CA Process Automation

Release Notes

Service Pack 04.2.01

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 is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

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.

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.

Contents

Chapter 1: Welcome 9

Documentation Bookshelf....10
Best Practices Documentation....11
CA Process Automation Support Home Page....11
Support Engagement Guidelines....12
Supported CA Process Automation Releases....13

Chapter 2: Installation Considerations 15

General CA Process Automation Upgrade Considerations....16
Language Certifications....16

Chapter 3: New Features 19

CA Process Automation Service Pack 04.2.01....19
  Configure Load Balancers for Agent Scalability....19
  Support for Oracle JDK7 Update 51....24
  Enhancement for SOAP based Operators....25
CA Process Automation Release 04.2.00....26
  Content Management Enhancements....27
  User Experience Improvements....29
  Java-Related Improvements....31
  CA EEM Release 12.51 Support....33
  Performance Improvements....37
  Communication Improvements....38
  Clustering Improvements....40
  Security Improvements....41
  Database Server Improvements....42
  Support for CA SiteMinder Secure Proxy Server (SPS)....42
CA Process Automation Service Pack 04.1.01....43
  DNS Lookup Bypass for Host Groups....43
  Double-Click Task to Initiate Reply....44
  Increased Initial Java Heap Size for 64-Bit Installations....44
  Customized OasisConfig.properties Is Retained After Upgrade....44
CA Process Automation Release 04.1.00....45
CA Process Automation Service Pack 04.0.01....49
CA Process Automation Version 04.0.00....52
  Full Browser-Based User Interface....52

Operator Enhancements 52
Usability Enhancements 53
Web Services HTTP Properties 54

Chapter 4: Retired Features 55

Package 55
XA Distributed Transaction Dependency 56
Self-Contained Mode 56
AIX and HP Platform Support for Orchestrators 56
Support for CA SiteMinder Web Agent on Apache and IIS 56
Ability to Share a Library Data Store Across Domains 57
Microsoft Internet Explorer 8 57
Direct LDAP and Active Directory Support 57
Log Viewer Objects 57
Retired and Replaced Operators 57
State Policies and Rules Engine 58
Telephony Application Programming Interface (TAPI) Support 58

Chapter 5: Fixed Issues in 04.2.01 59

Chapter 6: Known Issues 63

CPU Usage Spikes in server nodes with Secured Simplified Communication and Load Balancer 64
NSM Operators Fail on an Agent That Points to a 64-bit JDK 65
Agent Communication Defaults to Deprecated Method 65
NGINX on Windows Does Not Scale Like NGINX on Linux 65
CPU Usage Spikes with Secured Simplified Communication and NGINX 66
REST and Catalyst Operations Are Not Handled by CA SiteMinder SPS in One Case 66
Disabling of JBoss Seam Framework after an Upgrade 67
Microsoft User Access Control Prevents Successful Launch of Orchestrator Node 68
Potential Problem When Running CA Process Automation on a VMWare Server When Using the E1000 Network Interface 69
Turkish Operating System Required for Installing Turkish Version of CA Process Automation 70
CA EEM Release 8.4-to-12.0 Server Upgrade Issue 71
SOAP Operations in CA Process Automation 71
CA Process Automation Installation on Dual Stack (IPv4 and IPv6) Network Environments 72
Export Objects Can Contain Only English Characters 72
Google Chrome Fails First Attempt to Log Out Users Logged in Using NTLM 73
JDK 1.7 is Unable to Encrypt and Decrypt Passwords with Special Characters like "&" in SUSE 11SP1 73
Limitations in Internet Explorer 74
Oracle bug # 9347941 74

Sorting Automation Objects 75
Unable to Launch CA Process Automation using the Apache URL in Internet Explorer and Firefox 75
Limitations to Process Definition Upgrade 75
SERVER_CONNECT_FAILED Error 76
Documentation Known Issues 76
    Missing information in the Content Designer Reference Guide 77

Appendix A: Acknowledgments and License Agreements 79

Components Licensed under the Apache Software License v.2.0 81

Chapter 1: Welcome

Welcome to CA Process Automation Release 04.2.00. CA Process Automation is designed to speed the delivery of IT services while helping to remove manual errors. By defining, automating, and orchestrating processes across organizational silos that use disparate systems, CA Process Automation helps improve your productivity while also enforcing standards.

CA Process Automation lets you automate IT processes across multiple organizations and systems, reduce the service delivery time, and enforce standards and compliance policies across departments.

CA Process Automation helps you automate IT processes to:

- Reduce operational expenses
- Increase staff productivity
- Speed IT service delivery
- Improve service quality
- Enforce your compliance polices

This document contains information about new features, enhancements, resolved issues, known issues, and installation in this release, and tells how to contact CA Technical Support (see page 3).

Documentation Bookshelf

The CA Process Automation bookshelf provides convenient access to the following product documentation in both HTML format (for online viewing) and PDF format (for printing). Both formats include search features.

- *Release Notes*
- *Installation Guide*
- *Content Administrator Guide*
- *Content Designer Guide*
- *Content Designer Reference*
- *Web Services API Reference*
- *Production User Guide*
- *User Interface Reference*
- CA Process Automation scenarios

  A *scenario* is concise, modular information that explains how to interact with CA Process Automation to achieve specific goals.

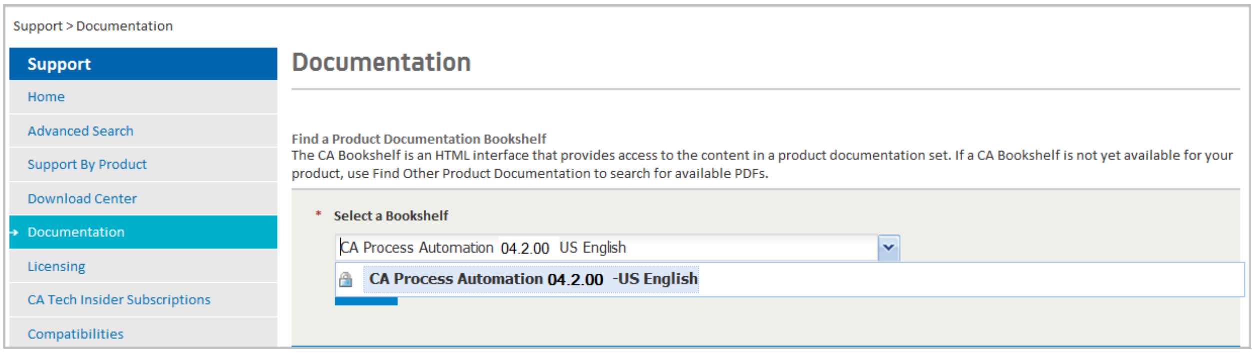
The CA Process Automation Bookshelf also includes the following features:

- Functionality to search the entire documentation set.
- Links for using the bookshelf, downloading Acrobat Reader, and contacting CA Technologies.
- Links to supplemental information about CA Process Automation such as videos, technical documents, educational courses, and other valuable resources.

You can view the bookshelf in the following ways:

- Through the Help menu in the CA Process Automation browser-based UI. The Book Shelf link is typically to the bookshelf on CA Support. If you are working in an environment without Internet access, the person who installs CA Process Automation provides a local copy that the Book Shelf link accesses.
- Through the bookshelf “quick” link on the home tab of the CA Process Automation browser-based UI.
- If CA Process Automation is not open, you can download it from CA Support.

  Log in is not required. Select Documentation and then select CA Process Automation, the release number, and language from the Select a Bookshelf drop-down list. Click Go to open the bookshelf.



Support > Documentation

Documentation

Find a Product Documentation Bookshelf
The CA Bookshelf is an HTML interface that provides access to the content in a product documentation set. If a CA Bookshelf is not yet available for your product, use Find Other Product Documentation to search for available PDFs.

* Select a Bookshelf

CA Process Automation 04.2.00 US English

CA Process Automation 04.2.00 -US English

The online help provides CA Process Automation workflows that can help you understand who does what and when. The scenario-based content provides drill-down information about lifecycle tasks that administrators, content designers, and production users perform. Additionally, you can get context-sensitive help for each operator on the Designer tab canvas. Context-sensitivity is at the tab level for the other tabs.

Best Practices Documentation

Click the Best Practices link under "Quick Links" on the Home tab to access the CA Process Automation Implementation Best Practices page. This page contains a collection of best practices documents and references to other supplemental material.

CA Process Automation Support Home Page

The CA Process Automation Support Home Page includes the following information to supplement this documentation set:

- The latest CA Process Automation product news
- Product status, including third-party software and operating system compatibilities that were released after publication of this documentation set

- Access to CA Process Automation downloads that include patches, documentation, and localization updates
- Knowledge Base updates

Use the "support" link in the Help menu in the CA Process Automation browser-based UI to access the CA Process Automation Support Home Page.

Support Engagement Guidelines

Support for CA Process Automation is available to licensed customers through X--Customer Support in the following circumstances:

- The core product installation reports errors.
- The product abends, reports errors, fails to initialize, or exhibits degraded performance.
- Core product functionality does not perform consistently with the documentation.
- You have a question about upgrading from a previous release or about CA Process Automation integration with other CA Technologies products.

CA Technologies provides alternative ways to engage support in the following situations:

- You need assistance using CA Process Automation functionality to complete specific tasks.
- You need guidance regarding best practices for using CA Process Automation.
- You need advice about implementing CA Process Automation in your environment.
- You need assistance with making the product work consistently with your defined workflow.
- You need assistance troubleshooting a process that you built.

Use the following resources for assistance in these situations:

- CA Process Automation Global User Community
- CA Services
- CA Partners
- CA Education, through your local or regional CA Technologies account manager

Supported CA Process Automation Releases

For information about releases that are no longer supported, see the End-of-Service and End-of-Life notices under Product News on the CA Process Automation home page.

For a complete list of supported platforms and requirements for the CA Process Automation Release 04.2.00 components, see the *Installation Guide*.

Chapter 2: Installation Considerations

This section highlights the following information:

- Significant changes to the CA Process Automation installation process
- Information about upgrading CA Process Automation
- Installation requirements that are introduced in the current release

See the *Installation Guide* for detailed information about these changes and the procedures to use to install, upgrade, and configure CA Process Automation.

This section contains the following topics:

General CA Process Automation Upgrade Considerations (see page 16)
Language Certifications (see page 16)

General CA Process Automation Upgrade Considerations

The *Installation Guide* that accompanies CA Process Automation 4.2 contains the information you need for successful upgrade. For example:

- Planning and pre-requisite checking is of paramount importance when upgrading to CA Process Automation 4.2. We strongly recommend that you read the "Upgrade to the Current Release" section in the *Installation Guide* before proceeding.
- Beginning with CA Process Automation v4.0, you must configure the product to use CA Embedded Entitlement Manager (CA EEM). If you previously used a directory service such as Microsoft Active Directory or another LDAP-compatible directory service with CA Process Automation, you can configure CA EEM to use it as the external user store.
- CA Process Automation 4.2 installation or upgrade requires that you have Java Development Kit (JDK) 1.7 on the target host. See "Platform Support and Requirements for CA Process Automation Components" in the accompanying *Installation Guide* for details such as this.
- The earliest release supported for upgrade is 3.1 SP01. If you are upgrading from an earlier release than 3.1 SP01, download CA Process Automation 3.1 SP01 from support and upgrade your release to r3.1 SP01. Then, upgrade from 3.1 SP01 to 4.2 as described in the CA Process Automation Release 04.2.00 *Installation Guide*.

  Note: The initial upgrade can take several hours to complete due to extensive schema changes.
- CA Process Automation 3.1 SP01 functions perfectly even when installed on machines with non-standard DNS host names, for example, a host name that includes the underscore character. This is not the case with CA Process Automation 4.2. Therefore, DNS host names must strictly adhere to naming standards. For more information, see the *Installation Guide*.

