CA Process Automation

Content Administrator Guide

Service Pack 04.2.02

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.

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

CA Technologies Product References

This document references the following CA Technologies products:

- CA Catalyst for CA Service Desk Manager (CA Catalyst Connector for CA SDM)
- CA Client Automation (formerly CA IT Client Manager)
- CA Configuration Automation (formerly CA Cohesion® Application Configuration Manager)
- CA Configuration Management Database (CA CMDB)
- CA eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA Infrastructure Insight (formerly Bundle: CA Spectrum IM & CA NetQoS Reporter Analyzer combined)
- CA NSM
- CA Process Automation (formerly CA IT Process Automation Manager)
- CA Service Catalog
- CA Service Desk Manager (CA SDM)
- CA Service Operations Insight (CA SOI) (formerly CA Spectrum® Service Assurance)
- CA SiteMinder®
- CA Workload Automation AE

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

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

- Example: How Touchpoints Enable Content Portability (see page 33)—This new topic describes how creating the same touchpoint name mapped to different agent hosts in different domains lets you seamlessly move a process across domains (or across environments) without change.
- Introduce New Users to CA Process Automation (see page 58)—This existing topic was updated to include references to the new *User Interface Reference*, which contains field descriptions.
- Example: One Individual in Two Referenced Active Directories (see page 63)—This new topic provides an example of CA Process Automation users being referenced by CA EEM from multiple Microsoft Active Directories, where the same user is defined to more than one referenced AD.
- Configure CA EEM Security Settings for the Domain (see page 133)—This existing topic was updated to include the Default Active Directory Domain value, a field that is valid only if CA EEM is configured to use multiple Microsoft Active Directory Domains.
- Configure Domain Properties (see page 140) —This existing topic was updated to include new fields that are related to host group configuration and to purging reporting data. Other topics similarly updated for host group configuration:
  - Configure Environment Properties (see page 153)
  - Configure Orchestrator Touchpoint Properties (see page 168)
  - Configure Orchestrator Host Properties (see page 174)
  - Ensuring Efficient Processing of Host Group References (see page 262)
- Install an Agent Interactively (see page 194)—This existing topic was updated to document a new checkbox for specifying whether the agent is to use simplified communication (with NGINX or F5) or deprecated communication (with Apache or F5). It is also noted that Windows supports jre7 as well as jre6. Other topics updated to address new communications:
  - Configure Agent Properties (see page 198)
  - About Agent Communication (see page 219)
  - Configure Agents to Use Simplified Communication (see page 220).
  - Configure Agents to Use Deprecated Communication (see page 220).
- Scenario: Set up Touchpoints for Design and Production (see page 225)—This new scenario combines existing information to show how configuration options used in a production environment differ from those used in a design environment.

- When to Avoid Using Host Group References as Targets (see page 263)—This new topic addresses an impact of specifying an IP address as an operator target for a process to be distributed to an environment or domain where the target would be a different host. Processes exported and imported as a content package cannot be modified.
- Configuring Operator Categories (see page 270)—All topics in this existing section were refactored to remove field descriptions that were added to the *User Interface Reference*.
- Plan the Folder Structure (see page 346)—This existing topic was rewritten to accommodate the requirements of exporting a folder as a content package. This new export method requires that all objects for a release version reside in the same folder.
- How to Prepare the Production Environment for a New Release (see page 359)—This existing process was rewritten for the new option, export folder as a content package, which replaced exporting a package automation object. Related topics include:
  - About Exporting and Importing a Content Package (see page 359)
  - Scenario: Export and Import Objects in a Content Package (see page 361) (This scenario includes an example as well as the procedures and related concepts.)
- Purge Objects and Folders (see page 376)—This existing topic was updated to include what happens when you attempt to purge checked out objects. This action is newly supported in CA Process Automation r4.2.

Contents

Chapter 8: Administer Agents 189

Chapter 12: Administer Operator Categories and Custom Operator Groups 265

Chapter 1: Getting Started

When you initially install CA Process Automation with CA EEM configured with an internal user store, it has a default administrator user with the following credentials:

User Name

pamadmin

Password

pamadmin

You can browse to a freshly installed product instance and log in with these credentials. A better approach is to create a user account in CA EEM during your first session, and then log in to CA Process Automation with the defined credentials.

After you log in, configure the settings with which to administer the security and configure the Domain.

This section contains the following topics:

Log In to CA EEM as the EiamAdmin User

The EiamAdmin user can log in to CA EEM and can manage identities (user accounts) and access policies.

Follow these steps:

1. Browse to the URL for the CA EEM instance that CA Process Automation uses:

   `https://`*`hostname`*`:5250/spin/eiam`

   hostname

   Defines the host name or IP address of the server where CA EEM is installed.

   Note: To determine the host name of the CA EEM that CA Process Automation uses, see the CA EEM Backend Server field on the CA Process Automation Configuration tab Security subtab.

2. From the Application drop-down list, select the value that you configured for the EEM Application name during installation.

   Note: This is the name under which you registered CA Process Automation with CA EEM.

3. Type **EiamAdmin** and the password that you defined for the EiamAdmin user.
4. Click Log In.

Create the First Administrator Account

You can create your own CA Process Automation user account in CA EEM and authorize full (Administrator) access to CA Process Automation.

Follow these steps:

1. Log in to CA EEM as the EiamAdmin user (see page 16).
2. Click the Manage Identities tab.
3. Click the icon next to Users in the Users palette.

   The New User page opens.

4. Type the User ID in the Name field that you want to enter as the User Name when you log in to CA Process Automation.
5. Click Add Application User Details.
6. Select PAMAdmins from Available User Groups and click > to move it to Selected User Groups.

   The group grants full access to all features in CA Process Automation.

7. Enter your own details in the Global User Details section of the user account profile.

8. (Optional) Complete the Global Group Membership field if you use CA Process Automation with another CA Technologies product that uses this CA EEM.
9. Create the password in the Authentication area that you want to enter when you log in to CA Process Automation.
10. (Optional) Complete the remaining fields on the New User page.
11. Click Save.

    A confirmation message states "Global User Details created successfully. Application User Details created successfully.
12. Click Close.
13. Click Log Out.

More information:

Use CA EEM to Change Your CA Process Automation Password (see page 46)
Grant CA EEM Access to Selected Administrators (see page 73)

Browse to CA Process Automation and Log In

The URL you use to access CA Process Automation depends on whether the Domain Orchestrator is configured with one node (nonclustered) or multiple nodes (clustered). You can browse directly to a nonclustered CA Process Automation. For a clustered CA Process Automation, browse to the associated load balancer. You can reach all Orchestrators in the domain by launching the URL to the Domain Orchestrator or to the load balancer for the Domain Orchestrator.

Follow these steps:

1. Browse the CA Process Automation.

   - For secure communication, use the following syntax:
     `https://server:port/itpam`

     Examples:
     `https://Orchestrator_host:8443/itpam`
     `https://loadBalancer_host:443/itpam`

   - For basic communication, use the following syntax:
     `http://server:port/itpam`

     Examples:
     `http://Orchestrator_host:8080/itpam`
     `http://loadBalancer_host:80/itpam`

   The CA Process Automation login page opens.

2. Enter the credentials from your user account.

   Note: If CA EEM is configured to reference users from multiple Microsoft Active Directories and CA Process Automation does not accept your unqualified user name, enter your principal name. One format for a principal name is *domain_name**user_name*.

3. Click Log In.

   CA Process Automation opens. The Home tab displays.

Set Language and Formats for Date and Time

By default, date and time data for the Domain Orchestrator appear in the browser time zone. During your first login session, you can set your preferred date and time formats and preferred language.

Note: The product stores all dates and times in Coordinated Universal Time (UTC).

Follow these steps:

1. Browse to CA Process Automation and log in (see page 18), if you are not already logged in.
2. In the toolbar, click your user name.
3. On the User Settings dialog, select your preferred date and time formats.
4. Verify and change the language setting, if necessary.
5. Click Save and Close.
6. Click OK.
7. Click Log Out.

   Your settings take effect when you log in again.

Update Out-of-the-Box Content

New predefined (out-of-the-box) content is periodically available. Only an administrator can import new predefined content. To ensure that the PAM_PreDefinedContent folder includes the latest predefined content, repeat the update procedure occasionally.

Follow these steps:

1. Delete previously imported content.
   a. Click the Library tab.
   b. Select the PAM_PreDefinedContent folder, click Delete, and then click Yes on the confirmation message.

      The PAM_PreDefinedContent folder is moved to the Recycle Bin. (Collapse the folder tree to see the Recycle Bin.)
   c. Select the PAM_PreDefinedContent folder in the Recycle Bin, then click Purge.
2. Click the Home tab.

3. Click Browse Out-of-the-Box Content.
4. Click Yes to confirm the import.

   The import process creates the PAM_PreDefinedContent folder with the latest content under the root directory of the Library tab.

Control the Timeout Interval

You can change the product timeout interval. By default, the product automatically logs off after 15 minutes of inactivity.

Follow these steps:

1. Log in as an administrator to the server where the Domain Orchestrator is installed.
2. Navigate to the following folder:

   install_dir/server/c2o/.config

   install_dir

   Defines the path where the Domain Orchestrator is installed.
3. Open the OasisConfig.properties file with an editor.
4. Use Find to locate the following property:

   managementconsole.timeout
5. Change the property value.
6. Save the file and exit.
7. Restart the Orchestrator service:
   a. Stop the Orchestrator (see page 186).
   b. Start the Orchestrator (see page 187).

More information:

Oasis Configuration Properties File (see page 400)

Recommended IE Browser Settings for NTLM Pass-Through Authentication

The recommended Windows Internet Explorer (IE) browser settings for NTLM pass-through authentication apply in the following cases, where CA EEM points to an external Active Directory:

- CA EEM uses NTLM pass-through authentication to authenticate CA Process Automation global users.
- Users use IE to browse to CA Process Automation.
- IE prompts for a user name and password.

Follow these steps:

1. From the IE Tools menu, select Internet Options, and then click the Security tab
2. Select the Local intranet icon, and then click Custom level.

   The Security Settings - Local Intranet Zone dialog opens.
3. Scroll to User Authentication and select Automatic logon only in Intranet zone.
4. Add the CA Process Automation URL to the Local Intranet zone.

About This Guide

The *Content Administrator Guide* focuses on tasks that users in the following roles perform:

- CA EEM administrators who set up CA EEM for CA Process Automation.
- CA Process Automation Content administrators with Domain Administrator, Environment Configuration Administrator, and Environment Content Administrator rights.

Content administrator tasks include:

- Setting up security.
- Configuring the product to support content development and production.

Before you begin using this guide, verify that the installation and setup tasks in the CA Process Automation *Installation Guide* are complete.

Notes:

- For work flows related to setting up a new content design environment or a new production environment, see the *Online Help*.
- For information about how content designers use web services methods, see the *Web Services API Reference*.
- For information about how content designers create processes and other automation objects, see the *Content Designer Guide.*
- For information about operators, see the *Content Designer Reference.*
- For information about how production users use the product in a production environment, see the *Production User Guide.*
- For information about how designers use the Operations tab during content design, see the *Production User Guide*.

Chapter 2: Overview for Administrators

This section contains the following topics:

Administration Task Overview

CA Process Automation provides the primary interface for content development. System administrators and content administrators use CA Process Automation for the following activities:

- Administer security.

  Security for CA Process Automation involves user authentication at login and role-based access. You define user accounts, custom groups, and policies that grant permissions through CA EEM.

- Administer the Domain.

  Domain is the term that is used to describe the enterprise view of the entire CA Process Automation system, including Orchestrators, agents, and process libraries. Domain administration includes adding environments, removing unused agents and touchpoints in bulk, and managing domain properties.

- Configure Orchestrators.

  An *Orchestrator* is the engine component of CA Process Automation that reads from the process library and executes processes. The first CA Process Automation Orchestrator that you install is the Domain Orchestrator. You can add more nodes to the Domain Orchestrator for added processing power and load balancing. If your users are geographically dispersed, consider adding a new standard Orchestrator in each location.

- Create and configure environments.

  An *environment* is an optional partition of the Domain that separates content development. Environments can be created for development, testing, and production or for different business units. Configuration includes adding touchpoints and creating touchpoint groups.

- Configure agents.

  An *agent* is CA Process Automation software that you install on a network host. Orchestrators that run processes can run certain steps of the process on agent hosts or remote hosts to which agents have SSH connections. Configuration includes associating touchpoints, proxy touchpoints, or host groups to agents.

- Map and configure touchpoints.

  A *touchpoint* is a logical entity used in operator definitions to represent the target agent or Orchestrator where some portion of the process executes. You can map a touchpoint to many agents at once and to different agents over time. Touchpoints provide flexibility in process implementation while reducing maintenance requirements for the processes themselves.

- Map and configure proxy touchpoints and host groups.

  Remote hosts, that is, hosts without an installed agent, can be targeted to execute operations as part of a running process. To enable connectivity, you establish SSH access from a host with an agent to the remote host. On the host with the agent, you configure either a proxy touchpoint or a host group. An operator can target a host with its proxy touchpoint name. A host group references remote hosts. An operator can target such a remote host with its FQDN or an IP address.

  Note: See Syntax for DNS Host Names (see page 397).

- Browse the library.

  A *library* is the repository containing operator objects and scripts that content designers assemble to create processes. Processes and other automation objects are stored in the library.

- Administer automation objects in libraries.

  Automation objects define processing, scheduling, monitoring, logging, and other configurable elements of a CA Process Automation package. Automation objects are stored in a library of a specific Orchestrator in a nonclustered architecture. Administration of automation objects includes the optional configuration of security settings on a library folder or object to control access for designated groups and users.

- Manage security for automation objects.

  You can create custom CA EEM policies for automation objects. For example, enable Touchpoint Security and create Touchpoint Security policies in CA EEM to limit who can run certain operators on specified high-valued targets. Enable Runtime Security and use Set Owner to grant process starting rights to only the owner of the process.

- Administer processes.

  An example of process administration is aborting failed processes from a process watch.

Tabs Overview

Availability of specific tabs in the product UI depends on access rights granted the logged-on user. When you log in to the product for the first time, the UI displays the tabs that this topic describes.

Note: You perform most configuration and administration tasks from the Configuration tab. For task flows related to each tab, see the *Online Help*.

Home

The Home tab helps you gain quick access to the objects on which you are working. You can use other links to gain quick access to information of general interest.

Library

Content administrators typically create and grant access rights to the folders.

Note: Content designers create objects and access them for edit from the Library tab folders. The Designer tab is the editor for process objects.

Folders

An administrator typically sets up a folder structure in the design environment. Folders contain subfolders and automation objects. The recommended practice is to create one folder for each process you automate, with a subfolder for each release version of that process. The process-level folders can be at the root level.

The folder that contains the release version of a process is exported as a content package and then imported to the production environment. The import process duplicates the folder structure in the production environment. The difference is that the production library contains only the release version of the process and related objects. Folders are not manually created in the production library.

Recycle Bin

The Recycle Bin at the bottom of the Orchestrator node contains folders and objects that were deleted. When you click Recycle Bin, you can select deleted folders and objects to purge (remove permanently) from the library or to restore to the library.

Search

Define folder, keyword, or date criteria by which to search for content objects in the Search field.

Contents

Content designers create instances of selected automation objects in a folder. They open the instances they create from the contents portion of the Library tab.

Designer

Content designers design a planned process on the Designer tab.

Operations

The Operations tab is used by users in the Production Users group. includes the following palettes:

Links

Displays information in the right pane for the following standard links:

Process Instances

Instances of processes that have been started. The bar chart in the Process Instances pane shows operators by state. The Process Instances pane also shows details for each operator.

Operators

Operators in started processes and tasks from schedules. The bar chart in the Operators pane shows operators by state. The Operators pane also shows details for each operator.

Tasks

Tasks that are assigned to users and groups. All users can view their specific task list, task lists for groups to which they belong, and tasks that are assigned to others. Administrators assign tasks to users or groups. A user takes an assigned task and replies to the User Interaction notification.

Active Schedules

Schedules that started active processes.

Global Schedules

Schedules that any user can use to start any process or selected operators. You can filter the display by date, by Orchestrator or agent touchpoint, and by whether the schedule is current or archived.

Start Requests

Requests that specified processes start on demand.

Content Packages

All users can monitor objects that are imported to the environment as content packages. When you click a content package in the left pane, the package properties display in the right pane.

Note: You can view the release version information for the following items that are included in content packages:

- Process instances
- Active schedules
- Global schedules
- Start requests

The product displays the content package name and content package release version for each object.

Process Watch

All users can monitor processes in all states, active schedules, operators, start requests, datasets, resources, and custom operators.

Start Requests

Users can view a bar graph of queued, running, completed, and failed start request instances. For a selected bar, users can view the instance name, scheduled time, state, start time and end time, and the user name.

Dataset

Users can display the structure of a selected dataset and its name/value pairs.

Resources

Users can select a resources object and then use the right pane to override the displayed Amount and Used values manually. Users can also change the State.

Schedules

Users can select a schedule and then use the right pane to set the following properties:

- The run date
- Whether to show the activity for all nodes or for a selected Orchestrator
- Whether to display archived schedules

Configuration

The administrator is responsible for configuring CA Process Automation access in the Configuration tab. By default, Environments, Orchestrators, and agents inherit settings that administrators configure at the Domain level. Operators inherit settings that administrators configure at the operator category level. The Configuration tab contains the following palettes:

Configuration Browser

Displays the following nodes:

Domain

Configure the Domain, the Default Environment, the Orchestrator touchpoint, the agent and proxy touchpoints, and the host groups.

Orchestrators

Configure the Domain Orchestrator and other installed Orchestrators.

Agents

Configure associations and settings for all installed agents.

Manage User Resources

The system administrator accesses the User Resources folder to add or update the scripts that are used to develop content. Administrators can upload JAR files to the Agent Resources folder or the Orchestrator Resources folder. The product shares the uploaded files when you restart agents or Orchestrators.

Installations

The system administrator installs other Orchestrators or cluster nodes for the Domain Orchestrator or other Orchestrators. Administrators also install agents.

Reports

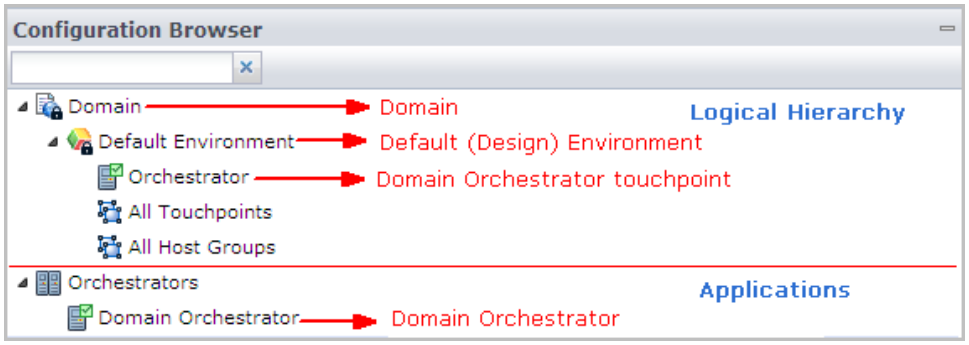
All users can access predefined reports or upload custom reports designed with the BIRT RCP Designer.

Relationships Among Components

As a CA Process Automation administrator, your responsibilities include:

- Configuration: Domain, Default Environment, or Orchestrator
- Installation and configuration to build out the Domain: Other Orchestrators and agents.
- Creating and configuring logical entities: Environments, touchpoints (including proxy touchpoints), and host groups.

Before you begin, it is helpful to understand the relationships among these physical and logical entities. The Configuration Browser palette on the Configuration tab displays a treeview of the logical hierarchy, the Orchestrators node, and the empty Agents node. The logical hierarchy initally consists of the Domain node with the Default Environment node. The expanded Default Environment node displays the Orchestrator, the empty All Touchpoints node, and the empty All Host Groups node.

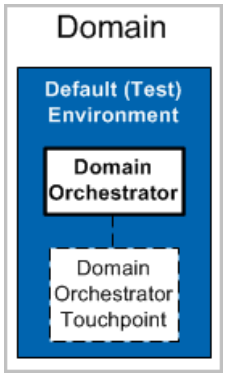


The Domain is the root node of the logical hierarchy. All Orchestrators that you install appear under the Orchestrators node. All agents that you install appear under the Agents node (not shown).

