

CA Release Automation - 5.0.2 Administration

Date: 28-Aug-2014

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

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Table of Contents

Automation Studio Administration	6
Release Operations Center Administration	8
Manage System Settings	9
Change System Settings	10
Change from Default to Local Fonts	10
How to Set Up Users and Permissions	11
Review the Prerequisites	12
User Roles	12
Permissions	13
How to Import Users and Groups	15
Import Users with a Batch File	16
Create a User	16
Create User Groups	16
Grant Permissions	17
Manage Execution Servers and Agent Groups	18
Create Execution Servers	18
Change Execution Server for Agents	18
Create Sibling Connections Between Execution Servers	19
Create Agent Groups	19
Assign Test Agents	20
Update Agent Configuration Properties	20
Restart an Agent on Windows	20
Create Execution Server and Agent Logs	21
Manage System Agents Groups	22
Add System Agents Groups	22

Manage Approval Gates	23
Setting Approval Gates	23
Confirm Manual Approval Gates	24
Run Approval Gates Approval Steps	24
Confirm ServiceNow Approvals	25
 Manipulate Services	 26
 Export Automation Studio Data	 27
Import Automation Studio Data	27
 Enable LDAP Integration	 28
 Configure Purge Settings	 31
 Update the Nexus Repository Password	 32

Administration

Contents

- [Automation Studio Administration](#)
- [Release Operations Center Administration](#)

Administration in CA Release Automation enables users with Superuser or Administrator roles to manage the configuration of the product, manage users, manage servers and agents, and to manage release objects.

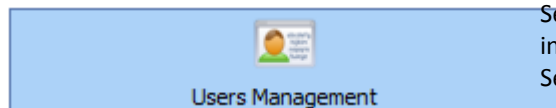
Note: CA Release Automation uses multiple Administrator roles. For more information, see [How to Set Up Users and Permissions](#).

Administration functions are split between Administration tabs in both Automation Studio and Release Operations Center.

Automation Studio Administration

Automation Studio provides the main product configuration and user management functions in CA Release Automation.

CA recommends that after installation, administrators should set up User and Permission Management, and then set up System Settings to configure CA Release Automation.

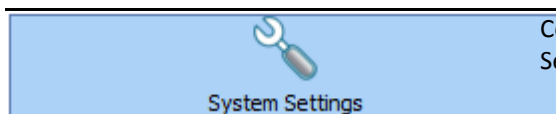


Set up users to access the functions they require in CA Release Automation.
See [How to Set Up Users and Permissions](#).

User Management

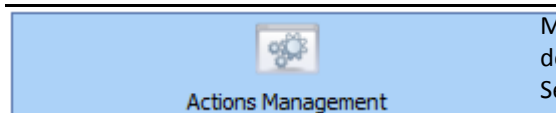


Permissions Management



Configure CA Release Automation settings.
See [Manage System Settings](#).

System Settings




Manage the individual operations available for deployment processes.
See [Manage Action Packs in Automation Studio](#) in [Actions and Custom Actions Development](#).
Note: Use Release Operations Center to download Action Packs.

Actions Management




Manage execution servers and agent groups in Automation Studio.
See [How to Deploy CA Release Automation Agents](#) in [Installation](#).
See [Manage Execution Servers and Agent Groups](#).
Note: Release Operations Center also contains Agent Management functions.

Agents Management

 Artifacts Management	Manage the component objects for deployment. See How to Manage Artifacts in Deployment Automation .
---	---

Artifacts Management

 Process Tags Management	Use tags to help identify specific processes. See How to Create an Automation Process in Deployment Automation .
--	--

Process Tags Management

Release Operations Center Administration

Users with Application, Environment, or Process/Release level permissions can execute the following tasks to manage deployments from the Administration tab in Release Operations Center.