Language Certifications

An *internationalized product* is an English product that runs correctly on local-language versions of the required operating system and third-party products. An internationalized product also supports local language data for input and output. Internationalized products support the ability to specify local language conventions for date, time, currency, and number formats.

A *translated product* (sometimes referred to as a localized product) is an internationalized product that includes local language support for the following items:

- The product user interface (UI)
- Online help and other documentation
- Local language default settings for date, time, currency, and number formats

This CA Process Automation release is internationalized and localized in the following languages:

- Brazilian Portuguese
- French
- German
- Italian
- Japanese
- Simplified Chinese
- Spanish
- Turkish
- US English

Visit the download area of the CA Process Automation Support Home Page for access to the latest localized documentation. Use the Documentation link in the CA Process Automation UI to access the CA Process Automation Support Home Page.

Chapter 3: New Features

This section contains the following topics:

CA Process Automation Service Pack 04.2.01 (see page 19)
CA Process Automation Release 04.2.00 (see page 26)
CA Process Automation Service Pack 04.1.01 (see page 43)
CA Process Automation Release 04.1.00 (see page 45)
CA Process Automation Service Pack 04.0.01 (see page 49)
CA Process Automation Version 04.0.00 (see page 52)

CA Process Automation Service Pack 04.2.01

CA Process Automation Service Pack 04.2.01 includes the following enhancements and improvements:

- Configure Load Balancers for Agent Scalability (see page 19)
- Support for Oracle JDK7 Update 51 (see page 24)
- Enhancement for SOAP based Operators (see page 25)

Configure Load Balancers for Agent Scalability

In this release, you can perform the following recommended configurations in the load balancers for agent scalability:

- Configure the NGINX Load Balancer (see page 20)
- Configure the Apache Load Balancer (see page 21)
- Configure the F5 Load Balancer (see page 23)

Configure NGINX Load Balancer

You can configure NGINX load balancer to increase the number of agents in a cluster setup for secure and non-secure communication.

Follow these steps:

1. Navigate to the folder (for example, nginx_install_dir/conf/NGINX.conf) that contains the NGINX.conf file.
2. Add the worker_rlimit_nofile property and set the value to 8192 in the NGINX.conf file.
3. Edit the value of the worker_connections property to 4096 in the NGINX.conf file.
4. Edit the worker_processes property value in the NGINX.conf file that is based on the number of agents you want to install.

   For example, to install 1000 agents in a two-node cluster setup, edit the worker_processes property value to 4 in the NGINX.conf file. Similarly, to install 2000 agents in a two-node cluster setup, edit the *worker_processes* property value to 8 in the NGINX.conf file.
5. Restart the NGINX load balancer.

Configure Apache Load Balancer

Make the changes in the workers.properties and uriworkermap.properties files to configure Apache load balancer to increase the number of agents in a cluster setup for secure and non-secure communication.

- workers.properties
  - Add "uiloadbalancer" in the list of workers that are used for mapping requests as follows:

    worker.list=uiloadbalancer, loadbalancer, status
  - Add the following entries to define load balancing behaviour for UI calls:

    worker.uiloadbalancer.type=lb

    worker.uiloadbalancer.balance_workers=node1

    worker.uiloadbalancer.sticky_session=1

    worker.uiloadbalancer.retries=1
  - Change the value of the following entry to "0":

    worker.loadbalancer.sticky_session=0
- uriworkermap.properties

  Change the value of the following entries to "uiloadbalancer"
  - /jmx-console
  - /jmx-console/*
  - /web-console
  - /web-console/*
  - /itpam/*
  - /itpam
  - /c2orepository/oasisHelp
  - /c2orepository/oasisHelp/*
  - /c2orepository/htmlFile/aboutUs/*
  - /c2orepository/htmlFile/language/*
  - /itpam/OasisPrimary
  - /itpam/JNLPRequestProcessor/installation
  - /itpam/clientproxy/c2oresourceaction
  - /itpam/clientproxy/c2oreportaction

Note: A new installation of CA Process Automation does not require any manual changes in the workers.properties and uriworkermap.properties files. For more information, see the Install a Load Balancer and Prepare Configuration Templates (Windows) section in the *CA Process Automation 4.2 Installation Guide*.

Additional Configuration for Apache Load Balancer for Secure Communication

To configure the load balancer for secure communication, see Configure Secure Communication (Windows) section of the *CA Process Automation 4.2 Installation Guide.*

Follow these steps:

1. Replace the following lines in Step 10.b of the installation procedure:

```
<VirtualHost *:80>
                JkMountFile conf/uriworkermap.properties
                RewriteEngine on
                RewriteCond %{HTTPS} on
                RewriteCond https://%{HTTP_HOST}%{REQUEST_URI}
^https://.*c2orepository*|MirroringRequestProcessor*|mirroringrepository*|Sta
rtAgent*|genericNoSecurity*|soapAttachment*|ServerConfigurationRequestServlet
*
                RewriteRule (.*) http://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
```

2. Restart the Apache load balancer.

Configure F5 Load Balancer

You can configure F5 load balancer to increase the number of agents in a cluster setup for secure and non-secure communication.

Follow these steps:

1. Follow steps 1 through 4 that are mentioned in the Create an F5 iRule for CA Process Automation section of the *CA Process Automation 4.2 Installation Guide*.
2. Specify the following updated iRule definition in the Definition text box:

```
when SERVER_CONNECTED {
    IP::idle_timeout 172800000
}

when HTTP_REQUEST {
                set PAMPOOL "PAMSRVRPOOL"
                set PAMWSPOOL "PAMJETTYPOOL"
                set NODE1 "10.130.5.146"
                set NODE2 "10.130.5.147"
                set WSPORT "443"

                switch -glob [HTTP::uri] {
                                "/jmx-console*" { pool $PAMPOOL }
                                "/web-console*" { pool $PAMPOOL }
               "/c2orepository*" { pool $PAMPOOL }
                                "/c2orepository/oasisHelp*" { pool $PAMPOOL }
                                "/c2orepository/htmlFile/aboutUs/*" { pool
$PAMPOOL }
                                "/c2orepository/htmlFile/language/*" { pool
$PAMPOOL }
                                "/c2orepository/htmlFile/installation/*" {
pool $PAMPOOL }
                                "/c2orepository/media*" { pool $PAMPOOL }
                                "/c2orepository/thirdParty*" { pool $PAMPOOL }

"/c2orepository/MainInstallerConfiguration.properties" { pool $PAMPOOL }
                                "/itpam*" { pool $PAMPOOL }
                                "/itpam/ServerConfigurationRequestServlet" {
pool $PAMPOOL }
                                "/itpam/MirroringRequestProcessor*" { pool
$PAMPOOL }
                                "/itpam/AgentConfigurationRequestServlet" {
pool $PAMPOOL }
                                "/itpam/StartAgent*" { pool $PAMPOOL }
                                "/itpam/OasisPrimary" { pool $PAMPOOL }
                                "/itpam/JNLPRequestProcessor*" { pool $PAMPOOL
}
                                "/itpam/JNLPRequestProcessor/installation" {
pool $PAMPOOL }
```

```
                                "/itpam/clientproxy/c2oresourceaction" { pool
$PAMPOOL }
                                "/itpam/clientproxy/c2oreportaction" { pool
$PAMPOOL }
                "/mirroringrepository*" { pool $PAMPOOL }
                                "/birt/*" { pool $PAMPOOL }
                                "/ws/node1" { pool $PAMWSPOOL member $NODE1
$WSPORT }
                                "/ws/node1*" { pool $PAMWSPOOL member $NODE1
$WSPORT }
                                "/ws/node2" { pool $PAMWSPOOL member $NODE2
$WSPORT }
                                "/ws/node2*" { pool $PAMWSPOOL member $NODE2
$WSPORT }
                                "/*" { pool $PAMWSPOOL }
                                default { pool $PAMPOOL }
                }
}
```

3. Restart the F5 load balancer.

Support for Oracle JDK7 Update 51

Previous versions of CA Process Automation use self-signed jars within the Java Web start applications for agent and orchestrator installation.

After the availability of JRE7u51/JDK7u51, Oracle escalated the javaws/JNLP security settings. Due to the default JVM security settings, applets, and web start applications that are self-signed or use self-signed jars fail to start.

To address the issue, CA Process Automation 04.2.01 Orchestrator and Agent components now only use CA-signed jars.

Note: If an agent uses JDK6, disable FIPS 140 compliance on all orchestrators (including each node of a clustered orchestrator). To disable FIPS 140 compliance on all orchestrators, set the *pam.fips.mode.enabled* parameter to “false” in the OasisConfig.properties file and restart the orchestrator.

Connector Installation Changes for Oracle JDK7u51 Support

If you use Oracle JDK7u51 and above on the CA Process Automation orchestrator, consider the following points:

- Upgrading to CA Process Automation 04.2.01

  When you upgrade CA Process Automation r4.x to CA Process Automation 04.2.01, install the 4.2.1 Classic Connectors to upgrade the existing classic connectors.

- Installing CA Process Automation 04.2.01

  For a new CA Process Automation 04.2.01 installation, install the CA Process Automation 04.2.01 Classic Connectors.

  Note: For more information on classic connectors, see the CA Process Automation Connector Readmes in the *Connector Installation Media*.

Enhancement for SOAP based Operators

Previously, the Operations Results pane for a particular Operator Dataset was populated with the SOAP response codes (HTTP status codes) for SOAP and Async SOAP operators only when a webservice call succeeded (200 response code) or an internal server error occurred (500 response code).

In this release, the Extract SOAP response code to dataset variable check box is added to the Call Results panel. When you select the check box, the Operations Results pane is populated with the SOAP response code (400 response code) for SOAP and Async SOAP operators.

CA Process Automation Release 04.2.00

CA Process Automation Release 04.2.00 includes the following enhancements and improvements:

- To move a new process and all of its objects from one Orchestrator to another, export a folder as a content package and then import the resulting file. This new method replaces the use of the deprecated Package automation object. For an introduction to content package, see Content Management Enhancements (see page 27).
- To keep your database from filling up with obsolete reports, you can now purge aged reporting data from the UI. For details about purging and other ease-of-use improvements, see User Experience Improvements (see page 29).
- To reduce a potential threat of misuse, the Invoke Java operator is now restricted to running on agents. For details about this and enhanced documentation on return Java types, see Java-Related Improvements (see page 31).
- To take advantage of new CA EEM features, upgrade CA EEM before you install or upgrade CA Process Automation. For details about changes to CA EEM that impact CA Process Automation, see CA EEM r12.51 Support (see page 33)
- You will find that CA Process Automation 4.2 works faster than it did in previous releases. For highlights on some important changes in this area, see Performance Improvements (see page 37).
- To take advantage of simplified communication between agents and a clustered Orchestrator, use a load balancer that supports web socket connections. For an overview of support for NGINX and configuration changes, see Communication Improvements (see page 38).
- For high availability, all nodes of a clustered Domain Orchestrator now act as only the primary node used to act. For an overview of changes related to the removal of the dependency on a primary node, see Clustering Improvements (see page 40).
- For an overview of changes that reduce threats, see Security Improvements (see page 41).
- The Orchestrator installation wizard now lets you specify a connection string to connect to an Oracle database server and also allows you to specify a SQL Server instance as a Database Server. See Database Server Improvements (see page 42)

Content Management Enhancements

Summary

- With the now deprecated Package object, it was easy to overlook required objects for the release version of the process you were exporting.
- Now, you assemble all of the objects needed by the new release of the process in the same export folder. Here, you can verify the completeness before exporting the folder as a content package.

  Note: If you are exporting objects that are not release-specific, you can export the folder as is, not as a content package.