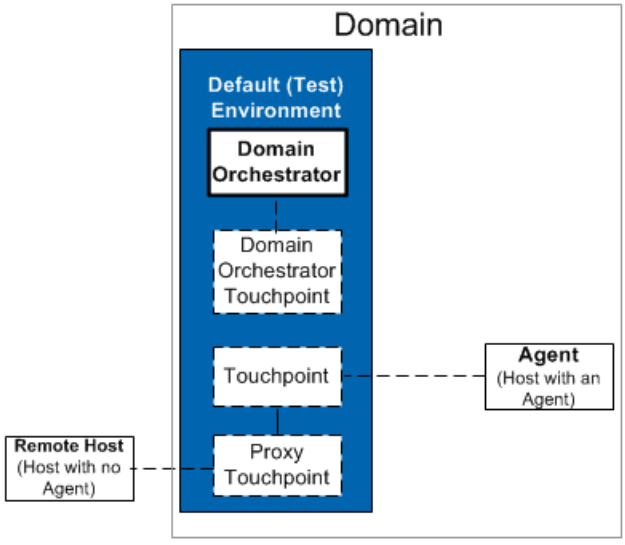
The term "touchpoint" refers to the association between an Orchestrator and an environment; a "touchpoint" also refers to the association between an agent and an environment. The illustration shows the Configuration Browser as it appears immediately after the first installation of CA Process Automation. Therefore, it does not include agents or agent touchpoints. Content designers use touchpoints as targets within the processes that they automate. (The use and advantage of touchpoints is elaborated on elsewhere.)

The Default Environment is typically dedicated to the design of automated processes. Content designers develop process that run on the Domain Orchestrator touchpoint. When the first process is ready to transition to production, you create a new environment; a "production environment" is added to the Domain.

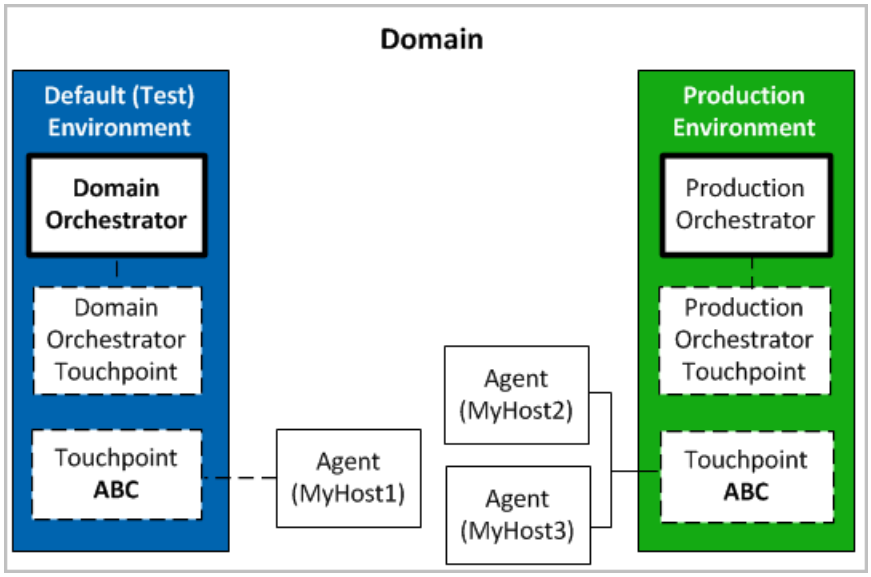
The following illustration shows the touchpoint as a block with a border of dashes. The illustration shows the association between the touchpoint and the Domain Orchestrator as a dashed line.



A process that runs on an Orchestrator can include operators that must target other hosts. Such targets typically require you to install a CA Process Automation agent and then associate touchpoints with the agent. Content designers access the agent through its touchpoint name. When it is not possible to install an agent on a target host, proxy touchpoints are used. A *Proxy touchpoint* extends touchpoint usage so that Orchestrators can run operators on a remote host (that is, on a host with no installed agent). When a touchpoint is configured with an SSH connection between the agent host and a remote host, it is a proxy touchpoint.



For each touchpoint with an association to the design environment, you add a touchpoint with the same name and associate it to the production environment. Thus, an operator that runs on Touchpoint ABC in the design environment also runs on a touchpoint named Touchpoint ABC in the production environment. In the test environment, you can associate the touchpoint with a single agent. To support high availability in the production environment, you can associate the corresponding touchpoint with two agents.



More information:

About the Domain Hierarchy, Orchestrators, and Agents (see page 145)

Example: How Touchpoints Enable Content Portability

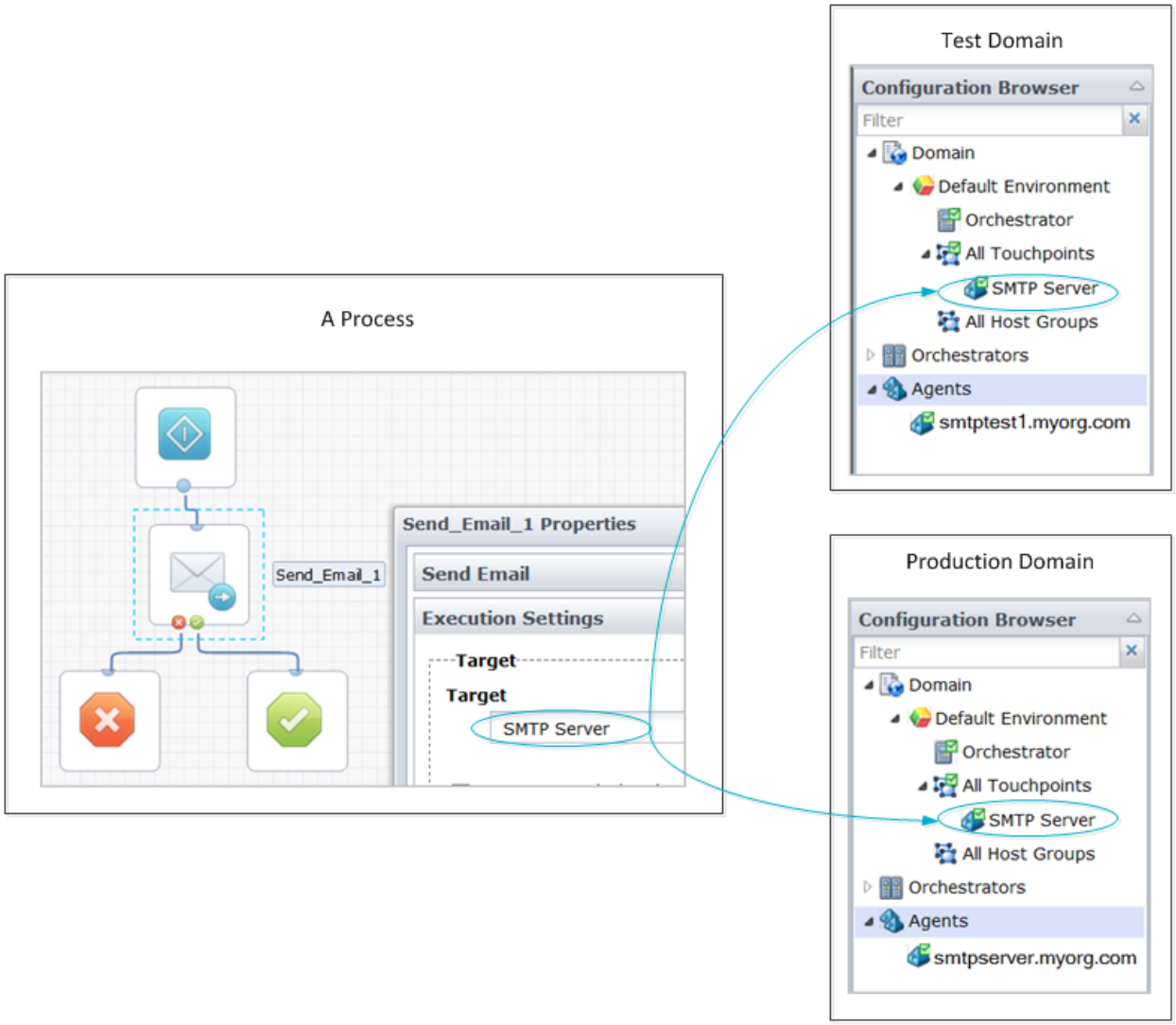
Consider an example deployment with a Test Domain and a Production Domain, each of which has its own SMTP server.

- smtptest1.myorg.com in the Test Domain
- smptserver.myorg.com in the Production Domain

The administrator installs an agent on each SMTP server and configures each agent with touchpoint named SMTP Server. A content designer creates a process with a Send_Email operator, where the execution target is set to the touchpoint name **SMTP Server**. This process can be deployed without changes to the Test Domain and to the Production Domain.

Note: The CA Process Automation guides and online help describe how to achieve content portability across environments within a single Domain.

A Process Can Be Deployed Without Changes to Multiple Deployment Domains



More information:

Touchpoint Implementation Strategy (see page 223)

Cardinality of Component Associations

As a CA Process Automation administrator, you build out the Domain by installing Orchestrators and agents. You partition the Domain by creating environments, where each environment has its own Library. You configure touchpoints for content designers to specify as targets for operators. Click the Configuration tab and open the Configuration Browser palette to display these entities.

The following rules govern cardinality between pairs of entities that can have an association:

Domain, Environments, Orchestrators, Agents

Orchestrators and agents are software components that are *physically* installed on hosts. The Domain and environments are *logical* entities.

- A CA Process Automation system has one, and only one, Domain.
- When a new CA Process Automation system is installed, the Domain has a Default Environment. The Default Environment contains the Domain Orchestrator.
- The Domain can have many environments. You can add environments to separate libraries. For example, you can dedicate the Default Environment to designing and testing new content. Then, you can create a separate production environment. Each environment must have at least one Orchestrator.

  Note: Typically, an administrator exports content from the Default Environment and then imports it to the production environment. You can also transfer content across Domains.
- An environment can have one or more Orchestrators. Each Orchestrator is installed on a separate host.

  Note: An Orchestrator can be *standard* or *clustered*. A clustered Orchestrator has multiple nodes. Each node is installed on a separate host. An Orchestrator appears as a single entity in the Configuration Browser, whether it is clustered or standard (nonclustered).
- The Domain can have as many agents as necessary. Agents are installed on hosts and are independent of environments.

Environments and Touchpoints

Environments and touchpoints are *logical* entities.

- Each touchpoint belongs to one environment.
- Each environment can have many touchpoints.
- For each touchpoint used in a release version of a process in the design environment, there must be an identically named touchpoint in the production environment. This enables the nonmodifiable process to run in the production environment.

Orchestrators and Touchpoints

After you install an Orchestrator, you create a touchpoint that associates the Orchestrator with a specific environment. Operators in a process target the touchpoint that is associated with the Orchestrator. The touchpoint association determines the environment in which the process runs.

- The Domain Orchestrator has a predefined touchpoint.
- Each Orchestrator is associated with only one touchpoint.
- A touchpoint that is associated with an Orchestrator cannot be associated with an agent. Touchpoint-to-Orchestrator and touchpoint-to-agent associations are mutually exclusive.
- An operator runs on the Orchestrator touchpoint that runs the process if the operator target is blank.

Agents and Touchpoints

To make an agent available as a target for an operator, associate the agent with a touchpoint, a proxy touchpoint, or a host group.

- You can associate an agent with one or more touchpoints.
  - When you associate an agent with one touchpoint, operators can run directly on a host with an installed agent by targeting the touchpoint.
  - When you associate an agent with multiple touchpoints on the same host, the touchpoints typically target different components on the host. For example, you could define one touchpoint to access a database and another to access a third-party product.
  - Each operator in a process runs on a touchpoint, which can be associated with an operator, an agent, or multiple agents. If operator-1 runs on Touchpoint-ABC in the design environment, it runs on a different touchpoint named Touchpoint-ABC in the production environment. Each member of this touchpoint pair is associated with a different environment. Each member of the touchpoint pair can be associated with the same agent or with different agents. This type of association provides the mechanism for defining processes that you can migrate across environments without changing the target host information.
- You can associate a touchpoint with one or more agents. You can assign the same priority to multiple agents, or you can assign a different priority to each agent.
  - When the agents have different priorities, operators run on the agent with the highest priority. If the highest priority agent is unavailable, operators run on an available agent with a lower priority. This design ensures that a target host is available.
  - When multiple agents with the same priority are associated with a touchpoint, operators run on a randomly selected agent. This design promotes load balancing.
  - A touchpoint that is associated with an Orchestrator cannot be associated with an agent.

Agents, Proxy Touchpoints, and Remote Hosts

A remote host refers to a host that is an operator target when installing an agent is not practical.

- You can associate an agent with one or more proxy touchpoints.
- A *proxy touchpoint* is a touchpoint that is configured with an SSH connection to one remote host. The remote host typically has no agent.
- When you associate an agent with a proxy touchpoint, operators in a process can target the proxy touchpoint to run on the remote host.

Note: An Orchestrator can distribute workload to a remote host without going through an agent by using the Run SSH Script operator in a process. The content designer defines configuration parameters (in the operator) that specify the host address and credentials to use to SSH into the remote host and run a script. See the *Content Designer Reference* for details about the Run SSH Script Operator.

Agents, Host Groups, and Remote Hosts

A *host group* is a group of remote hosts. You typically configure host groups with a common host name pattern or with an IPv4 subnet expressed in the CIDR notation.

- You can associate an agent with one or more host groups.
- You can associate a host group with one or more agents.
- When an agent is associated with a host group, you configure the SSH connections manually. Configure an SSH connection from the agent host to each remote host that the host group references.
- When an agent is associated with a host group, operators in a process can run on a referenced remote host. Operators target the IP address or FQDN of the remote host.

Note: For non-interactive SSH communication with a remote host, use a proxy touchpoint or a host group. For interactive SSH communication with a remote host, use the Run SSH Script operator. See the *Content Designer Reference* for details about the Run SSH Script Operator.

Security

As an administrator, your concerns for CA Process Automation security can include:

- Securing the CA Process Automation application (see page 39).
- Suspending or disabling a user account (see page 40).
- Securing data transfer with strong ciphers (see page 41).
- Securing data transfer between CA Process Automation and CA EEM (see page 41).

More information:

Administer Basic CA EEM Security (see page 43)

Securing the CA Process Automation Application

One aspect of securing the application is preventing unauthorized users from logging in. Another is limiting the use of functionality that is based on the role of the logged-on user. Securing the application includes the following mechanisms:

Authentication

The product uses CA EEM to authenticate users at login. CA EEM compares the credentials users enter at login with user name and password combinations in User Accounts. The user can log in only if CA EEM finds a match.

Administrators can help protect the product from an unauthorized login by requiring users to change passwords periodically and by suspending or disabling default accounts. For more information, see:

- Change Your Own Password in CA EEM (see page 46)
- Suspend or Disable a User Account (see page 40)

Authorization and role-based security

The product uses CA EEM to authorize logged-in users. CA EEM lets users perform tasks only on those parts of the user interface for which they are authorized. Authorization for the PAMAdmins, Designers, and Production Users groups is set by default. Users added to these groups inherit the authorization.

Administrators can define role-based security so that users who belong to different groups access only parts of the product necessary for the role they perform. Administrators can also use CA EEM policies to assign trusted users to activities for which misuse can cause the greatest damage. This aspect of access control is a separate consideration from the group role to which individual users are assigned.

More information:

User Authentication and Authorization in FIPS Mode (see page 379)

Suspending or Disabing a User Account

You can suspend or disable a user account in the following cases:

- The user no longer needs access to CA Process Automation but the user record must be retained for auditing purposes.
- You have reasons to prevent the specified user from accessing CA Process Automation temporarily or permanently.
- The predefined credentials made available to you at installation now represent an internal security threat. Because the credentials for the pamadmin and pamuser are documented, it is a good practice to make them unavailable after they have served their purpose.

Follow these steps:

1. Log on to CA EEM.
2. Click Manage Identities.
3. Under Search Users, select Application User Details and click Go.
4. Click the name of the target user.
5. Scroll to the Authentication area and take one of the following actions:
   - Click Suspended
   - Click Disable Date, select the date at which the disable is to take effect, and click OK.
6. Click Save.

Note: You can also reverse the suspension or enable a disabled account. You can use the disable/enable feature to defer the availability of a new account to the time you specify.

Securing Data Transfer with Strong Ciphers

When CA Process Automation components are installed on Java virtual machines, JVMs such as Java 6 allow Medium and Weak ciphers in communications with agents. To secure these communications, add strong cipher values to the Oasis.Config properties file in the following directory:

install_dir\server/c2o\config\

The following properties relate to ciphers used in SSL communication:

jboss.ssl.ciphers

Specifies a comma-separated list of ciphers to use for SSL communication between the Domain Orchestrator and clients such as browsers and web services. The cipher list can vary by the operating system and JVM that are on the host. The following example shows a typical specification of strong JBoss ciphers:

```
jboss.ssl.ciphers=SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA
_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_DS
S_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE
_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA
```

jetty.ssl.ciphers

Specifies a comma-separated list of ciphers to use for SSL communication with agents. The product adds this property to agents during silent installation. The following example shows a typical specification of Jetty ciphers:

```
jetty.ssl.ciphers=SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA
_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA
```

Securing Data Transfer Between CA Process Automation and CA EEM

CA Process Automation uses encryption to secure stored and transmitted data. If the CA EEM FIPS mode is set to on, CA Process Automation secures stored and transmitted data with FIPS-140-2 validated cryptographic modules.

More information:

FIPS 140-2 Support (see page 377)
When CA Process Automation Uses Encryption (see page 377)

Types of Authentication

CA EEM authenticates and authorizes all users who browse to CA Process Automation. CA EEM can authenticate users in either of the following ways:

- Use the credentials that users enter in a form-based login dialog.
- Use the NTLM protocol, if NTLM pass-through authentication is configured. This feature is often selected when CA EEM is configured to use Microsoft Active Directory as an external directory. The user credentials are automatically loaded to CA EEM for this configuration.

When a user browses to CA Process Automation, the Orchestrator determines the type of authentication to use:

Form-based

The CA Process Automation login page opens. The user enters credentials and login processing begins.

NTLM

The NTLM protocol authenticates the user to the CA EEM server and the Home page opens.

Chapter 3: Administer Basic CA EEM Security

When you install CA Process Automation or upgrade, CA Process Automation is registered with CA EEM. CA EEM provides access policy management, authentication, and authorization services for many CA Technologies products. Security administration varies depending on whether you are setting up security for the first time or you have upgraded CA Process Automation. If you are upgrading, security requirements depend on whether you previously used CA EEM or LDAP for user authentication. Whether you are new or upgrading, if you plan to load user accounts from an external directory server into CA EEM, a separate set of procedures are required.

This chapter addresses using CA EEM to assign each user one of four default roles, whether you are creating user accounts, have existing user accounts, or are loading user accounts from an external directory.

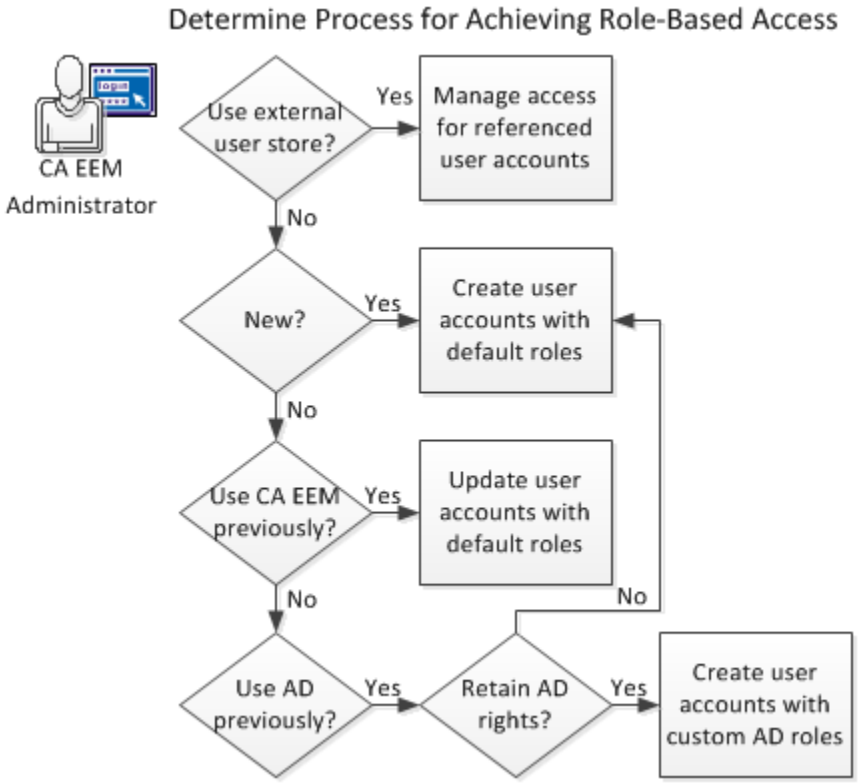
See Administer Advanced CA EEM Security (see page 71) if you are creating custom roles and custom policies.

This section contains the following topics:

Determine Process for Achieving Role-Based Access

Security administration with CA EEM varies for the following scenarios:

- New or upgrade installation with a referenced directory server: You have configured CA EEM such that authentication is based on credentials that are loaded into CA EEM as global user accounts from an external user store. You are ready to assign an application group to each global user that reflects the role performed in CA Process Automation.
- New installation with a local CA EEM: You are ready to define CA Process Automation users in CA EEM.
- Upgrade installation, where you previously used CA EEM: You can update user accounts for users who design processes or who use processes transitioned to the production environment. Open each account and select one of the new application groups: Designers or Production Users.
- Upgrade installation, where you previously used Microsoft Active Directory or similar LDAP server. You are ready to create user accounts of your existing users in CA EEM. You can either assign a default group to users or you can create custom groups that permit you to retain the roles you used with AD.



