification Manager methods are categorized into specific types of methods. When sending a notification, you can request that Notification Manager use only one or some of the possible method types for notification. For example, suppose John Smith has two active schedules, one assigned to use the Email 1 method and the other assigned to use the Alphanumeric Pager 1 method. If you have an urgent problem that requires John Smith's immediate attention, you can use the Pager method type on the notification request to force Notification Manager to use only those methods assigned to this method type. Because Alphanumeric Page 1 is a Pager method type, John Smith is notified using the Alphanumeric Pager 1 method instead of the Email 1 method.

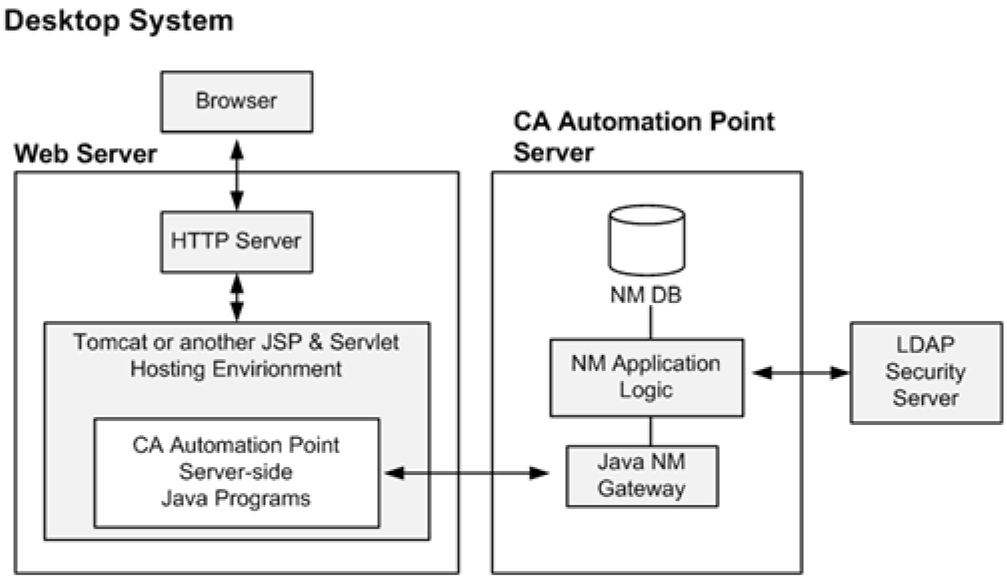
# Notification Website

Using the Notification Website, you can perform these major tasks:

- Create, modify, and delete contacts, methods, and logins
- Send notifications
- View the status of notifications that you send
- Adjust your own schedule

## Notification Website Architecture

The following illustration shows the primary elements that work together to provide the Notification Website.


Desktop System
Browser
Web Server
HTTP Server
Tomcat or another JSP & Servlet Hosting Envirionment
CA Automation Point Server-side Java Programs
CA Automation Point Server
NM DB
NM Application Logic
Java NM Gateway
LDAP Security Server

This illustration shows a separate web server and a CA Automation Point server; however, a site could also configure the web server functionality directly on the CA Automation Point Server.

Note that your web server environment must provide a servlet hosting facility. CA Automation Point redistributes the free Apache Tomcat servlet hosting application for those sites that do not have their own servlet hosting software. For details, see the *Administrator* Guide.

## Notification Website Security

CA Automation Point provides a security mechanism for the Notification Website that maximizes platform independence, while at the same time provide the widest user base with maximum functionality. It incorporates these security principles:

- **Physical Security**

  The CA Automation Point server and the web server are expected to run behind the corporate firewall within the company intranet on the company property. Your company controls any direct access to the physical site, the computers, and the software on them.

- **Data Encryption**

  The data transmitted to and from the Notification Website is encrypted and protected. The webmasters at your site control the means for establishing secure data transmission mechanisms, such as SSL (Secure Sockets Layer), between the web server and the client browsers that are connected. The data transmitted between the web server and the AP server is encrypted using proprietary algorithms.

- **Authentication**

  The Notification Website is protected from illicit users. The identity of a user is verified and confirmed before he or she is allowed to use the Notification Website.

- **Authorization**

  The Notification Website prevents authenticated users from using the website in unauthorized ways. User privileges and permissions are checked before a legitimate user is allowed to access particular information or to use particular methods.

**Note:** LDAP security can be used for either or both authentication and authorization. For more information, see the *Administrator Guide*.

## Notification Website Home Page

The Notification Website is divided into three major areas, which are represented by buttons on the home page. These buttons direct you to pages where you can perform major tasks.

## Update Notification Policies

The Update Notification Policies page is the entry point to web pages for the three Notification Manager components that comprise notification policy. You access this page by clicking the Update Notification Policies button on the home page.

You can use the links on the Update Notification Policies page to access the Add, Modify, and Delete pages for each of the three Notification Manager components. You can also use the menu system to navigate to any area of notification policy.

## Modify Individual Contact

The staff administrator can use the Modify Individual Contact page to modify information about an individual contact (person), including the contact's schedule. (There is also a web page for a group.) The bottom part of the page shows the notification schedule, which emphasizes methods used to notify that person.

Contacts can use other web pages to modify their own schedules. Other pages enable a staff administrator to modify Notification Manager methods and logins.

## Access Privileges

All web pages on the Notification Website have separate access privileges. You can probably grant the privilege to update a contact's own schedule to most people. Privileges to modify other people's schedules and to modify the methods themselves are usually granted to fewer people.

# The Notification Process

This section explains how the notification process works.

The Notification runtime process begins when CA Automation Point issues the single command NMFIND to initiate a notification. The NMFIND command does the following:

1. Automatically accesses the database to gather notification and individual schedule information
2. Automatically executes algorithms for multiple notification attempts, forwarding, and escalation
3. Automatically executes the appropriate notification server operations to accomplish the desired form of notification
4. Optionally provides acknowledgement of results to multiple targets

**Note**: For detailed information on how to set up Notification Manager, see the *Administrator Guide*.

# Index