Details

CA Process Automation Release 04.2.00 introduces Content Package, a new automation object that is created during one type of export.

Content Package

Content designers use a content package to bundle the release of a newly automated process such that its component objects cannot be modified by consumers who use the process in the production environment.

Specifically, after designers create, test, and refine a new process, they prepare a folder for export as a content package. In the folder, they assemble the release version of each object that the process uses. This folder must contain all objects used by the process; it cannot contain any unused or obsolete objects. The folder is exported as a content package to secure the release version of the objects after import. The folder structure that you establish for a project in the design environment is replicated in the production environment upon import. An imported content package contains a set of baselined objects for the same release. Users in the destination environment cannot modify the release version values of objects in an imported content package.

Note: For the details about export and import, see "Scenario: Export and Import Objects in a Content Package" in the *Content Administrator Guide*.

Required Folder Structure for a Content Package

A folder to be exported as a content package contains release-specific objects. Objects can be in the export folder or in a subfolder of the release-specific export folder. Folders contain a process object, all of the objects that use the process, and all objects that the process uses. All objects are marked with the same release version value as the folder release version. For an upgrade, the folder contains changed and unchanged objects. The automation objects that are imported in a content package cannot be modified; their assigned release version cannot be modified.

Use Datasets for Redistributable Content

The recommendation for redistributable content is to use datasets for the configuration parameters. Consider this case: A host group represents hosts with names matching a specified pattern or IP addresses within a specified subnet. An operator Target field can contain an IP address or host name of a host in a host group or it can contain a dataset reference to a host in a host group. In the design environment, the IP address or host name refers to a host used for testing the process.

When you export process objects in a folder as a content package, consider these points:

- Operators *cannot* be modified in the import environment.

  If an operator Target field contains an IP address or host name of a host used in the design environment, the imported process cannot run successfully. The operator Target entry cannot be modified in the import environment to an IP address of a host used in production.

- Datasets *can* be modified in the import environment.

  The content designer can create a dataset variable that stores an IP address. Then, the content designer enters that dataset variable in the Target field for the operator. An administrator in the import environment can update the dataset variable with an IP address value that a host group in the import environment references. The imported process can then run successfully.

Release Properties of a Folder Targeted for Export as a Content Package

A content designer can provide release information for a folder before an administrator exports the folder as a content package. The Release tab contains the Release Version property and a Value field for entry of the release version. Optionally, you can add user-defined properties with values that provide other details about the content package. For example, you can add contact information for the content designer.

Content Packages Palette in Operations Tab

A new action Operations_Content_Packages is introduced in CA EEM that allows users or groups to view the Content Packages palette in the Operations tab. This permission is granted to all default groups. When you upgrade CA Process Automation, the users and groups who can use Process Watch can also view Content Packages.

For the details about configuring CA EEM for the Process Automation application, see the *Content Administrator Guide*.

User Experience Improvements

Summary

- Support for purging aged Reporting data.
  - Formerly, there was no easy way to purge reporting data. Any application that shared storage with the Reporting database could be affected if the database reached capacity.

    Note: We recommend that the Reporting database be located in a dedicated database instance.
  - Now, at the Domain level, you can schedule a daily purge of reporting data over a configured age. You can also purge on demand all reporting data started within a specified date range. See the *Content Administrator Guide* for details.

    Note: The default settings enable process reporting and enable operator reporting, but do not schedule purging.
- Support for deleting and purging checked-out objects.
  - Formerly, you had to check in an object before it could be deleted or purged.
  - Now, an administrator can delete and purge checked-out objects.
- Persist WSDL URL in SOAP operator wizard.
  - Formerly, entries for WSDL URLs were not saved.
  - Now, you can use the WSDL explorer to select a previous entry from a drop-down list.
- Install as Windows Service option is set as the default for Orchestrator installations on a Windows server. You can also start the caitpamserver service from the command line.

Details

You can now purge reporting data as you can purge archived instance data for the processes you run. Purging criteria is based on the start time of a process or operator. (This is different from the criteria used for purging archived processes, which uses the end time.)

Options include:

- Purge the Reporting data daily at the specified time; data that is older than the configured number of days is deleted.
- Do not schedule a purge of reporting data.
- Purge all reporting data within a specified date range on demand.

All Orchestrators in all environments in a Domain typically share a common Reporting database, by default. Purge settings apply only to this common Reporting database. An administrator can edit the OasisConfig.properties file to change the configuration of a selected Orchestrator to point to an external reporting database. The reporting data settings and actions that are configured through the UI apply only to the common Reporting database; they do not apply to external reporting databases.

To increase the control that authorized users have over the Library, administrators can delete objects that are in checked-out status. This ability extends to content designers who own the checked-out objects.

- Administrators can purge checked out objects from the Recycle Bin.
- To alert administrators when selected objects or folders include checked-out objects, the purge process lists any checked-out objects in the confirmation message. The administrator can then verify that the checked-out objects were not inadvertently deleted before confirming the purge.

Java-Related Improvements

Summary

- Document JavaScript functions that return Java types
  - Formerly, we did not document JavaScript functions that return Java types.
  - Now, the *Content Designer Reference* contains the topic, "Return Types." For each system function return type, a table describes the effect on a Javascript variable being assigned the return value, and the CA Process Automation dataset variable type created.
- Invoke Java operator changes and enhancements.
  - Formerly, you could execute the Invoke Java operator on an Orchestrator or on an agent. The Invoke Java operator uses custom Java code. Administrators want to prevent the execution of any custom code that could corrupt the Orchestrator or that conflicts with its execution.
  - Now, the Invoke Java operator can only be executed on an agent. A new Required Main Method dialog provides a coding example that you can copy into the area that the operator uses. The example provides directions for usage.

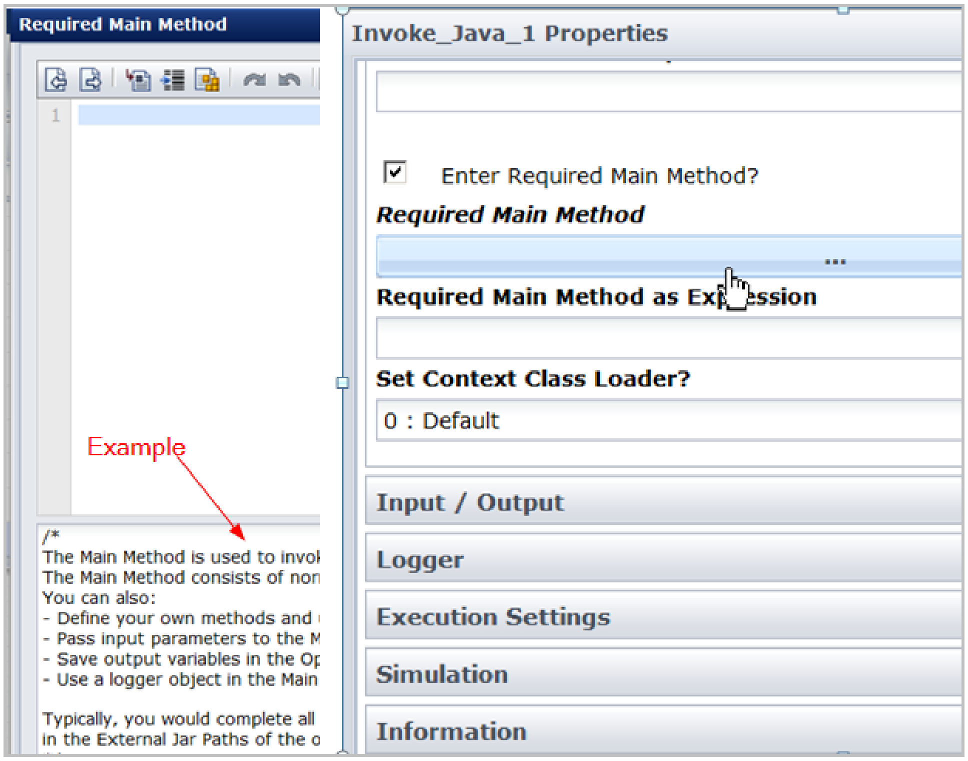
Details

Previously, the Invoke Java operator could be run on Orchestrators. For security reasons, this operator can now be run only on agents. This change prevents the running of custom code that could inadvertently corrupt CA Process Automation components. See Where Operators Can Run in the *Content Designer Reference*.

For existing processes that include an Invoke Java operator that targets an Orchestrator, change the target so that the operator runs on an agent. If you require the operator to run on the host where the Orchestrator runs, we recommend that you install an agent for this purpose on that same host.

We recommend that you install a dedicated agent on another host and run any Invoke Java operator that is used in new processes on this dedicated agent.

A new example panel has been added inside the Required Main Method text area of the Invoke Java operator. You can display or hide the example with a click of the Hide Examples button. The MyAccount.jar file is required to run the provided java example. The installation or upgrade process adds the MyAccount.jar file to User Resources (located in the invoke_java_op_example_jars folder) in the Domain Orchestrator. CA Process Automation then mirrors the MyAccount.jar file throughout the other nodes in your system. See "Resource for Running Invoke Java Operator Example" in the *Content Administrator Guide*.



```
/*
The Main Method is used to invol
The Main Method consists of non
You can also:
- Define your own methods and
- Pass input parameters to the M
- Save output variables in the Op
- Use a logger object in the Main

Typically, you would complete all
in the External Jar Paths of the o
```

☑ Enter Required Main Method?

Required Main Method

Set Context Class Loader?

0 : Default

The Use Strict Java Mode? input field is no longer in the *Invoke Java* operator, but was moved to the *Utilities Module* properties. The new Invoke Java operators use the value that is configured at the module level. Any Invoke Java operators that you created with CA Process Automation releases before Release 04.2.00 retain this input field. The value of this field dictates whether the operator uses Strict Java Mode.

Other UI changes include:

- The Invoke Java operator has new labels and detailed tooltips that explain the use of each field.
- The tab on the module properties for the Utilities module was changed to Default Invoke Java Operator Properties.

CA EEM Release 12.51 Support

Summary

If you plan to upgrade CA EEM to Release 12.x, do this upgrade before upgrading or installing CA Process Automation. Then all the new CA EEM features are immediately available. If you upgrade CA EEM after installing CA Process Automation, you can easily reinstall or configure the existing installation to take advantage of the new CA EEM features.

- CA EEM SDK r12 support.
  - Formerly, CA Process Automation supported CA EEM Release 8.4 and used the CA EEM SDK major version 8. Certificates used 1024-bit keys.
  - Now, if you are using CA EEM Release 12.x, the CA Process Automation installation processes loads CA EEM SDK major version 12 when you register the application with CA EEM. If you do not register, the CA Process Automation installation process provides prompts that help you choose the SDK version to load. The certificates that CA Process Automation uses to connect to the CA EEM server are generated with the same key lengths as CA EEM certificates (1024, 2048, or 4096).
- CA EEM multiple Microsoft Active Directory domains support.
  - Formerly, you could reference users from a single Microsoft Active Directory domain when you configured CA EEM to use an external user store.
  - Now, if you are using CA EEM Release 12.51, you can reference users from multiple AD domains.

Details for CA EEM SDK 12 Support

Interactive installation process selects, or prompts the user to select, the appropriate CA EEM SDK

CA Process Automation uses a CA EEM release-specific SDK to communicate with CA EEM.

When you install CA Process Automation Release 4.2 or upgrade from a previous release, you can register the CA Process Automation application with CA EEM (recommended) or you can bypass registration (not recommended).

- If you register the application, CA Process Automation determines the release of your CA EEM and chooses the appropriate CA EEM SDK version.
- If you do not register the application, CA Process Automation presents a prompt with guidelines on how to select the SDK version based on the CA EEM version.