Based on your result of the decision chart, see the appropriate section:

- Manage access for referenced user accounts (see page 60).
- Create user accounts with default roles (see page 54).
- Update user accounts with default roles (see page 59).
- Create user accounts with custom AD roles.

  See How to Transition Roles Used in Active Directory to CA EEM (see page 111).

Browse to CA EEM and Log In

To manage users, user groups, and policies that grant permissions in CA Process Automation, log in to the configured application in CA EEM.

Follow these steps:

1. Browse to the CA EEM that CA Process Automation uses. Use the following URL:

   `https://hostname:5250/spin/eiam`

   The CA Embedded Entitlements Manager dialog opens.
2. From the Application drop-down list, select the name configured at installation in the EEM Application name field.

   Note: The default name is Process Automation.
3. Type one of the following sets of credentials:
   - Type **EiamAdmin** and the CA EEM administrator password that was established during the installation process.
   - Type your user name and password if the CA EEM administrator has granted you CA EEM access. The CA EEM administrator can grant CA EEM access to selected administrators (see page 73).
4. Click Log In.

Use CA EEM to Change Your CA Process Automation Password

The administrator typically assigns a temporary password when setting up user accounts for the internal user store. All CA Process Automation users with user accounts created in CA EEM can change this password before you log in to CA Process Automation. Then, you can change your CA Process Automation password at the interval that password policies define.

Note: This ability does not apply when CA EEM references user accounts from an external user store such as Microsoft Active Directory. In this case, maintain your password within the referenced directory.

Use CA EEM to change your CA Process Automation password.

Follow these steps:

1. Open a browser and enter the URL for the CA EEM server that CA Process Automation uses. For example:
   https://*hostname_or_IPaddress***:5250/spin/eiam/**

   To identify the host name or IP address of the CA EEM that CA Process Automation uses, see the CA EEM Backend Server field on the CA Process Automation Configuration tab Security subtab.
2. Log in to CA Embedded Entitlements Manager (CA EEM) from the log In dialog:
   a. For Application, select <Global>.
   b. Delete EiamAdmin if this default name appears in the User Name field.
   c. Enter your CA Process Automation user name and password.
   d. Click Log In.
3. Under Self Administration, click Change Password.
4. Reset your password:
   a. Enter your CA Process Automation user name and old password.
   b. Enter your new password in both the New password and Confirm password fields.
   c. Click OK.

   CA Process Automation accepts your updated credentials when you log in.

Role-Based Access to Configuration

Role-based access is implemented in CA EEM, where PAMAdmins (for administrators), Designers, and Production Users are three application-specific groups. Each group is granted permissions to access only functionality relevant to the respective role. The fourth default group, PAMUsers, can be used as the basis for custom groups, where applicable.

PAMAdmins (Administrators)

Administrators have full access to the Configuration tab. Administrators configure settings at all levels of the Domain hierarchy. The Installation and Manage User Resources palettes are present on the Configuration tab only for users who are administrators.

Designers

CA EEM grants users in the Designers group the ability to view the Configuration Browser and configuration settings on Configuration tab. Content designers can examine whether specific agents have failed or whether a specific category of operators is disabled on a specified touchpoint.

Production Users

CA EEM grants users in the Production Users group the ability to view the Configuration tab.

Default Groups and Default User Credentials

CA EEM provides four default groups for CA Process Automation. Each group has a default user. You can experience the CA Process Automation presented to members of each by logging in to CA Process Automation as its default user. High-level descriptions and credentials for default users follow:

PAMAdmins

The PAMAdmins group is granted full permissions in CA Process Automation. You can assign this group to all administrators.

Default user credentials

User Name: pamadmin

Password: pamadmin

Designers

The Designers group is granted permissions that are typically sufficient for users who design automated processes.

Default user credentials

User Name: pamdesigner

Password: pamdesigner

Production Users

The Production Users group is granted sufficient permissions for users who interact with automated processes in the production environment.

Default user credentials

User Name: pamproduser

Password: pamproduser

PAMUsers

The default PAMUsers group is granted minimal permissions. The CA EEM administrator can use this group as the basis for custom groups. This group grants the ability to log in to CA Process Automation, examine reports, and view the state of operations.

Default user credentials

User Name: pamuser

Password: pamuser

Detailed permission descriptions follow:

- PAMAdmins group permissions (see page 49).
- Designers group permissions (see page 50).
- Production Users group permissions (see page 51).
- PAMUsers group permissions (see page 52).

Editing the default roles or creating custom roles is an advanced feature.

PAMAdmins Group Permissions

The CA EEM policies that CA Process Automation supplies grant all permissions to the PAMAdmins application group. Assign this group to administrators who need full access to CA Process Automation. The PAMAdmins group provides the following tab-level access:

Home

Administrators in the PAMAdmins group have full access to the Home tab. Full access consists of the permission to log in to CA Process Automation and use the Home tab (PAM40 User Login Policy).

Library

Administrators in the PAMAdmins group have full access to the Library tab, which consists of the following permissions:

- View the Library tab (PAM40 LibraryBrowser Policy).
- Control the library folders and folder contents (Environment_Library_Admin rights in the PAM40 Environment Policy).
- Configure the variables common to a custom operator group and publish the group configuration to the Configuration Browser palette Modules tab (PAM40 Group Config Policy).

Designer

Administrators in the PAMAdmins group have full access to the Designer tab, which consists of the following permissions:

- View the Designer tab (Designer policy).
- Full rights in the Designer tab (Environment_Library_Admin rights in the PAM40 Environment Policy).

Operations

Administrators in the PAMAdmins group have full access to the Operations tab, which consists of the following permissions:

- View all palettes on the Operations tab (PAM40 Operations Policy).
- Full permissions (Environment_Library_Admin rights in the PAM40 Environment Policy).

Configuration

Administrators in the PAMAdmins group have full access to the Configuration tab, which consists of the following permissions:

- View all palettes in the Configuration Browser palette (PAM40 Configuration Policy).
- Configure at the Domain level or complete a task that requires locking the Domain (PAM40 Domain Policy).
- Configure at the Environment level or complete a task that requires locking an environment (Environment_Config_Admin rights in the PAM40 Environment Policy).
- Install the agents or Orchestrators (PAM40 Configuration Policy).
- Manage User Resources (PAM40 Configuration Policy).

Reports

Administrators in the PAMAdmins group have full access to the Reports tab. Full access consists of the permissions to view the Reports tab, generate reports, and add new reports (PAM40 Reports Policy).

Designers Group Permissions

By default, the Designers application group contains permissions that users in the design environment require. The Designers group provides the following tab-level access:

Home

Users in the Designers group can log in to CA Process Automation and can use the Home tab (PAM40 User Login Policy).

Library

Users in the Designers group have the following access to the Library tab:

- View the Library tab (PAM40 LibraryBrowser Policy).
- Read the Library tab, including permission to view, export, and search automation objects (PAM40 Environment Policy).
- Control (view, navigate, edit, delete, create) folders in the Library tab and control all automation objects in the respective editors (PAM40 Object Policy).

Designer

Users in the Designers group have the following access to the Designer tab:

- View the Designer tab (PAM40 Designer Policy).
- Design automated processes and control (view, navigate, edit, delete, and create) all automation objects in the respective editors. The Designer tab is the process automation object editor (PAM40 Object Policy).

Operations

Users in the Designers group have the following access to the Operations tab:

- View all palettes on the Operations tab (PAM40 Operations Policy).
- Control the schedules that the Operations tab displays (PAM40 Schedule Policy).
- Inspect and modify the dataset automation object (PAM40 Dataset Policy).
- Control, start, and monitor the process automation object (PAM40 Process Policy).
- Control the resources automation object (PAM40 Resources Policy).
- Start and dequeue the start request form policy (PAM40 Start Request Form Policy).
- View the release version of an imported content package and view the objects that the package contains.

Configuration

Users in the Designers group can view the tabs for any node they select in the Configuration Browser palette (PAM40 Configuration Policy).

Reports

Users in the Designers group can view the Reports tab, generate reports, and add reports. The Designers group is based on the PAMUsers group, which also has these permissions.

Production Users Group Permissions

By default, the Production Users application group contains permissions that users in a production environment require. The Production Users group provides the following tab-level access:

Home

Users that are assigned to the Production Users group have access to log in to CA Process Automation and use the Home tab (PAM40 User Login Policy).

Library

Users in the Production Users group have the following access to the Library tab:

- View the Library tab (PAM40 LibraryBrowser Policy).
- Read the Library tab (PAM40 Environment Policy, which is a prerequisite to PAM40 Object Policy).
- Navigate the folder structure in the Library tab and view the automation objects that each folder lists (PAM40 Object Policy).

Operations

Users in the Production Users group have the following access to the Operations tab:

- View all palettes on the Operations tab (PAM40 Operations Policy).
- Control the schedules that the Operations tab displays (PAM40 Schedule Policy).
- Inspect any dataset that the Operations tab Dataset palette displays (PAM40 Dataset Policy).
- Monitor or start any process that the Operations tab displays (PAM40 Process Policy).
- Start and dequeue the start request form that the Operations tab displays (PAM40 Start Request Form policy).
- View the release version of an imported content package and view the objects that the package contains.

Configuration

Users in the Production Users group can view the tabs for any selected node in the Configuration Browser palette (PAM40 Configuration Policy).

Reports

Users in the Production Users group can view the Reports tab, generate reports, and add reports (PAM40 Reports Policy).

PAMUsers Group Permissions

By default, the PAMUsers application group contains basic permissions. You can use this group to supplement the custom groups that you create for fine-grained role-based access. The PAMUsers group provides the following tab-level access:

Home

Users in the PAMUsers group can log in to CA Process Automation and can use the Home tab (PAM40 User Login Policy).

Library

Users in the PAMUsers group have the following access to the Library tab:

- View the Library tab (PAM40 LibraryBrowser Policy).
- Read the Library tab (PAM40 Environment Policy).

Operations

Users in the PAMUsers group can view the Operations tab (PAM40 Operations Policy).

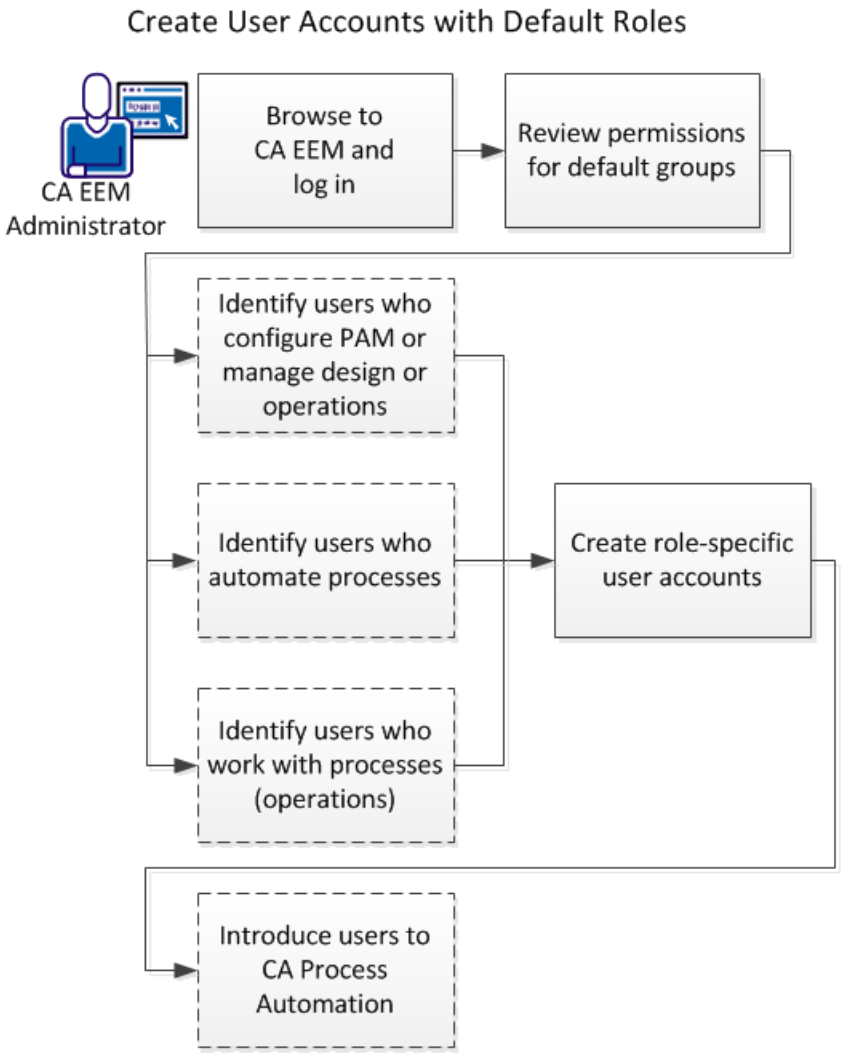
Reports

Users in the PAMUsers group can view the Reports tab, generate reports, and add reports (PAM40 Reports Policy).

Create User Accounts with Default Roles

When the installer configures CA EEM to use the internal user store, the CA EEM administrator creates a user account for each CA Process Automation user. These user accounts are used to authenticate users when they log in to CA Process Automation. To authorize these users to access features required by their roles, the CA EEM administrator assigns the appropriate default group to each user account.

The following illustration shows how to create user accounts with default roles. The dashed lines indicate the tasks that you perform outside of CA Process Automation.



Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Review permissions for default groups.

- PAMAdmins group permissions (see page 49)
- Designers group permissions (see page 50)
- Production Users group permissions (see page 51)

3. Create role-specific user accounts (see page 55).
4. Introduce new users to CA Process Automation (see page 58).

Create Role-Specific User Accounts

Create role-specific user accounts:

- Grant PAMAdmins group permissions (see page 49) to CA Process Automation administrators.
- Grant Designers group permissions (see page 50) to content designers.
- Grant Production Users group permissions (see page 51) to production users.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click Manage Identities.
3. In the Users palette, click the New User button.

   The New User page opens.
4. In the User Name field, type the user ID to assign to the user account.

   The user types this value in the User Name field at login.
5. Click Add Application User Details.

   The pane refreshes to show the Application Group Membership section.
6. In the Application User Group Membership section, select the appropriate group and click the Select Item button to move the selected group to the Selected User Groups list. For example:
   - If the user is a CA Process Automation administrator, select PAMAdmins.
   - If the user is a content designer, select Designers.
   - If the user is a production user, select Production Users.
7. Enter the global user details.
   a. Type the name in the First Name and Last Name fields.

      The title bar displays these values when the user logs in to CA Process Automation.

   b. Complete the other fields in the General area as appropriate.

8. (Optional) If you use CA Process Automation with another CA Technologies product that uses this CA EEM, complete the Global Group Membership section.
9. Provide temporary authentication information for this user account:
   a. Select Change Password at Next Login.
   b. Type a temporary password in the New Password field.
   c. Type the same temporary password in the Confirm Password field.
10. (Optional) Complete the remaining fields on the New User page.
11. Click Save, and then click Close.
12. (Optional) Click Log Out.

More information:

Use CA EEM to Change Your CA Process Automation Password (see page 46)
Grant CA EEM Access to Selected Administrators (see page 73)

Create User Accounts with Basic Access

PAMUsers is a default group that grants the use of the Home tab and the Reports tab, and grants read-only access to the Library tab and the Operations tab. A user with only PAMUsers access can become familiar with the product, but cannot create or configure objects.

Use this group as the basis for custom groups.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Identities tab.
3. Click New User.
4. Type the user ID to assign to the user account in the Name field.
5. Click Add Application User Details and then click > to move PAMUsers to the Selected User Groups.
6. Enter the global user details.
7. Type and verify a password.

   Users can log in to CA EEM with their CA Process Automation credentials and can change their password.
8. (Optional) Complete the remaining fields on the New User page.

9. Click Save and click Close.
10. Click Log Out.

Introduce New Users to CA Process Automation

To help the new users become productive, give them the following information:

Access information

- The CA Process Automation URL. This could be the Domain Orchestrator URL or the URL to the load balancer for the Domain Orchestrator. Optionally, you can browse to the URL of any specified Orchestrator.
- Login information. Users log in with the user name and password that are configured in their CA EEM user account.
- The CA EEM URL. Users log in with the user name and password that you assigned, and then they self-assign a new password.

  Note: If CA EEM references one or more external Microsoft Active Directories, users do not need to log in to CA EEM. Passwords are maintained by the AD.

Access to resources for quickly getting up to speed

- Recommend that users complete the CA Process Automation tutorials that they can access from the Home tab.
- Show the users that they can access the bookshelf by selecting the Book Shelf option from the HELP link in the toolbar. From the bookshelf, users can access the guides for their role.

  The guides for each application group (role) are:

  PAMAdmins

  Release Notes

  Installation Guide

  Content Administrator Guide

  User Interface Reference

  Designers

  Content Designer Guide

  Content Designer Reference

  Web Services API Reference

  Production User Guide

  User Interface Reference

  Production Users

  Production User Guide

  User Interface Reference

Update User Accounts with Default Roles

Upgrade users who previously assigned PAMAdmins (or ITPAMAdmins) as the group for designers or production users can improve security. If you are and upgrade user, consider assigning the following default groups to users who perform the following roles:

- Designers
- Production Users

Note: If you previously assigned PAMUsers (or ITPAMUsers) to user accounts of individuals who worked with Task Lists, Default Process Watch, or User Requests, reassign the Production Users group to these accounts.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Identities tab.
3. Expand the Search Users palette, select Application Users, enter the following criteria, and then click Go.
   - Attribute: Group Membership
   - Operator: LIKE
   - Value: PAMAdmins

   The list of user accounts currently assigned to the PAMAdmins group displays.
4. Click the name of a user who is a designer or a production user.

   The selected user account opens.
5. Select PAMAdmins from the Selected User Groups and click the left arrow

   The selected group is removed from the Selected User Groups.
6. Select the applicable group from Available User Groups and click > to move it to Selected User Groups.
   - For content designers, select Designers.
   - For production users, select Production Users.
7. Click Save, then click Close.
8. Click Log Out.

Manage Access for Referenced User Accounts

If you reference an external user store during CA EEM installation, global groups and user accounts are automatically loaded into CA EEM. CA Process Automation allows the loading of up to 10000 accounts with a configurable parameter that extends the CA EEM setting of 2000. For information about customizing this setting, see Set Maximum Number of CA EEM Users or Groups (see page 61).

The user accounts from a referenced external user store are loaded as read-only records. If a new user needs an account, create it in the external user store. The new record is automatically loaded. You can provide access to CA Process Automation at either the global group level or the global user level.

You configure CA EEM to grant access to CA Process Automation and its components, but the referenced user store manages authentication. To log in to CA Process Automation, the global users with login access use the user name and password (or the principal name and password) in the referenced user store.

Note: You cannot use CA EEM to update the user records stored in an external user store.

To manage access for users with accounts stored in an external user store, consider the following approaches.

- Add an application group to each global user account.

  Search for each global user by name. Assign one of the default application groups (PAMAdmins, Designer, Production Users, or PAMUsers) or a custom group to the global user account. You can also create global groups and add selected global users to them.

  Important! Always enter criteria when searching to avoid displaying all entries in an external user store.

- Add a global group to CA Process Automation access policies, then select the actions to grant.

  Specifically, add the global group to the predefined policies that provide the access you want all users in the group to have. For example, add the global group to the PAM40 User Login Policy to let all global users in that group log in to CA Process Automation. To give access to the Designer tab, add the group to the PAM40 Designer Policy.

- Create a dynamic group that consists of selected global users or global groups. Custom application groups can be added to a dynamic group.
- Follow the documented procedure Integrating Active Directory with CA EEM.

  This procedure gives all users in your AD full access to CA Process Automation without any configuration in CA EEM. While easy to implement, it lacks the security of role-based access.

Important! For third-party LDAP servers, configure the following parameter under the ou=system context level:

```
ou=Global Groups
```

Set Maximum Number of CA EEM Users and Groups

Before you integrate a large referenced user store, determine if the store contains more than 10,000 users and groups. The eem.max.search.size default value (10000) is the threshold for how many users and groups CA Embedded Entitlements Manager can accept during transfer. The CA Process Automation default (10000) extends the CA EEM default (2000).

Increase the eem.max.search.size value if the following message appears when you search for available users without defining search criteria:

```
Maximum search limit exceeded.
```

To override the default threshold in the OasisConfig.properties file, set the following parameter to a new value:

```
eem.max.search.size = 10000
```

If you are integrating a large referenced directory, set the value to more than 20000.