Environment Configuration	Configure environments for use with deployments.
Rollback	Configure rollback settings in the event of deployment failures. See How to Manage Environments in Deployment Automation .
Approval Gates	Set up approval gates for use during deployment. See Manage Approval Gates .
Agent Groups	Manage agent groups in Release Operations Center. See Manage System Agents Groups . Note: Automation Studio also contains Agent Management functions.
Actions Management	Download Action Packs and manage actions in Release Operations Center. See Manage Action Packs in Release Operations Center in Actions and Custom Actions Development . Note: Automation Studio also contains Action Management functions.
Health Monitoring	Monitor the status of your servers, agents, and deployments. See Manage and View the Health Monitor in Reporting .

Manage System Settings

Contents

- [Change System Settings](#)
- [Change from Default to Local Fonts](#)

Users with either a Superuser or Administrator accounts can change various default system parameters such as:

- Audit Design Changes
- Audit Design Interval
- Audit report Page Size
- Grace Period Time
- Import Demos
- Max process tags
- Monitoring data: clean every (in minutes)
- Monitoring data: clean server every (in minute)
- Monitoring data: life length (in minutes)
- Monitoring data: life length of server (in minutes)
- SMTP Email
- SMTP Password
- SMTP Port
- SMTP Requires Login
- SMTP Server
- SMTP User
- Show Deprecated Actions
- Unix Agent Default Installation Dir
- WAKE_UP_PERSISTENCY_SCHEDULE
- Windows Agent Default Installation Dir

Change System Settings

To change the Automation Studio default parameters, change the system settings.

Follow these steps:

1. From the Automation Studio UI, click Administration.
2. Select System Settings.
3. Double-click the Parameter name, input the change, and click Save.
4. Click OK to confirm.

Note: For the change to take effect, restart Automation Studio.

After the restart, the parameter change appears on the system setting page.

Change from Default to Local Fonts

To support the use of special characters, including double-byte characters, and local fonts in Automation Studio, change the font settings.

Follow these steps:

1. On the Automation Studio UI click file, and select Use Local OS Font.

Important! Save any work before you select to restart.

2. Click Yes.
Automation Studio closes
3. Restart Automation Studio
After the restart local fonts are enabled.

How to Set Up Users and Permissions

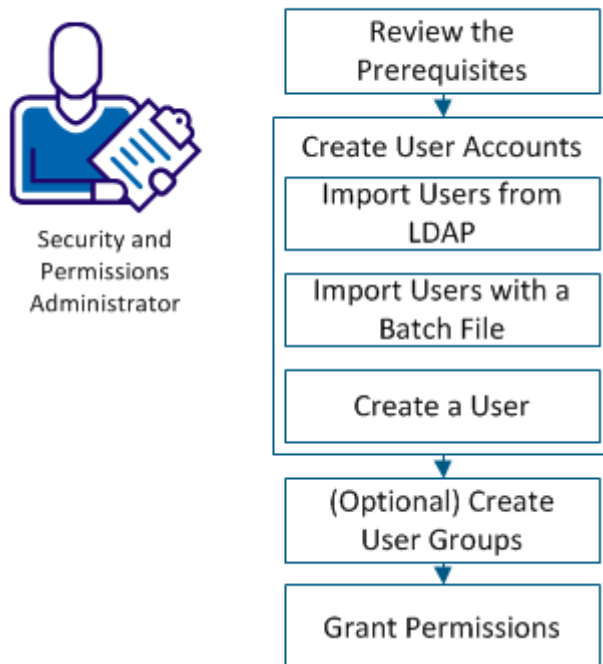
Contents

- [Review the Prerequisites](#)
 - [User Roles](#)
 - [Permissions](#)
- [How to Import Users and Groups](#)
- [Import Users with a Batch File](#)
- [Create a User](#)
- [Create User Groups](#)
- [Grant Permissions](#)

As a security and permissions administrator, you manage access to CA Release Automation. Before users of CA Release Automation can perform their tasks, you must grant them appropriate access based on their roles. CA Release Automation provides targeted access to specific functionality with user roles and permissions.

