CA Automation Point

Installation Guide

Release 11.4.1

technologies

Second Edition

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:

Note: In PDF format, page references identify the first page of the topic in which a change was made. The actual change may appear on a later page.

- Updated the Requirements for the RequestService web service client Java API and command line program (see page 16) section.
- Added the Client Setup Installation Modes (see page 31) section.
- Updated the Unattended Setup (see page 33) section.
- Updated the Single-Client Install by UserMulti-Client Install by Multi-Users (see page 30) section.
- Updated the Single Client Install by Administrator for All Users (see page 29) section.
- Updated the Client Setup Overview (see page 29) section.
- Updated the Install a Remote Client without Distribution Media (see page 34) section.

Contents

Chapter 1: Introduction 9

Chapter 2: System Information 15

Chapter 3: Installation 27

Chapter 4: Migration Information 39

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

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)

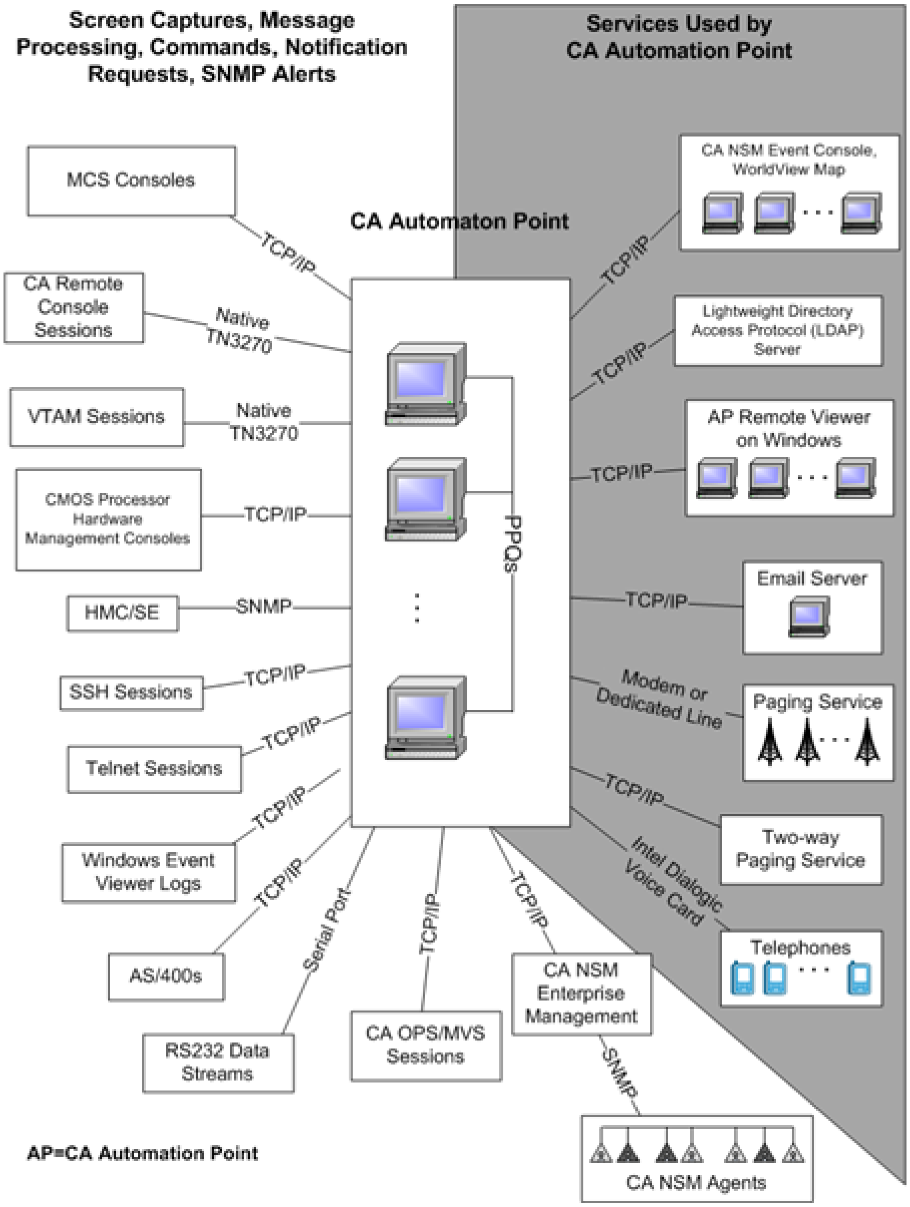
CA Automation Point Servers

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.

Chapter 2: System Information

This section contains the following topics:

Operating System Support

The term Windows refers to the Microsoft Windows operating system, including Windows Server 2008 and Windows 7. Unless specifically designated, Windows refers to any Microsoft Windows operating system supported by CA Automation Point.

CA Automation Point runs on the Intel chip version of Windows, not the MIPS or Alpha version.

CA Automation Point requires the Windows operating system to have the OEM code page set to either 437, 850, or 858.

Requirements for the CA Automation Point Server Components

You must have one of the following installed:

Operating System	Edition	32- bit or 64-bit
Microsoft Windows Server 2003	Standard, Enterprise, or Datacenter	x86 or x64
Microsoft Windows Server 2003 R2	Standard, Enterprise, or Datacenter	x86 or x64
Microsoft Windows Server 2008	Standard, Enterprise, or Datacenter	x86 or x64
Microsoft Windows Server 2008 R2	Standard, Enterprise, or Datacenter	x64 only

Note: Microsoft must currently support the operating system (including service pack levels) installed on the CA Automation Point server.

Requirements for the CA Automation Point Client Components (Remote Viewer Client or Speech Notification Client)

You must have one of the following installed:

Operating System	Edition	32- bit or 64-bit
Windows XP	Home or Professional	x86 only
Windows Vista	Home Premium, Business, or Ultimate	x86 or x64
Windows 7	Home Premium, Business, or Ultimate	x86 or x64
Microsoft Windows Server 2003	Standard, Enterprise, or Datacenter	x86 or x64
Microsoft Windows Server 2003 R2	Standard, Enterprise, or Datacenter	x86 or x64
Microsoft Windows Server 2008	Standard, Enterprise, or Datacenter	x86 or x64
Microsoft Windows Server 2008 R2	Standard, Enterprise, or Datacenter	x64 only

Note: The client components are usually installed in an environment in which software other than CA Automation Point client components software is also installed. Typically, CA Automation Point software is not the overriding factor in resource requirements for your workstation. Microsoft must currently support the installed operating system (including service pack levels).