Follow these steps:

1. Log on as an administrator to the server where the Domain Orchestrator is installed.
2. Navigate to the following folder:

   install_dir/server/c2o/.config

   install_dir

   Refers to the path where the Domain Orchestrator is installed.
3. Open OasisConfig.properties with a text editor.
4. Use Find to locate the eem.max.search.size parameter.
5. Change the value from 10000 to an appropriate value.

6. Save the file and close the text editor.
7. Restart the Orchestrator:
   a. Stop the Orchestrator (see page 186).
   b. Start the Orchestrator (see page 187).

Search for Identities that Match Specific Criteria

When you reference a large external user store, specify search criteria. The search criteria limit the returned global user account records to the one you require or to a relevant subset. For example, specify **First Name LIKE John** to retrieve the names of all users with the first name John.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click Manage Identities.
3. Select Global Users in the Search Users pane.
4. Review the Attribute drop-down list and determine whether any listed attribute has a value for the user or users for whom you plan to search.
   - If yes, select one or more applicable attributes. For example, select First Name and Last Name.
   - If no, select the ellipsis (...) and enter the name of the attribute on which to search.
5. Select the operator for the expression and enter a value for the attribute that applies to the target user accounts. The value can be a partial value. For example, enter s* to search for all records where the value of the selected attribute begins with the letter "s".

   Important! Always enter criteria when searching to minimize the time it takes to retrieve entries from an external user store.
6. Click Go.

   The names of the global users who match your selection criteria appear in the Users pane. The names appear in "Last Name, First Name" format.

Example: One Individual in Two Referenced Active Directories

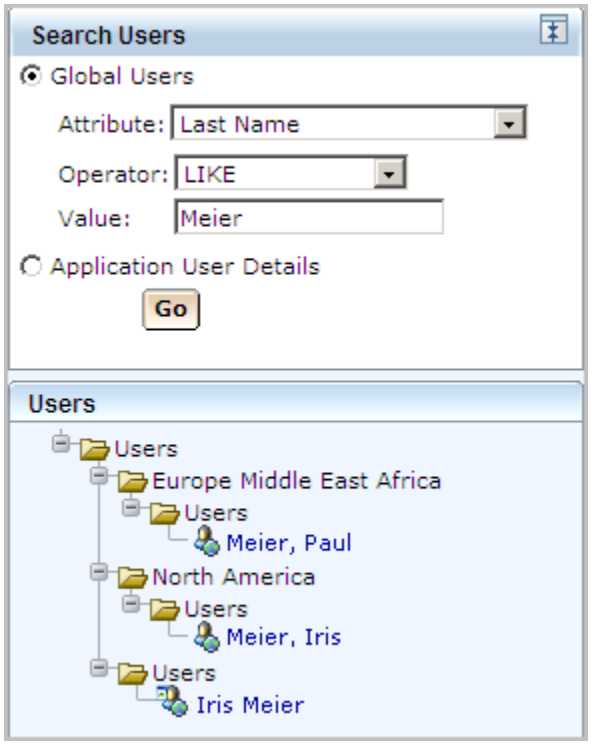
Assumptions:

- Prior to upgrading CA Process Automation, CA EEM referenced an external directory, a Microsoft Active Directory. The CA EEM release was r8.4
- Later, but still prior to upgrading CA Process Automation, CA EEM was upgraded from r8.4 to r12.51. The CA Process Automation users, that is, referenced AD users who were assigned to an application group, retained the group assignment after the CA EEM upgrade. The global users assigned to the Designers group who owned automation objects, retained the object ownership.
- During the CA Process Automation upgrade to r4.2, the installer selected to reference multiple ADs, a feature supported as of CA EEM r12.5.
- The CA EEM administrator now needs to assign an application user group to selected global users from the additional ADs. The administrator also re-assigns application groups to CA Process Automation users from the original AD.
- The CA EEM administrator enters search criteria for a user in one of the newly referenced AD domains. This user happens to be in two domains, the existing domain and a new domain. Although typically, each user is in one domain, it is possible for users to be in more than one AD domain. When this happens, the two user accounts are treated as different users, even though they may refer to the same individual.

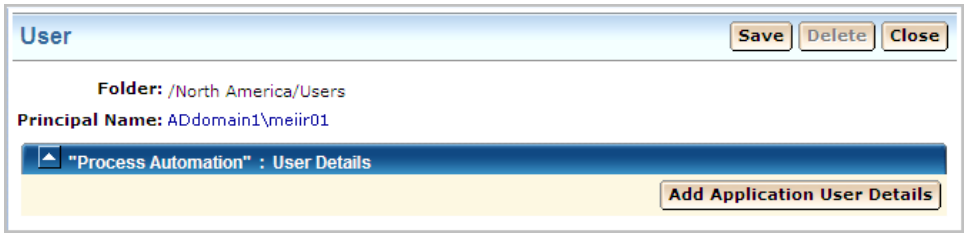
The following procedure shows how this example would appear in the CA EEM Search results and corresponding user records.

Follow these steps:

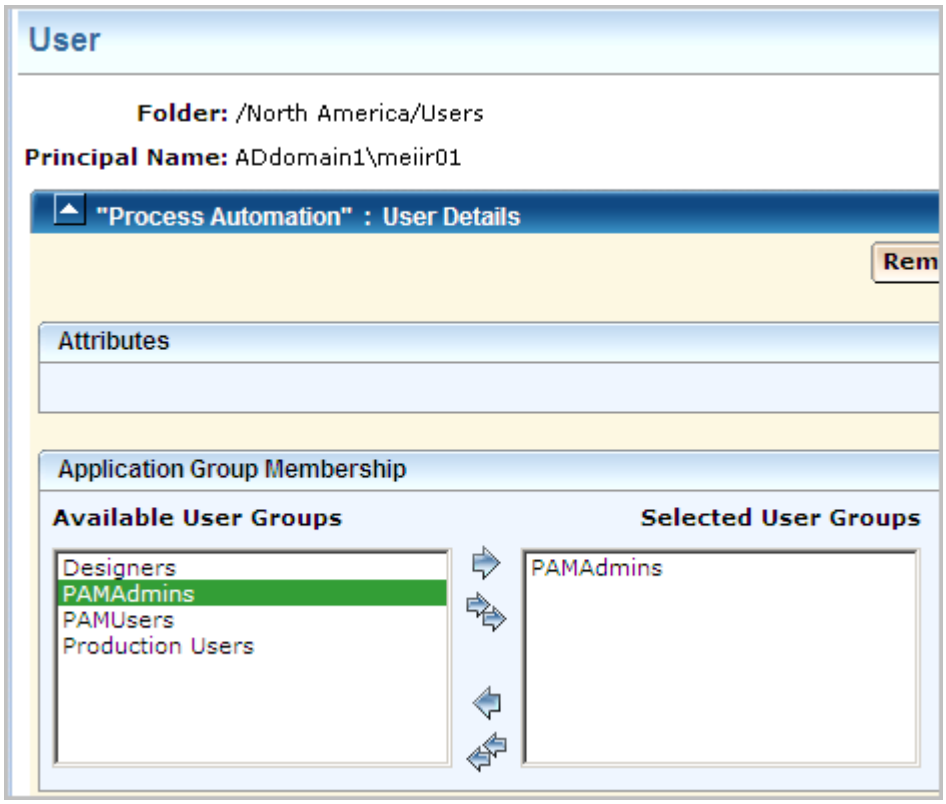
1. Log into CA EEM as the CA EEM administrator.
2. Click Manage Identities. Enter search criteria for Global Users. The example search is for all AD users with the last name of Meier.



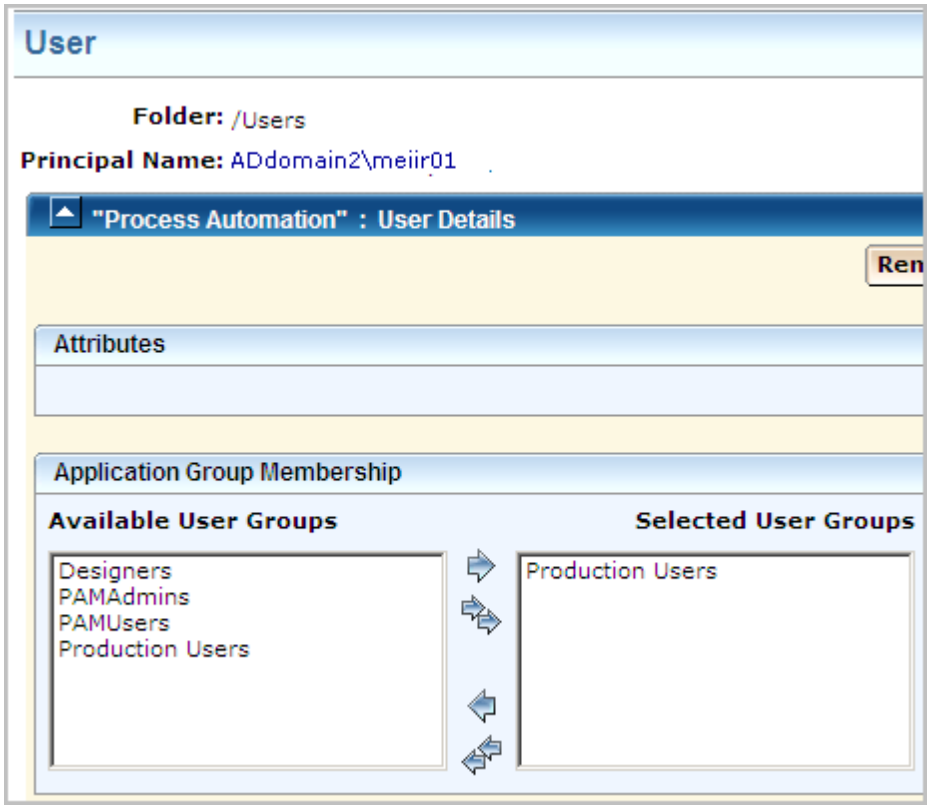
2. Select one of the displayed global users, for example, Meier, Iris. The User account panel opens. This represents the record from the newly referenced AD domain. Click Add Application User Details.



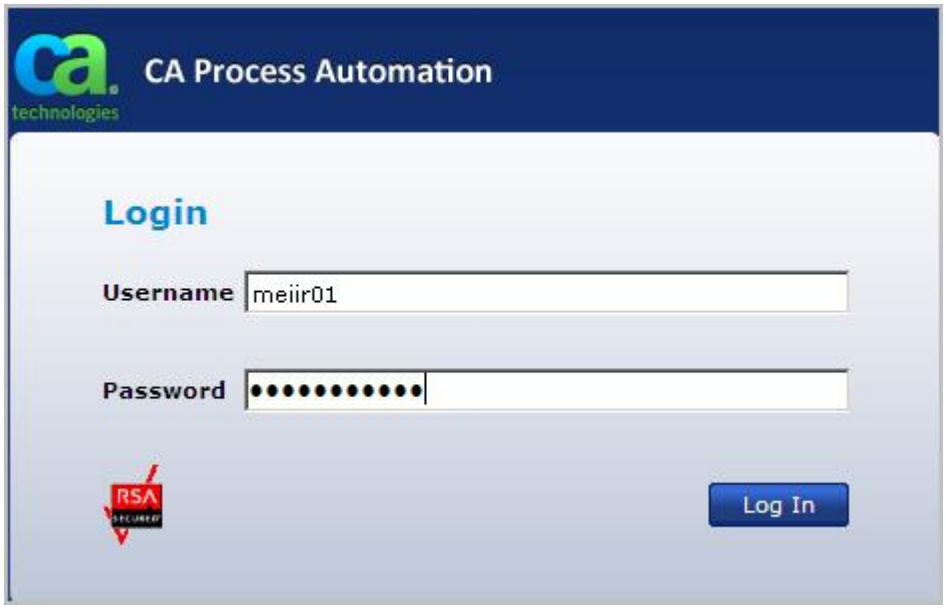
3. Select the PAMAdmins user group to create administrator permissions to CA Process Automation for this user.



4. Select the other Global User entry from the Search results. Notice that this one displays ADdomain2, not ADdomain1 and has Production Users permissions. This represents the existing user record.



5. The user in the AD domain that was originally referenced, can log in to CA Process Automation with the unqualified user name, if that domain is set as the default domain. (All users from the additional domains must enter their principal name for Username at login. So, for this example, entry of the unqualified user name logs the user in with Production Users permissions. To get PAMAdmins permission, the user would enter ADdomain1\meiir01 in the Username field.



About Global Users

All users that are defined to CA EEM are global users. The global users can be one of the following types:

- Users for whom you create global user accounts, where you supply all details, including assigning an application group and specifying a password.
- Users that are defined in CA EEM for use with another CA product. You search for such global users and provide CA Process Automation access by assigning a CA Process Automation application group to each user. Such global users log in to CA Process Automation with the credentials previously defined in CA EEM.
- Users that are defined in an external user store that you identify when you install CA EEM. You search for such global users and provide CA Process Automation access by assigning a CA Process Automation application group to each user. Such global users log in to CA Process Automation with the credentials defined in the external user store.

  Note: Users enter credentials as either their principal name (*domain name**user name*) and password or their user name and password. The principal name is *accepted* when CA EEM uses Microsoft Active Directory as the external user store and multiple domains are referenced during the installation. The principal name is *required* when the source AD domain for the user is not the default domain.

If you use the CA EEM internal user store, you create global users and you assign application groups. If you reference an external user store, you retrieve global users and you assign application groups.

Assign an Application Group to a Global User

To grant role-based access to a user, assign an application group to the respective global user account.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Search for identities that match the specified criteria (see page 62).
3. Under Users, select the target user name.

   The selected user account opens.
4. Click Add Application User Details.

   The Application Group Membership dialog opens.

5. Select the appropriate group from Available User Groups, and then click the right arrow (>) to move it to Selected User Groups.
6. Click Save.

   The target global user can now log in to CA Process Automation. After the authentication process, the user can access the functionality the product grants to all members of the assigned application group.

About Dynamic User Groups

A *dynamic user group* consists of global users that share one or more attributes. It is created through a special dynamic user group policy. The resource name is the dynamic user group name and membership is based on filters that are configured on user and group attributes.

You can create a dynamic user group that consists of Users, Application Groups, Global Groups, or Dynamic Groups. For example, you can create a dynamic user group of Global Groups or Application Groups that is based on Name, Description, or Group Membership. Similarly, you can create a dynamic user group of Users with different roles based on a common attribute in their global user profile. For example:

- Job title
- Department or office
- City, state, or country

The EiamAdmin user can create Dynamic User Group Policies.

Create a Dynamic User Group Policy

You can create a dynamic user group policy.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click Manage Access Policies, and then click New Dynamic Group Policy to the left of Dynamic User Group Policies.
3. For Name, enter a group name that identifies a common property of the group of users. Optionally, enter a description.
4. Select a policy type. The default is Access Policy.

5. Select Identities as follows:
   a. For Type, select one of the following values, and then click Search Identities.
      - User
      - Application Group
      - Global Group
      - Dynamic Group
   b. For Attribute, Operator, and Value, enter the expression that sets the membership criteria for the group and then click Search.

      Example:

      Select User, enter **Job Title Like Manager**, and click Search. The process returns all users with the job title "Manager".
   c. From the search results, select the users to add as members of this dynamic group. To move your selections to the Selected Identities list, click the right arrow (>).
6. For Actions, select belong.
7. In the Add Resource field, enter the value that you entered in the Name field, and then click Add.

   The process adds the selected identities to the dynamic user group you created.
8. (Optional) Add more filters.
9. Click Save.

   The policy that you created appears when you click the Dynamic User Group Policies link.

Chapter 4: Administer Advanced CA EEM Security

You can use CA EEM to create fine-grained access policies to meet stringent security requirements. You can create custom policies, create groups that use these custom policies, and assign your custom groups to user accounts. Or, you can assign users directly to custom policies. You can define custom policies to limit access to one or more specified folders with or without subfolders. Access levels include view, navigate, edit, delete, and create, where permissions are additive. You can limit user access to a specified environment. You can also modify the access defined to default groups.

Customization is needed to extend the default access. For example, customization is used to grant administrators access to CA EEM, create access similar to that afforded by the previous LDAP implementation, and limit access to servers containing sensitive information or critical business processes.

The Permissions Reference section includes the details that support all types of customization.

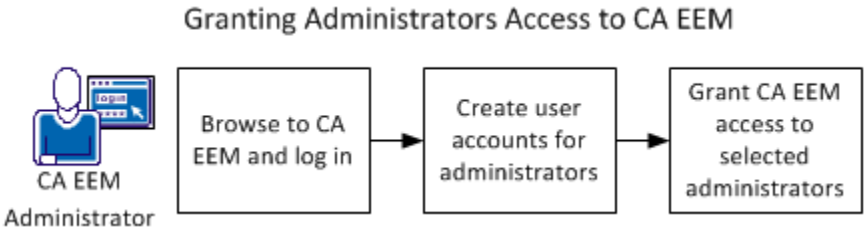
This section contains the following topics:

Granting Administrators Access to CA EEM

CA EEM provides security for CA Process Automation. CA EEM maintains the credentials in user accounts that allow users to log in to CA Process Automation. CA EEM authenticates users at login and allows login if the user ID and password are found in a user account. User accounts are associated with groups. CA EEM authorizes users at login based on their group assignments.

EiamAdmin is the predefined user name of the CA EEM administrator. The CA EEM administrator is the role that gives users access to CA Process Automation. During installation of CA Process Automation, you specify a password for the EiamAdmin user. Only users who know the EiamAdmin password can log in to CA EEM. We recommend that you restrict knowledge of this password to a few trusted individuals.

The EiamAdmin user can define a policy that grants to selected CA Process Automation administrators the ability to create custom groups, policies, and user accounts. This access is sufficient but more limited than that of EiamAdmin. The process follows:



1. Browse to CA EEM and log in (see page 45).
2. Create user accounts for administrators.
3. Grant CA EEM access to selected administrators (see page 73).

More information:

Grant CA EEM Access to Selected Administrators (see page 73)

Grant CA EEM Access to Selected Administrators

CA EEM access is required to manage user accounts, groups, and policies. By default, you must know the EiamAdmin password to log in to CA EEM with the application set for CA Process Automation. Typically, knowledge of this password is highly restricted because the EiamAdmin user has full control of CA EEM. However, the EiamAdmin user can grant CA EEM login access to other administrators and can specify the objects that they can manage. The following procedure shows how to grant to selected administrators the ability to manage user accounts, groups, and policies. This procedure includes defining a new group, creating a custom policy for the group, and assigning the group to user accounts.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Create EEMAdmins, an CA EEM administrators group, members of which can create user accounts, custom groups, and custom policies.
   a. Click the Manage Identities tab.
   b. Click Groups.
   c. Click New Application Group.
   d. Enter a name for the group (for example, EEMAdmins).
   e. (Optional) Add a description.
   f. Click Save.

   Note: Do not select an Application Group.

3. Create a policy that grants the ability to create user accounts, custom groups, and custom policies. Assign EEMAdmins as the identity for this policy.
   a. Click the Manage Access Policies tab.
   b. Click Scoping Policies.
   c. Click the link to Administer Objects.
   d. Click Save As and enter a name for this policy (for example, Administer Users and Policies)
   e. Click OK.
   f. Select [User] EiamAdmin and [User] CERT-application-name from the Selected Identities list, and then click Delete.
   g. Click Search Identities for Type Group, and then click Search.
   h. Select the new group (EEMAdmins) and click the right arrow to move the user group (ug) to Selected Identities.
   i. Select and delete all of the resources *except* ApplicationInstance, Policy, User, UserGroup, GlobalUser, GlobalUserGroup, and Folder.
   j. Verify that the read and write actions are selected.
   k. Click Save.

   Your policy resembles the following example:

Scoping Policies

Name/Description	ResourceClassName	Options	Identities	Actions	Resources
Administer Users and Policies Specified users or group can create user accounts, custom groups, and custom policies.	SafeObject	Explicit Grant	ug: EEMAdmins	read write	ApplicationInstance Policy User UserGroup GlobalUser GlobalUserGroup Folder

4. Add the EEMAdmins group to the user accounts of selected administrators:
   a. Click the Manage Identities tab.
   b. Click Application User Details for Search Users.
   c. Select Group Membership as the attribute, LIKE as Operator, and PAMAdmins as Value.
   d. Click Go.

      The CA Process Automation administrators are listed.
   e. Click the name of an administrator.

      The user account of the selected administrator opens. EEMAdmins is displayed as an available user group.
   f. Click the right arrow to move EEMAdmins to Selected User Groups.
   g. Click Save.
5. Repeat Step 4 for each administrator to whom to grant CA EEM rights.

Customizing User Access with CA EEM Policies

You can customize user access to CA Process Automation tabs, palettes, and access to different automation objects. To extend changes to everyone in a default group, you can change the default policies.

You can restrict user access to specified folders. For example, you can create a folder for each designer and restrict designers access to their own folder and folders designed for common use.

You can restrict access to a specified environment for specified users. For example, you can restrict environment access for members of the Production Users group, such that they can access only the production environment. They, then, cannot access the design environment.

