CA Automation Point

Release Notes

Release 11.4.3

CA Technologies Product References

This document references the following CA Technologies products:

- CA Common Services (CCS)
- CA Automation Point
- CA Network and Systems Management (CA NSM)
- CA OPS/MVS Event Management and Automation (CA OPS/MVS)
- CA MICS® Resource Management Q&R Workstation (CA MICS Q&R Workstation)

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 Problem Records (see page 14) section.

Contents

Chapter 1: Enhancements and Changes

This section discusses enhancements and changes that were made to the product with this release of CA Automation Point.

Notification Manager Website Enhancements

A Notification Details section was added to the Notification Status page. This section displays when and for whom the selected notification was issued. This new section also includes additional status information for the selected notification request, including the methods that were used for notification.

A Filter section was also added to the Notification Status page. This section allows you to restrict the displayed notification requests to those requests that match the specified filter criteria.

The previous time limitation for displaying notification requests (those requests that are issued within the last 24 hours) has been removed.

Three new Basic Privileges were added to the Notification Website. These new privileges are:

View all contacts

Users with this privilege can view (but not modify) all contacts and their notification schedules.

View all notifications

Users with this privilege can view all notification requests currently stored in the notification policy database using the Notification Status page.

Answer all notifications

Users with this privilege can provide an answer to any outstanding notification request.

Primary Control Mode

CA Automation Point Release 11.4.3 brings several enhancements to the Primary Control Mode feature. It is now possible to dynamically transfer primary control between different users that are connected to the same session. Each session connection now also includes an indication of its primary control state. The configuration for primary control mode is also enhanced to allow a more fine-grained control of the feature. All of these enhancements are backward compatible with older supported versions of Remote Viewer, however the client side documentation for these changes is available only after upgrading to the 11.4 version of Remote Viewer in the AP Viewer Help.

Single Sign-On

The Single Sign-on feature can be enabled when Windows Security for remote viewing is selected. This feature allows anyone that is logged in to a Windows workstation using a user account that is recognized by the CA Automation Point server to connect to it without retyping login credentials. This feature typically applies to environments where workstations are part of a Windows domain and where Active Directory user accounts are used.

Web Service API

We provide a web service API to enable third-party applications on a remote computer to make requests and receive data to/from a CA Automation Point server. This API performs operations on CA Automation Point notifications, on host sessions that CA Automation Point monitors, and on messages within those sessions. For more information, on an introduction to our web service capabilities see the *CA Automation Point Product Guide*.

The CA Automation Point web service components have been enhanced to recognize the XML 'encoding' attribute, which specifies the character set of an XML document. Any character set supported by the Java virtual machine can be used.

To support the character set enhancements, the RequestService client-side Java API has been altered. Any customer Java programs which call the RequestService API must be modified and recompiled to work correctly. The Customer programs that directly call the web service server-side API are unaffected. The RequestService command-line interface is also unaffected.

The RequestService client-side Java API and command-line interface have been enhanced to encode automatically URIs using percent (%) escape sequences specified by the Internet Engineering Task Force (IETF).

The Request Service client-side Java API and command line interface have been verified on Unix System Service (USS) under z/OS 1.13. A separate USS distribution of this client component is now available in our Sample directory after CA Automation Point is installed.

Client Setup Installation Modes

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

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.

The CurrentUser mode does not require Administrator privileges to perform the installation but the deployed applications are only available to the user account under which the installation was performed.

Unattended Installation

A sample script that shows how to execute an unattended client installation is available.

For more information, see the *CA Automation Point Installation guide*.

WebMV Time Format

The ability to switch between 12 hour and 24 hour time formats has been added to WebMV. For more information, see the *CA Automation Point Administrator Guide*.

Permissions on AP Msg Recall Window

Permissions can now be assigned to the AP Msg Recall window. Previously, all users had FULL permission on the AP Msg Recall window.

Java 7 Runtime Requirement

Several components of CA Automation Point are written in the Java programming language. You are required to install the Java Runtime Environment (JRE) to run these components. CA Automation Point redistributes version 7 of the JRE. The Java components of CA Automation Point are also compiled using version 7 of the Java Development Kit (JDK). To provide additional functionality to the Java language, the Java vendor (Oracle) has changed how the Java source code is represented in binary form. Due to the binary representation change, all Java code that is compiled using JDK version 7 requires JRE version 7 or greater to execute. To use any Java components that CA Automation Point provides, first install JRE version 7. When upgrading from a previous release of CA Automation Point, the Java product components that are configured previously are disabled during the product upgrade process. These components can be enabled using the Configuration Manager application which enforces the installation of JRE version 7.