Requirements for the RequestService web service client Java API and command line program

The RequestService API and command line program execute on the same versions of Windows listed for the CA Automation Point Components. The RequestService API and command line program can also execute under the Linux operating system. CA verified the operation of these CA components under the 64 bit (x64) CentOS 6.2 version of Linux. CA has also verified these components for use on Unix System Services (USS) under z/OS 1.13.

Database Requirements for the Workstation Housing the Notification Manager Database

A Notification Manager database requires an instance of Microsoft SQL Server. The following versions of Microsoft SQL Server can be used to store Notification Manager policy information in either a named instance or the default (unnamed) instance:

Database	Minimum Service Pack	Edition	32- bit or 64-bit
SQL Server 2005	Service Pack 4	Standard, Workgroup, or Enterprise	x86 or x64
SQL Server 2008	Service Pack 2	Standard, Workgroup, or Enterprise	x86 or x64
SQL Server 2008 R2	Service Pack 1	Standard, Workgroup, or Enterprise	x86 or x64

The SQL Server instance used to maintain the Notification Manager Database requires the following:

- Mixed-mode authentication
- Dictionary sort order of case-insensitive or case-sensitive
- 1252 Character Set

Note: The version of SQL Server (including service pack levels) must be currently supported by Microsoft.

Requirements for the CA Automation Point Server Connecting Remotely to a Notification Manager Database

A CA Automation Point Server that connects remotely to a Notification Manager Database does not require any Microsoft SQL Server components to be installed, unless IPv6 support is required. If you require IPv6 support, you must install the Microsoft SQL Server client connectivity tools on the CA Automation Point server machine.

System Requirements

This section lists the following information about the hardware and software used with CA Automation Point:

- Types or models of hardware
- Suggested manufacturers
- Required versions of software

These specifications apply only to the workstation on which the server components of CA Automation Point are installed. This workstation is referred to as the CA Automation Point workstation throughout the CA Automation Point documentation.

Note: The client components are generally installed in an environment in which software *other than* CA Automation Point client components software is also installed. Typically, CA Automation Point software is *not* the overriding factor in resource requirements for your workstation.

Hardware Requirements

This section describes hardware requirements for CA Automation Point.

Client-only Requirements

These requirements apply when executing only the client programs of CA Automation Point:

- 550 MHz Pentium processor (or the minimum processor requirements that are specified for the operating system, whichever is larger)
- 1 GB RAM (or the minimum memory requirements that are specified for the operating system, whichever is larger)
- 80 GB hard drive

Server Requirements

The following sections discuss requirements for installing CA Automation Point on a server machine.

Basic CA Automation Point Processing Load

These requirements apply when executing the full server-side programs of CA Automation Point (such as system automation) on a relatively small number of sessions (perhaps with notifications). We recommend that you install the product on a Windows-certified server-class workstation with the following minimum attributes:

- 2 GHz Pentium processor (or equivalent)
- 2 GB RAM
- 80 GB hard drive

High-Volume CA Automation Point Processing Load

These requirements apply when executing a combination of CA Automation Point functions or when the server also has CA NSM installed. This combination of functions may include high levels of system automation, notifications, or web server interaction. We recommend that you install the product on a Windows-certified server-class workstation with the following minimum attributes:

- 2.4 GHz Pentium dual-core processor (or equivalent)
- 4 GB RAM
- 160 GB hard drive

Notification Server Requirements

If you plan to use the notification server component for voice notification, you must install the following hardware and related software:

- A Dialogic Voice Card. For a list of recommended Dialogic Voice cards, see the Solution Document for G193464 on CA Support Online.
- The Dialogic Voice Card drivers provided with this release of CA Automation Point.

Software Requirements

The following software is required *only* if you are using the specified functionality:

- If you are using Web Message Viewer (Web MV) on the CA Automation Point server machine:
  - Microsoft Internet Information Server (IIS)
  - Oracle Java Runtime Environment (JRE) 1.7 (CA is redistributing this component on the product DVD).
- If you are using the Web MV GUI on a client machine:
  - Microsoft Internet Explorer 7.0, 8.0, or 9.0.

- If you are using Notification Manager, one of the following is required:
  - Microsoft SQL Server 2005 Service Pack 4 or greater
  - Microsoft SQL Server 2008 Service Pack 2 or greater
  - Microsoft SQL Server 2008 R2 Service Pack 1 or greater
- If you are enabling two-way paging support in the Notification Server on the CA Automation Point server machine:
  - Microsoft Internet Explorer 7.0, 8.0, or 9.0 (WCTP protocol only).
  - If an authenticating proxy server is used to gain access to the Internet, this proxy server must support the Basic authentication method. This proxy server also supports the relay of credentials when multiple proxies are used in a chain (WCTP protocol only).
  - The Microsoft XML Parser (Version 6) is included and automatically installed with the CA Automation Point distribution (WCTP protocol only).
  - If the WCTP protocol is used to issue two-way page requests, the paging service must support version 1.1 of the WCTP protocol.
- If you are using the Notification Website with the included Apache Tomcat Java Servlet environment:
  - Oracle Java Runtime Environment (JRE) 1.7 (CA redistributes this component on the product DVD).
- If you are accessing the Notification Website on a client machine:
  - Microsoft Internet Explorer 7.0, 8.0, or 9.0.
- If you are using RequestService web service client Java API or command-line program on a client machine:
  - Oracle Java Runtime Environment (JRE) 1.7 (obtain version according to a client machine platform from http://www.java.com).

Installation Considerations

There are several things you should consider before you can successfully install and configure CA Automation Point.

Standard User and C:\Program Files

With Windows Server 2008, standard users are prevented from writing to any files or folders under the *C:\Program Files* folder. The CA Automation Point installation program selects default directories to avoid placing user data under the *C:\Program Files* folder. If you override the default and place the user files folder under *C:\Program Files*, such as in the folder *C:\Program Files\CA\CA Automation Point\UserData*, Windows Server 2008 blocks a standard user's write access to that data. Therefore, we cannot support the use of CA Automation Point on Windows Server 2008 using a standard user with its user files folder is located under the *C:\Program Files* folder.