You can restrict access to touchpoints that map to servers that hold sensitive information or perform a critical business function with Touchpoint Security policies.

Control Caches of CA EEM Updates

CA Process Automation does not immediately reflect the changes when policies, user groups, and user accounts are modified in CA EEM. CA Process Automation does not always query CA EEM directly for authorization queries. CA EEM does not send CA Process Automation individual changes as they occur. Instead, CA Process Automation relies on the following caches:

- An CA EEM-side cache of changes to policies, user groups, and user accounts that CA EEM sends to CA Process Automation.

  A Security setting on the Configuration tab controls the cache refresh rate. You can update the setting at the Domain level or for a selected environment.

- A CA Process Automation-side secondary cache of the query results that CA EEM returns to CA Process Automation.

  When the security function validates user permissions, it looks first at the age of the secondary cache.

  - If the cache age is equal to or less than the configured value, the security function uses the permission data in the cache.
  - If the cache age is greater than the configured value, the security function sends a request to CA EEM. The security function refreshes the secondary cache with the query results and resets the cache age to 0 seconds.

When you test custom policies with a test user, you can view the results as soon as CA EEM sends changes to CA Process Automation. To update CA Process Automation more frequently, reduce the update interval. To optimize the product performance when you finish testing, increase the cache refresh interval.

As you use the following procedure to change the CA EEM-side cache refresh rate, consider using a fast refresh rate only in the design environment. Optionally, change the maximum age of the secondary cache on the server that hosts the target Orchestrator for testing.

Follow these steps:

1. Change how often CA Process Automation gets updates from CA EEM. Set the standard interval at the Domain level.
   a. Click the Configuration tab.

      The Configuration Browser palette opens with Domain selected. The Security tab is displayed.

   b. Click Lock.

   c. Edit the CA EEM Cache Update Interval (in seconds) setting as necessary, based on the frequency with which CA EEM is updated.

      - While you are testing the impact of CA EEM changes, set the update interval to **60** seconds.
      - When you finish testing, set the update interval to **1800** seconds (the default).

   d. Click Save.

   e. Select Domain and click Unlock.

   f. Restart the Domain Orchestrator.

      - Stop the Orchestrator (see page 186).
      - Start the Orchestrator (see page 187).

2. Change the rate at which CA EEM sends authorization changes to CA Process Automation for a selected environment.

   a. Click the Configuration tab and expand Domain in the Configuration Browser palette.

   b. Select the target environment and click Lock.

   c. On the Security tab, edit the CA EEM Cache Update Interval (in seconds) setting as necessary, based on whether you are actively testing user authorizations.

      - While you are testing customizations, set the update interval to **60** seconds.
      - When you finish testing, set the update interval to **1800** seconds (the default).

   d. Click Save.

   e. Select the environment and click Unlock.

   f. Restart the Orchestrators in the environment you updated.

      - Stop the Orchestrator (see page 186).
      - Start the Orchestrator (see page 187).

3. Change the maximum age (in seconds) of the secondary cache that contains user permissions.

   Note: It is not typically necessary to change this internal parameter.

   a. Log on to the server on which the target Orchestrator is configured.

   b. Navigate to the following folder or directory:

      install_dir`/server/c2o/.config/`

   c. Open the OasisConfig.properties file.

   d. Add the following parameter, if it does not exist:

      `eem.cache.timeout`

   e. Assign a value (in seconds).

      Setting this parameter to 0 turns off this cache so that CA Process Automation requests user permissions from CA EEM when required. The product uses the default value (30) when this parameter is not present in the OasisConfig.properties file.

      `eem.cache.timeout=30`

   f. Save the file.

   g. Restart the Orchestrator service.

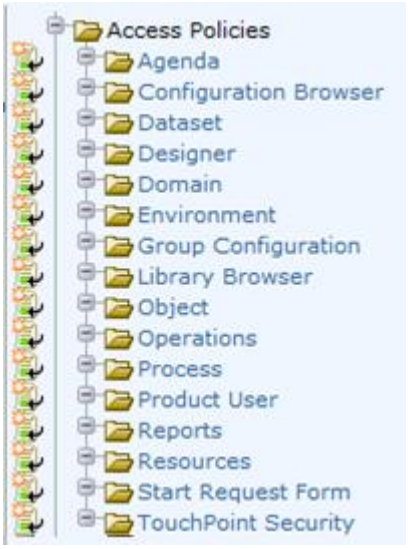
      - Stop the Orchestrator (see page 186).
      - Start the Orchestrator (see page 187).

More information:

Configure CA EEM Security Settings for the Domain (see page 133)

Default Resource Classes and Custom Policies

CA Process Automation Resource Classes are listed under Access Policies in CA EEM. You can create an original custom policy for any resource class or base it on a predefined policy.



Most of the CA EEM resource classes include predefined policies.

You can use Save As to save the predefined Access Policies with a new name, and then customize as necessary. Creating a custom policy that is based on a predefined policy helps you achieve the following results:

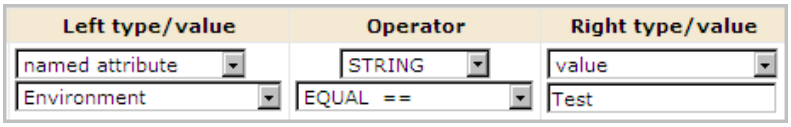
- Provide the assigned group a permission that the predefined policy does not grant. For example, the custom policy can grant the Designers group access to the Configuration tab Installation palette so that they can install agents.
- Remove a permission or access that a predefined policy grants. For example, your custom policy can remove PAMUsers group access rights to the Reports tab.
- Replace a default group (for example, PAMAdmins), with groups that better reflect the product roles that your site defines. For example, you can have three administrator levels instead of one. Assign PAMAdmins to your Domain administrator and create separate administrator groups that administer content and perform configurations for each environment.

  Note: For more information about creating separate access rights for Content Administrators and Configuration Administrators, see Create User Accounts with Custom AD Roles (see page 111).
- Add one or more filters for fine-grained access. For example, you can specify ENVIRONMENT equal to an environment name as a filter. The environment filter is often used in user-defined Touchpoint Security policies.

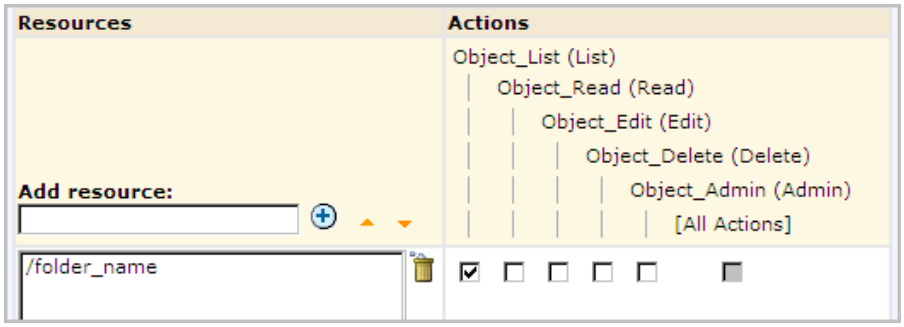
Consider the process and start request form objects in terms of the SOAP access level calls through web services. When you create a policy with the Process resource class, you grant specified users or groups Process Start (Start) or Process_Control (Control) rights. If the user who invokes the Execute Process method has the Start permission or the Control permission, the method runs successfully. When you create a policy with the Start Request Form resource class, you grant specified users or groups StartRequestForm_Start (Start) or StartRequestForm_Dequeue (Dequeue) permissions. If the user who runs the Execute Start Request Form method has the Start permission or the Dequeue permission, the method runs successfully. If the user who runs the method does not have execute rights on the target object, the method fails. The SOAP operator dataset records method failure messages.

You can create a custom CA EEM policy that grants or denies access by specified groups to any specified automation object. For example:

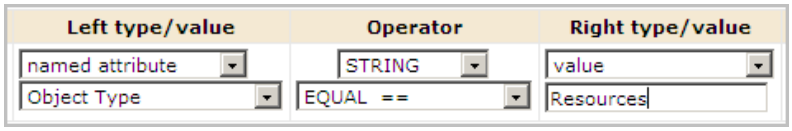
- Limit access to a specified environment with the Agenda, Dataset, System, Process, Resources, Start Request Form, and Touchpoint Security policies. Add a filter where Environment is the named attribute and your environment name is the value. The STRING Operator is EQUAL ==. In the following filter example, Test is the Environment name:



- Limit access to a specified folder or object with the Object policy. Add a resource such as */folder_name* or */folder_name/object_name*. In the following example, /folder_name represents the name of the folder where the automation object resides.



You can also create a custom policy for the Object resource class. Policies on Object provide a filter to specify the object type to which the policy applies. Add a filter where the named attribute is Object Type and the value is an object type. The STRING Operator is EQUAL ==. In the following filter example, Resources is the Object Type name:



Other valid values include:

- The resource classes:
  - Agenda, the resource class for Schedule.
  - Dataset
  - Process
  - Resources
  - Start Request Form
- Calendar
- Custom Icon
- Custom Operator
- Folder
- Interaction Request Form
- Process Watch

How to Customize Access for a Default Group

You can customize the access default access in the following ways:

- Add an action to a default group.
- Revoke an action from a default group

Any changes you make to the assignments of a default group affect all users who are assigned to that group.

The process for customizing access for a default group follows:

1. Review permissions for default groups (see page 47).
2. Identify a permission required at your site that a default group is missing.
3. Determine the action and policy that controls that access.
   - If the permission is to access a tab or palette, see Permissions by Tab (see page 98).
   - If the permission is on an automation object, see Permissions on Automation Objects (see page 104).
4. Create a policy based on an existing policy (see page 83), where the existing policy is a predefined, default policy.
5. Grant or revoke an action for a default group (see page 83).

Create a Custom Policy Based on an Existing Policy

You can create a custom policy based on a default policy or based on another custom policy.

CA Process Automation provides a policy for almost all resource classes. You can modify default policies directly since they are editable. However, there is no easy way to revert to the original. You can institute a practice that preserves the predefined policies so you can compare a revision with the original or revert to it.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click Manage Access Policies.
3. Click the name of the access policy to modify.
4. Click the policy link in the policy table.
5. Click Save As and enter a custom policy name.
6. Click Save.
7. If the custom policy is to replace a predefined policy, open the predefined policy and click Disable. Then click Save.

Note: Your custom policy is ready for customization.

Grant or Revoke an Action for a Default Group

You can grant a new action to a default group. You can also revoke a predefined action from a default group.

Follow these steps:

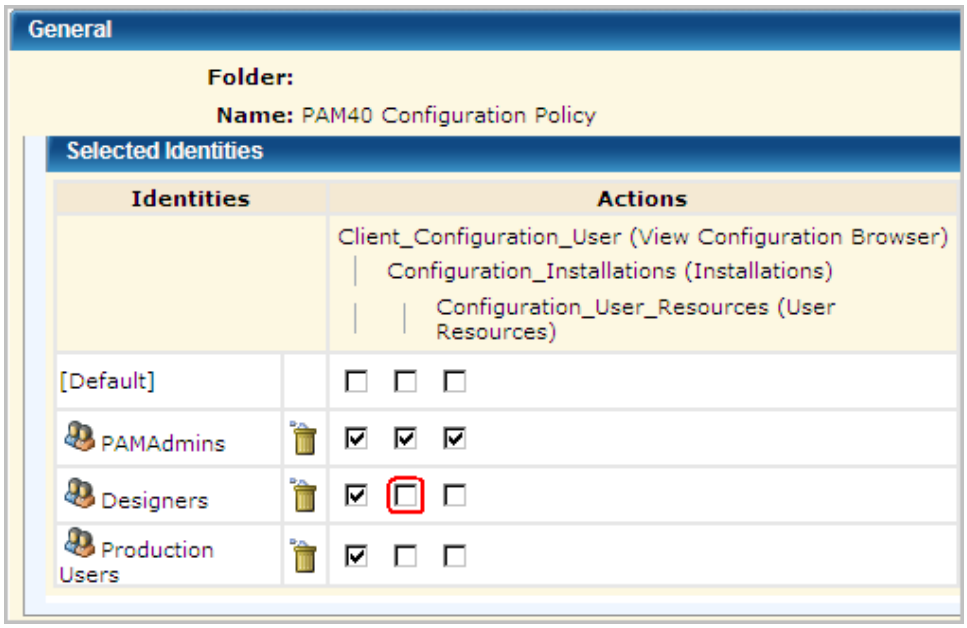
1. Open the custom policy that you created for this purpose.
2. In the Designers row for Selected Identities, click or clear the action that you identified.

   Note: See Example: Grant Designers the Ability to Perform Installations (see page 84).
3. Click Save.

   Your custom policy goes into effect the next time CA EEM sends updates to CA Process Automation.

Example: Grant Designers the Ability to Perform Installations

By default, Designers have no access to the Installation palette on the Configuration tab. You can add the ability for users in the Designers group to install agents. Check Configuration_Installations (Installations) for Designers on the PAM40 Configuration Policy.



Example: Grant Designers the Ability to Publish Groups for Custom Operators

By default, Designers cannot perform the following actions on groups for custom operators:

- Lock the group configuration for a custom operator
- Define a group with variables that are appropriate for a set of custom operators
- Unlock the group configuration, publishing the group

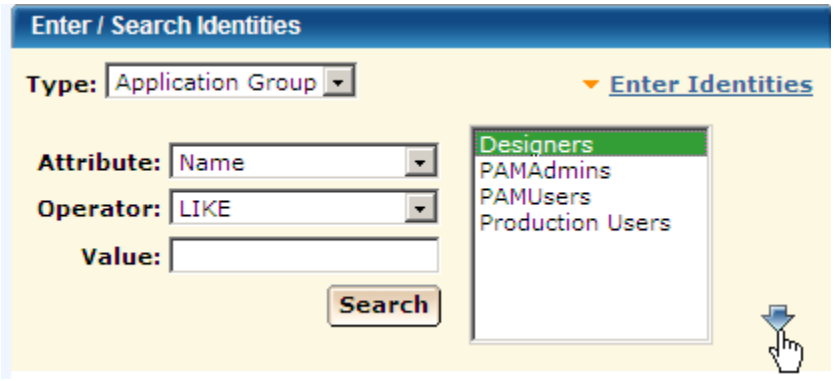
Published custom operator groups appear on the Modules tab in the Configuration Browser.

You can grant content designers permission to create and publish custom operator groups.

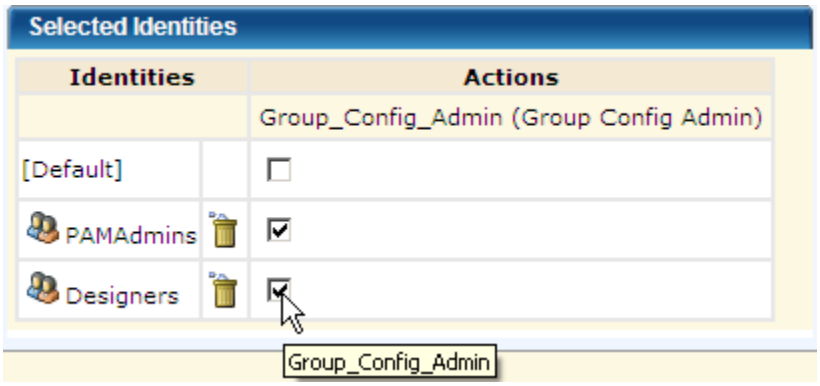
Follow these steps:

1. Log in to CA EEM.
2. Click Manage Access Policies.

3. Open the Group Configuration Policy.
   a. Click Group Configuration.
   b. Click the PAM40 Group Config Policy link.
4. Add the Designers application group to the Selected Identities list.
   a. Select Application Group from the Type drop-down list.
   b. Click Search Identities.
   c. Accept the default entries for the following fields, then click Search:
      - **Attribute:** Name
      - **Operator:** LIKE
      - **Value:** This field is blank by default.
   d. Select Designers and click the down arrow:



5. Select the action Group_Config_Admin for the Designers group.



6. Click Save.

How to Restrict Access by Environment

The Designer and Production User default groups are designed for the typical case where there are two environments:

- Design environment (Default Environment)
- Production environment (user-defined environment)

Members of the Designer group create the automated business processes in the Design environment. Designers design processes, design interaction request forms, and design datasets, for example.

Members of the Production Users group use the designed processes, the designed forms, and the designed datasets. For example, production users start processes, inspect datasets, and reply to interaction requests.

You can save the following policies as custom policies to restrict the Designers group to the design environment and Production Users to the production environment.

- Agenda
- Dataset
- Process
- Resources
- Start Request Form

Example: Environment Filter

You can limit access to schedules by environment. For example, you can use the Default Environment for design and add a Production Environment for using the processes and related objects that have been transitioned to production.

The following example filter for Schedules restricts members of the Designers group to the Default Environment. It restricts members of the Production Users group to the production environment.

Name/Description	ResourceClassName	Filters
Custom Schedule Policy with Environment Restrictions Restrict Schedule automation object for Designer group to Default Environment and Production User group to Production Environment	Agenda	WHERE ((ug:Name == val:Designers 1 AND req:action {} val:Control 1 AND name:Environment == val:Default Environment) OR (ug:Name == val:Production Users AND req:action {} val:Control AND name:Environment == val:Production Environment))

You can customize policies based on the following default policies with similar filters:

- PAM40 Dataset Policy
- PAM40 Process Policy
- PAM40 Start Request Form Policy
- PAM40 Resources Policy

Open the default policy. Save it as a custom policy. Change the type to Access Policy. Then, add the filter.

How to Customize Access with a Custom Group

The basic procedure for customizing access with a custom group follows:

1. Create a custom group (see page 87).
2. Add the custom group to a default policy (see page 89).

   Here, you grant permissions for specified actions to the custom group.
3. Assign the custom group to user accounts (see page 90).

   You can assign more than one group to a user account to extend permissions for that user.

Note: For examples of this procedure, see How to Transition Roles Used in Active Directory to CA EEM (see page 111).

Create a Custom Group

You can create a custom application user group in CA EEM. To grant that group rights, add the group to policies and select appropriate actions. Finally, assign the group to individual user accounts.

Note: The policies to which you must add a custom group depend on whether you base the group on an existing group.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Identities tab.
3. Click Groups.
4. On the Groups panel, click the New Application Group button next to Application Groups to create a custom group.
5. Enter a name for the group in the Name field.
6. (Optional) Enter a description for the group.

7. (Optional) In the Application Group Membership selection group, select PAMUsers to include permissions for basic access. In this case, you can limit the permissions that you grant to this custom group. You do not need to grant permissions that are granted to the PAMUsers group.

   Note: If you leave the Selected User Groups area blank, the custom group must include permissions for basic access.

8. Click Save.

   The product displays the new group as an application user group option when you define new users.

9. (Optional) Select Show application groups under Search Groups, and then click Go.

   The product displays your new group with other groups (including the default groups).

10. Click Close.

More information:

Add a Custom Group to a Default Policy (see page 89)

Add a Custom Group to a Default Policy

A simple way to customize access privileges is to create custom groups and add those groups to selected default policies. With this approach, you do not create any custom policies. You identify the actions, or permissions, in the default policies that individuals you assign to the custom group need.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Create a custom group for users that are to perform the same set of tasks in CA Process Automation.
   a. Click the Manage Identities tab.
   b. Click Groups.
   c. Click New Application Group.
   d. Enter the name of the group.
   e. Do not add an application group membership.
   f. Click Save.
3. Open the default policy containing the action you want to grant.
   a. Click the Manage Access Policies tab.
   b. Click the link for the appropriate resource class under Access policies.
   c. Click the link in the Policy Table for the policy to update.

      The selected policy opens.
4. Grant a selected permission to the custom group.
   a. Under Enter/Search Identities, select Application Group from the Type drop-down list and click Search.
   b. Select the custom group from the list and click the down arrow.
   c. The custom group appears in the Selected Identities list.
   d. Select the check box for each action to grant.
   e. Click Save.

   The custom group is added to the selected policy.

Assign a Custom Group to User Accounts

You can assign a custom group (role) to a user account during the process of creating that user account. Or, you can edit an existing user account to add the new application user group.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Identities tab.
3. Create or access the target user account.
   - Click New User to add a user account.
   - Use Search Users to retrieve an existing user account.
4. If creating a new account, enter the user account ID in the Name field, enter details about the user under Global User Details, enter a temporary password and select Change Password at Next Login.
5. Click Add Application User details.
6. Select the custom group from Available User Groups and click > to move it to Selected User Groups.
7. Click Save, then click Close.
8. Repeat for each user that is to have the permissions granted to the custom group.
9. Click Log Out.

How to Customize Access for a Specified User

You can restrict which objects a specified CA Process Automation user can view and the actions that user can perform. You can create CA EEM rules such that a user can only see or use one automation object instance or one automation object. This type of access is possible only when content designers work with library objects in working folders. In this case, the release versions of objects are copied to a release-specific folder for export as a content package.