Implemented Demand Analysis Requests (DARs)

The following DARs have been implemented with this release of CA Automation Point:

16439557-1: Read only access to contacts

The new privilege View All Contacts has been added to Notification Manager. This privilege allows the user to view (but not modify) detail and schedule information of any contact defined in the notification policy database.

16439566-1: Read only access to notifications

The new privilege View A*ll Notifications ha*s been added to Notification Manager. This privilege allows the user to view detailed information about any notification request stored in the notification policy database.

16439580-1: Notification status panel

The Notification status page now contains a Details section where you can review notification status and progress.

16439519-1: Acknowledge notification via web

16439629-1: NmAdmin can answer all calls

The *Notification Status pag*e now allows the user to provide an answer for any notification request that is waiting for an answer.

16423372-1: Display priority on contact *page*

The notification priority that is *ass*igned to a personal schedule is now displayed directly on either the Modify Individual or Modify Group pages.

20495233-1: Add item number to NM call tree display

The notification call tree that is displayed by the NMFIND REXX program now displays the item number of the current notification request on each call tree branch.

Chapter 2: Known Issues

The following sections discuss known behavior in CA Automation Point Release 11.4.3.

This section contains the following topics:

Problem Records

The following Problem Records have been created:

#710 - FIX REQUIRED TO WORK WITH JAVA.7U51

Oracle has changed the way security works with this version of Java. Specifically Applets and web start applications are affected. This change could affect the ability to log on to WebMV or the Notification Website, or both.

#711 - APOLLNT.EXE MESSAGE MISHMASH RESISTANCE FIX

The apollnt.exe was failing and had to be restarted to allow Windows message automation.

#712 - WEBMV LOGON FIX

The first log-on failure caused further attempts to fail.

#713 - HAF CRASH

HAF is throwing an exception error.

#714 - GLV THROWING EXCEPTION

GLVs are throwing exception errors.

#716 - VIRTUAL TERMINAL OUT OF SCREEN CRASH

AP Desktop was failing because of access violation in the virtual session emulator.

#717 - REMOTE MANAGER EXCEPTION

Remote Manager was failing because of access violation in the debug message.

#718 - WIN-REMOTE CCI CONNECTION LOST

The CCI connection between CA OPS/MVS and the Automation Point machine is not restored automatically when the Windows machine is rebooted.

#719 - VOX CRASH WITH OPEN OBJECT REXX

When using Open Object REXX 4.2, executing VOX commands in the command prompt causes vox.exe to crash.

#720 - TRACE-IN-MEM CRASH

Under special circumstances, looping threads can generate 1000 trace-in-mem messages between two regular log messages and rewrite log message text while it is being formatted, causing a virtually inexplicable crash.

#721 - LOCKED FONT FILES DURING AP INSTALL

Upon installation a new version of Automation Point would sometimes report locked font files during installation. Under these circumstances, the user sees error messages stating that these files could not be overwritten.

#722 - RECONNECT TOO SOON

Reconnect sometimes triggers too early and gets stuck in a loop.

#723 - UNABLE TO DOM OPS MESSAGES FROM WEBMV

Action messages from an internal session window, such as the OPS/MVS window, could not be DOMed from WebMV. The user would receive the following error message: Command execute permission is required to DOM Action Messages.

#729 – Fixes included in 11.4.2.1

- Poodle remediation.

- 21936392: Unable to use delete key when renaming session in Configuration Manager.

- 21966092: Allow action messages captured from the built-in OPS session to be added to the action message table. This allows the GETMSGI processor to retrieve these action messages and the DOM processor to DOM these messages.

- 22031560: Products Stop Working On Every log roll. Every two days, when the rules engine forced a log roll at midnight, the AP Desktop would get into a deadlock condition and crash after 8 minutes.

- 21947161: Fix traceInMem exception caused by wrong number of vs-style parameters.

- 22004570: If multiple Remote Viewer clients request the same session window at nearly the same time, the Remote Manager service would crash.

- 21936380: Under certain conditions, the Session Definition Set dialog within the Configuration Manager application would not allow the user to enable a session.

- 22051128: Asorexx.exe 50-90 % Cpu when using AS/400 Manager component. The 5292 console would stop drawing the screen when a '0xFE' character was detected in the datastream.

- Added support for the SSH CTR cipher mode.

- Made the "Found NULL in old screen image" log message a debug message to avoid filling up the log.

#731 – Fixes included in 11.4.2.2

- 21936371: Prevent a previously deleted session definition from stopping the creation of a new session with the same name.

#734 – Fixes included in 11.4.2.3

- 00042124: Allow notification messages than span multiple lines to be imported using the ADDRESS VOX NMIMPORT command.

- 00045564: Added more message IDs to the list of messages displayed during NIP so that the console driver can detect when the console is in NIP mode.