By default in Release 11.2, CA Automation Point used the *C:\Program Files\CA\Unicenter Automation Point\Site* folder for its user data. We cannot support the following upgrade sequence because it leads to the unsupported situation described previously.

1. Upgrade an existing installation of CA Automation Point Release 11.2 to Release 11.4.1 with its Site directory located under *C:\Program Files* on Windows Server 2003.
2. Upgrade Windows Server 2003 to Windows Server 2008 on that machine.

If you have upgraded CA Automation Point from Release 11.2 to Release 11.4.1 on Windows Server 2003 and you must upgrade Windows Server 2003 to Windows Server 2008 on that machine, we recommend that you perform the following steps:

1. Use Configuration Manager's *Manage Site Files* dialog to export your configuration settings.
2. Copy your exported data to a safe location.
3. Uninstall CA Automation Point Release 11.2.
4. Upgrade Windows Server 2003 to Windows Server 2008.
5. Install CA Automation Point Release 11.4.1.
6. Import your previously saved configuration settings.

Files in Use

During installation, ensure that all files that are to be copied or deleted and their directories are not in use. If you receive a message that a copy or delete operation has not completed successfully or that files or directories are in use, shut down any open applications and if necessary, use Task Manager to close any hidden tasks that may be running. Then click Retry. If you click Ignore, Abort, or Cancel in this situation, Setup does not complete the requested operation and may result in a call to Technical Support.

A file or directory can be locked (considered *in use*) because of NTFS permissions on it or its directory hierarchy, or because a process outside the control of CA Automation Point is using it. If NTFS permissions are not the problem, shut down the process or processes that are causing the locks. The following partial list shows processes that you should consider shutting down. For some of these processes, you may need to use Task Manager or the Services Administrative tool to shut them down.

- Any editor (for example, Notepad)
- Command Prompt windows
- Windows Explorer windows
- Any antivirus program
- Any HTTP server for Web Message Viewer (for example, Microsoft IIS)
- Any JSP Server for the Notification Manager Website (for example, Apache Tomcat)
- The Notification Manager database manager (SQL Server)
- Any component of CA NSM WorldView, Event Management, or CCI
- Cam.exe: (CA NSM Message Queuing Server service)
- Caunisrv.exe (CA-Unicenter service)
- Ccinrsd.exe (CA-Unicenter (NR-Server) service)
- Ccirmtd.exe (CA-Unicenter (Remote) service)
- DISCSRV.EXE (CA-AutoDiscovery service)
- INETINFO.EXE (IIS Admin Service service)
- IPXDSCVR.EXE (CA-IPXDiscovery service)
- Lic98Rmt.exe (CA-License Client service)
- Microsoft Outlook
- Tomcat.exe or Tomcat7.exe (Apache Tomcat service)
- Quenetd.exe (CA-Unicenter (Transport) service)
- SEVPROP.EXE (CA-Unicenter TND Severity Propagation service)
- TaskMgr.exe (Task Manager)
- Wvschdsv.exe (CA-Unicenter Discovery Scheduler service)

Important! apServerInstall.exe and apClientInstall.exe should never be stopped because they are required by the installation program.

Important! Sometimes the Windows kernel locks a file or directory. If you have shut down everything that Task Manager allows and the files or directories are still locked, then reboot your system and retry the installation before performing any other operations.

Apache Tomcat Installation Considerations

Upgrade Previous Versions of Tomcat

CA Automation Point redistributes Apache Tomcat version 7.0. If you do not use Apache Tomcat for applications other than CA Automation Point, we recommend that you uninstall older versions of Apache Tomcat. The Apache Tomcat installation process does not automatically uninstall a previous version.

To uninstall Apache Tomcat and upgrade to the latest version.

1. From the Windows Control Panel, select Administrative Tools, Services.

   The Services list appears.

2. Select Apache Tomcat from the list and click Stop the service.
3. From the Windows Control Panel, uninstall the previous version of Apache Tomcat.
4. In Configuration Manager, navigate to Expert Interface, Notification Services, Notification Manager, NM Website.

   The NM Website Dialog appears.

5. Clear the Enable access to the notification website check box and click the OK button.
6. Navigate to Expert Interface, Infrastructure, Web Services.

   The Web Services Dialog appears.

7. Disable all Web Service modules and click the OK button.
8. Navigate to Expert Interface, Infrastructure, Java/Tomcat Installation.

   The Java/Tomcat Installation Dialog appears.

9. Select the Install button for the Apache Tomcat component.
10. After Apache Tomcat installs, on the NM Website Dialog, check Enable access to the notification website and check Use local Java Servlet environment.
11. On the Web Services Dialog, enable any required Web Service modules.

Coexist with Previous Versions of Apache Tomcat

When running both an older and a newer version of Apache Tomcat simultaneously, configure one of the copies of Apache Tomcat to operate on a different TCP/IP port number. Configure the appropriate applications to communicate to Apache Tomcat through that port. After installing the new version of Apache Tomcat, use Configuration Manager to redeploy both the Notification website and any required Web Service modules under this version of Tomcat.

To redeploy the Notification website and Web Service modules under the new version of Apache Tomcat.

1. Open the NM Website dialog.
2. Uncheck or clear the Use local Java Servlet environment.
3. Click OK to save and close the dialog.
4. Reopen the NM Website dialog.
5. Select Use the Local Java Servlet environment.
6. Click OK to save and close dialog.
7. Open the Web Services dialog.
8. Disable all Web Services modules.
9. Click OK to save and close the dialog.
10. Reopen the Web Services dialog.
11. Enable any required Web Service modules.
12. Click OK to save and close the dialog.
13. Recycle Apache Tomcat.

Backward Compatibility with a Previous Version of Apache Tomcat

You can continue to run the CA Automation Point Notification Website with previous versions of Apache Tomcat. However, you must reconfigure Apache Tomcat to utilize an installation of the 1.7 version of the Java Runtime Environment.