Silent installation process includes new CA EEM SDK value

- New variable in response.varfile: **eiamSDKLevel**
- New Installation and Upgrade
  - No EEM application registration

    Uses value in eiamSDKLevel to choose the EEM SDK

    If eiamSDKLevel value is not set to 8 or 12 then the installation fails with the following log message:

    "Please set the variable 'eiamSDKLevel' in the response.varfile to either 8 or 12".
  - EEM application registration

    The silent installation process automatically retrieves the CA EEM server version and chooses the EEM SDK to use in CA Process Automation.

CA Process Automation supports three certificate lengths (1024, 2048, and 4096) for CA EEM SDK major version 12

Communication between CA Process Automation and CA EEM is secured with CA EEM certificates and with CA Process Automation certificates. CA Process Automation certificates must have the same key length as CA EEM certificates. During registration, the CA Process Automation certificates are generated with key lengths that match CA EEM certificates. By default, CA EEM certificates have 1024-bit keys.

If, after installation, new CA EEM certificates are generated with longer key lengths, you must regenerate CA Process Automation certificates. For details, see "Example Scenario: Configure the Existing Installation to Regenerate CA Process Automation Certificates" in the *Installation Guide*.

Details for Multiple Microsoft Active Directory Domains Support

The Domain Orchestrator installation process lets you connect to your active CA EEM server. CA Process Automation Release 4.2 supports CA EEM Release 8.4 through CA EEM Release 12.51. When using CA EEM Release 12.51 and you reference an external user store, you can add multiple Microsoft Active Directories.

New Installation

The CA Process Automation installation process prompts you to configure how to store the global information for CA Process Automation users. You can store global users in the internal data store or you can reference users from one or more external LDAP directories. To reference users, you select one of the following configuration types:

- Basic LDAP Directory
- Multiple Microsoft Active Directory Domains
- Microsoft Active Directory Forest

If you reference multiple ADs or an AD forest, CA Process Automation users must log in with their principal name (*domain-name**user-name*) and password. You can configure one of the domains as the Default AD Domain; users in this AD domain can log in with just their user name and password.

Microsoft NTLM pass-through authentication enables CA Process Automation users to login the CA Process Automation without entering credentials in the login dialog. To provide users with direct access to CA Process Automation, configure Microsoft NTLM.

Note: The CA EEM administrator grants CA Process Automation permissions to selected AD users. The administrator enters the user name as query criteria in CA EEM. When the user record is returned by AD, the administrator associates a CA Process Automation default group (for example, Designers) with that record.

Upgrade Installation

If your CA EEM Release 8.4 used an external AD directory and you upgrade to CA EEM Release 12.51, you can select Basic LDAP Directory as your option for "reference from an external LDAP directory." In this case, your application group assignments, custom policies, and ownership of Library automation objects are retained.

If your CA EEM Release 8.4 used an external AD directory and you upgrade to CA EEM Release 12.51, you can select Multiple Microsoft Active Directory Domain or a Microsoft Active Directory Forest as your option for "reference from an external LDAP directory." In this case, application group assignments, custom policies, and ownership of Library automation objects are *not* retained.

Important! If you previously referenced users from an Active Directory and you now want to reference users from multiple ADs that include this original AD, take the following actions to reinstate user permissions and object ownership:

- CA EEM Requirement: You must reassign application groups to existing users. If you created custom policies or custom groups, you must reassign the users with their principal names.
- CA Process Automation Library Requirement: Users must set the ownership of their objects. Ownership is then displayed with the principal name of the owner.

During the upgrade installation, you identify the AD to use as the default domain. You can identify the Active Directory to which the current CA Process Automation users belong, but that is not a requirement. Users belonging to the default domain can log in to CA Process Automation with an unqualified user name. Users belonging to other AD domains must specify their principal name at login.

Note: For the details, see the *Installation Guide* and the *Content Administrator Guide*.

Performance Improvements

The following summary focuses on performance improvements.

- Many performance improvements are not surfaced directly in the UI, but you will notice that CA Process Automation works faster.
- Messaging Service
  - Formerly, CA Process Automation used JBoss for embedded messaging.
  - Now, CA Process Automation 4.2 uses an external instance of ActiveMQ for messaging. This means that ActiveMQ runs in a separate JVM. However the lifecycle of ActiveMQ (for example, start and stop) is coupled to and managed by the Orchestrator service.
- CA Process Automation run-time performance improvements
  - Speed with which users are authorized to use features.
  - Speed with which the operator Target field is processed when it contains an IP addresses or hostname.
- Optimized Task List retrieval - The amount of time it takes to display the Task Lists on the Home tab and on the Operations tab has been reduced.
- Optimized named dataset locking
  - Formerly, when an operator accessed a named dataset (for read or write), a global cluster-wide lock required other operators accessing other named datasets to wait until this global lock was released.
  - Now, a check box (General Properties) for dataset objects let you specify whether to use the deprecated locking mechanism that implements a cluster-wide lock when an operator accesses a named dataset. If you clear this option, when an operator accesses a named dataset (for read or write), the lock is applied to only the named dataset being accessed. This lock does not interfere with other operators accessing other named datasets. This option is cleared by default for new dataset objects and selected for dataset objects imported from previous versions.

    These details about optimized named dataset locking are documented in the *User Interface Reference.*

Communication Improvements

The following summary focuses on communication improvements.

- Simplified agent communication.
  - Formerly, connections between Orchestrators and Agents were initiated bi-directionally using non-standard internet ports (7001, 7003, 8080, 8443). This was problematic for agents residing behind firewalls, proxies, and NAT routers. This style of communication is referred to as deprecated communication. Simplified communication was not available.
  - The new simplified communication initiates connections from the agent to the Orchestrator using only standard internet ports (80, 443). An Orchestrator sends messages to an agent using a persistent websocket connection. This connection is established from the agent using standard internet ports.

    Note: You can configure existing agents to change from deprecated communication (default) to simplified communication. See the *Content Administrator Guide* for agent configuration details. Configure a load balancer that supports web socket connections. See the *Installation Guide* for details.
- NGINX load balancer support
  - Formerly, Apache was the recommended software load balancer used for clustered Orchestrators. However, Apache does not support simplified agent communication.
  - Now, CA Technologies recommends NGINX as a software load balancer that supports simplified communication. For caveats, see the next section, New Recommendations for Load Balancers. The installation media includes a sample configuration file for this load balancer. See the *Installation Guide* for information about setting up NGINX.

    Note: Optionally, you can use another load balancer that supports persistent web socket connections.
- New Recommendation for Load Balancers

  The following recommendations for CA Process Automation 4.2 are listed in order of preference:
  - (Preferred) Use a hardware load balancer, for example, use F5.
  - Use a software load balancer on Linux, for example, NGINX.
  - If you must run a software load balancer on Windows, use NGINX, but be aware that the number of agents that can be operated using the simplified communication is limited to approximately 300.
- Changes to Apache Templates - You must update your Apache configuration with the updated templates supplied on the installation media as a prerequisite to upgrade.

Note: After you have upgraded CA Process Automation and verified that everything is working as expected, you can install and configure NGINX and switch load balancers. Reconfigured and restarted agents can then use simplified communication.

- Changes to F5 Updated F5 iRule Definition.
  - Previously there was one pool PAMSRVR with either 8080 (unsecure) or 8443 (secure) for the port.
  - Now there is an additional pool (PAMJETTYPOOL) that supports simplified communication with either 80 or 443 for the port. If upgrading, you add the new pool; if setting up F5 for the first time you create two pools and add members with different ports.
- Changes to F5 when configuring secure communication
  - Previously, you could use a self-signed certificate and a key file to enable SSL communication.
  - To use the new r4.2 simplified communication, you must upload SSL certificate file from the CA Process Automation keystore and create client and server profiles that link these certificates.

Clustering Improvements

The following summary focuses on clustering improvements.

- Removal of primary node dependency in clustered Domain Orchestrator
  - Formerly, dependencies on the primary node (first node installed) represented a potential single point of failure. That is, if the primary node went down, another node in the cluster did not take on the activities being performed by the primary node. This prevented the expected high availability of the Domain Orchestrator. Activities that used to depend on an active Domain Orchestrator primary node included: (1) mirroring newly deployed JAR files, (2) installing agents or other Domain Orchestrator nodes, and (3) deploying files uploaded as User Resources or Reports.
  - Now, there are no dependencies associated with the primary node in a clustered Domain Orchestrator. A clustered Domain Orchestrator now functions with high availability.
- Implications of removal of primary node dependency on F5 iRule
  - Formerly, the iRule included the variables MyPool, PrimaryIP, and PrimaryPort. PrimaryIP and PrimaryPort referred to the primary node of the Domain Orchestrator.
  - Now, MyPool is the only iRule variable.
- Ability to configure a new Domain with existing domain settings and certificates
  - Formerly, the Domain.xml and certificates were present on the file system only. So, if the Domain went down, the configuration and certificates were lost.
  - Now, the Domain.xml and certificates are moved to a central database. This move eliminates the single point of failure if the Domain Orchestrator goes down. It also improves performance when accessing agent data from the UI.

Security Improvements

- The Invoke Java operator can now run only on agents. This change removes the potential for an internal user to inadvertently corrupt an Orchestrator with custom code added to this operator. For details on changes to the Invoke Java operator, see Java-Related Improvements (see page 31).
- Communication between CA EEM and CA Process Automation can now be secured with certificates with longer key lengths if you use CA EEM r12.5. For details on support for new certificate lengths, see CA EEM r12.51 Support (see page 33).
- HTTPOnly flag set in Orchestrator session cookies.
  - Formerly, CA Process Automation Orchestrators did not set the HttpOnly flag when creating session cookies.
  - Now, as a security enhancement, Orchestrators set the HttpOnly flag when creating session cookies. This helps prevent cross-site scripting and other types of attacks.

Database Server Improvements

The following summary focuses on database server improvements.

- MS SQL server named instance now supported for Database Server
  - Formerly, when you configured the Database Server for Microsoft SQL Server during installation, you could not specify the instance name.
  - Now you can configure a SQL Server instance for the Database Server in addition to the existing Oracle, SQL Server and MySql database servers.
- XA dependency has been removed.
  - In CA Process Automation 4.0 or 4.1, if you used a SQL Server database server, you had to enable XA distributed transaction support.
  - Now, the dependency on XA has been removed.
- When installing the Domain Orchestrator, you can specify a connection string to connect to an Oracle database.

Support for CA SiteMinder Secure Proxy Server (SPS)

CA Process Automation has previously supported Single Sign On through integration with CA SiteMinder. This support has been upgraded to use CA SiteMinder Secure Proxy Server (SPS).

To support simplified communication, which is not supported by Apache, this upgrade eliminates the need for the CA SiteMinder Web Agent on Apache.

CA Process Automation 4.2 Installation and upgrade uses only CA SiteMinder SPS. When you upgrade CA Process Automation 4.2, you provide the CA SiteMinder SPS details to use SSO instead of Web Agent on Apache. For more information, see Install the Domain Orchestrator section in the *CA Process Automation Installation Guide*.

More information:

Support for CA SiteMinder Web Agent on Apache and IIS (see page 56)

CA Process Automation Service Pack 04.1.01

The Service Pack 4.1 SP01, included the following enhancements:

- DNS Lookup Bypass for Host Groups (see page 43)
- Double-click Task to Initiate Reply (see page 44)
- Increased Initial Java Heap Size for 64-Bit Installations (see page 44)
- Customized OasisConfig.properties Is Retained After Upgrade (see page 44)

DNS Lookup Bypass for Host Groups

To improve performance of identifying an operator target that is expressed as a host name or IP address, the following property has been added to the Properties tab for Domain and Environments.

□ **Lookup DNS when matching target in Host Groups?**

Formerly, the processing behavior was as if this option was enabled. Now that the option is surfaced in the UI, you can disable the option and bypass DNS lookups.