Use this scenario to guide you through the process:

How To Set Up Users and Permissions



This diagram shows the steps to set up users and permissions in CA Release Automation

1. [Review the Prerequisites](#).

2. Create user accounts using any of the following methods:
 - If you use LDAP authentication to manage users, [Import Users from LDAP](#).
 - If you need to create multiple user accounts without importing from LDAP, [Import Users with a Batch File](#).
 - If you need to grant access to a single user, [Create a User](#).
3. [\(Optional\) Create User Groups](#).
4. [Grant Permissions](#).

Review the Prerequisites

Verify the following prerequisite to ensure that you can set up users and permissions:

- You have authorization as a Superuser or Security and Permissions Administrator.
- You understand the user roles and permissions. For more information, see [User Roles](#) and [Permissions](#).
- If you require LDAP authentication, see [Enable LDAP Integration](#).

User Roles

In CA Release Automation, user roles determine user access rights.

CA Release Automation includes the following user roles:

- **User**
Provides access to the Reports panel.

Note: Users cannot view applications unless they also have the appropriate application-level permissions.

- **Superuser**
Provides access to all panels and tabs.

Important! For the initial login, the default superuser credentials are user name *superuser* with password *user*. We recommend changing this password immediately after installation.

- **Admin User**

Provides access to administrative tasks.

Assign specific roles to Admin Users as follows:

- **Security and Permissions Administrator**

Manages users and permissions.

- **Servers Administrator**

Manages servers and agents.

- **General System Administrator**

Imports new action packages and defines general system settings.

Note: Admin Users cannot access applications.

Permissions

Permissions control access to screens and functions. You can assign permissions for operations on a server group or in an application. In applications, you can assign permissions at the environment level and at the process level.

Note: Permissions for users and groups aggregate. When you assign a user to a group, the user has the group permissions and individual user permissions.

CA Release Automation includes the following permission types:

- Server group permissions
- Application-level permissions
- Environment-level permissions
- Process-level permissions

Server group permissions define the server group that a user can access.

Note: Any user with execution permissions can run reports. The reports are limited to areas where the user has execution permissions.

Application-level permissions:

- **Can View Application**

This permission is an initial permission level that is required for other application, environment, and process level permissions. A user with this permission can:

- View component actions, flows, and parameters.
- View architectures, server types, and processes.
- Copy components from the current application to another application to which the user has permissions.
- View usages for components and parameters.
- View the Reports tab and the process activity for the application.

- **Application Owner**

Grants full permissions on a specific application and all the environments of that application.

- **Application Publisher**

Enables a user to publish any process in any environment under the current application. By default, the Application Designer permission is enabled.

- **Application Designer**

Enables a user to create and design processes and components under the current application.

- **Can View Design Components**

Enables a user to view all objects in the Components tab and Processes tab in Automation Studio for the current application.

- **Execute Processes in All Environments**

Enables a user to execute all processes in all environments under the current application.

- **Can View Execution Components**

Enables a user to view the Environments tab in Automation Studio for the current application.

- **Execute Releases in All Environments (Release Operations Center)**

Enables a user to execute all releases in all environments under the current application in Release Operations Center.

- **Release Template Designer (Release Operations Center)**

Enables a user to create and design templates in all environments under the current application in Release Operations Center.

Environment-level permissions:

- **Environment Admin**

Enables a user to execute all processes in Automation Studio, and design releases and execute all releases in Release Operations Center for the current environment.

- **Can Execute All Processes**

Enables a user to execute all processes in Automation Studio for the current environment.

- **Release Designer (Release Operations Center)**

Enables a user to design releases in Release Operations Center for the current environment.

- **Can Execute All Releases (Release Operations Center)**

Enables a user to execute all releases in Release Operations Center for the current environment.

Process/release level permissions:

- **Individual processes**

Enables a user to execute individual processes.