Different Java Versions Installed on the CA Automation Point Server

If you have installed an earlier version of the Java Runtime Environment (JRE) or an earlier version of the Java Development Kit (JDK) for use with an earlier release of CA Automation Point, you can uninstall either or both, then install the JRE distributed with CA Automation Point. To run CA Automation Point Release 11.4.1, you must have JRE version 1.7 or greater. JRE version 1.7 is redistributed by CA with CA Automation Point.

Web MV and IIS 7.0

The Web Message Viewer server component (Web MV) uses Microsoft's Internet Information Services component (IIS) to provide remote access to the Web MV client application (written as a Java Applet). With the Microsoft Windows Server 2008 operating system, a newer version of this IIS component (version 7.0) is now bundled as an available server role. This newer version of IIS includes several enhancements over the previous version (version 6.0), including newer interfaces to configure and manage IIS itself. These new management interfaces are not backward-compatible with the previous version of IIS, so Microsoft has included an optional role service for the Web Server (IIS) server role to allow an application to use the same interface to manage both IIS 6.0 and IIS 7.0.

To allow Web MV to work in both IIS 6.0 and IIS 7.0 environments, CA Automation Point uses the previous IIS management interfaces (available in IIS version 6.0). For the Web MV server component to integrate with IIS 7.0 on the Microsoft Windows Server 2008 operating system, you must install the optional Web Server role service that provides IIS 6.0 compatibility. This Web Server role service is named *IIS 6 Management Compatibility*. Because a default IIS 7.0 installation does not include this role service, you must explicitly select this service for installation.

Interaction with UAC

When installing CA Automation Point on operating systems that have User Access Control (UAC) enabled, there may be a delay before the initial setup window displays. This is because the UAC service copies and scans the setup executable before launching it.

Operating systems with UAC include Windows Vista, Windows 2008, and Windows 7.

Optional Interface Components

When installing any of the optional Interface components (CA OPS/MVS EMA, CA NSM Event Manager, or CA NSM WorldView), make sure that a network connection is available on that computer. If there is no network connection, the installation of some or all of the interface components may fail.

Note: This does not impact the setup of the CA Automation Point Server or Client components.

Chapter 3: Installation

This section contains the following topics:

Review the Export Declaration

The U.S. government has completed a technical review on the encryption capabilities within CA Automation Point and has provided a Commerce Classification of CCATS # G058390 and 5D002 ENC.

Before You Install CA Automation Point

Before you begin installing CA Automation Point, be aware that the new version of the product removes any older version that has been previously installed. If an older version is present, your current configuration is automatically backed up. You also have the opportunity to continue using your current configuration for the new installation.

Install CA Automation Point

Note: If you plan to upgrade from Release 11.2 of the product, see the section Upgrade from CA Automation Point Release 11.2 or Release11.3 (see page 33).

CA Automation Point is distributed on two DVDs. DVD #1 contains all of the CA Automation Point product software. DVD #2 contains drivers for Dialogic brand voice cards (System Release 6.0 PCI for Windows, Service Update 266).

Note: The Dialogic drivers provided with CA Automation Point will *not* run under Windows Server 2003 64-bit. These drivers will run on all other CA Automation Point-supported operating systems.

To install CA Automation Point

1. Log on to Windows using an account with Administrator authority.

2. Insert CA Automation Point DVD #1 into the DVD drive on your workstation.

   The CA Automation Point DVD Launcher program should begin automatically. If it does, click Install Server or Install Remote Client.

   If this application does not start automatically, do the following:

   a. Click Start on the taskbar, and then choose Run.

   b. In the Open field of the Run dialog, type d:\setup.exe (where *d:* is the letter of the drive that contains the CA Automation Point DVD) and then click OK.

3. The installation wizard guides you through the installation. Follow the instructions on the dialogs.

   Note: At the beginning of the installation, a dialog informs you that if you have any features of CA Automation Point running, they will be stopped. At this point, any existing release of the product is stopped, and then removed once the installation process begins.

   You will perform the following tasks during the installation:

   - Accept the license agreement

   - Reuse or delete user data found from a previous installation.

     A dialog for these options appears only if Setup detects user data in an existing copy of CA Automation Point on your machine. In that case, you are given the following options:

     - Use the configuration data from the existing copy to configure the copy you are installing.

     - Delete the user data. The end result will be the same as if an earlier version of the product had not been found.

       Note: Either way, your user data is automatically backed up into the *Export* directory under your User directory path.

   - Select the features you want to install. When you run the Server installation, both server and client components are installed. If you are running the Remote Client installation, only Client components are installed.

     Note: The interfaces to companion products are already installed if CA NSM is installed on the computer.

   - Select a location to install the program

     The CA Automation Point installation program prompts you for a *Product installation folder* where the program is installed and *User files folder* location where you want all site-specific files to be stored. You can accept the defaults or choose another directory location. We recommend that you use defaults, which have been selected so that many of CA Automation Point's executables can be run by Standard Users.

- Review settings

  Note: Any old version of CA Automation Point will be erased if you proceed.

  Important! If, during setup, you receive a message telling you that files or directories are in use and the operation cannot be completed, see Installation Considerations (see page 20) for instructions on completing that operation.

- Copy program files

4. If a reboot is required to complete the installation process, the setup program requests a reboot. Click the *Reboot Now* option to reboot the workstation.

Note: An installation log is created in the C*A Automation Point Logs* directory.

Client Setup Overview

The Client setup program can be installed in two different modes.

AllUsers

A client installed by an administrative user account can be accessed by all user accounts.

CurrentUser:

A client installed without administrative privileges can be accessed only by the user account that installed it.

Single Client Install by Administrator for All Users

To install the Client in AllUsers mode by default run Client Installation by an administrative user account. Installed in AllUsers mode, the Client is accessible by any user account that is logged on to the local machine. Only an administrative user account can uninstall or upgrade the Client.

Single-Client Install by UserMulti-Client Install by Multi-Users

Before setting up the local machine to operate in CurrentUser mode, ensure that a previously installed Client in AllUsers mode is uninstalled.

To install the Client by default on the local machine in CurrentUser mode run Client Installation by any standard user account. The installed Client is accessible only by the standard user account that installed it. Similarly, the Client can only be uninstalled or upgraded by the standard user account that installed it. These restrictions also apply to Client Installation by an administrative user account using the /CurrentUser command-line option to override the default /AllUsers option.