Follow these steps:

1. Set up designer-specific folders (see page 92).
2. Create a user account with no group assignment (see page 92).
3. Add the user to selected default policies (see page 94).
4. Create a custom Object policy with path permissions (see page 96).
5. Create a custom policy for a specified object type (see page 97).

Note: Log in to CA Process Automation as the specified user and verify that the access is correct.

Set up Designer-Specific Folders

You can design the folder structure at your discretion. For fine-grained access, design the structure so you can specify a path to objects of a specific type in the policy for that automation object. To restrict a user (or group) to specific object types or to specific object types in specified projects, set up a folder structure that allows such a restriction. For example, set up a Work In Progress (WIP) folder withe a folder for each designer.

WIP/designer1

Each designer has a separate working folder. Each designer folder contains a set of folders, one for each type of automation object on which the developer works. A folder for dataset can include datasets for multiple projects that a single designer developed.

/project1/releaseVersion1

Each project has a specific folder, with a subfolder for each release version. When a release version of a process is ready to transition to production, copy the objects from the working folders to the release version folder. The release version folder is the folder that the product exports as a content package.

Follow these steps:

1. Browse to CA Process Automation and log in (see page 18).
2. Click the Library tab.
3. Select the root folder, click New, and then select Folder.
4. Enter a short name for the new folder.
5. Repeat these steps as appropriate to create the necessary folder structure.

Create a User Account with No Group Assignment

You can create a user account with no group assignment. This is part of the process for creating fine-grained access, where you restrict the user to designing and testing objects of one particular type.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Identities tab.

3. Click the icon next to Users in the Users palette.

   The New User page opens.

4. Type the User ID to assign to the user account in the Name field.

   This name is the name the user types in the User Name field at login.

5. Enter the global user details.

   a. Type the name in the First Name and Last Name fields.

      The title bar displays these values when the user logs in to CA Process Automation.

   b. Complete the other fields in the General area as appropriate.

6. (Optional) Complete the Global Group Membership field if you use CA Process Automation with another CA Technologies product that uses this CA EEM.

7. Type and verify a password to associate with the account in the Authentication area.

   Give to users the temporary password you configure so that they can change their own passwords.

8. (Optional) Complete the remaining fields on the New User page.

9. Click Save, then click Close.

10. Click Log Out.

More information:

Use CA EEM to Change Your CA Process Automation Password (see page 46)
Grant CA EEM Access to Selected Administrators (see page 73)

Add the User to Selected Default Policies

You can grant CA Process Automation permissions to a user identity in either or both of the following ways:

- Assign a user group to the user account.
- Add the user account to selected policies. In each policy, assign selected actions to the user identity

If you are working with custom policy and fine-grained user roles, we recommend that you grant basic access by assigning the PAMUsers group to the user account and then extending that access with policy action assignments.

If you prefer to grant access with policies alone, begin by providing basic access. Add the user account name to the following policies and actions:

- PAM40 User Login Policy: Console-Login (User)
- PAM40 Environment Policy: Environment_Library_User (User)
- PAM40 Library Browser Policy: LibraryBrowser_User (Library Browser User)

You can grant fine-grained access to the Operations tab. You can limit user access to specified actions on specific objects types.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Access Policies tab.
3. Add the user to the PAM40 User Login Policy.
   a. Click the link for Product User under Access policies.
   b. Click the PAM40 User Login Policy link in the Policy Table.
   c. Set Type to **User**, and click Search Identities.
   d. Click Search.
   e. Select the user identifier from the displayed list and click the down arrow.
   f. Select Console-Login (User) for the user you added.
   g. Click Save and click Close.

4. Add the user to the PAM40 Environment Policy.
   a. Click the link for Environment under Access policies.
   b. Click the PAM40 Environment Policy link in the Policy Table.
   c. Set Type to **User**, and click Search Identities.
   d. Click Search.
   e. Select the user identifier from the displayed list and click the down arrow.
   f. Select Environment_Library_User (User) for the user you added.
   g. Click Save and click Close.
5. Add the user to the PAM40 Library Browser Policy.
   a. Click the link for Library Browser under Access policies.
   b. Click the PAM40 Library Browser Policy link in the Policy Table.
   c. Set Type to **User**, and click Search Identities.
   d. Click Search.
   e. Select the user identifier from the displayed list and click the down arrow.
   f. Select LibraryBrowser_User (Library Browser User) for the user you added.
   g. Click Save and click Close.
6. Grant the user access to two objects on the Operations tab. Add the user to the PAM40 Operations Policy and specify only two actions.
   a. Click the link for Operations under Access policies.
   b. Click the PAM40 Operations Policy link in the Policy Table.
   c. Set Type to **User**, and click Search Identities.
   d. Click Search.
   e. Select the user identifier from the displayed list and click the down arrow.
   f. Select Operations_Datasets (Datasets) for the user you added.
   g. Select Operations_Resources (Resources) for the user you added.
   h. Click Save and click Close.

Create a Custom Object Policy with Path Permissions

Create a custom Object access policy with the Object access policy. The number of entries you make depends on the depth of the path. Enter one line for each path level, beginning with the root folder (/).

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Access Policies tab.
3. Create a custom Object policy to restrict a specified user to a specified path in the library.
   a. Click the New Access Policy link for Object under Access policies.
   b. Enter a name.
   c. Select Access Control List for Type and click OK to the verification message.
   d. Click Search Identities with Type set to User.
   e. Click Search. Select the user identifier from the displayed list and click the right arrow.
   f. Type a forward slash (/) in the Add resource field and click Add.
   g. In the same field, type / followed by the name of the folder containing the objects to which the user is restricted. Click Add.
   h. Select Object_List (List) for the root folder (/).
   i. Select Object_List (List) for the */folder* path. Repeat this step if there is a */folder/subfolder* path.

      Note: You can enter /folder/subfolder* and select "Treat as regular expression" to include all folders subordinate to the specified subfolder.
   j. Click Save. Click Close.

Create a Custom Policy for a Specified Object Type

Create a policy for the type of object to which the restriction applies. Then specify the actions to allow on the selected object type. Choose from the following policy types:

- Agenda
- Dataset
- Process
- Resources
- Start Request Form

Note: For details on permissions, see the Permissions Reference (see page 98) section.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Access Policies tab.
3. Create a custom policy for the object type you want to restrict.
   a. Click the New Access Policy link for one of the following resource types: Agenda, Dataset, Process, Resources, Start Request Form.
   b. Enter a name.
   c. Select Access Control List for Type and click OK to the verification message.
   d. Click Search Identities with Type set to User.
   e. Click Search. Select the user identifier from the displayed list and click the right arrow.
   f. In the Add resource field, type the full path containing the object type that you selected. Click Add.
   g. In the same field, type a forward slash (/) and then type the name of the folder containing the objects to which the user is restricted. Click Add.
   h. Select the permission to grant.
      - Agenda: Agenda_Control (Control). Agenda refers to Schedules.
      - Dataset: Dataset_Inspect (Inspect), Dataset_Modify (Modify).
      - Process: Process_Control (Control), Process_Monitor (Monitor), Process_Start (Start).
      - Resources: Resources_Control
   i. Click Save. Click Close.
4. (Optional) Add a filter to limit by Environment.

5. Repeat this procedure for dependent objects. Consider, for example, Datasets. Datasets are meaningful only in the context of another object type. If you selected Datasets, create another policy for, say, Resources.

Permissions Reference

The following tables list all permissions with dependencies and filters:

- Permissions by Tab (see page 98)
- Permissions on Automation Objects (see page 104)
- Permissions Dependencies (see page 106)
- Filters for Permissions (see page 110)

Permissions by Tab

The actions that are selected on predefined CA EEM policies grant permissions to tabs, palettes, folders, and automation objects. The following tables describe the permissions that each action grants to groups (identities) in the corresponding resource policies.

If you create custom policies from these resource classes, use the corresponding tables as a guide for assigning permissions.

Home Tab

Action Key (Localized Name)	Resource Class for Policy	Permissions
Console_Login (User)	Product User	Log in to CA Process Automation and use the Home tab.

Library Tab

The following table lists permissions in order from the lowest level to the highest level. To view the Library tab, you must have the LibraryBrowser_User permission and either the Environment_Library_User or the Environment_Library_Admin permission. For more information, see Permissions Dependencies (see page 106).

Action Key (Localized Name)	Resource Class for Policy	Permissions
LibraryBrowser_User (Library Browser User)	LibraryBrowser (Library Browser)	View access to the Library tab.

Action Key (Localized Name)	Resource Class for Policy	Permissions
Object_List (List)	Object	■ View folder or automation object in the Library Browser. ■ Define customized library views.
Environment_Library_User (User)	Environment	Prerequisite to many Operations tab permissions. ■ Access to Orchestrators added to environments. ■ View, export, search automation objects in the Library tab if the access is set.
Object_Read (Read)	Object	Navigate a folder path and open any automation object in the corresponding designer orviewer. *Implicit:* List
Object_Edit (Edit)	Object	Edit a folder or an automation object in a folder. *Implicit:* Read, List
Object_Delete (Delete)	Object	Delete a folder or delete an automation object added to a folder. *Implicit:* Edit, Read, List
Object_Admin (Admin)	Object	Create a folder or any automation object. *Implicit:* Delete, Edit, Read, List
Environment_Library_Admin (Content Administrator)	Environment	Create, Delete, Edit, Read, and List on all automation objects in the Library tab.
Group_Config_Admin	Group Configuration	Access Group Config tab. See Permissions on Automation Objects (see page 104) for permissions granted on custom operators.

Designer Tab

Users with access to the Designer tab are typically also granted access to the Library tab. Designers need at least the following Library tab permissions to save a process they are designing:

- LibraryBrowser_User
- Environment_Library_User
- Object_Edit (which includes the Object_List and the Object_Read permissions)

Action Key (Localized Name)	Resource Class for Policy	Permissions
Designer_User (Designer User)	Designer	View access to the Designer tab.

Operations Tab and Palettes

Designers require access to the Operations tab in the design environment; production users require access to the Operations tab in the production environment. To view the Operations tab, you must have either the Environment_Library_User or the Environment_Library_Admin permission. For more information, see Permissions Dependencies (see page 106).

Action Key (Localized Name)	Resource Class for Policy	Permissions
Operations_Process_Watch (Process Watch)	Operations	■ Open the Process Watch palette in the Operations tab. ■ View all the processes in the selected state, active schedules, active operators, and User Requests.
Process_Monitor (Monitor)	Process	■ Open a running process instance in the Process Designer. ■ Monitor progress. ■ Set breakpoints. *Implicit:* List
Process_Start (Start)	Process	Start a process instance. *Implicit:* Monitor, List
Process_Control (Control)	Process	Suspend, restart, resume, or abort process instances. *Implicit:* Start, Monitor, List

Action Key (Localized Name)	Resource Class for Policy	Permissions
Operations_Schedules (Schedules)	Operations	View Active Schedules link in the Operations tab.
Agenda_Control (Control)	Agenda	Activate and deactivate a schedule on a touchpoint. *Implicit:* Read, List
Operations_Datasets (Datasets)	Operations	Open the Operations tab Datasets palette.
Dataset_Inspect (Inspect)	Dataset	View a dataset object and read the variable values in the dataset. *Implicit:* List
Dataset_Modify (Modify)	Dataset	Create, Edit, and Delete the dataset object. *Implicit:* Inspect, Read, List
Operations_Resources (Resources)	Operations	Open the Operations tab Resources palette.
Resources_Control (Control)	Resources	■ Lock unlock, take, return, or add a parameter to a resource. ■ Add or remove a resource unit. *Implicit:* Read, List
Operations_User_Requests (User Requests)	Operations	Open the Operations tab User Requests palette.
Operations_Content_Packages (Content Packages)	Operations	Open the Operations tab Content Packages palette.
Operations_Task_List (Task List)	Operations	■ Use the Operations tab Task List link and view tasks for yourself, your group, or any group. ■ Access your tasks from the Home tab.
StartRequestForm_Dequeue (Dequeue)	Start Request Form	Dequeue a process that a start request form put in the queue. *Implicit:* Start, List
StartRequestForm_Start (Start)	Start Request Form	Start a task that a start request form defines. *Implicit:* List

Action Key (Localized Name)	Resource Class for Policy	Permissions
Execute	TouchPoint Security	Run scripts or programs in operators. The product derives the impacted operators from specified operator categories. The impact occurs when the target is a specified touchpoint in a specified environment.

Reports Tab

The following table lists the action relevant to using the Reports tab.

Action Key (Localized Name)	Resource Class for Policy	Permissions
Reports_User (Reports User)	Reports	■ Open the Reports tab ■ Upload custom reports ■ View or delete predefined, shared, or private reports.

Configuration Tab and Palettes

The following table lists the actions that impact permissions on the Configuration tab. To view the Configuration Browser on the Configuration tab, you must have the Client_Configuration_User permission. For more information, see Permissions Dependencies (see page 106).

Action Key (Localized Name)	Resource Class for Policy	Permissions
Client_Configuration_User (View Configuration Browser)	Configuration Browser	View the Configuration tab Configuration Browser.
Environment_Configuration_Admin (Configuration Administrator)	Environment	■ Add New Group, Add Touchpoint, and Add Host Group in the Configuration Browser. ■ Edit the configuration at the environment level, including security, properties, operator categories, custom operator groups, and triggers.

Action Key (Localized Name)	Resource Class for Policy	Permissions
Domain_Admin (Administrator)	Domain	■ In the Configuration Browser palette, lock or unlock the Domain, add Environment, invoke Bulk Agent Removal, and invoke Bulk Touchpoint Removal. ■ Edit the configuration at the Domain level, including security, properties, operator categories, custom operator groups, and triggers. ■ Update the Orchestrator Resources folder and the Agent Resources folder contents in the Manage User Resources palette.
Configuration_User_Resources (User Resources)	Configuration Browser	Open the Configuration tab Manage User Resources palette and update the User Resources folder contents.
Configuration_Installations (Installations)	Configuration Browser	Open the Configuration tab Installation palette and start installing an agent, Orchestrator, or cluster node of an Orchestrator.

More information:

Permissions Dependencies (see page 106)

Permissions on Automation Objects

The following table describes permissions that you can grant on various automation objects through custom CA EEM policies. You can grant permissions to any application groups in CA EEM. Access to automation objects and folders on any Orchestrator in an environment requires User or Content Administrator access in the Environment policy. Environment is the parent resource class to the resource classes for automation objects.

Some permissions implicitly include other permissions. When you select a specific permission, implicit permissions are selected simultaneously. When you grant an explicit permission, you implicitly grant all other permissions beneath it in the permissions hierarchy.

When you deny an implicit permission, you deny all other permissions above it in the permissions hierarchy. List permission is implicit to every other permission and dependent on no other permissions. You can deny all permissions for a group on a folder with a custom Object policy that denies permissions with List. Revoking List permission revokes every other permission on an automation object. However, revoking other permissions never revokes List permission.

Action Key (Localized Name)	**Resource Class for Policy**	**Permissions**
Object_Admin (Admin)	Object	Create a folder or create any automation object **Implicit:** Delete, Edit, Read, List
Object_Delete (Delete)	Object	Delete a folder or delete an automation object added to a folder. **Implicit:** Edit, Read, List
Object_Edit (Edit)	Object	Edit a folder or edit an automation object in a folder. **Implicit:** Read, List
Object_Read (Read)	Object	Navigate a folder path and open any automation object in the corresponding designer or viewer. **Implicit:** List
Object_List (List)	Object	View a folder or view an automation object in the Library Browser. Define customized views of the library.
Environment_Library_Admin (Content Administrator)	Environment	Create, Delete, Edit, Read, and List all automation objects.

Action Key (Localized Name)	Resource Class for Policy	Permissions
Environment_Library_User (User)	Environment	View, export, and search automation objects if the access is set. **Note**: Implicitly inheritable by Resource Classes for automation objects
Agenda_Control (Control)	Agenda	Activate and deactivate a schedule on a touchpoint. **Implicit:** Read, List
Dataset_Modify (Modify)	Dataset	Create, Edit, and Delete the dataset object. **Implicit:** Inspect, Read, List
Dataset_Inspect (Inspect)	Dataset	View a dataset object and read values of variables in the dataset. **Implicit:** List
Process_Control (Control)	Process	Suspend, restart, resume, or abort instances of a process. **Implicit:** Start, Monitor, List
Process_Start (Start)	Process	Start an instance of a process. **Implicit:** Monitor, List
Process_Monitor (Monitor)	Process	Open a running instance of a process in the Process Designer, monitor progress, and set breakpoints. **Implicit:** List
Resources_Control (Control)	Resources	Lock, unlock, take, return, or add a parameter to a resource. Add or remove a resource unit. **Implicit:** Read, List
StartRequestForm_Dequeue (Dequeue)	Start Request Form	Dequeue a process that a start request form queued. **Implicit:** Start, List
StartRequestForm_Start (Start)	Start Request Form	Start a task that a start request form defined. **Implicit:** List
Execute	TouchPoint Security	Run scripts or programs in operators derived from specified operator categories that target specified touchpoints in a specified environment.

Action Key (Localized Name)	Resource Class for Policy	Permissions
Group_Config_Admin	Group Configuration	Define parameters for a custom operator group when defining a custom operator. **Follow these steps:** ■ Lock the custom operator group on the Group Configuration tab. ■ Add pages and variables. ■ Save the configuration. ■ Unlock the custom operator group. Unlock publishes the named custom operator group configuration. Publication makes the group configuration available on the Modules tab in the Configuration Browser at the Domain and environment levels.

More information:

Permissions Dependencies (see page 106)

Permissions Dependencies

The following table describes the dependent resource class action (permission) for each resource class action in the predefined CA EEM policies for CA Process Automation.

Consider the dependencies when you assign only custom groups (without PAMUsers) to user accounts.

As the table summarizes, you can assign an Action Key in a custom policy for a Resource Class to a custom group. If you create such a custom policy, assign that custom group to a Dependent Actions Key.

Action Key (Localized Name)	Resource Class for Custom Policy	Dependent Actions Key (Localized Name)
Console_Login (User)	Product User	
Reports_User (Reports User)	Reports	Console_Login (User)
Environment_Library_User (User)	Environment	Console_Login (User)

Action Key (Localized Name)	Resource Class for Custom Policy	Dependent Actions Key (Localized Name)
Environment_Library_Admin (Content Administrator)	Environment	Console_Login (User)
Environment_Configuration_Admin (Configuration Administrator)	Environment	Console_Login (User)
Domain_Admin (Administrator)	Domain	Console_Login (User)
Client_Configuration_User (View Configuration Browser)	Configuration Browser	Console_Login (User)
Configuration_User_Resources (User Resources)	Configuration Browser	■ Console_Login (User) ■ Client_Configuration_User (View Configuration Browser) ■ Domain_Admin (Administrator) for access to the Agent Resources and the Orchestrator Resources folders.
Configuration_Installations (Installations)	Configuration Browser	Console_Login (User)
LibraryBrowser_User (Library Browser User)	Library Browser	■ Console_Login (User) ■ Environment_Library_User (User) or Environment_Library_Admin (Content Administrator)
Operations_User_Requests (User Requests)	Operations	■ Console_Login (User) ■ Environment_Library_User (User) or Environment_Library_Admin (Content Administrator)
Operations_Process_Watch (Process Watch)	Operations	■ Console_Login (User) ■ Environment_Library_User (User) or Environment_Library_Admin (Content Administrator)
Operations_Task_List (Task List)	Operations	■ Console_Login (User) ■ Environment_Library_User (User) or Environment_Library_Admin (Content Administrator)
Operations_Schedules (Schedules)	Operations	■ Console_Login (User) ■ Environment_Library_User (User) or Environment_Library_Admin (Content Administrator)

Action Key (Localized Name)	Resource Class for Custom Policy	Dependent Actions Key (Localized Name)
Operations_Resources (Resources)	Operations	■ Console_Login (User) ■ Environment_Library_User (User) or Environment_Library_Admin (Content Administrator)
Operations_Datasets (Datasets)	Operations	■ Console_Login (User) ■ Environment_Library_User (User) or Environment_Library_Admin (Content Administrator)
Operations_Content Packages (Content Packages)	Operations	■ Console_Login (User) ■ Environment_Library_User (User) or Environment_Library_Admin (Content Administrator)
■ Object_List (List) ■ Object_Read (Read) ■ Object_Edit (Edit) ■ Object_Delete (Delete) ■ Object_Admin (Admin)	Object	■ Console_Login (User) ■ Environment_Library_User (User)
Agenda_Control (Control)	Agenda	■ Console_Login (User) ■ Environment_Library_User (User) ■ Object_List (List) with resource/*folder* **Note:** If the object is created in the root folder, Object_List is not necessary.