- **Individual release templates (Release Operations Center)**

Enables a user to execute releases that are created from specific templates in Release Operations Center.

How to Import Users and Groups

If you use LDAP authentication, import user information from the LDAP server to create user accounts.

Follow these steps:

1. Browse the LDAP server for a list of users.
2. Select the LDAP users to import into CA Release Automation.
3. Log in to Automation Studio.
4. Open the Administration tab of the Navigation Panel, and click System Settings.
5. Select and specify the LDAP user import values.
6. Select User Management, and click the arrow next to the + icon in the Users panel.
7. Select Import from LDAP.
8. Type the information in the Import Users dialog.
9. (Optional) To use Active Directory standards for user look up, select Active Directory.
10. (Optional) To use SSL for user authentication with LDAPS, Select Use SSL.
11. Click Load to generate a list of LDAP Users.
12. Select a user role, and select administration levels if the Role is Admin User.
Note: For more information about users roles, see [User Roles](#).
13. Click Import to accept the list of loaded users, and click Save.
CA Release Automation creates the selected user accounts from the information on the LDAP server.
14. (Optional) To add Groups, click the arrow next to the + icon in the Groups panel, and follow the same steps.

Note: After the users are imported, the user email address can be edited to the alias (short-name).

Import Users with a Batch File

To create multiple user accounts, use a tab-delimited data file that provides the individual user attributes.

Note: To assign Superuser or Admin User to a user created with a batch file, edit the user account. For more information on user roles, see [User Roles](#).

Follow these steps:

1. Log in to Automation Studio.
2. Open the Administration tab of the Navigation Panel, and click User Management.
3. Click the arrow next to the + icon in the Users panel, and select Load from File.
4. Create a tab-delimited text file according to attributes listed in the Load Users window.
5. Click File in the Load Users dialog. Select the batch file in the Open dialog and click open.
6. Click Load to load the selected file.
When the loading process completes, the Load Users message opens. This window provides detailed information about the load process.
The users have access to CA Release Automation.

Create a User

When a new user requires access to CA Release Automation, create a user account.

Follow these steps:

1. In the Administration tab of the Navigation Panel, select User Management.
2. In the User panel, click the + icon.
3. Specify the required information, and select an authentication method.
4. Select a user role, and select administration levels if the Role is Admin User.
Note: For more information on users roles, see [User Roles](#).
5. Click Save.
The user has access to CA Release Automation.
You can now edit the user, add the user to groups, assign permissions, or delete the user.

Create User Groups

Multiple users may share responsibilities and require the same permissions. To assign permissions to multiple users at the same time, create User Groups.

Follow these steps:

1. In the Administration tab of the Navigation Panel, select Users Management.
2. Click the + icon in the Groups list.
3. Specify a Group Name and a Description.
4. (Optional) Select a Role, and select Admin User type if applicable.

Note: The Role applies to all users in the group in addition to the role of the specific user.

5. Click Create.
CA Release Automation creates the User Group.
6. Select a user in the Users list, and click the right arrow to add the selected user to the user group. Add all appropriate users to the user group.
You can now add or remove users, edit the user group, or delete the user group.

Grant Permissions

To provide access to specific CA Release Automation functions, assign permissions according to their role.

Follow these steps:

1. In the Administration tab of the Navigation Panel, select Permissions Management.
2. Select a user or user group from the Users and Groups list.
3. Select the Server Groups tab or the Application Structure tab.
4. Select the Server Group or Application, and select appropriate permissions.

Important! When granting environment- and process-level permissions, select the Can View Application permission in the appropriate application.

Note: For more information about permissions, see [Permissions](#).

5. Click Save.
The user or users in the group can now perform their assigned tasks.

Manage Execution Servers and Agent Groups

Contents

- [Create Execution Servers](#)
- [Change Execution Server for Agents](#)
- [Create Sibling Connections Between Execution Servers](#)
- [Create Agent Groups](#)
- [Assign Test Agents](#)
- [Update Agent Configuration Properties](#)
- [Restart an Agent on Windows](#)
- [Create Execution Server and Agent Logs](#)

Automation Studio manages multi-tier applications by channeling data and instructions to CA Release Automation Execution Servers installed at Data Centers. Execution Servers provide the information to the Agents installed on each of the Data Center servers.