Client Installation that is run by varying standard user accounts on the local machine results in multiple installed copies of the Client. Each user account is able to access or retain Client data created by the user account's session activity. When a new release of the Client is available, each copy of the installed Client must be upgraded by the user account that installed it.

Client Setup Installation Modes

The client setup program can be installed in two different modes: *AllUsers* and *CurrentUser*.

AllUsers

Use the AllUser mode when the user account performing the installation has Administrator privileges.

The AllUsers mode allows you to deploy the client applications in a way that makes them available to all users logged in to the system. When performing this installation, the user account requires Administrator privileges.

CurrentUser

Use the CurrenUser mode when the user account does not have Administrator privileges.

The CurrentUser mode does not require Administrator privileges to perform the installation. However the deployed applications are only available to the user account where the installation was performed. This mode enables deployment of the client applications in restricted environments where Administrator privileges are not readily available. The client installation can be deployed in CurrentUser mode on one machine as many times as needed under different user accounts. This procedure allows multiple users to use the client applications while still not requiring Administrator privileges during a deployment. The fact that CurrentUser mode does not require Administrator privileges is achieved by writing files and registry values to user-specific locations. The default installation paths are different in this mode. These paths point to a location under the user profile directory where the user has write access permissions by default. When overriding these default installation paths, select directories where the user has previously been granted write access permissions.

By default the AllUsers mode is used when the user account performing the installation has Administrator privileges. The CurrentUser mode is used by default when the user account does not have Administrator privileges.

Command-line options can be used to select the desired mode. The /AllUsers command-line option selects the AllUsers mode. The installation aborts if the AllUsers mode is selected this way and the user account does not have Administrator privileges. The /CurrentUser command-line option selects the CurrentUser mode.

Examples:

```
D:\clientInstall\apClientInstall.exe /AllUsers
D:\clientInstall\apClientInstall.exe /CurrentUser
```

The unattended installation sample script is located in the unattended/samples directory on the installation media. This script shows how these command-line options can be used to deploy the CA Automation Point client applications.

Important! Installing the product in both the AllUsers and CurrentUser modes at the same time on a single machine is not supported. If at any time a transition from an AllUsers-mode deployment to a CurrentUser-mode one is required, the product has to be uninstalled first. The same applies to the opposite transition from a CurrrentUser to an AllUsers deployment.

Note: When performing an unattended installation (see page 33), the /CurrentUser command-line switch is required to confirm that a CurrentUser mode installation is acceptable. This restriction is in place to prevent an accidental deployment in CurrentUser mode due to insufficient privileges. Similarly, the /AllUsers command-line option can be used during an unattended installation to ensure the AllUsers mode is being used.

How CA Common Service Components are Installed

CA Automation Point incorporates CA Common Services (CCS) to provide connectivity to CA NSM Event Management, CA NSM WorldView, and CA OPS/MVS. Selecting any of these options automatically installs the relevant CCS components.

When selecting CA NSM Event Manager and/or CA NSM WorldView, either establish a connection to a previously created remote CA NSM repository database, or create a local CA NSM repository database during the CA Automation Point installation. CA OPS/MVS EMA does not require a database connection.

The CA Automation Point installation program always successfully completes the installation of a CA Automation Point server before it installs any CCS components. When an error occurs while installing CCS components, the CA Automation Point server is unable to use the connections to the CCS components, but will be otherwise operational.

If CCS installation errors occur, you can reinstall the CCS components without having to completely reinstall CA Automation Point. From a Windows command prompt, type the following command:

```
ccsReinstall
```

This program asks for the path of the CA Automation Point DVD, and which companion product interfaces you want to install.

Unattended Setup

The file Readme.txt located in the unattended directory on the installation media outlines the procedures necessary to run an unattended installation or uninstallation.

Additionally, a sample script that shows how to execute an unattended client installation is available in the unattended/samples directory on the installation media. Read the Readme.txt file, before using this sample.

Install with CA Software Delivery

You can retrieve and install CA Automation Point using the CA Software Delivery (USD) application. Use the SD Explorer interface on a USD server to do this. For details on this process, see the CA Software Delivery *Administrator Guide*.

You can also register CA Automation Point with USD using an application called SDREGISTER.EXE. This utility is located in the softwareDelivery directory on the installation media. The file Readme.txt in the same directory explains how to use this application.

To Add Features or Reinstall CA Automation Point

If you want to add any optional feature or reinstall CA Automation Point, rerun the Setup installation program after the initial installation is complete. Your configuration data will not be removed or modified by the Setup program. Be aware that every time you run the CA Automation Point installation program, it will shut down the currently installed version.

To Uninstall CA Automation Point

To uninstall CA Automation Point, use the Add/Remove Programs or Programs and Features facility in the Windows Control Panel.

Upgrade from CA Automation Point Release 11.2 or Release 11.3

If you plan to upgrade from CA Automation Point Release 11.2 or Release 11.3, consider the points in this section before proceeding with the installation.

Uninstall a Previous Version

If you plan to install CA Automation Point Release 11.4.1 on a machine that is currently running the product, you do not need to uninstall the previous version. The installation program automatically handles any uninstallation steps that need to be performed.

Back Up Your Current Configuration

To back up your CA Automation Point configuration, use the Export and Import utility. This utility is accessible from the Manage Site Files option in the Configuration Manager File menu. After exporting your configuration, copy the *Export* directory to a backup location. This *Export* directory can be found under the *%AXC_SITE_PATH%* directory in Release 11.2 and under the *%AP_SITE%* directory in Release 11.3 and higher..

Note: For more information on this utility, see the *CA Automation Point Administrator Guide*.

Your configuration is also automatically backed up by the installation program into the Export directory. In CA Automation Point Release 11.2, the default Site directory resided under the default installation location. During an upgrade, the installation program does not change the location of this Site directory. However, any previously exported Site directories are moved underneath the new *Export* directory location. The new *Export* directory is loc*ated* underneath the User files folder directory.