By default, this field is set to “Enabled” for the Domain, and “Inherit from Domain” for each Environment. "Inherit from Domain" means that the Domain setting is used when resolving Host Groups in any environment. These settings match the behavior implemented in earlier versions of CA Process Automation.

While setting this option to Enabled allows users to freely mix the use of IP addresses and host names, the resulting processing can incur significant overhead. Compare the required processing summarized on the following table:

	Target is host name	**Target is IP address**

Enabled	■ Performs a DNS lookup for the hostname and retrieves all associated IP addresses. ■ Attempts to match the host name to a Host Group’s list of host name patterns. ■ Attempts to match each of its IP addresses to a Host Group’s list of IP address ranges. ■ If a match is found, runs the operator on the target.	■ Performs a DNS lookup for the IP address and retrieves the hostname. ■ Attempts to match the IP address to a Host Group’s list of IP address ranges. ■ Attempts to match each of its host names to a Host Group’s list of host name patterns. ■ If a match is found, runs the operator on the target.
Disabled	■ Attempts to match the host name to a Host Group's list of host name patterns. ■ If a match is found, runs the operator on the target.	■ Attempts to match the IP address to a Host Group's list of IP address ranges. ■ If a match is found, runs the operator on the target.

Note that the "Disabled" setting incurs the risk of not finding a match if the target is expressed as an IP address but the Host Group identifies this same host with a host name pattern. Similarly, CA Process Automation would not find a target expressed as a host name if the Host Group list identifies this host within a specified subnet.

Double-Click Task to Initiate Reply

Formerly, the only way to reply to a task in the Tasks section of the Operations tab was to select Reply from the right-click menu for that task. Now, you can initiate a reply by double-clicking the task. This enhancement was added for ease of use.

Increased Initial Java Heap Size for 64-Bit Installations

The default max memory for the JVM is now set to 2048m when CA Process Automation is installed or upgraded using the 64-bit installer.

Customized OasisConfig.properties Is Retained After Upgrade

Manual modifications to the OasisConfig.properties file are now retained after an upgrade.

CA Process Automation Release 04.1.00

CA Process Automation Release 04.1.00 includes the following new features:

Common Script Editor

This advanced code editor lets you create, edit, and debug various types of scripting and markup languages.

Note: For more information about the CA Process Automation Code Editor, see "The CA Process Automation Code Editor" in the *Content Designer Guide*.

Process Documentation

Content designers can generate detailed process documentation, including visual representations of the process that feature details and dependencies at the process and the operator level. You can generate the process documentation in PDF format.

Note: For more information about process documentation, see the *Content Designer Guide*.

NTLM Pass-Through Authentication

EEM NTLM authentication lets you bypass entering credentials in the CA Process Automation login dialog and instead lets you log in to CA Process Automation using Windows credentials (through CA EEM). This feature applies when CA EEM is configured to use Microsoft Active Directory as the external user store and NTLM is enabled.

Note: For more information, see the following documentation:

- "Prerequisites for Configuring NTLM Authentication," "Reference Global Users and Global Groups from Microsoft Active Directory," "Enable NTLM Pass-Through Authentication After Installation," and "Upgrade Prerequisites" in the *Installation Guide*.
- "Configure Web Services," "How Authentication and Authorization Work," and "Oasis Configuration Properties File" in the *Content Administrator Guide*.
- "HTTP URL Information," "HTTP Proxy Information," and "HTTP Operators: Common Output Ports" in the *Content Designer Reference*.
- "Google Chrome Fails First Attempt to Log Out Users Logged in Using NTLM" in the *Release Notes*.

Form Designer User Experience

When content designers open a start request form or an interaction request form from the Library Browser, the Form Designer editor opens. The Form Designer editor provides the following new capabilities:

- Added support for SOAP and RESTful Web services in forms, such as populating form elements using SOAP / RESTful APIs.
- Copy and paste for easy re-use of form elements.
- Drag and drop form elements.

- Tooltips for form element properties.
- Common JavaScript Editor.

Note: For details about the Form Designer, see the "Forms" chapter of the *Content Designer Guide*, particularly "The Form Designer."

Management and Performance enhancements

Administrators with Domain_Admin permissions, such as members of the PAMAdmins group, can disable (or re-enable) the following options:

- Operator level reporting.
- Operator level recovery.
- Process level reporting.
- Process level logging.

Note: For details about configuring these options, see "Configure Domain Properties" in the *Content Administrator Guide*.

Catalyst Interoperability and API

The Catalyst container and Catalyst Process Automation Services are both embedded in CA Process Automation. Communication is optimized among the Catalyst container, Catalyst Process Automation Services, and CA Process Automation.

The following enhancements are included in the current release:

- Catalyst 3.2 is certified.
- RESTful API enhancements for headless control and monitoring impact the following: query and control processes, interaction request forms, start request forms, datasets, module configuration, content import and export, and alerts.
- Catalyst Process Automation Services is enabled by default.

Note: For details, see the "RESTful API Reference" chapter in the *Web Services API Reference*. See also "Apache Load Balancer Configuration for Catalyst RESTful API (Windows)" in the *Installation Guide*.

Operator Enhancements

Content designers have two new operators and updated support by SOAP operators.

- Process Progress operator

  You can set the progress of a process using the Process Progress operator. You can monitor the process progress through user-defined reports and in the Operations tab (Process Instances link).

  Note: For details, see "Process Progress Operator" under "Standard Operators" in the *Content Designer Reference*.

- Apply XSLT operator

This operator lets you to apply a predefined style sheet to transform an XML source document to another presentation-oriented format, such as HTML, XHTML, or SVG.

Note: For details, see the "Apply XSLT Operator" under "Utilities" in the *Content Designer Reference*.

- SOAP operators

  These operators support NT LAN Manager (NTLM) authentication to authenticate clients to a Windows server.

  Note: For details, see "Soap Call Data Parameters" and "SOAP Call Data Properties" in the *Content Designer Reference*.

Process Management

Content designers can better manage processes through the following enhancements:

- Content designers can use the duration attribute to specify the expected duration for a process or report. This enables designers to track the actual duration compared against the expected duration.

  Note: For details, see "Define the Run Duration for a Process" in the Library Browser section of the *Content Designer Guide*.

- Content designers can now add progress markers as part of their process definition. This lets production users track processes based on progress.

  Note: For details, see the "Process Progress Operator" and the "setProcessProgress" method in the *Content Designer Reference*. The "Process Instances" section in the *Production User Guide* now includes Progress as a displayed attribute.

Content Creation and Management

Content creation and management enhancements impact custom operators and content management.

Custom Operators:

- Ability to hide variable from output dataset.

  Note: For details, see "Custom Operator: Dataset Tab" in the *Content Designer Guide*.

- Ability to create module level configuration so that configuration data (such as named connections) can be shared between multiple custom operators.

  Note: For details on custom operator groups, see the following documentation:

  - To create a custom operator group, see Custom Operator: Settings Tab" in the *Content Designer Guide*.
  - To define parameters for a custom operator group and publishing the custom group to the Modules tab in the same Domain, see "Configure and Publish a Custom Operator Group" in the *Content Designer Guide*.

- To publish a custom operator group configuration to another Domain, see "Import an Object, a Folder, or a Package" in the *Content Designer Guide*.
- To configure (or delete) a custom operator group, see "Configure Values for a Custom Operator Group" and "Delete a Custom Operator Group Configuration" in the *Content Administrator Guide*.
- To override custom operator group values at the environment level, see "Enable or Disable a Custom Operator Group" and "Override Inherited Values for a Custom Operator Group" in the *Content Administrator Guide*.
- To review the new CA EEM resource class Group Configuration and the related action key Group_Config_Admin, see the "Permissions Reference" section for in the *Content Administrator Guide*.
- To extend the configuration right to content designers, see "Example: Grant Designers the Ability to Configure Groups for Custom Operators" in the *Content Administrator Guide*.
- To review task flow, see "Scenario: How to Work with Custom Operator Groups" on the CA Process Automation section of the Support website.

Content Management

Content designers or administrators can specify a release-specific value for the new Release Version attribute for objects to be packaged for export for a release. The exporter can specify that this attribute is to be nonmodifiable in the import environment. When this attribute is locked, content designers can easily identify whether objects customized for a specific release have been changed since being imported to the production environment.

Note: For details about release versions, see the following topics in the "Release Objects to Another Environment" chapter of the *Content Designer Guide*:

- "Release Versions."
- "View Release Version Information."
- "Set the Release Version of Objects to Export."
- "Export an Object, a Folder, or a Package" addresses how to set the Export Release Versions in Nonmodifiable Mode option.
- "Release Version and Baseline Status of Imported Objects."

The *Content Administrator Guide* contains topics in the section "How to Prepare the Production Environment for a New Release" that touch on release versions.

Reporting

Reporting is enhanced in the following ways:

- Extended data in the reporting database is to be in line with Process Watch: custom instance name, duration, progress, organizational information, parent-child information.

- New database views provide easy access to PAM historic data and replaces PAM legacy reporting DB schema. You can use the following database views to generate the user-defined reports:
  - Process_Instances.
  - Automation_Objects.
  - Operator_Instances.

  Note: For details, see "Reporting DB Views" in the *Production User Guide*.
- New: Process Duration Status Report.

  Note: This new report is referenced in the "Working with Predefined Reports" topic in the *Production User Guide*.
- All reports updated to leverage schema updates.

CA Process Automation Service Pack 04.0.01

New features in CA Process Automation 4.0 SP01 include:

- A warning message now displays when CA Process Automation refreshes or closes with unsaved changes.
- Process instance information now displays in the Operations tab for start request forms. You can correlate the start request form instance with the process associated to that start request form. A new Process Instance column displays in the start request form grids under the Operations tab, with the new "Open Process Instance" right-click menu option for each start request form.
- The Assign User Task operator now lets you send a notification that contains the direct URL to a task. A new "Task ID" operator parameter is populated once the operator executes. Users can then use this variable to trigger emails, notifications, and so on.
- New system functions are now available to generate CA EEM tokens:

  getEEMArtifactTokenForUser(username,password)

  This method returns an CA EEM token for single use.

  getEEMCredentialsTokenForUser(username,password)

  This method returns an CA EEM token for multiple uses.

getEEMArtifactToken (certificateFilePath, certPassword/keyFilePath)

The input parameters of this method are the relative path of the certificate file and certificate password (in the case of non-FIPS mode) or the relative path of the key file (in case of FIPS mode). This method returns the CA EEM token for a single use.

getEEMCredentialsToken (certificateFilePath, certPassword/keyFilePath)

The input parameters of this method are the relative path of the certificate file and certificate password (in the case of non-FIPS mode) or relative path of the key file (in case of FIPS mode). This method returns the CA EEM credential token for multiple use.

isFIPSMode()

This method return true if the CA EEM server is running in FIPS mode.

- Web service methods have been updated:
  - A process or a start request form that is initiated through a Web service can now be tagged with a unique user-provided ID. Web service methods have been enhanced to let you obtain the status of a process or start request form that has been submitted with such a tag. If a process starts directly, or if the start request form starts a process, then CA Process Automation returns the task ID of the process. Updated/new Web service methods that are affected by this change include:
    - checkStartRequestStatus
    - executeProcess
    - executeStartRequest
    - getProcessStatus
    - ImportObject
    - ControlProcess
  - You can now control process archiving through a Web service. The executeProcess and executeStartRequest Web service methods have been enhanced to support an additional parameter which lets the caller exempt that process from normal archiving.
- The Value field can now be expanded in the properties of a dataset. This expansion applies for String, Integer, Long, and Double data types.
- Dataset scrolling is improved when expanding nested variables.
- The new getOrchestratorURL() system function returns the URL of the Orchestrator and facilitates the dynamic creation of URLs for use with specific Interaction Request Forms. In the case of a cluster, getOrchestratorURL() returns the URL of the load balancer.