Create Execution Servers

To allow Agents to receive application instructions, add Execution Servers.

Follow these steps:

1. Click the Administration tab, and select Agents Management.
2. Click Add, and select Execution Server.
3. Type the Host, Port, and Protocol details, and click Save.
The Agents list refreshes, and the new Execution Server appears in the Agent list.

Note: You can also edit, and delete, Execution Servers.

Change Execution Server for Agents

To reconfigure the instructions passed from an Agent, change the Execution Server the Agent distributes instructions to during the deployment process.

Important! Check the Execution Server before updating to verify that the agent is not participating in any deployment process as the Agent restarts after a change.

Follow these steps:

1. Click the Administration tab, and select Agents Management.

2. In the Agents list, select an agent.

Note: To select multiple agents, press CTRL.

3. Right-click the Agent, and select Change execution server of the selected agents.

4. Select the new Execution Server the agent reports to.

5. Click Save.

The Agents list refreshes, and the new Execution server appears in the Details panel for the Agent.

Note: An agent reports to the first server selected when using multiple Execution Servers. You cannot change the order.

Create Sibling Connections Between Execution Servers

To allow Agents to communicate with other Agents across Execution Servers, create a sibling connection between the Execution Servers.

Follow these steps:

1. Click the Administration tab, and select Agents Management.
2. Select the Execution Server.
3. Right-click the agent, and select Change execution server of the selected agents.
4. Click the Add custom execution server.
5. Type the Host Name, or IP address, and the Port Number.

Note: Use the following format: <ComputerName>-ES2. The default port is 8080.

6. Click OK, and click Save.
The Agents panel refreshes, and the new Execution Server connection appears in the Details panel.

Create Agent Groups

Define Agents into Agent Groups that are designated to handle special functions during the process execution. If one agent is not available to retrieve an artifact, the artifact is retrieved using another agent that is defined in the group.

Note: A single agent can simultaneously belong to any number of Agent Groups.

Follow these steps:

1. Click the Administration tab, and select Agents Management.
2. Click the Add new agents group.

3. Type the group name and description, and click Save.
The screen refreshes, and the new Agent group appears.
4. Select the agent in the Agents list.
5. Select the group in the Agent Groups list, and click the "Move to the right" arrow.
The Agent Groups list refreshes, and the agent appears in the selected group.

Assign Test Agents

To use Agents for testing actions, flows, and processes, while modeling applications in Automation Studio, create Test Agents.

Follow these steps:

1. Click the Administration tab, and select click Test Agents Management.
2. Select an agent, and click the Move items to the right arrow.

The agent appears in the Test Servers group.

Update Agent Configuration Properties

When the network settings of a server are changed, you can update the agents TCP Port and Secure Communication settings to reflect the change.

Follow these steps:

1. Click the Administration tab, and select Agents Management.
2. Select the agent, and right-click.
3. Select Change properties of selected agents.
4. Type the details that you want to change, and click Save.
The agents restarts with the selected changes

Restart an Agent on Windows

To restart an Agent that is installed on a Windows computer that failed during the deployment process.

Note: You can only restart Agents that are running on Windows and connected to an Execution server running on Windows.

Follow these steps:

1. Click the Administration tab, and select Agents Management.

2. Select the Agent.

Press CTRL to select multiple agents.

3. Right-click, and select Restart selected agents.
4. Type in the user name and password for the Agent.
The Agents restarts.

Create Execution Server and Agent Logs

The Execution Server and Agent logs track processes and errors in Automation Studio for the selected execution server or agent. To review run jobs, create an Execution Server or an Agent log.