Note: For more information, see section File Directory Structure in the *CA Automation Point Administrator Guide.*

Install a Remote Client without Distribution Media

You can install a CA Automation Point Remote Client on a computer that does not have access to the installation media (that is, one that does not have access to the product DVD).

- From a computer from which you can read the installation DVD, copy the *apClientInstall.exe* installation program from the *clientInstall*\ folder on the distribution media to a network shared drive that is accessible to the target computer.
- From the target computer, establish a connection to the network shared drive and run *apClientInstall.exe* to install the Remote Client.

Install the Notification Website Application on a Non-CA Automation Point Machine

If you decide to run the Notification Website application on a machine other than the CA Automation Point server machine, you must manually deploy the web application archive file (.WAR file) into your JSP/Servlet engine. The Notification Website application is packaged in the *caapnfy.war* file, which can be found in the *installdir*\classes directory on the CA Automation Point server machine. For instructions on how to deploy this application, see the JSP/Servlet environment documentation.

Before You Start CA Automation Point

Before you start CA Automation Point for the first time, consider the information in this section.

Initial Configuration

If you installed the server component, you need to configure CA Automation Point before you start the product for the first time. Configuration Manager provides a wizard to guide you through this process. The Wizard Interface lets you functionally configure the automation facilities and notification services that are essential for CA Automation Point to perform various functions.

Configuration Manager also provides the Expert Interface, which lets you access the settings of the CA Automation Point components, letting you drill down and quickly make changes to specific features.

For detailed information on Configuration Manager, the Wizard Interface, and the Expert Interface, see the *Administrator Guide*.

Set Up Licensing

When you purchase CA Automation Point, you receive a license certificate with your order. To run CA Automation Point on a Server machine, you need to access your license for the product.

To access your CA Automation Point license

1. Within the *ca_lic* directory (usually located under the *Program Files\CA\SharedComponents* directory, or at the root of the machine), search for a file named *ca.olf*.
2. If the *ca.olf* file *does not exis*t, use a text editor to create a file with that name. Copy all of the information from the Execution Key from your license certificate into this file, and save it into the *ca_lic* directory.
3. If the *ca.olf* file *does exist*, open it using a text editor and make the following edits:
   a. Replace all lines beginning with ID_ with the ID_ lines indicated in the Execution Key from your license certificate.
   b. At the bottom of the file, immediately following any existing FEATURE lines, add the FEATURE line from the Execution Key from your license certificate.

      Notes:

      - Do not remove any existing FEATURE lines.
      - The FEATURE line may wrap to a second line on the license certificate, but it must be entered on a single line with no carriage return in the *ca.olf* file.

   c. Save the edited ca.olf file into the *ca_lic* directory.

To make the license installation process easier, a merged license file based on your Site ID is available to download from http://ca.com/support.

Note: Check your license certificate for the most up-to-date licensing instructions.

Monitoring Licensing Messages

To ensure that CA Automation Point is properly licensed, you can do one of the following:

- Monitor the AP Msg Recall window located on the Automation Point Desktop application
- Monitor the Windows application event log for CA Licensing messages.

To monitor licensing messages sent to the AP Msg Recall window, you can write rules to capture the AXC0554W and AXC0555W messages.

To monitor licensing messages sent to the Windows application event log, you can configure the Automation Point Desktop application to monitor this event log using the Events Interface section of the Configuration Manager application.

Understanding CA Automation Point Licensing Codes

There are two types of licensing codes for CA Automation Point:

- Licensing codes for the base product
- Licensing codes for optional 3270 connections

Licenses for 3270 connections include all connections to 3270 console family, regardless of connection type. Starting with CA Automation Point Release 11.3, these licenses also include connections to the 5250 family of consoles.

The following table lists information about license codes:

License Name	Code	Category	Release Introduced
Unicenter Automation Point	2UNA	base product	4.0
CA Automation Point	2UNB	base product	11.3
Unicenter Automation Point 3270 Interface Option	2UNI	3270/5250 console connection	4.0
Unicenter Automation Point 3270 Interface Option	2UN3	3270/5250 console connection	11.1
CA Automation Point 3270/5250 Option	2UN4	3270/5250 console connection	11.3

License keys are accepted from the release when they were first introduced (see previous table). Valid newer keys override keys from older releases. Although valid licensing keys from previous releases still work with newer releases, newer keys allow for higher connection counts, as shown in the following table:

		Licensed Connections	
Name	**Code**	**Minimum**	**Maximum**
Unicenter Automation Point 3270 Interface Option	2UNI	16	16
Unicenter Automation Point 3270 Interface Option	2UN3	12	32
CA Automation Point 3270/5250 Option	2UN4	16	64

How You Find Information

This section tells you where to find information on CA Automation Point features and functionality.

CA HTML Bookshelf

The CA Automation Point documentation set is available in both HTML and PDF formats, which you can access from the CA Automation Point HTML Bookshelf. HTML provides robust online viewing and search capabilities, while PDF provides a print-friendly option.

The HTML bookshelf features include:

- A single help screen that displays all documentation for this release.
- An all-in-one search tool that searches the entire documentation set and returns matches found in both the HTML and PDF formatted documentation, without the need for a specialized .PDX index file.
- Additional links for using the Bookshelf, downloading Acrobat Reader, and contacting CA.

The CA Automation Point Bookshelf is available on the product DVD and on CA Support Online (http://ca.com/support).

Online Help

CA Automation Point provides HTML Help for many of its dialogs. To view help for a dialog, click the help button ? on that dialog.

Chapter 4: Migration Information

If you are upgrading from either Release 11.2 or Release 11.3, read the following migration topic:

- How You Upgrade Notification Manager Databases (see page 39)

If you are upgrading from Release 11.2, read the following migration topics:

- How Site Files are Managed (see page 42)
- Export and Import Utility (see page 44)
- Removal of NETBEUI Network Transport from PPQs (see page 45)
- VIO Sessions (see page 45)
- HLLAPI and Cut Mode Connection Support (see page 46)
- CONNECT and DISCONNECT Key Operations (see page 46)
- Removal of MAPI Support (see page 46)
- CA NSM Security Server (see page 46)
- 3205 Terminal Type Support (see page 46)

How You Upgrade Notification Manager Databases

This section describes how you upgrade an existing Notification Manager database. The NM database resides within the CA MDB (Management Data Base). CA Automation Point Release 11.4.1 can upgrade any version of the CA MDB running under a supported version of SQL Server.