- The existing XML for out-of-the-box content has been updated to include additional features.
- The description for an object in the Library now displays as a tooltip.
- In the Forms Designer, you can now select forms from a drop-down menu that is populated dynamically. Previously, forms were located through a search.
- The Evaluate Expression operator and the Monitor Event operator now include dataset assistance when using of any of their keywords.
- Process dataset variables now display during design time.
- The CA Process Automation installer now supports installation of CA Process Automation in Embedded Mode.
- In the Forms Designer, there is a provision to expand the right-hand side properties of a form, resulting in more space to enter JavaScript functions. You can right-click and select Expand. Also, assistance support has been added on Ctrl+Space.
- Module and trigger properties now open in a new pop-up window.
- For custom operators, there is a new "Read Only" parameter. This property governs whether the given parameter always takes value from the base operator and is not editable for the end users of the custom operator.
- In the Trigger tab of the Configuration Browser, if you open the properties of an SNMP Trigger, a Browse button is now available for the ProcessPath field.
- Dynamic forms now support custom images. You can upload a custom image through Manage User Resources (on the Configuration tab) to a user-created folder, which is accessible over a URL. You can also copy/host the images on another web server as long as they are accessible with an absolute URL.
- A warning message now displays for tear-off windows if you close/refresh them without saving your changes.
- Saving any user preferences through the Resource Editor (such as pagination, the number of records, columns to display and hide, and so on) also saves them in CA Process Automation User Preferences.
- CA Process Automation now provides the ability to right-click a variable in a dataset and select "View Expression". You can also copy the expression for the dataset variable and then paste it wherever needed.
- You can now upload resources (including JARs) to the Agent Resources and Orchestrator Resources in the Manage User Resources palette on the Configuration tab. All JARS uploaded to the Agent Resources are included in the agent’s classpath upon the restart of the agent. All JARS uploaded to the Orchestrator Resources are included in the Orchestrator’s classpath upon the restart of the Orchestrator.
- When creating a custom operator, you can now double-click to select a base operator.

CA Process Automation Version 04.0.00

New features included in CA Process Automation v4 include the following:

- Full Browser-Based User Interface (see page 52)
- Operator Enhancements (see page 52)
- Usability Enhancements (see page 53)
- Web Services HTTP Properties (see page 54)

Full Browser-Based User Interface

CA Process Automation now has a single, completely redesigned user interface. There is no more dependency on the Java runtime engine to use the new interface. CA Process Automation v4 also includes support for the latest browser versions.

Operator Enhancements

This CA Process Automation release includes the following operator enhancements:

- Loop operator enhancements
  - Loop Count Variable
  - Loop Duration Variable
  - Additional loop execution option
- The Comments operator supports HTML.
- Operators support directly running classes in external jars through “JavaObjects”.
- Operator searching is improved. An operator palette filter capability makes it easy to find specific operators.
- A new Invoke Java Operator enables users to invoke Java classes, so that Java APIs from target systems can be integrated directly into CA Process Automation.

Usability Enhancements

CA Technologies has redesigned the CA Process Automation user interface as follows to improve the user experience:

- Major feature sets are grouped into tabs. Users see and have access only to the features necessary to their role.
- The home page provides users with easy access to key features of CA Process Automation. It also provides users with direct access to online and out-of-the box content, as well as recently modified processes, pending tasks, and system activity. The home page is customizable and allows quick access to items frequently used.
- Users can "tear off" selected UI components into new windows.
- Designing processes has been streamlined and improved with a workspace that is easier to navigate and enables access to important information in a single view.

  The process designer provides the following features:

  - Users can drag and drop units of work (*operators*) to a canvas and link them with process flows.
  - Users can pin, hide, move, or resize the Properties pane for displaying and modifying operator attributes.
  - At design time, users can drag and drop variables to exchange data between operators easily.
  - Users can pan and zoom the canvas to navigate processes easily.
  - Enhanced operator run-time and configuration state indicators.
  - A Custom Icon Editor lets users create custom icons to tailor the visual appearance of an operator.
- The library can act on multiple automation objects.
- The Report management tab lets users manage and run reports.
- The Configuration tab provides centralized system configuration and deployment of CA Process Automation components and resources.
- A dynamic forms designer lets users create flexible human interaction forms that comply with web standards.
- A centralized dashboard lets users manage and interact with automated processes and associated objects.
- A new Operations dashboard allows users to surface key metrics of processes and operators. This dashboard comes with drill-down capability so that users can inspect status, diagnose or correct any issues discovered.
- Several of the new user interface elements support direct URL access which enables embedding parts of CA Process Automation UI into other browser-based applications and portals.

Web Services HTTP Properties

Web Services HTTP Properties contains a new field that you can use to validate the SSL certificate for HTTP calls.

To use this validation for operators that were designed in CA Process Automation r3.1, select the Default Validate SSL Certificate check box at the Web Services category level. For more information, see the *Content Designer Reference*.

Chapter 4: Retired Features

The following features have been retired in either because functionality had limited utility or usage by our client base, or to remove unnecessary complexity.

Release 04.2.00

Package (see page 55)

XA Distributed Transaction Dependency (see page 56)

Self-Contained Mode (see page 56)

AIX and HP Platform Support for Orchestrators (see page 56)

Support for CA SiteMinder Web Agent on Apache and IIS (see page 56)

Ability to Share a Library Data Store Across Domains (see page 57)

Release 04.1.00

Microsoft Internet Explorer 8 (see page 57)

Version 04.0.00

- Direct LDAP and Active Directory Support (see page 57)
- Log Viewer Objects (see page 57)
- Retired and Replaced Operators (see page 57)
- State Policies and Rules Engine (see page 58)
- Telephony Application Programming Interface (TAPI) Support (see page 58)

Package

Package

Beginning with CA Process Automation Release 04.2.00, the package object is no longer available for bundling shortcuts to other automation objects. This release restricts you to creating and editing the existing package objects. You cannot check in, check out, cut, copy, or paste a package object.

A content designer can only import an existing package object to another CA Process Automation installation. The imported package is read-only. The package object is unavailable for any reference through the Object Browser in interaction request forms, start request forms, custom operators, and process watch.

You cannot create a package object reference in the Object Browser (for example, in forms or datasets), and you cannot edit the existing references.

The product retains the package object usage for backward compatibility.

XA Distributed Transaction Dependency

CA Process Automation 4.2 no longer requires database servers to support XA. If you use a SQL Server database server, you no longer have to enable XA support. However, if you have already enabled XA support on your SQL Server, no action is needed. CA Process Automation can work with both XA and non-XA data resources.

Details on setting up your system for XA have been removed from the documentation.

Self-Contained Mode

The CA Process Automation 4.2 installation wizard permits you to install CA Process Automation only in standard mode; self-contained mode is no longer an option. You cannot upgrade from a 4.1 self-contained CA Process Automation to a 4.2 release.

The self-contained CA Process Automation was intended for demonstrations only; it used an internal Derby database for the three types of CA Process Automation databases and used pam-user.properties for user authorization. Thus, external databases and CA EEM were not required.

AIX and HP Platform Support for Orchestrators

CA Process Automation 4.2 continues to support the AIX and HP platforms for agents. However, support for the AIX and HP platforms for Orchestrators is being retired as of CA Process Automation 4.2.

Support for CA SiteMinder Web Agent on Apache and IIS

CA Process Automation 4.2 does not support CA SiteMinder Web Agent on Apache and IIS.

More information:

Support for CA SiteMinder Secure Proxy Server (SPS) (see page 42)

Ability to Share a Library Data Store Across Domains

Since CA Process Automation Release 3.1, it has been possible to share a Library data store across Orchestrators in environments belonging to different Domains.

As of CA Process Automation Release 4.2, you can share a Library data store across Orchestrators only if the Orchestrators are in the *same* Domain. For example, you can share a Library for all Orchestrators in the same environment.

Microsoft Internet Explorer 8

CA Process Automation Release 04.1.00 is not supported on Windows Internet Explorer 8.

Direct LDAP and Active Directory Support

LDAP or AD users can continue to use them for Directory Services, but must access them as external directory services through CA EEM.

Log Viewer Objects

This feature was rarely used and was retired to remove unnecessary complexity.

Retired and Replaced Operators

The following operators are replaced in this CA Process Automation release:

Derivation

The *Or* operator replaces this operator.

Run Detached ITPAM Process

The base *Start Process* operator options replace this operator.

Run Inline ITPAM Process

The base *Start Process* operator options replace this operator.

Date-Time Wait

The *Check Date-Time* operator replaces this operator.

The following operators are retired in this CA Process Automation release:

- Telephony Alert
- Sound Alert
- Break Sound Alert

Operator replacements are implemented automatically when they are first opened after upgrade, or during the report phase. In the rare case when a process contains a retired operator, a nonfunctioning equivalent replaces the retired operator and the user is instructed to modify the process.

Note: For a complete list of modules and operators with their former and current names and categories, see the *Content Designer Reference*.

State Policies and Rules Engine

This feature was rarely used and was retired to remove unnecessary complexity.

Telephony Application Programming Interface (TAPI) Support

The TAPI standard is used primarily to let computers interface with modems and specific PBX hardware. This feature was rarely used and was retired to remove unnecessary complexity.

Chapter 5: Fixed Issues in 04.2.01

The following issues are fixed in 04.2.01:

Defect ID	Defect Description
64871	**Custom operator variables are not resolved when used as dataset names or array indices** When a custom operator's field is used as a macro or variable inside brackets for indices or dataset, Operator. is not prefixed to the macro or variable during processing, so it is not resolved/expanded. For example, if you have dataset[MACRO_NAME], MACRO_NAME is not expanded.
68168	**CA Process Automation fails to start after upgrade to CA Process Automation 4.2** CA Process Automation fails to start after upgrade to CA Process Automation 4.2 with Null pointer exceptions in the c2o.log file due to some fields missing in Domain.xml.
65433	**PAM Orchestrator fails to start after upgrading to CA Process Automation 4.2** An error occurs while saving Domain.xml in the database since the NoofActiveProcesses field is set as cstring, instead of integer.
67352	**PAM SOAP operators do not support two-way SSL certificate authentication** When SOAP or HTTP operators in CA Process Automation connect to a HTTPS webservice, a two-way SSL certificate authentication is not supported. The following properties are added in the OasisConfig.properties file to support two-way authentication: ■ pam.soap.keystore.path: Specifies the path to the keystore. ■ pam.soap.keystore.pwd: Specifies the keystore password. This password must be set for all private keys inside the keystore.
61807	**Issue with Read From File operator with CA Process Automation server 4.1** When you upgrade the CA Process Automation production server to version 4.1, the Read from File operator on the server is causing a 'xcopy' issue. To fix the problem, the following entry is added in the c2oagtsvcw.conf file: set.PATH=%PATH%;%SystemRoot%\System32\

Defect ID	Defect Description

64759	**Issue with PAM WSDL wizard**
	When CA Business Service Insight web service is used for fetching the penality detail with the SOAP operator, the BSI WSDL wizard displays the following error:
	Could not connect to specified service
	The following exception is shown while loading CA Business Service Insight web service:
	`Caused by: java.lang.StackOverflowError`
	`at com.ca.pam.server.XMLGenerator.updateSchemaNs(XMLGenerator.java:129)`
	`at com.ca.pam.server.XMLGenerator.updateSchemaNs(XMLGenerator.java:133)`
	`at com.ca.pam.server.XMLGenerator.updateSchemaNs(XMLGenerator.java:133)`
	`at com.ca.pam.server.XMLGenerator.updateSchemaNs(XMLGenerator.java:133)`
	`at com.ca.pam.server.XMLGenerator.updateSchemaNs(XMLGenerator.java:133)`
	`at com.ca.pam.server.XMLGenerator.updateSchemaNs(XMLGenerator.java:133)`
	`at com.ca.pam.server.XMLGenerator.updateSchemaNs(XMLGenerator.java:133)`
	`at com.ca.pam.server.XMLGenerator.updateSchemaNs(XMLGenerator.java:133)`
	`at com.ca.pam.server.XMLGenerator.updateSchemaNs(XMLGenerator.java:133)`

Defect ID	Defect Description
67765	**CA Process Automation treats 202 response of the web service call as a failure** When a web service call is sent to the Orchestrator, a Http 202 response is created that is treated as a failure since the response contains a Null value.
56571	**Process dataset created destroyed at runtime** After suspending the process in CA Process Automation, when you reset a failed operator, the process dataset created from the operator at runtime is lost permanently.
67959	**Mail triggers unable to read JVM parameters** Mail triggers in CA Process Automation are unable to read JVM parameters from Oasisconfig.properties file.
67711	**Run SSH Command operator's Command output is truncated** Run SSH Command operator when connected to the SSH server creates a buffer that does not contain the commands sent by the operator.