Follow these steps:

1. Click the Administration tab, and click Agents Management.
2. In the Agents list, select an Execution Server or Agent.
3. Right-click an Execution Server or Agent, and select Collect Logs.
4. Click Target Path, and select the destination path.
5. Click Collect Logs.
The Collecting Log dialog opens and notifies you once the process is complete.

Manage System Agents Groups

Contents

- [Add System Agents Groups](#)

In Release Operations Center, system agents operate outside the deployment environment but serve the deployment by performing tasks like artifact retrieval and approval request. To ensure agent availability to perform a task that you assign to an agent group, assign system agents to the group.

Add System Agents Groups

To ensure continuous agent availability during artifact retrieval and approval requests, add system agents to system agents groups.

Follow these steps:

1. Click the Administration tab, select Agent Group.
2. Click New, and Type a name and description.
3. In the Group Type list, select a type for the group:
 - **Artifact Retrieval**
Group for artifact retrieval.
 - **Approval Runner**
Group for approval gate processing.
4. In the Retrieval Agent table, select agents for the group.

Note: To locate agents in a large table, use Search.
5. Click Save.
The new group appears in the Agent Groups list.

Manage Approval Gates

Contents

- [Setting Approval Gates](#)
- [Confirm Manual Approval Gates](#)
- [Run Approval Gates Approval Steps](#)
- [Confirm ServiceNow Approvals](#)

Release Approval Gates enables an environment administrator to define the following approval gates for an application environment:

- Manual Approval - Release Operations Center internal approval gate.
- Approval Step - Automatic approval that is based on success of a Release step.
- ServiceNow Approval - Bind manual release approval to a given ServiceNow Change Request.

Approval Gates Definitions:

- Define Approval Gates at the environment level before template or release creation.
- Define the exceptions at the template level, including overriding settings for all approval gates.
- Define multiple approval gate types for an environment or template.
- Approval Step and ServiceNow Approval types can be set not to require approval at the release level.

Setting Approval Gates

The approval gates can be set for various combinations of approval types:

- Manual
- Approval step
- ServiceNow configuration

at the environment and template levels. Definition on the template level supersedes definition on the environment level. The ServiceNow Approval Gates process uses the ServiceNow Change Request ticketing functionality. A user can set an option to ignore the ServiceNow approval process during the Change Request number definition.

To configure the appropriate approval types, select and set the approval gates.

Follow these steps:

1. Click the Administration tab, and select Approval.
2. Select the Application and the Environment.
3. Select the Environment tab or the Template tab.
 - a. In the Environment tab, click Add Approval Gates.
 - b. In the Templates tab, select a template, and click Edit.
4. Select the approval type.
 - a. For Approval Step, specify the Process, the Tag Version, and the Agent Group.
 - b. Set ServiceNow approvals at the environment level, and type the URL, User, and Password.
5. (Optional) At the template level, to override environment level approval settings, select Override settings for all approval gates.
6. Click Save.

The approval gates definition are set.

Confirm Manual Approval Gates

For manual approval gates, a user confirms or denies approval. The Release window displays for a release that is created and defined for manual approval.

Note: The permissions and role that is required to confirm approval gates are: the Release Designer, the Environment Administrator, and the Superuser.

To approve a release set for manual approval, confirm the manual approval gates.

Follow these steps:

1. Select the Releases tab, select Deployments.
2. Select the Application, and click Approvals.
3. Click the Approval Gates tab, and click Approve.
4. Click OK to confirm the approval.

The approval message appears in the Approval Gates tab.

Run Approval Gates Approval Steps

The release approval step approval gates can be used together with the manual approval gates. When the release execution reaches the Approval Step, the status changes to Pending.

To proceed to the next step in the deployment, approve pending approval steps.

Follow these steps:

1. In the Releases tab, click the Approval Gate tab.
2. Click Run.
3. In the Start Approval Step confirmation dialog, click Run.
4. (Optional) To run the release automatically after the approval step completes, select Run Release Automatically.
The step is approved and the deployment continues to the next step.