Notification Manager Database Upgrade considerations

The database schema in CA Automation Point Release 11.4.1 has changed to support enhancements to the Notification Manager website and new ADDRESS VOX commands. This database schema is compatible with previous versions of CA Automation Point starting with Release 11.2. All notification data created in previous releases is retained during an upgrade to Release 11.4.1.

However, the following limitations apply when accessing notification request entries created with a different version of Notification Manager:

- Notification request entries created in a previous version of CA Automation Point do not contain detailed notification status information. This expanded notification status information is only available for requests that are submitted from CA Automation Point Release 11.4.1.
- Notification request entries utilizing the ASK parameter of the NMFIND program created in CA Automation Point Release 11.4.1 store the answer choices separately from the question text. These answer choices are not available to instances of CA Automation Point Release 11.3 or earlier that share the same *Notification Manager* database.

To upgrade a CA Automation Point server that connects to a local Notification Manager database

Follow these steps:

1. Start the CA Automation Point Release 11.4.1 installation program.
2. Select the *Install server* option.
3. Proceed through the installation dialogs until the NM database upgrade dialog displays.
4. Select Yes. The Notification Manager database upgrade takes place immediately.
5. Continue with the CA Automation Point upgrade.

Note: You can only upgrade CA Automation Point from Release 11.2 or Release 11.3 to Release 11.4.1. If you have an earlier release of CA Automation Point, upgrade to CA Automation Point Release 11.2 or Release 11.3 before upgrading to Release 11.4.1.

Note: When the NM database resides on the same machine as an older CA Automation Point server, we recommend backing up your configuration. Run the ADDRESS VOX NMEXPORT command before each upgrade step to create a backup of your database. This backup procedure is not mandatory but is helpful to restore the previous release.

Note: When *No* is selected in the NM database upgrade dialog, NM database is not upgraded and Notification Manager and NM Website is disabled. To enable NM database run Configuration Manager and follow the instructions.

To upgrade a Notification Manager database on a different machine than the CA Automation Point server.

Follow these steps:

1. Start the CA Automation Point Release 11.4.1 installation program on your CA Automation Point server.
2. Select the *Install server* option. No NM database questions are asked. Complete the upgrade.

Follow the instructions in the section entitled How You Create Or Update a Notification Manager Database on a Non-CA Automation Point server in the *CA Automation Point Administrator Guide*.

To upgrade multiple CA Automation Point servers that connect to a single NM Database

CA Automation Point Release 11.2 and Release 11.3 can share the same Notification Manager database with CA Automation Point Release 11.4.1. The limitations for this cross-release database sharing are described in Notification Manager Database Upgrade considerations (see page 40).

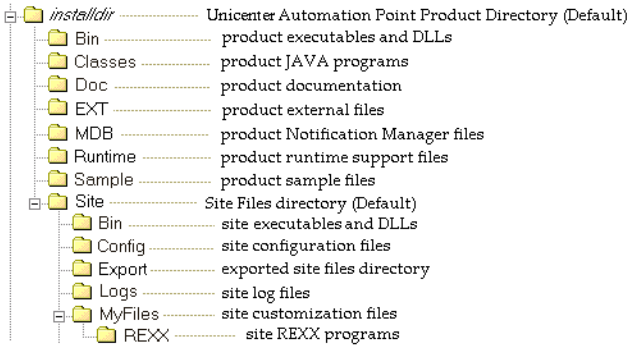
Upgrade the Notification Manager database as described in this section. You can then upgrade the remaining CA Automation Point servers pointing to that database in any order without impacting the operations of other CA Automation Point servers.

We recommend upgrading all CA Automation Point server installations that are connected to a single NM Database expediently to this new version. This database upgrade provides full functionality and limits the impact to Notification Website users.

How Site Files are Managed

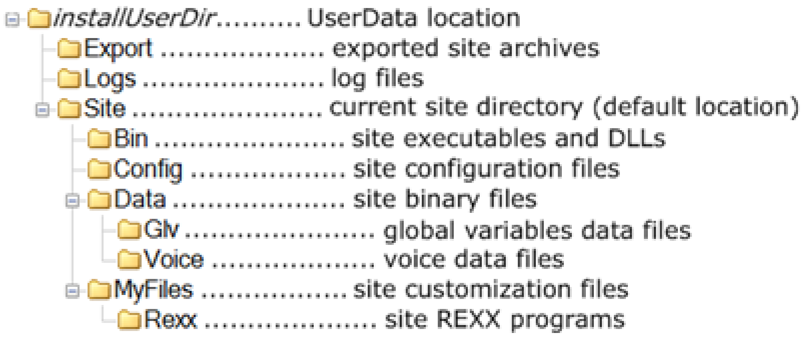
CA Automation Point keeps customer-modified data separate from CA-distributed data so that when a patch or upgrade is run, it leaves the customer-modified data intact. All customer-modified data is kept under the Site files directory (the system-level environment variable *%AP_SITE%* will be populated to point to the current Site directory in use by CA Automation Point).

In CA Automation Point Release 11.2 and earlier, the Site directory resided under the same parent directory as the rest of CA Automation Point. The following diagram shows this structure:



```
installdir ........ Unicenter Automation Point Product Directory (Default)
  Bin ........ product executables and DLLs
  Classes ........ product JAVA programs
  Doc ........ product documentation
  EXT ........ product external files
  MDB ........ product Notification Manager files
  Runtime ........ product runtime support files
  Sample ........ product sample files
  Site ........ Site Files directory (Default)
    Bin ........ site executables and DLLs
    Config ........ site configuration files
    Export ........ exported site files directory
    Logs ........ site log files
    MyFiles ........ site customization files
      REXX ........ site REXX programs
```

With this release of CA Automation Point, the Site files can reside under their own parent directory in a location independent of the install directory. The CA Automation Point installation program prompts you for a *UserData* path where all site-specific files will be stored. You can accept the default (recommended) or you can choose another directory location. The default has been selected so that many CA Automation Point executables can be run by Standard Users. Under Windows Server 2008 or later, the *UserData* path resides under the *ProgramData* directory. The following diagram shows this new structure:



```
installUserDir.......... UserData location
  Export ................... exported site archives
  Logs ..................... log files
  Site ...................... current site directory (default location)
    Bin ...................... site executables and DLLs
    Config .................. site configuration files
    Data .................... site binary files
      Glv ...................... global variables data files
      Voice .................... voice data files
    MyFiles ................. site customization files
      Rexx .................... site REXX programs
```

However, the CA Automation Point installation program will *not* prompt you for a *UserData* location on upgrades from a previous release. On upgrade installations running on a pre-Windows 2008 operating system, you do not need to move the Site files to a user-writable location because the Windows operating system does not require it.