Chapter 6: Known Issues

This section describes known issues in CA Process Automation Release 04.2.00.

This section contains the following topics:

CPU Usage Spikes in server nodes with Secured Simplified Communication and Load Balancer (see page 64)
NSM Operators Fail on an Agent That Points to a 64-bit JDK (see page 65)
Agent Communication Defaults to Deprecated Method (see page 65)
NGINX on Windows Does Not Scale Like NGINX on Linux (see page 65)
CPU Usage Spikes with Secured Simplified Communication and NGINX (see page 66)
REST and Catalyst Operations Are Not Handled by CA SiteMinder SPS in One Case (see page 66)
Disabling of JBoss Seam Framework after an Upgrade (see page 67)
Microsoft User Access Control Prevents Successful Launch of Orchestrator Node (see page 68)
Potential Problem When Running CA Process Automation on a VMWare Server When Using the E1000 Network Interface (see page 69)
Turkish Operating System Required for Installing Turkish Version of CA Process Automation (see page 70)
CA EEM Release 8.4-to-12.0 Server Upgrade Issue (see page 71)
SOAP Operations in CA Process Automation (see page 71)
CA Process Automation Installation on Dual Stack (IPv4 and IPv6) Network Environments (see page 72)
Export Objects Can Contain Only English Characters (see page 72)
Google Chrome Fails First Attempt to Log Out Users Logged in Using NTLM (see page 73)
JDK 1.7 is Unable to Encrypt and Decrypt Passwords with Special Characters like "&" in SUSE 11SP1 (see page 73)
Limitations in Internet Explorer (see page 74)
Oracle bug # 9347941 (see page 74)
Sorting Automation Objects (see page 75)
Unable to Launch CA Process Automation using the Apache URL in Internet Explorer and Firefox (see page 75)
Limitations to Process Definition Upgrade (see page 75)
SERVER_CONNECT_FAILED Error (see page 76)
Documentation Known Issues (see page 76)

CPU Usage Spikes in server nodes with Secured Simplified Communication and Load Balancer

Symptom:

When a clustered Orchestrator is configured to use secure (HTTPS) communication and agents are configured to use simplified communication with an NGINX load balancer, CPU usage spikes can occur in server nodes when the orchestrator is restarted while multiple agents are active.

Solution:

Note: This is not a recommended approach. Use the following approach only for the above problem.

To fix the problem, configure the clustered Orchestrator to use non-secure (HTTP) communication between load balancer and orchestrator as follows:

1. Add the following properties in the OasisConfig.properties file for all orchestrator nodes:
   - pam.transport.unsecured.connector.flag: Set the value to true.
   - pam.transport.unsecured.connector.port: Specify an integer value. Default value is 80.
2. Edit the following entries in the secure-pam-server.conf file to enable non-secure websocket connection between Load Balancer and nodes:
   - // websocket connections

     upstream node1{

     server <hostname of machine where you have installed node1>: Specify the same port number as pam.transport.unsecured.connector.port

     }

     Note: Specify the same port number as pam.transport.unsecured.connector.port for upstream node2.
   - Change https to http in the following entries:

     ```
     location = /ws/node1 {
                     proxy_pass http://node1; }
     location /ws/node1/ {
                     proxy_pass http://node1;}
     location = /ws/node2 {
                     proxy_pass http://node2;  }
         where node2 is the upstream name
             location /ws/node2/ {
     ```

```
proxy_pass http://node2; }
```

Restart Orchestrator nodes and Load Balancer.

NSM Operators Fail on an Agent That Points to a 64-bit JDK

An agent that is installed on a CA NSM host must use a 32-bit JDK to execute NSM connector operators in a process. If an agent on a CA NSM host uses a 64-bit JDK to execute NSM connector operators in a process, that process will fail.

Agent Communication Defaults to Deprecated Method

The documentation wrongly states that the communication default for agents that are created with CA Process Automation Release 4.2 is simplified communication. However, the default is deprecated communication. Deprecated communication is the default for new agents and upgraded agents.

NGINX on Windows Does Not Scale Like NGINX on Linux

Symptom:

You cannot expect high performances and scalability if you configure NGINX on a Windows host.

For example, if you configure NGINX on a Windows host, that load balancer will not support web socket connections from each cluster node to each of 300 agents.

Solution:

Install NGINX on a host with a UNIX or Linux operating system. If you must use a host with a Windows operating system, then configure F5 as the load balancer for each CA Process Automation clustered Orchestrator.

CPU Usage Spikes with Secured Simplified Communication and NGINX

Symptom:

When a clustered Orchestrator is configured to use secure (HTTPS) communication and agents are configured to use simplified communication with an NGINX load balancer, CPU usage spikes can occur have in server nodes.

Solution:

For agents to use simplified communication when a clustered Orchestrator is configured to use secure (HTTPS) communication, use an F5 load balancer rather than an NGINX load balancer.

REST and Catalyst Operations Are Not Handled by CA SiteMinder SPS in One Case

Symptom:

When a CA Process Automation standalone Orchestrator that is configured to use secure (HTTPS) communication is integrated with CA SiteMinder Secured Proxy Server, REST and Catalyst operations are not handled using CA SiteMinder SPS URLs.

Solution:

When a CA Process Automation standalone Orchestrator that is configured to use secure (HTTPS) communication is integrated with CA SiteMinder Secured Proxy Server, perform REST and Catalyst operations using the direct CA Process Automation URLs.

Disabling of JBoss Seam Framework after an Upgrade

CA Technologies Support has notified customers about a high risk remote code vulnerability affecting certain releases of CA Process Automation, including Service Pack 04.0.01 (4.0 SP01)and Release 04.1.00 (4.1). The vulnerability occurs in the bundled JBoss Seam component and is known as CVE-2010-1871. CA Technologies recommends that you disable the JBoss Seam component to resolve the vulnerability when **upgrading** from the following CA Process Automation releases:

- Service Pack 04.0.01 (4.0 SP01)
- Release 04.1.00 (4.1)

Important! New installations of CA Process Automation 4.1 SP01 and 4.2 have Seam disabled by default. In this case, the following manual remediation is *not* required. However, if you did not perform these steps during the 4.1 SP01 upgrade, you should do so now.

Follow these steps:

1. Stop the CA Process Automation service.
2. Delete the contents of the following directories:

   ```
   install_dir\server\c2o\.tmp
   install_dir\server\c2o\temp
   install_dir\server\c2o\tmp
   install_dir\server\c2o\work
   ```

3. Create a backup directory outside of the CA Process Automation directory tree (for example, "PAM-Seam-Backup").
4. Move the following folders from <PAM_Home>\server\c2o\deployers to the backup location:

   ```
   seam.deployer
   webbeans.deployer
   ```

5. Move the following folder from <PAM_Home>\server\c2o\ to the backup location:

   ```
   admin-console.war
   ```

6. Start the CA Process Automation service.

Note: The preceding instructions disable the JBoss Admin Console.

1. If the JBoss Admin Console is temporarily needed:
   a. Stop the CA Process Automation service.
   b. Move the admin-console.war folder from the backup location to *install_dir*\server\c2o\.
   c. Start the CA Process Automation service.
2. When the Admin Console is no longer needed:

a. Stop the CA Process Automation service.

b. Move the admin-console.war folder from the backup location to *install_dir*\server\c2o\.

c. Start the CA Process Automation service.

Microsoft User Access Control Prevents Successful Launch of Orchestrator Node

Windows operating systems have an option in User Accounts in the Control Panel, that lets you Turn User Account Control on or off. User Account Control limits application software to standard user privileges unless an administrator explicitly specifies administrative privileges for that application software.

User Account Control can be present in the following Microsoft Windows operating systems:

- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows Server 2012

To install a cluster node, either turn off the UAC temporarily or grant administrative privileges for the CA Process Automation software.

Symptom:

When launching the second node install from a Windows machine with an active User Account Control setting, the download takes place, but then the javaw.exe process ends and the installation is not launched.

Solution:

1. Log into the server where you plan to install a second node for the Domain Orchestrator or other Orchestrator.
2. Go to User Accounts in the Control Panel and clear the option to Use User Account Control (UAC).
3. Reboot the server.

Potential Problem When Running CA Process Automation on a VMWare Server When Using the E1000 Network Interface

Symptom:

The root causes of this problem are rare, sporadic, socket I/O failures, which may leave the calling software waiting indefinitely for a read to complete.

From the users perspective the most typical symptom will be the unexpected hanging of processes that normally complete without issue, which resume and complete as expected following a restart of the CA Process Automation Orchestrator. This can impact a small subset of processes, or all running processes. It has no correlation with Orchestrator uptime, and may manifest shortly after a restart, or, after days, weeks, or months of otherwise flawless Orchestrator functionality.

This problem has only been seen in environments running high volumes of CA Process Automation processes. In most environments where the E1000 NIC is installed the problem has never occurred, or occurred so infrequently that it has not been detected.

Solution:

This problem is very difficult to confirm. If this problem occurs, often the CA Process Automation thread is stuck on a socket read, and no relevant errors are written to the log files, and confirmation of the problem requires reviewing a series of Java thread dumps taken during an occurrence of this problem to confirm the operator is stuck on a socket read.

When errors are observed in relation to this problem, they tend to indicate generic connection errors which could have other legitimate and unrelated causes. The following is such an example:

```
2013-07-24 18:55:23,219 WARN  [org.hibernate.jdbc.AbstractBatcher]
[nPool Worker-23] exception clearing maxRows/queryTimeout
com.microsoft.sqlserver.jdbc.SQLServerException: The connection is
closed.
                at
com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDriverErro
r(Unknown Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerConnection.checkClosed(Unkno
wn Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerStatement.checkClosed(Unknow
n Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerStatement.getMaxRows(Unknown
Source)
                at
org.jboss.resource.adapter.jdbc.CachedPreparedStatement.getMaxRows
(CachedPreparedStatement.java:367)
```

```
                at
org.jboss.resource.adapter.jdbc.WrappedStatement.getMaxRows(Wrappe
dStatement.java:378)
                at
org.hibernate.jdbc.AbstractBatcher.closeQueryStatement(AbstractBat
cher.java:272)
                at
org.hibernate.jdbc.AbstractBatcher.closeQueryStatement(AbstractBat
cher.java:209)
```

. . . and so on.

In these cases identification of the problem is tentative, and other causes for communication failure must be excluded.

Frequent process failure, or a repeatable failure of an individual operator or operators likely indicate other unrelated problems within the process design or Orchestrator functionality.

At sites where this problem has been confirmed, reconfiguring the VMWare server from an E1000 Network Interface Card driver to a VMXnet-3 NIC driver is seen to be a very effective mitigation.