Confirm ServiceNow Approvals

The confirmation of a ServiceNow approval requires that an entry in Release Operations Center uses a ServiceNow Change Request number. When the Change Request number is approved in ServiceNow, ServiceNow sends a message to Release Operations Center approving the release.

To approve and execute the Release Operations Center entry, confirm the ServiceNow approval.

Follow these steps:

1. In the Releases tab, select the release waiting for ServiceNow approval.

Note: Identify the releases waiting for ServiceNow confirmation by the Change Request not defined message.
2. In the Approval Gate pane, click Edit.
3. Specify the appropriate ServiceNow number.
4. (Optional) To verify the number, click Check.
After the verification, the Approval Gate dialog displays the request response from ServiceNow.
5. Click Save.
Release Operations Center delays the release until ServiceNow sends the change request number approval response.

Manipulate Services

Use the following commands on Linux platforms to control the Nolio Server service. Run the commands at the Command prompt.

- Install the service:

```
./nolio_server.sh install
```

- Start the service:

```
./nolio_server.sh start
```

- Stop the service:

```
./nolio_server.sh stop
```

- Restart the service:

```
./nolio_server.sh restart
```

- Query the status of the service:

```
./nolio_server.sh status
```

Export Automation Studio Data

Contents

- [Import Automation Studio Data](#)

To back up or transfer your application design objects, export data.

Follow these steps:

1. Click File on the menu bar, and select Export.
2. Select the elements you want to export.
3. Click Export, and click close when the export completes.
 - By default, Automation Studio saves the data in <My Documents>\export.dat.
 - The export of large applications may take an extended period of time. CA Technologies recommends that you increase the session timeout values of your firewall.

Import Automation Studio Data

To add architectures from another system or restore backed-up data, import data.

Follow these steps:

1. Click File on the menu bar, and select Import.
2. Click File, select the file to import, and click Open.
3. Select the elements to import.
4. (Optional) Select Import Published Processes.

Note: Importing published processes allows you to edit the processes but increases the length of the import.
5. Click Import.
 - If the import includes Used Actions, verify that you want to import the actions, and click Import.
 - If the import includes a component, follow the Import Wizard.
6. Click Close when the import completes.

The imported elements are available for use.

Enable LDAP Integration

To link CA Release Automation with an existing LDAP solution, enable LDAP integration. The LDAP integration enables users or groups to authenticate directly from the LDAP.

Notes:

- You can select only one type of LDAP integration, General, or Active Directory to enable simultaneously.
- To use SSL to import users or to communicate with the LDAPS server to perform user authentication, the distributed.properties file requires configuration.

Follow these steps:

1. Close all Automation Studio client UIs.
2. Stop the Management Server service:

Linux:

```
./bin/nolio_server.sh stop
```

Windows:

Run services.msc (In %windir%\system32\), in the list of running services, find "Nolio Release Automation Server", and click "Stop".

3. Locate and update webapps/datamanagement/WEB-INF/distributed.properties.

4. Uncomment the required lines and provide the required inputs for General or Active Directory:

Authenticate using Active Directory:

#Uncomment and edit following lines to be able to log in with your Active Directory domain user.
#NOTE: User will see nothing in ASAP, unless he is a member of some security group in
#the domain, which was previously imported to ASAP, and granted with permissions
#to some application#NOTE: only one type of LDAP integration, General or Active Directory, can be enabled at the same time.

```
#use.active.directory.authentication=true
#use.active.directory.domain=<domain name, e.g: mycompany.com>
#use.active.directory.url=<ldap url, e.g: ldap://server.domain.com>
#use.active.directory.user.username=<ldap domain user that has permissions to see other users >
#use.active.directory.user.password= <password of the user defined in use.active.directory.user.username>
```

Authenticate using LDAP:

#Uncomment and edit following lines to be able to log in with your a user defined in your local LDAP.
#NOTE: User will see nothing in ASAP, unless he is a member of some security group in
#the domain, which was previously imported to ASAP, and granted with permissions
#to some application
#NOTE: only one type of LDAP integration, General or Active Directory, can be enabled at the same time.

```
#use.general.ldap.authentication=true
#use.general.ldap.url=<ldap url, e.g: ldap://localhost:10389>
#use.general.ldap.user.fqdn=<fully qualified DN of domain user that has permissions to see other users, e.g:uid=admin,ou=system>
#use.general.ldap.user.password=<password of the user defined in use.general.ldap.user.fqdn>
```

5. To add the Root Certificate to Nolio, run the following command from the command line:

```
D:\Program Files\Nolio\NolioAutomationCenter>..\jre\bin\keytool.exe -import  
-alias hmroot -file d:\temp\root.certificate -keystore  
..\jre\lib\security\cacerts
```

Password: changeit

The certificate name is "root.certificate".

The certificate alias is "hmroot".

The keytool and cacerts are located in:

C:\Program Files\CA\ReleaseAutomationServer\jre\bin\keytool.exe

C:\Program Files\CA\ReleaseAutomationServer\jre\lib\security\cacerts

6. Restart the Management Server service:

Linux:

```
./bin/nolio_server.sh start
```

Windows:

Run services.msc (In %windir%\system32\), in the list of running services, find "Nolio Release Automation Server", and click "Stop".

Users are authenticated from LDAP when logging in.

Configure Purge Settings

Release Operation Center automatically purges unnecessary data to free up system space. A user with the Superuser role can configure the purge settings in the following ways.

- Set the interval and maximum duration time of a purge.

Note: When no exclusions are configured upon installation or upgrade of Release Automation, the first purge cycle occurs on top of the hour set.

- Create, specify the application, environment, content, and activate or deactivate a purge job.
- Set purge exclusion periods to prevent the purging cycles to run during the defined periods.

To create a purge job, or to set exclusions, configure the purge settings.

Note: If no purge job is configured and activated, no data is purged.

Follow these steps:

1. Click Administration, and select Purge Settings.
2. To set the Interval and Maximum Duration, click Edit.

Limits: Intervals are set from two to eight hours and Maximum Duration from one to five hours.

Note: Intervals are required to be higher than the Maximum Duration.

3. To create a purge job, click New, type the Name, and click Save.
The purge job is created.
4. Select the purge job, specify the parameters, and click Save.
The purge job is active.
5. (Optional) To set exclusions, specify the date and time, and click Add.
The data is purged based on the configured purge settings.

Update the Nexus Repository Password

Content

CA Release Automation uses the Nexus Repository password to connect to the repository during the installation process. If the repository password is changed and not updated in CA Release Automation, the installation fails.

To prevent a CA Release Automation installation failure, update the Nexus Repository password.

Follow these steps:

1. Access the `encrypt_password` utility that is located in the scripts directory and run it from the installation directory.

Windows: `C:\Program Files\CA\ReleaseAutomationSever\encrypt_password.bat`

Linux: `encrypt_password.sh`

Example:

`C:\Program Files\CA\ReleaseAutomationSever\encrypt_password.bat hello`

The encrypted password is: 53FD7CF681D223F5

The original password is: hello

2. Copy the encrypted password.
3. Access `<RA Install Directory>\conf`, and in `nolio-repo.properties`, update the password property.

Note: Due to the password being encrypted, paste in the copied password from step 2.

Example:

Nolio-repo-properties:

#If you intend to use the encrypted repository password, Please use the `encrypt_password.bat/sh` utility to encrypt the password.

type=nexus

scheme=http

hostname=

port=8080

repository=/nexus/content/repositories/noli

actionRepositoryPath=/nexus/content/repositories/nolio-actions

username=admin

password-53FD7CF681D223F5

passwordEncrypted=true

deleteAnonymousUser=false