Action Key (Localized Name)	Resource Class for Custom Policy	Dependent Actions Key (Localized Name)
■ Dataset_Inspect (Inspect) ■ Dataset_Modify (Modify)	Dataset	■ Console_Login (User) ■ Environment_Library_User (User) ■ Object_List (List) with resource/*folder* **Note:** If the object is created in the root folder, Object_List is not necessary.
■ Process_Control (Control) ■ Process_Monitor (Monitor) ■ Process_Start (Start)	Process	■ Console_Login (User) ■ Environment_Library_User (User) ■ Object_List (List) with resource/*folder* **Note:** If the object is created in the root folder, Object_List is not necessary.
Resources_Control (Control)	Resources	■ Console_Login (User) ■ Environment_Library_User (User) ■ Object_List (List) with resource/*folder* **Note:** If the object is created in the root folder, Object_List is not necessary.
■ StartRequestForm_Start (Start) ■ StarRequestForm_Dequeue (Dequeue)	Start Request Form	■ Console_Login (User) ■ Environment_Library_User (User) ■ Object_List (List) with resource/*folder* **Note:** If the object is created in the root folder, Object_List is not necessary.
Execute	Touchpoint Security	■ Console_Login (User) ■ Environment_Library_User (User) ■ Object_List (List) with resource/*folder* **Note:** If the object is created in the root folder, Object_List is not necessary.
Group_Config_Admin	Group Configuration	■ Console_Login (User) ■ Environment_Library_User (User) ■ Object_List (List) with resource/*folder* ■ Object_Edit (Edit) with resource/*folder*

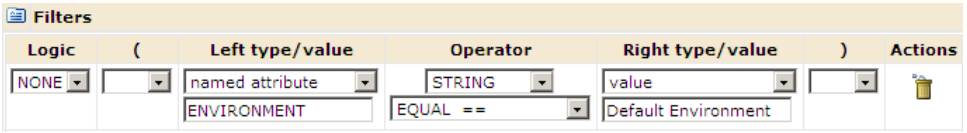
More information:

Permissions on Automation Objects (see page 104)
Permissions by Tab (see page 98)

Filters for Permissions

CA EEM defines permissions as Resource Class actions. You can, optionally, use filters to limit the actions that you allow a group or user. For example, you can scope permissions so that they apply to the assigned group in the configured environment only.

The following Filters example illustrates the use of ENVIRONMENT as the named attribute for the filter. Policies that are defined with the Access Policies type let you add filters.



The actions in the following table belong to policies based on the referenced resource class.

Action Key (Localized Name)	Resource Class for Policy	Named Attribute for Filter
Object_List (List) Object_Read (Read) Object_Edit (Edit) Object_Delete (Delete) Object_Admin (Admin)	Object	SECURITY_CONTEXT_ID SECURITY_CONTEXT_GRP ENVIRONMENT OBJECT_TYPE
Agenda_Control (Control)	Agenda	ENVIRONMENT
Dataset_Inspect (Inspect) Dataset_Modify (Modify)	Dataset	ENVIRONMENT
Process_Control (Control) Process_Monitor (Monitor) Process_Start (Start)	Process	SECURITY_CONTEXT_ID SECURITY_CONTEXT_GRP ENVIRONMENT
Resources_Control (Control)	Resources	ENVIRONMENT
StartRequestForm_Start (Start) StarRequestForm_Dequeue (Dequeue)	Start Request Form	ENVIRONMENT

Action Key (Localized Name)	Resource Class for Policy	Named Attribute for Filter
Execute	TouchPoint Security	ENVIRONMENT TOUCHPOINT

How to Transition Roles Used in Active Directory to CA EEM

If you previously used Microsoft Active Directory (AD) or LDAP for authentication and authorization, you can transition to CA EEM with any of the following approaches:

- Create user accounts. Assign one of the default groups to each account.

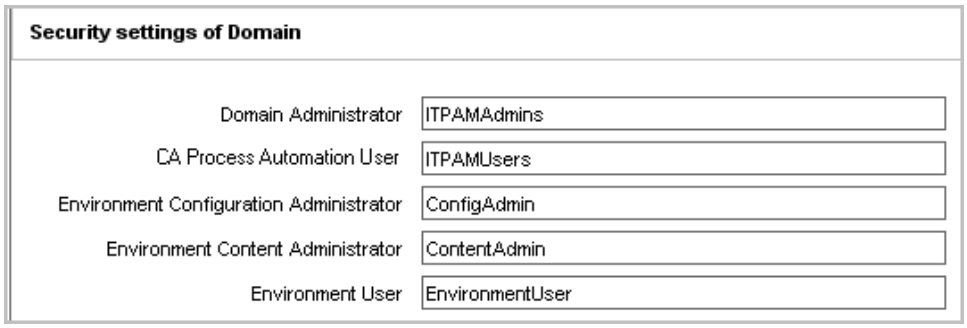
  Note: See Review Permissions for Default Groups (see page 47).

- Point to AD as an external user store.

  Note: See Manage Access for Referenced User Accounts (see page 60). See Integrate Active Directory with CA EEM.

- Create custom groups that reflect your AD roles. Add these groups to CA EEM policies and grant the required permissions. Create user accounts. Assign one of your custom groups to each account. This section addresses this approach.

Assume that you defined Security settings of the Domain in Active Directory with these groups: ITPAMAdmins, ITPAMUsers, ConfigAdmin, ContentAdmin, and EnvironmentUser.



To migrate role-based access from Active Directory to CA EEM manually, use the following process.

Follow these steps:

1. Migrate role-based access for users in the Domain Administrator role.

   See Create User Accounts for Administrators.

2. Migrate role-based access for users in the CA Process Automation User role.

   See Create User Accounts with Basic Access (see page 56).

3. Migrate role-based access for users in the Environment Configuration Administrator role as follows:
   a. Create the custom ConfigAdmin group (see page 112).
   b. Grant permissions to the custom ConfigAdmin group (see page 113).
   c. Create user accounts for Environment Configuration Administrators (see page 114).
4. Migrate role-based access for users in the Environment Content Administrator role as follows:
   a. Create the custom ContentAdmin group (see page 114).
   b. Grant permissions to the custom ContentAdmin group (see page 115).
   c. Create user accounts for Environment Content Administrators (see page 115).
5. Migrate role-based access for users in the Environment User role.

   See Create User Accounts for Production Users.

Create the Custom ConfigAdmin Group

You can create a custom ConfigAdmin group for users in the Environment Configuration Administrator role.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Identities tab, click Groups, and click New Application Group.
3. Type **ConfigAdmin** as the name of the group, or type a name of your choice.
4. (Optional) Enter a description for the group.
5. Click Save.

   Note: Do not add an application group membership.
6. Click Close.

Grant Permissions to the Environment Configuration Administrators Group

You can grant permissions to the Environment Configuration Administrators custom group by adding this group to selected policies and selecting the required actions.

Follow these steps:

1. Log in to the CA Process Automation application in CA EEM.
2. Click the Manage Access Policies tab.
3. Grant to the ConfigAdmin group the ability to log in to CA Process Automation and display the Home page.
    a. Click the Product User link under Access Policies.
    b. Click the PAM40 User Login Policy.
    c. Select Application Group for Type under Enter/Search Identities, click Search Identities, and click Search.
    d. Select the custom group, ConfigAdmin, and click the down arrow.
    e. Select Console_Login for the new identity.
    f. Click Save.
4. Grant to the ConfigAdmins group the permissions to lock an environment and take any action that requires the environment to be locked.
    a. Click the Environment link under Access Policies.
    b. Click the PAM40 Environment Policy link in the Policy Table.
    c. Add the Identities. Search for groups. Specify Application Group for type, click Search Identities, and click Search.
    d. Select ConfigAdmin and click the down arrow.
    e. Select Environment_Configuration_Admin (Configuration Administrator) permission.
    f. Click Save. Click Close.
5. Grant to the ConfigAdmin group the permissions to access the Configuration tab and install Orchestrators and agents.
    a. Click Configuration Browser.
    b. Click PAM40 Configuration Policy.
    c. Search for ConfigAdmin and add the group to Selected Identities.
    d. Select Client_Configuration_User (View Configuration Browser) and Configuration_Installations.
6. Click Close.

Create User Accounts for Environment Configuration Administrators

You can create user accounts for individuals performing the role of Environment Configuration Administrator.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Identities tab.
3. Click New User.
4. Enter the user ID as the Name.
5. Click Add Application User Details.
6. Select the ConfigAdmin group and click the right arrow.
7. Enter Global User details as needed.
8. Enter a temporary password twice in the Authentication section.
9. Click Save.
10. Repeat this procedure for each user in the Environment Configuration Administrator role.

Create the Custom ContentAdmin Group

You can create a custom group in CA EEM called ContentAdmin for users in the Environment Content Administrator role. You can base this group on the Default Designer group to automatically get the permissions assigned to the Designer group.

Follow these steps:

1. Log in to the CA Process Automation application in CA EEM.
2. Click the Manage Identities tab.
3. Click Groups.
4. Click New Application Group.
5. Enter ContentAdmin as the name of the group and optionally a description
6. Select Designers under Available User Groups and click the right arrow to move Designers to Selected User Groups.
7. Click Save.
8. Click Close.

Grant Permissions to the Custom ContentAdmin Group

You can grant permissions to the custom Environment Content Administrator group by adding this group to default policies and selecting the required permissions. Many of the policy permissions are already granted to ContentAdmin because you based this group on the default Designers group. You add the administrator rights to the folders, automation objects, and editors in the Library tab.

Follow these steps:

1. Log in to the CA Process Automation application in CA EEM.
2. Click the Manage Access Policies tab.
3. Click the Environment link under Access Policies.
4. Click the PAM40 Environment Policy link in the Policy Table.
5. Add the Identities. Search for groups. Specify Application Group for type, click Search Identities, and click Search.
6. Select ContentAdmin and click the down arrow.
7. Select Environment_Library_Admin (Content Administrator) permissions.
8. Click Save.
9. Click Close.

Create User Accounts for Environment Content Administrators

You can create user accounts for individuals performing the role of Environment Content Administrator.

Follow these steps:

1. Browse to CA EEM and log in. (see page 45)
2. Click the Manage Identities tab.
3. Click New User.
4. Enter the user ID as the Name.
5. Click Add Application User Details.
6. Select the ContentAdmin group and click the right arrow.
7. Enter Global User details as needed.
8. Enter a temporary password twice in the Authentication section.
9. Click Save.
10. Repeat this procedure for each user in the Environment Content Administrator role.

Touchpoint Security with CA EEM

The purpose of Touchpoint Security is to limit access to business-critical hosts or hosts with highly sensitive information to a group of high-privileged users.

This section applies only if you have enabled Touchpoint Security for touchpoints in one or more environments.

- To determine whether Touchpoint Security is enabled on touchpoints mapped to candidate hosts, review the Touchpoint Security configuration in the touchpoint properties. If it is marked Inherit from Environment, consider changing the configuration to Enabled.
- To determine whether a specific touchpoint mapped to a host that needs protection is protected, review the filters in the Touchpoint Security policies.

More information:

Configure Domain Properties (see page 140)
Configure Environment Properties (see page 153)
Configure Properties for the Design Touchpoint (see page 226)
Configure Orchestrator Touchpoint Properties (see page 168)
Approach to Configuring Touchpoint Security (see page 143)

Grant Users CA EEM Access to Define Touchpoint Security Policies

By default, the EiamAdmin user is the only user who can log in to CA EEM. If you employ a policy-based Touchpoint Security approach, you can authorize certain users to create Touchpoint Security policies in CA EEM. Authorize content designers who design processes with operators that execute on touchpoints mapped to hosts that have high business value. Such touchpoints can be protected through Touchpoint Security policies that specify the users who are authorized to execute these operators.

To grant specified policy designers CA EEM access and authorization to create policies with the Touchpoint Security resource class

1. Log in to the CA Process Automation application in CA EEM.
2. Click the Manage Access Policies tab.
3. Click New Scoping Policy.

4. Complete the General section as follows:

   Name

   Specifies the name of this scoping policy. For example, Users Creating Touchpoint Security Policies.

   Description

   (Optional) Provides a short description. For example, Enables specified users to create custom policies only with the Touchpoint Security resource class.

   Calendar and Resource Class Name

   Skip the Calendar option and accept the default entry SafeObject for Resource Class Name.

   Type

   Specify Access Control List.

   Note: A message appears that changing policy type resets some of the filters. Click OK.

5. For Identities, add the names of all of the users who design processes to which Touchpoint Security applies. Users added to this policy are granted login access to CA EEM and the ability to create Touchpoint Security policies. A Touchpoint Security policy specifies the users to authorize to execute operators from a given operator category on a specified Touchpoint.

   Note: If you want to test this policy, create a user with the default user group and add that user name here. After you save this policy, log in to CA EEM with your test user name. Notice that the only thing you can do in CA EEM is create a policy with the Touchpoint resource class.

   a. Accept User as Type or select another value.

   b. Click the Search Identities link.

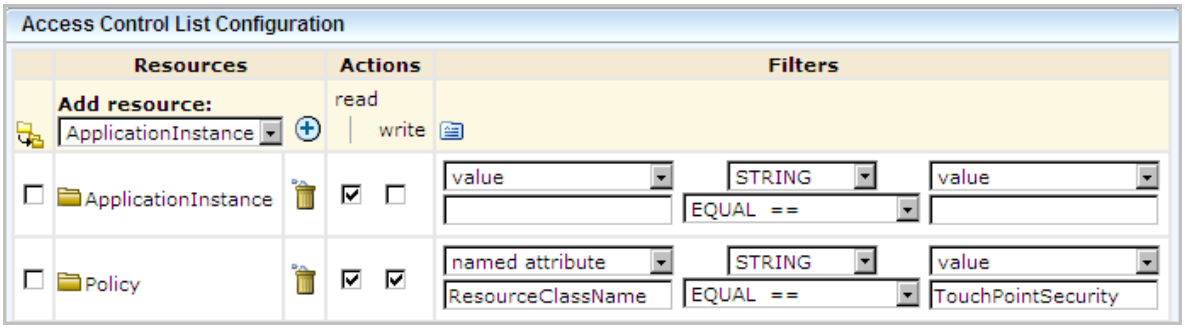
   c. Enter search criteria that includes the planned user or group and click Search.\

   d. Select a user or group from the displayed list of available identities and click the right arrow.

      The selected user or group appears in the Selected Identities list.

   e. Repeat this process for each user to whom you want to authorize to create Touchpoint Security Policies.

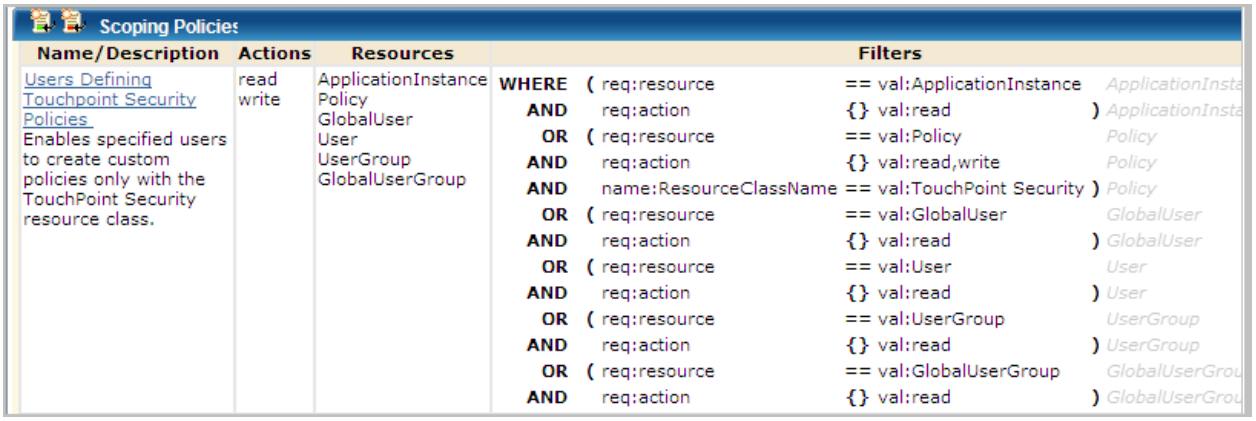
6. Configure the Access Control List as follows:
   a. Select each of the following resources from the drop-down list and click Add to add them to the list.
      - ApplicationInstance
      - Policy
      - User
      - GlobalUser
      - UserGroup
      - GlobalUserGroup
   b. Click read for all resources. Click write for Policy
   c. Click Filters.
   d. For Policy, select named attribute from the first drop-down list. In the field under named attribute, enter ResourceClassName. In the value field after EQUAL, enter TouchPointSecurity. Do not enter a space between TouchPoint and Security.



   e. Leave the rest of the fields on the filters page as is.

7. Click Save.
8. Verify that the Access Control List Configuration matches the following example exactly. The system adds a space between TouchPoint and Security.

9. Verify that your policy resembles the following example. In the example, the missing columns indicate that ResourceClassName is SafeObject, the Options value is Explicit Grant, and Identities is your list of users. These are users who design processes for Touchpoint Security and create an associated policy.



About Touchpoint Security

Touchpoint Security lets you secure touchpoints associated with business-critical hosts and hosts that contain sensitive data. You can secure such touchpoints against unauthorized access. You can create Touchpoint policies that specify selected users or a high-privileged group as the only identities that can execute an operator on that target. Policies specify identities that are authorized to execute certain operators on specified touchpoints. The operators that run programs and scripts are contained in specified operator categories.

In summary, CA EEM Touchpoint Security policies authorize specified identities to execute scripts in operators from specified categories on specified touchpoints in a specified environment.

Consider the following example snippet of a simple Touchpoint Security policy.

Identities	Actions	Resources	Filters
ug:High-PrivilegedUsers	[All Actions]	✓ Regex Compare Network Utilities Module Process Module File* Module	**WHERE** (name:Environment == val:Production **AND** (name:Touchpoint == val:SensitiveHostTP1 **OR** name:Touchpoint == val:SensitiveHostTP2 **OR** name:Touchpoint == val:SensitiveHostTP3))

The example is a portion of a policy. The policy allows only users in the High-PrivilegedUsers group to execute any operator from specified categories on specified touchpoints in the Production environment. The example touchpoints are named SensitiveHostTP1, 2, and 3. Specified Access Control IDs include the Network Utilities module and the Process module (for Command Execution),. File* Module includes both File module for File Management and the File Transfer module.

Note: See Identify the Access Control IDs to Add as Resources (see page 123).

A process with an operator target protected by a Touchpoint Security policy can finish successfully only it runs as an authorized user. The user under which the process runs is specified as an Identity in the policy. The policy identifies users by name or group membership, operators by the access control IDs associated with source categories, and touchpoints by name, environment, or both.

Touchpoint Security policies secure access to individual target hosts by controlling who executes operators on a specific touchpoint or host group. A process instance runs on behalf of a user. When the process executes an operator on a touchpoint or host group specified in a CA EEM Touchpoint Security policy, CA EEM attempts to authorize that user. CA EEM verifies that the user is specified as an Identity in a Touchpoint Security policy for that touchpoint. If the process instance is running on behalf of an unauthorized user, then the operator fails.

You specify sensitive hosts as touchpoints, proxy touchpoints, or host groups.

You can limit access to specified hosts to high-privileged users. You can grant access to a specified user or group that has been granted the following prerequisite access:

- Granted Console_Login (User) action in the PAM40 User Login Policy.
- Granted Environment_Library_User (User) action in the PAM40 Environment Policy.

Use Cases: When Touchpoint Security is Necessary

Touchpoint security is necessary in the following cases:

- A host in your environment that can be an operator target contains sensitive information, such as social security numbers, credit card numbers, or health details. You want to limit access to this sensitive process to a single person or a small high-privileged group.

  The target can be any of the following hosts:

  - The host with an agent that is associated with a touchpoint.
  - The host with an agent that is associated with a proxy touchpoint with an SSH connection to a remote host.
  - The host with an agent that is associated with a host group that references and has a connection to remote hosts.
- When you are running an agent on a host as the root user (UNIX), the administrator (Windows), or some user with specific rights. Suppose that you have a reason to run all scripts and programs on that agent under the same identity as the agent itself. That is, you do not want to switch to another user that requires credentials. To prevent a security risk, you can restrict low-privileged users from running scripts under the same identity as the agent, such as the root user.

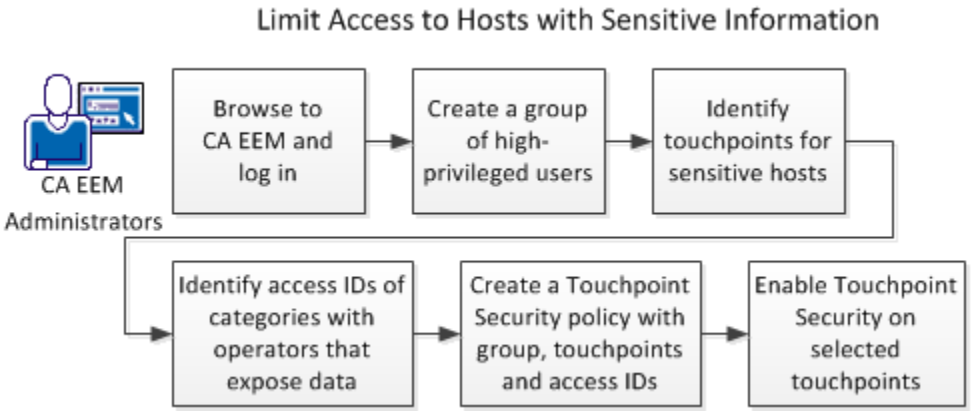
- When you are leveraging host groups that define default operating system credentials for running Command Execution operators on entire subnets. Suppose that you have a reason to run all scripts and programs on that host group using the operating system credentials. You want to prevent a security risk by disallowing low-privileges users from creating and running any script using operating system credentials.
- Users who run a process can select operator targets at runtime for operators that have a variable in the target field. An operator target is typically a touchpoint, although it can be a proxy touchpoint, an FQDN, or an IP address that a host group references. This flexible design lets any user who is authorized to run the process select a target at runtime.