#737 – Fixes included in 11.4.2.4

- 00096496: Modified the Remote Manager service to recover after the AP Desktop is shutdown to allow for the AP Desktop to be restarted remotely.

- 00081029: The ACKNOWLEDGEAP and ACKNOWLEDGEOPS options of the NMFIND.REX program were modified to permit the use of a single quote in the TELL string of the notification text.

#738 – Fixes included in 11.4.3.0

- 00018210: Prevent iSeries HMC connections from encountering a prolonged X-SYSTEM wait state.

Session Definition Sets

If you have multiple session definition sets and you have applied the event monitoring settings to only a subset of these session definition sets, and then you activate one of the session definition sets to which event monitoring settings were not applied, you will not see the sessions that are associated with the monitored event when CA Automation Point is started. However, when you go into the particular event monitoring dialog, all settings appear enabled.

MDB Cell Error During Installation of CA Common Services

During the installation of CA Automation Point's interfaces to CA NSM or CA OPS/MVS EMA, you can encounter an error. This message states 'MDB Cell setup has failed'. This error message gives you the opportunity to continue or cancel the installation. Select continue and the installation completes successfully, and all components CA Automation Point uses operate successfully. CCS DIA DNA component issues this error message. CCS automatically installs the CCS DIA DNA component but CA Automation Point does not use this component.

Open File Dialog during Installation

In rare cases, a generic Open File dialog appears during the installation process requesting a file with an .exe extension. This dialog happens under some circumstances when CA Secure Socket Adapter is installed on the system (usually as part of another CA product).

You can close the Open File dialog by clicking Cancel on the dialog; the CA Automation Point setup should finish successfully. The only side effect of this issue is that the Windows Add/Remove facility now contains two separate entries for CA Secure Socket Adapter. These entries have no impact on the runtime operations of CA Automation Point. If you want to remove the obsolete entry, contact CA Technical Support for further assistance.

CA Automation Point and CA MICS Q&R Workstation

CA Automation Point and CA MICS Q&R Workstation cannot be installed on the same machine. CA MICS Q&R Workstation uses an older version of CA Common Communication Interface (CCI) than CA Automation Point does. The new CCI installed with CA Automation Point causes CA MICS Q&R Workstation services to fail.

Very Long Site Path or Session Definition Set

When you specify a very long customized user files folder during installation or specify very long session definition set names, CA Automation Point configuration data may not be saved or imported properly. We recommend that all session definition set names and the install user files directory are no more than 100 characters long.

Note: Install user directory path is stored in environment variable %AP_DATA%. Session definition set name is used as part of file name that stores session definitions and stored under %AP_DATA%\Site\config directory. Other various configuration and user files are stored under %AP_DATA% as described in "How Site Files are Managed" in the *CA Automation Point Installation Guide*. All previously mentioned file paths must be valid Windows paths and are subject to length limit of MAX_PATH (259 characters). Also consider possible files and session definition sets you will import or store in this directory structure in the future.

Notification Manager Issues

This section discusses known issues regarding the Notification Manager.

CA Product Compatibility

The Notification Manager component of CA Automation Point uses version 1.5 of the CA Management Database (MDB) to store notification policy data. When you install other CA products to operate against the same MDB, you must be aware of your database compatibility for all such products.

- When CA applications for your site have been designed to operate with MDB 1.5, no special actions are required to install and use those applications.
- When creating a fresh Notification Manager database with CA Automation Point and installing other applications that do not yet support version 1.5 of the MDB. Before, installing these products make your MDB backwardly compatible. The steps that are required for this backward compatibility process are available at the CA technical support site. Locate this procedure by selecting the Advanced Search link on the main page and using the keywords “CA Management Database Mixed Version Installation”.

Notification Monitoring Applies to Both CA OPS/MVS and CA NSM Event Manager

When you enable the monitoring of notification requests from CA OPS/MVS, you automatically enable the monitoring of notification requests from CA NSM. The reverse is also true. If you do not want CA Automation Point to monitor one of these two sources, do not select any hosts for that source, and CA Automation Point will not perform any unnecessary monitoring.

Dialogic Voice Card Drivers on Windows 64-bit Operating Systems

The Dialogic installation program that is provided on the CA Automation Point installation DVD2 supports 64-bit operating systems, but only under Windows Server 2008 64-bit. The installed Dialogic drivers do *not* run under Windows Server 2003 64-bit.

Notification Manager Status of Initializing

Under certain circumstances, the initializing status of a notification request that is submitted and displayed by the Notification Website does not progress beyond the initializing state. If a notification request remains in the initializing state for an extended period, the notification request can be considered a failure and should be re-issued. If you continue to see that the notification requests do not progress past the Initializing state, verify that the Notification Server is correctly configured to establish a database connection. Also, make sure that the database server is ready to accept database connections and the Notification Server is currently active.