CA Technologies is hesitant to declare this a complete resolution as the incident rate for this is very rare and timeframe between occurrences even with the E1000 NIC can be quite long.

If verification of the issue is required prior to making this change, please contact Support for assistance setting up the logging and Java thread dumps required to troubleshoot and verify this particular issue.

Turkish Operating System Required for Installing Turkish Version of CA Process Automation

You can only install the Turkish version of CA Process Automation components on computers using a Turkish operating system.

CA EEM Release 8.4-to-12.0 Server Upgrade Issue

If the CA EEM instance used by a CA Process Automation instance to be upgraded has been upgraded from CA EEM Release 08.4.00 to Version 12.0.00, you can experience installer errors during the CA Process Automation application upgrade.

To avoid the error, upgrade CA EEM directly to Release 12.5 or Release 12.51.

If the upgrade was to CA EEM Release 12.0, follow these steps before upgrading CA Process Automation:

1. Browse to CA EEM and log into the CA Process Automation application with the CA EEM administrator credentials. By default, the user name is EiamAdmin.
2. Click the Manage Access Policies tab and then click Scoping Policies, the last item in policy list.
3. Click on the first link (DelegatedPolicyAccess).
4. Click Save.
5. Launch the CA Process Automation installer and proceed with the CA Process Automation upgrade.
6. When you reach the CA EEM Security Settings page, click the Register button and follow the prompts to upgrade the CA EEM application.

   A confirmation message informs you that the application upgrade is successful.

SOAP Operations in CA Process Automation

If the CA Process Automation host name starts with a numerical value, SOAP operations do not work in CA Process Automation. We recommend not using a numeric value as a starting value for a host name.

CA Process Automation Installation on Dual Stack (IPv4 and IPv6) Network Environments

If you install CA Process Automation on dual stack (IPv4 and IPv6) network environments, CA Process Automation may fail to boot up.

Symptom:

When you install CA Process Automation on dual stack (IPv6 and IPv4) network environments, you may experience issues while bringing up or accessing the following CA Process Automation components across network:

- Domain Orchestrators
- Orchestrators
- Agents

Solution:

Disable IPv6 stack on the host system where any of the following CA Process Automation components are running and restart the services:

- Domain Orchestrators
- Orchestrators
- Agents

Export Objects Can Contain Only English Characters

Due to a Microsoft Windows limitation, a folder name with non-English characters gets exported to pam_export.xml instead of *FolderName*.xml. Likewise, an object name with non-English characters gets exported to pam_export.xml instead of *ObjectName*.xml.

As a best practice, when preparing to export a folder, a release-specific folder as a content package, or an object, where the name of the folder or object includes non-English characters, be sure to rename the folder or object prior to export.

Google Chrome Fails First Attempt to Log Out Users Logged in Using NTLM

When CA EEM is configured to use Microsoft Active Directory as the external directory and to use NTLM authentication, you can browse to CA Process Automation with the Google Chrome browser and bypass the Login dialog. When you click the Log Out link, your UI refreshes but logout does not occur. When you click the Log Out link a second time, a Login UI requesting credentials opens.

You should be able to log out of CA Process Automation on your first attempt. This behavior is specific to the Google Chrome browser and is not a CA Process Automation issue.

JDK 1.7 is Unable to Encrypt and Decrypt Passwords with Special Characters like "&" in SUSE 11SP1

In CA Process Automation 4.1, JDK 1.7 is unable to encrypt and decrypt passwords with special characters such as & in SUSE 11SP1.

Symptom:

When you use SUSE 11 SP1with the Microsoft SQL 2k8 on Microsoft Windows 2k8, JDK 12.7 throws an exception and the CA Process Automation application does not start. The exception is thrown when the Microsoft SQL-SA password has special characters such as &.

Solution:

Uninstall the JDK 1.7 rpm on SUSE linux and install JDK 1.6.X.

Limitations in Internet Explorer

Internet Explorer limits the agent installation in a network other than the network where Domain Orchestrator is installed.

Symptom:

Access the Domain Orchestrator using Internet Explorer and install the CA Process Automation Agent in a network other than the network where Domain Orchestrator is installed. The installation may fail while downloading JAR files for installation.

Solution:

A possible cause of this sporadic issue might be that Java is unable to load JAR files while routing through the proxy in Internet Explorer. To mitigate this issue, change Java Network Settings to the Direct Connect option before you install the Agent.

Follow these steps:

1. Open the Java Control Panel on the host system where you install the Agent.
2. Open Network Settings from the General tab.

   The Network Settings page appears.
3. Select the Direct Connect option and click OK to save changes.
4. Install the Agent.

Oracle bug # 9347941

Important! When running with versions of the Oracle RDBMS prior to release 11.1.0.7, CA Process Automation would occasionally encounter the known Oracle RDBMS defect 9347941 in which concurrent inserts of CLOB data where the individual column values exceed 52K bytes in size have such columns updated incorrectly with data past the 52K offset replaced by spaces. This issue has been seen using both 10g and earlier 11g versions of the Oracle RDBMS.

Symptom:

CA Process Automation process would freeze. Reset the process at the corresponding operator where the process is frozen to continue the process execution to complete. This infrequent issue occurs only with extremely high rates of update contention.

Solution:

This has not been seen when running either version 11.1.0.7 or 11.2.0.2 of Oracle, and we recommended that sites using Oracle for their CA Process Automation databases run version 11.1.0.7 or 11.2.0.2 or higher.

Sorting Automation Objects

For compatibility with previous releases, CA Process Automation r4.x would not support sorting automation objects on 'Type' column. Because the sorted order in the UI is different from the sorted order in the database at the back end, CA Process Automation does not support sorting by type.

Unable to Launch CA Process Automation using the Apache URL in Internet Explorer and Firefox

Symptom:

You cannot launch CA Process Automation using the Apache URL in Internet Explorer and Firefox after enabling NTLM authentication in a cluster environment. This issue is specific to Internet Explorer and occurs when the load balancer is used in secure mode. The CA Process Automation UI appears blank once you log in.

Solution:

Comment the following lines in httpd-ssl.conf. httpd-ssl.conf can be found under *ApacheInstallDir*\conf\extra\httpd-ssl.conf (for example, C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\extra\ httpd-ssl.conf).

```
#BrowserMatch ".*MSIE.*" \
# nokeepalive ssl-unclean-shutdown \
# downgrade-1.0 force-response-1.0
```

CA Process Automation successfully launches.

Limitations to Process Definition Upgrade

A primary goal of CA Process Automation upgrades is that existing content continues to behave identically to previous versions to preserve your investment in existing processes. Exceptions such as retired functionality are rare and carefully considered.

However, the following minor differences exist because of current implementation limitations:

Some link customizations do not translate.

Most customized link attributes translate to the new Process Designer, with the following exceptions:

- Links defined with styles other than "solid" display as "dashed"
- Links defined with the “curved” shape display as “orthogonal”

This limitation only affects how links are displayed, and does not affect link operation.

Processes upgraded or imported from previous releases do not allow design-time browsing of output parameters.

Design-time generation of output variables is a CA Process Automation v4.0 feature and is available only for new processes. This limitation does not affect run-time function of the processes, but prevents users from previewing output variables.

Custom Icons do not display.

Custom Icons that were developed before CA Process Automation v4.0 do not display in CA Process Automation v4.0. Instead, operators and custom operators display the default CA Process Automation v4.0 icon for the base operator.

SERVER_CONNECT_FAILED Error

This error can occur after you apply a CA Process Automation upgrade or patch:

```
SERVER_CONNECT_FAILED Status Code: 400
```

Clear the browser cache and restart the browser-based UI.

Documentation Known Issues

This section describes the documentation known issues in CA Process Automation 04.2.01:

Missing information in the Content Designer Reference Guide

Symptom:

A note is missing before Step 3 in the Add an SSL Certificate to CA Process Automation section in the *Content Designer Reference Guide*.

Solution:

The following note has been added before step 3 in the Add an SSL Certificate to CA Process Automation section in the *Content Designer Reference Guide:*

Note: If the jssecacerts file exists in the jre/lib/security directory, import the certificate in the jssecacerts file as shown in step 3.B and specify “jssecacerts” in the trustStore flag in step 4.B. Else, import the certificate in the cacerts file as shown in step 3.A and specify “cacerts” in the trustStore flag in step 4.A.

Appendix A: Acknowledgments and License Agreements

Components that are licensed under the Apache 2.0 License are listed in the following topic:

- Components Licensed under the Apache 2.0 License

PDF users can find the following license agreements in the \Bookshelf Files\TPSA folder of the CA Bookshelf. You can navigate to the TPSA folder and its files if you download the bookshelf. HTML users can link directly to the license agreements from the following links.

- Apache 2.0 License
- Apache Active MQ 5.8.0
- Apache Tuscany SDO
- Beanshell v.2.0b4
- BIRT 2.3.2.2
- Castor Software
- CodeMirror 2.25
- CodeMirrorUI 0.0.16
- Derby 10.8.1.2
- ej technologies
- el-api 2.2
- el-impl 2.2
- Hibernate Software 3.3.2
- HSQLDB 1.8
- Hypersonic SQL Group
- J2ssh 0.2.7
- JAXP 1.4.2
- JBoss 5.1
- JGO 5.1.5
- JGoodies Looks 2.2.0
- JGroups 2.6.22.Final
- JNA 3.4.0
- JSHint r07
- JSW (Java Service Wrapper) 3.2.3
- jTDS 1.3.1
- Netx 0.5
- Oracle 11G JDBC Driver

- Rhino 1.6R4
- Xalan-j 2.7.1

Components Licensed under the Apache Software License v.2.0

This product includes the following components that are licensed under the Apache 2.0 license:

Apache log4j 1.2.15

This product includes Apache log4j 1.2.15, which is distributed in accordance with the Apache license agreement.

Commons CLI 1.2

This product includes Apache Commons CLI 1.2, which is distributed in accordance with the Apache license agreement.

Commons Lang 2.1

This product includes Apache Commons Lang 2.1, which is distributed in accordance with the Apache license agreement.

Commons Logging 1.1.1

This product includes Apache Commons Logging 1.1.1, which is distributed in accordance with the Apache license agreement.

Commons.net 2.2

This product includes Apache Commons.net 2.2, which is distributed in accordance with the Apache license agreement.

Derby 10.8.1.2

This product includes Derby 10.8.1.2, which is distributed in accordance with the Apache license agreement.

Drools 4.0.0

This product includes Drools 4.0.0, which is distributed in accordance with the Apache license agreement.

google-gson 1.7.1

This product includes google-gson 1.7.1, which is distributed in accordance with the Apache license agreement.

httpclient 4.2.3

This product includes httpclient 4.2.3, which is distributed in accordance with the Apache license agreement.

jetty 8.1.10

This product includes Jetty 8.1.10, which is distributed in accordance with the Apache license agreement(s).

json-simple 1.1.1

This product includes json-simple 1.0 which is distributed in accordance with the Apache license agreement.

L2FProd 0.2

This product includes L2FProd, which is distributed in accordance with the Apache license agreement.

Mime4j 0.6

This product includes Apache Mime4J 0.6, which is distributed in accordance with the Apache license agreement.

SNMP4j 1.8

This product includes SNMP4J 1.8, which is distributed in accordance with the Apache license agreement.

Tomcat connector 1.2.20

This product includes Apache Tomcat Connectors 1.2.20, which is distributed in accordance with the Apache license agreement.

wss4j 1.5.8

This product includes Apache wss4j 1.5.8, which is distributed in accordance with the Apache license agreement.

XML Schema 1.4.2

This product includes Apache XMLSchema 1.4.2, which is distributed in accordance with the Apache license agreement.

XMLSec 1.4.4

This product includes Apache xmlsec 1.4.4 which is distributed in accordance with the Apache license agreement.