Note: During an upgrade installation of CA Automation Point, any preexisting files found in the *Bin* or *Distrib* (formerly *RUNTIME*) directories that are not among the product-distributed files to be installed, are moved into the *UserData* directory structure. These files are either user files or formerly distributed files that are no longer supported in the current release. You can choose to retain or delete these files under the *UserData* directory structure.

Export and Import Utility

CA Automation Point Release 11.2 is not supported on the Windows 2008 Server operating system. The Export and Import Utility supports moving configuration settings from a CA Automation Point Release 11.2 server installation to a clean server installation of CA Automation Point Release 11.4.1 server. This utility also supports moving configuration settings from one CA Automation Point Release 11.4.1 server to another.

Migration of your current configuration settings is handled automatically during an upgrade installation.

You can move configuration settings from CA Automation Point on one machine to a clean install of CA Automation Point on another machine in one of the following ways:

- Perform an upgrade and export settings.
- Manually migrate configuration settings

To migrate configuration settings by upgrading.

1. Upgrade the server to CA Automation Point Release 11.4.1.
2. Export CA Automation Point configuration settings from the source machine.
3. Copy the exported zip file to the destination machine.
4. Run importSess on the destination machine and point to the exported zip file on the local destination machine.

To manually migrate configuration settings from Release 11.2 to a clean CA Automation Point Release 11.4.1 installation.

1. On a CA Automation Point Release 11.2 or Release 11.3 server machine, choose the Manage Site Files option in the File menu of Configuration Manager to run the Export and Import utility.
2. Export your site configuration settings to standby Sites. For more information, see the *CA Automation Point Administrator Guide*.
3. Find the folder with exported Site configuration. This folder is in the *%AXC_SITE_PATH%\Export*.
4. Copy the entire exported Site folder to a removable storage device, such as USB flash drive.
5. When migrating stored Web MV user data, copy the following files under the *StoredApMsgs* folder in your CA Automation Point installation directory to your removable storage device:
   - userConfig.CDX
   - userConfig.DBF
   - userConfig.FPT

6. On a CA Automation Point Release 11.4.1 server machine, copy the exported Site configuration folder from the removable storage device to the *%AP_DATA%\Export* folder on the server.
7. If you also saved Web MV user data, copy the *userConfig.** files to the *%AP_HOME%\StoredApMsgs* folder on the server.

   Note: Web MV user files can have the .CDX, .DBF, or .FPT file extension.
8. On the CA Automation Point Release 11.4.1 server machine, choose the Manage Site Files option in the File menu of Configuration Manager to run the Export and Import utility. The exported Site configuration from CA Automation Point Release 11.2 appears in the list of Standby Site Archives.
9. In the list of Standby Site Archives, select the items that you want to import and click Import to Site.

Your configuration settings are imported to CA Automation Point.

For more information about the Export and Import utility, see the section Managing Site Files in the *CA Automation Point Administrator Guide*.

Removal of NETBEUI Network Transport from PPQs

Support for the NetBIOS protocol has been removed in CA Automation Point Release 11.3.

The CA Automation Point PPQ utility has traditionally supported various implementations of the NetBIOS network protocols to provide backward compatibility with older versions and PPQs running on OS/2. Microsoft no longer installs NETBEUI in Windows XP during a typical installation and has dropped it completely from Windows Server 2003. Because TCP/IP is now prevalent and NETBEUI cannot be routed over a WAN, NETBEUI is no longer a configurable network transport for PPQs.

The CA Automation Point Release 11.4.1 upgrade installation process automatically removes any previously configured NetBIOS NetBEUI transports and retains remaining network transport settings. If no transport is specified, the network transport is reset to the default, Local Communications Only.

VIO Sessions

The default working directory for VIO sessions changed in CA Automation Point Release 11.3. The new working directory for VIO sessions is the *Site\MyFiles* directory. In previous releases, the default working directory was the RUNTIME directory.

HLLAPI and Cut Mode Connection Support

CA Automation Point Release 11.3 dropped support for HLLAPI (Attachmate EXTRA!) and cut mode (Coaxial) connection types. The native TN3270 connection type is now the only available 3270 connection type. To migrate HLLAPI and cut mode sessions to TN3270, set their Host Name/IP and Port values in Configuration Manager.

CONNECT and DISCONNECT Key Operations

The meaning of CONNECT or DISCONNECT key operations changed in CA Automation Point Release 11.3. These operations were previously used to connect and disconnect HLLAPI sessions. For more information on how they have changed, see Customizing Special CA Automation Point Files in the *CA Automation Point Administrator Guide* and the discussion of the SESSCNTL command in the *CA Automation Point Command and Keyword Reference Guide.*

Removal of MAPI Support

CA Automation Point Release 11.3 dropped support for the MAPI email feature. This release supports only the SMTP protocol. Any previously configured MAPI settings will be deactivated when you install this release. If you configured MAPI in previous releases of CA Automation Point, you must reconfigure your email settings in Configuration Manager to use the SMTP protocol.

CA NSM Security Server

CA Automation Point Release 11.3 dropped support for the CA NSM Security Server. If you configured CA Automation Point to use the CA NSM Security Server, this configuration will be deactivated when you install this release. CA Automation Point will not allow you to establish a remote connection until you reconfigure your security settings with Configuration Manager.

3205 Terminal Type Support

CA Automation Point Release 11.3 dropped support for the 3205 terminal type used for processor consoles on bipolar mainframes. Any session previously configured with this terminal type will be deactivated during runtime and needs to be either reconfigured to another terminal type or removed.

Index