Apache Tomcat Monitor Fails to Start as a Standard User

The version of Apache Tomcat that is shipped with CA Automation Point includes a component named the Apache Tomcat Monitor. This component runs in the system tray area and allows you to control the running status of the Apache Tomcat server. Because this Apache Tomcat Monitor program requires permission to interact with system services, it cannot be executed as a standard user. A standard user is defined as a user account not in the Administrators permission group. As a result, if a standard user signs in to the CA Automation Point server machine, the Apache Tomcat Monitor displays an error message and shuts down. The error message that is displayed is Unable to open the service ‘Tomcat7’.

To allow this program to execute properly when launched as a standard user, the privilege level of the Apache Tomcat Monitor executable must be elevated to run as an administrator. The Microsoft Windows Server 2003 operating system does not provide a compatible permission elevation technique that allows this Tomcat Monitor program to start successfully when executed from a standard user account. When using the Microsoft Windows Server 2008 or later operating system, use the following steps to change the properties of the Apache Tomcat Monitor executable to allow a standard user to run this program with elevated privileges.

To change user permissions.

1. Locate the tomcat7w.exe program in Windows Explorer (the default directory is C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin).
2. Right-click the name of this file and select the Properties context menu item.

   The tomcat7w Properties dialog displays.
3. Select the Compatibility tab and click either the "Show settings for all users" button or the "Change settings for all users" button at the bottom of the dialog.

   A new tomcat7w.exe Properties dialog displays with a single tab entitled Compatibility for all users.
4. At the bottom of this dialog, in the Privilege Level group box, select the Run this program as an administrator.

   The Apache Tomcat Monitor executable will now execute with the required privileges when run from a standard user account.

After making this change, a standard user may need to specify the administrator password each time they sign into the Microsoft Windows Server 2008 or later machine to launch the Apache Tomcat Monitor application.

No ADDRESS TNG Error Text

When the CA-AP NSM Gateway service is not running, and a REXX program that calls an ADDRESS TNG command executes, the ADDRESS TNG command fails with error code 30. This command failed because the CA-AP NSM Gateway service must be running to enable ADDRESS TNG commands. However, the TNG.ERROR stem variable does not contain any text to explain this scenario.

Version of AP Help from AP Viewer May Not Correspond to Your CA Automation Point Server

The help that is provided by the 'AP Help' entry in the AP Viewer menus describes the capabilities of the CA Automation Point Server Desktop. This help is installed with the AP Viewer client, and that client may be at a different release than the CA Automation Point server to which you connect. Therefore, the help could describe a different version of CA Automation Point than the version running on your server.

Remote Viewer Windows Do Not Open after Layout Load

Loading Remote Viewer layouts in rapid succession can prevent one or more remote windows from opening. Subsequent attempts to load these windows will fail. To fix this problem, restart Remote Viewer.

Changing Fonts Causes Layouts to Load Incorrectly

When you change the set of fonts available to CA Automation Point, and subsequently load a layout saved before such a change, desktop windows may be sized incorrectly. This may happen after you use the Customize Fonts feature of Configuration Manager or the /fonts command-line switch.

To correct the window size, change the window font size by using the Select Font option from the Window menu, then save the layout.

ADDRESS AXC GETVAR with Non-existent Variables

When issuing the following REXX command:

```
GETVAR varname rexxvar
```

if the variable *varname* does not exist (it has not been previously set), return code in RC is 0, and *rexxvar* is set to an empty string.

Configuration Manager Process Does Not Close

Sometimes when you close Configuration Manager, the settings are saved and the interface closes, but the process remains in the process list. Because you can launch another Configuration Manager process, this problem does not have any functional impact. You can use the Windows Task Manager to end the running process.

Stored passwords lost when importing configuration or during an upgrade install

In rare cases passwords configured in Release 11.2 or older can disappear in Release 11.3 or higher. This issue can happen during an upgrade installation from Release 11.2 or during an import of a site that was exported from Release 11.2. Passwords configured in CA Automation Point r11.3 and higher are unaffected.

Use Configuration Manager to check if they are missing and re-enter them if necessary. Affected passwords are:

- Automation > Automation Services Startup Options > Security Context for AP Desktop > Password
- Automation > Events Interface > CA NSM WorldView Repository > Password
- Notification Services > Notification Services Startup Options > Security Context for Notification Server > Password
- Notification Services > Notification Manager > NM Setup > NM Database > Admin

Appendix A: Third-party Software Acknowledgements

This section provides information about third-party software acknowledgments. The third-party license agreements are available in the \Bookshelf Files\TPSA folder in the CA Bookshelf.