  A security issue occurs when an available touchpoint requires limitations to its access. Consider the case where an operator can successfully run on two different touchpoints, each of which represents a Service Desk application. One touchpoint represents a Service Desk that is designed for general access while the other touchpoint is designed for administrators only. Touchpoint Security permits only administrators to run this example operator on the touchpoint that is designed for administrators. Touchpoint Security policies in CA EEM limit access.

Touchpoint Security is also useful for process designers. During process development, different designers install an agent on their personal hosts and create touchpoints for their agents. They typically do not want other users running operators on their local hosts. Touchpoint Security can provide this protection. When Touchpoint Security is configured to be active, authorization to run each operator on the selected target is verified at run time. Policy enforcement restricts users who run a process to running operators only on touchpoints for which they are authorized.

Limit Access to Hosts with Sensitive Information

Touchpoint Security answers the need to limit access to business-critical hosts and hosts on which you store sensitive information. The following illustration suggests an approach to accomplish this security goal.



Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Create a group of high-privileged users.

   See Create the Custom ContentAdmin Group (see page 114).
3. Identify the touchpoints that are associated with sensitive hosts.

   See View the Touchpoints and Host Groups for a Selected Agent (see page 201).
4. Identify the categories with operators that expose data.
5. Identify the Access Control IDs associated with the categories.
   - See Example: Secure Critical Touchpoint (see page 126)s for Access Control IDs to consider.
   - Find the descriptions of each category in the section Operator Categories and Where Operators Run (see page 311).
   - See the *Content Designers Reference* for operator descriptions.
6. Create a Touchpoint Security policy with this group, operator categories, and touchpoints.

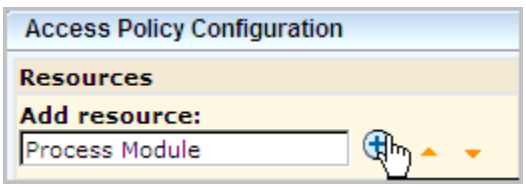
   See Create a Touchpoint Security Policy (see page 125).
7. Enable Touchpoint Security on selected touchpoints.
   - See Configure Touchpoint Properties (see page 226).
   - See Configure Proxy Touchpoint Properties (see page 246).
   - See Configure Host Group Properties (see page 253).

More information:

Approach to Configuring Touchpoint Security (see page 143)

Identify the Access Control IDs To Add as Resources

When you create a Touchpoint Security policy, you do not directly identify the operators that act on touchpoints you want to secure. Instead, you identify the categories to which those operators belong. You identify the categories, not by name, but by Access Control ID.



Not all categories contain operators that could compromise the security of a host with sensitive information. Evaluate the impact of operators before adding resources.

You can identify the Access Control ID to add as a resource to a Touchpoint Security policy.

Follow these steps:

1. Browse to CA Process Automation and log in (see page 18).
2. Click the Configuration tab.
3. Select an agent from the Agents node and then select the Modules tab.
4. Note the names as they appear in the Access Control ID column.

Properties | Modules | Associated Tou... | Audit trails

Name ▲	Enable/Disable	Access Control ID
Catalyst		Catalyst Module
Command Execution	Inherit from Environment	Process Module
Databases	Inherit from Environment	JDBC Module
Date-Time		Date-Time Module
Directory Services	Inherit from Environment	LDAP Module
Email	Inherit from Environment	Mail Module
File Management	Inherit from Environment	File Module
File Transfer	Inherit from Environment	File Transfer Module
Java Management	Inherit from Environment	JMX Module
Network Utilities	Inherit from Environment	Network Utilities Module
Process Control		Workflow Module
Utilities	Inherit from Environment	Utilities Module
Web Services	Inherit from Environment	SOAP Module

Important! The Access Control ID column lists module names. Refer to this list when you enter selected module names in the Resources field in a Touchpoint Security policy.

Create a Touchpoint Security Policy

Running a process runs specific operators on specified targets in a specified sequence. A custom Touchpoint Security policy grants permission to specified users or groups to run specified operators on specified targets. The CA EEM administrators can create a touchpoint security policy.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Access Policies tab.
3. Click the New Access Policy button for Touchpoint Security under Access policies.
4. On the new access policy form for the Touchpoint Security resource class, enter a name for the custom Touchpoint Security policy.

   The Enter/Search Identities section lets you specify the target user or group.
5. Select the type of target to which to grant access:
   - Select User if the target is a global user.
   - Select Global Group if the target is a group from a references user store.
   - Select Application Group if the target is a custom group you defined or is a default group.
6. Click Search Identities.
7. Select the identities to which this policy applies, and then click the down arrow.

   The Selected Identities list displays your selection.
8. Select the Execute action.
9. In the Add resource field, type the Access Control ID for the Source Operator Category that includes the operators to which this policy applies. For example:
   - Type **Process Module** for the Command Execution operator category.
   - Type **File Module** for the File Management operator category.
   - Type **File Transfer Module** for the File Transfer operator category.
   - Type **Network Utilities Module** for the Network Utilities operator category.

   You can enter regular expressions to cover the appropriate operator categories and then select Treat resource names as regular expressions. For example, an entry of File* would include operators in the File Management and File Transfer categories.
10. Click Add.

11. Add a filter that specifies the environment that contains the policy targets:
    - Set the named attribute to Environment.
    - Set the STRING operator to EQUAL.
    - Set the value to the *environment_name*.
12. Add other filters that specify the targets by touchpoint name:
    - Set the named attribute to Touchpoint.
    - Set the STRING operator to EQUAL.
    - Set the value to the *touchpoint_name*.
13. Click Save.

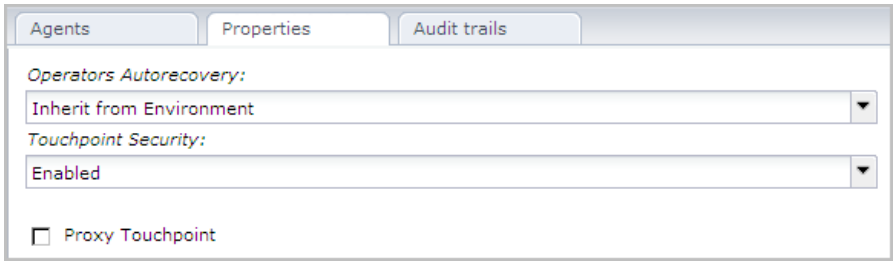
    If the Touchpoint Security policies are configured for enforcement, the product evaluates and enforces the policy.

Example: Secure Critical Touchpoints

Touchpoint security ensures that the ability to run operators on business-critical hosts is limited to a small group of high-privileged users. The easiest way to protect sensitive hosts is to create one Touchpoint Security policy and list each of the associated touchpoints in a filter. Then enable Touchpoint Security on the properties setting for each of these touchpoints.

Example: Touchpoint Security Configuration for a Critical Touchpoint

The following example shows the properties of a selected touchpoint. When Touchpoint Security is set to Enabled, the process evaluates each attempt to run an operator on this touchpoint against the Touchpoint Security policies.



Example: Touchpoint Security Policy for Critical Touchpoints

To ensure that only high-privileged users run operators on sensitive hosts in your production environment, create one Touchpoint Security policy. In the Touchpoint Security policy, add the Access Control ID associated with each category containing operators that could pose a risk. Add a filter for your environment. Add a filter for each touchpoint that references sensitive hosts.

Consider the following example Global Touchpoint Security Policy. The example policy grants the High-Privileged Users group authorization to run scripts or programs using operators in five categories on high-risk touchpoints. Access Control IDs represent the five categories. This policy applies to the specified touchpoints only in the Production environment.

Access Policies - "TouchPoint Security"

Name/Description	ResourceClassName	Options
Global Touchpoint Security Policy Authorizes High-Privileged group to execute risk posing Operators on Sensitive Hosts in Production.	TouchPointSecurity	Explicit Grant

Identities	Actions	Resources	Filters
ug:High-PrivilegedUsers	Execute	Process Module File Module File Transfer Module JMX Module Network Utilities Module	WHERE name:Environment == val:Production AND name:Touchpoint == val:TP-SensitiveHost1 OR name:Touchpoint == val:TP-SensitiveHost2 OR name:Touchpoint == val:TP-SensitiveHost3 OR name:Touchpoint == val:TP-SensitiveHost4 OR name:Touchpoint == val:TP-SensitiveHostn

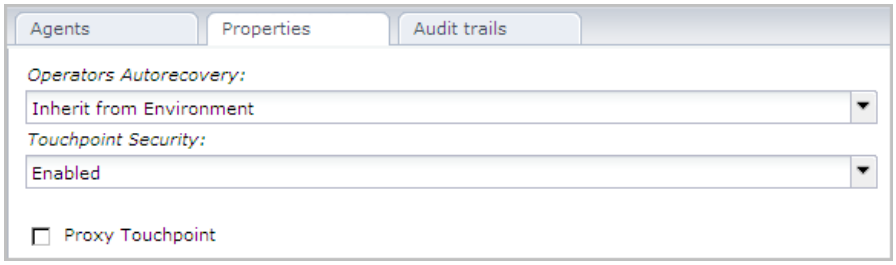
Example: Secure the Touchpoint for My Host

Suppose you install an agent on your host and do not want anyone but you to execute operators on your host. To use Touchpoint Security to protect a host that is critical to you, consider performing the needed tasks in the following sequence.

1. Install an agent on the host.
2. Associate a touchpoint in a specified environment with that host.
3. Create a Touchpoint Security policy that lists yourself as the Identity. Add the Access Control ID for each category with operators that can run on touchpoints associated with agents.
4. Configure Touchpoint Security as Enabled in Touchpoint Properties for that host.

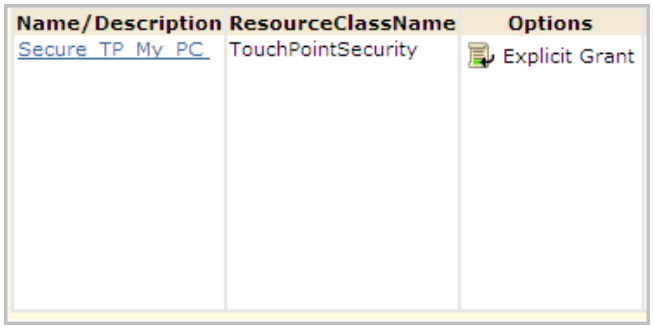
Example: Set Touchpoint Security to Enabled on My PC Touchpoint

The Touchpoint Security parameter for the selected Touchpoint, MyPC-TP, is set to Enabled.



Example: Create a Touchpoint Security Policy that Allows only Me to Execute Operators on My PC Touchpoint

In the following example, assume that the protected host belongs to a user named MyPCowner. Notice that MyPCowner is the only Identity authorized to execute operators on the touchpoint, MyPC-TP. Here, the Access Control IDs are associated with all categories with operators that can execute on an agent host. In this case, the references include categories of operators that do not make changes to the host. The idea in this example is that the user wants no access to the host associated with the MyPC-TP touchpoint by any outside user. Only MyPCowner can run processes on MyPC-TP when Touchpoint Security is enabled.



Name/Description	ResourceClassName	Options
Secure_TP_My_PC	TouchPointSecurity	Explicit Grant

The touchpoint name is specified as the value in the filter.

Identities	Actions	Resources	Filters
MyPCowner	Execute	Process Module JDBC Module LDAP Module Mail Module File Module File Transfer Module JMX Module Network Utilities Module Utilities Module SOAP Module	**WHERE** name:Environment == val:Test **AND** name:Touchpoint == val:MyPC-TP

Authorizing Runtime Actions with CA EEM

CA Process Automation provides fine-grained access control on operations and user actions on specific automation objects such as processes, datasets, calendars, and schedules. Control includes traditional read/write rights and rights to launch a process and monitor its instances. Access rights are enforced at all external interfaces, including the CA Process Automation UI and Web services. In addition, CA Process Automation provides ways to secure operations on target hosts so that only authorized users can execute them.

To limit who can perform any of the following runtime actions, create a CA EEM policy and specify the users or group to authorize.

- Execute scripts or programs within operators derived from specified categories that target specified touchpoints in a specified environment.
- Control a schedule, including activate and deactivate.
- Inspect or modify a dataset.
- Control a process instance, including suspend, restart, resume and abort.
- Control a resource, including lock, unlock, take, return, or add a variable to a resource. Add or remove a resource unit.
- Dequeue or start a start request form.

Additionally, you can create a policy that authorizes read/write rights on any other automation object.

More information:

Permissions on Automation Objects (see page 104)
Permissions Dependencies (see page 106)
Filters for Permissions (see page 110)

Change Ownership for Automation Objects

The user who creates an automation object or folder is, by default, the owner. The owner has full control of the automation object or folder. An owner can switch the ownership to another CA Process Automation user.

Note: The CA EEM Environment_Content_Administrator permission grants full control of all automation objects and folders. All administrators who belong to the PAMAdmins group have this permission.

If you enable Runtime Security, then only the process owner (or an administrator) can start that process.

Follow these steps:

1. Click the Library tab.
2. Select one or more objects including folders.
3. Click the Set Owner toolbar button.
4. In the Available Users list, select the user account to set as the new owner. Use search to find matching user accounts.
5. Click Save and Close.

Chapter 5: Administer the CA Process Automation Domain

In CA Process Automation, the Domain encompasses the entire system. Domain administration includes all tasks performed only by an administrator with Domain Administrator rights. Tasks include adding environments, removing unused agents and touchpoints in bulk, and configuring security, properties, operator categories, and triggers at the Domain level. This chapter is devoted to only tasks performed during the initial setup of a freshly installed CA Process Automation. Subsequent chapters address tasks that are typically performed during content development.

This section contains the following topics:

Lock the Domain

Administrators can lock the Domain. A lock protects the Domain from simultaneous updates by multiple users. Before making any configuration change at the Domain level, lock the Domain.

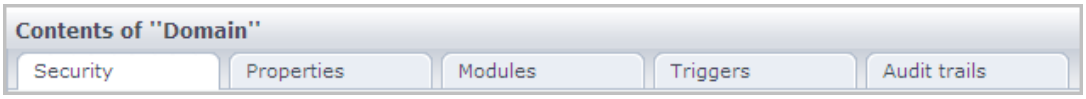
Follow these steps:

1. Click the Configuration tab.
2. Select Domain on the Configuration Browser palette and click Lock.

When you complete configuration changes, select Domain and click Unlock.

Configure the Contents of the Domain

When you select Domain in the Configuration Browser, the following tabs appear under Contents of "Domain":



- Security

  See Configure CA EEM Security Settings for the Domain (see page 133).

- Properties

  See Configure Domain Properties (see page 140).

- Modules

  See Configuring Operator Categories (see page 270). This topic is followed by the configuration procedure for each operator category. A description of each category precedes each configuration procedure.

- Triggers

  See How to Configure and Use Triggers (see page 314). This topic is followed by configuration details for each trigger type.

- Audit Trails

  See View the Audit Trail for the Domain (see page 335).

More information:

Maintaining the Domain (see page 381)

About Configuration Inheritance

Configuration at the Domain level includes the following types of settings:

- Security
- Properties
- Operator categories
- Triggers

Descendant objects of the Domain include the Default Environment, user-defined environments, the Domain Orchestrator, and agents. Descendant objects of a given environment include user-defined Orchestrators, touchpoints including proxy touchpoints, and host groups.

Certain settings configured at the Domain level are, by default, inherited by all or specific descendant objects within the Domain. For example, all environments can inherit operator category settings from the Domain. Orchestrators can inherit operator category settings from their environment.

Because agents can operate across environments, inheritance can be from directly from the Domain or from the environment, depending on the environment configuration. Operator category settings can be overridden at the agent level. Agents inherit the heartbeat frequency property setting directly from the Domain.

Typically, configurations are inherited by default. Triggers are an exception. Trigger configurations are disabled by default at lower levels, but can be inherited after being enabled.

Configure CA EEM Security Settings for the Domain

Most of the CA EEM security settings are established during the Domain Orchestrator installation. One CA EEM instance manages security for the CA Process Automation Domain. Therefore, these same settings apply to all environments in the Domain and to all Orchestrators within all environments. You can change the read-only settings by reinstalling the Domain Orchestrator.

Follow these steps:

1. Click the Configuration tab.

   The Security tab displays.

2. Examine the settings that were created at installation. For example, the EEM Application Name value is the value that you must enter for Application in the following cases:

   - When you log in to CA EEM to create user accounts.
   - When you assign default groups to new or referenced users.

3. Examine the CA EEM Cache Update Interval value.

   This value expresses the interval (in seconds) between CA EEM cache updates. The CA EEM cache contains current CA Process Automation user account, group, and policy settings. When CA EEM updates the cache, it sends CA Process Automation the contents of the refreshed cache. The default value, which optimizes the system performance, is 1800 seconds (30 minutes).

   - The default value is adequate after all users are configured in CA EEM.
   - To make this task go more quickly, reduce the update interval to the minimum (60 seconds) while you test and refine custom policies. Consider reducing the interval at the environment level for the environment on which you test.

4. Examine the Default Active Directory Domain value, if set.

   This value is set only if CA EEM is configured to use an external user store and Multiple Microsoft Active Directory Domains is selected. CA Process Automation users referenced in the AD domain specified here can log in with an unadorned user name. CA Process Automation users referenced in other selected AD domains are authenticated with their principal names (that is, *domain_name**user_name*). The same difference in naming conventions extends to how user identities are referenced in the main pane of the Library tab.

5. To reset either of the editable values:

   a. Select the Domain node and click Lock.

   b. Select a new value.

   c. Click Save.

   d. Select the Domain node and click Unlock.

   If you reduced the CA EEM Cache Update Interval, consider suppressing the CA Process Automation permissions cache. See Control Caches of CA EEM Updates (see page 76).

More information:

Control Caches of CA EEM Updates (see page 76)
Manage Certificates (see page 384)
Start the Orchestrator (see page 187)

Change the CA EEM FIPS Mode Security Setting

During installation, the CA EEM FIPS mode property is set to on or off. This setting determines the algorithms that are used to encrypt data that is transferred between CA EEM and CA Process Automation. When FIPS mode is on, the algorithms are compatible with FIPS 140-2. When CA Process Automation is installed with an CA EEM configured with FIPS Mode set to on, the FIPS-compliant certificate setting is displayed as selected.

Important! The FIPS setting for CA Process Automation must match the FIPS setting for CA EEM. If FIPS-mode is used by CA EEM, CA Process Automation must use FIPS-compliant certificates.

You can change the FIPS-compliant certificate security setting at the following levels:

- Domain
- Environments
- Orchestrators

Regardless of the level where the FIPS-compliant certificate setting is changed, it impacts the entire Domain. The Domain has one CA EEM. The FIPS-compliant certificate setting must reflect the CA EEM FIPS Mode setting and an iGateway file setting.

Important! Confer with your Domain Administrator before changing any CA EEM security setting. Security settings have widespread impact.

Follow these steps:

1. Obtain the EEM Certificate password from the installer.
2. Shut down CA Process Automation on all Orchestrators except the Domain Orchestrator, if applicable.
3. Log on to the server where the CA Process Automation Domain Orchestrator is installed and do the following;
   a. Shut down CA Process Automation.
   b. Stop the Orchestrator service. For example, from the Windows Start menu, select CA, CA Process Automation 4.0, Stop Orchestrator Service.
4. Log on to the server where CA EEM is installed and do the following:
   a. Shut down CA EEM.
   b. Stop the CA iTechnology iGateway service.

5. Navigate to the ...\CA\SharedComponents\iTechnology folder.
6. Change the FIPS mode setting in the igateway.conf file.
   a. Open igateway.conf for edit. For example, right-click igateway.conf and select Edit with Notepad++.
   b. Locate the line with the FIPSMode setting. For example:

      ```
      Line 4: <FIPSMode>off</FIPSMode>
      ```

   c. Change the value from off to on or from on to off.
   d. Save the file and close it.
7. Run the iGateway Certificate Utility (igwCertUtil) to convert the CA EEM certificate types as follows:
   - If you are changing CA EEM FIPS mode to on (changing a cleared check box to a selected check box), do the following:
     - Create a pem certificate type, PAM.cer, and PAM.key.
     - Replace the PAM.p12 certificate with the pem certificate type.
   - If you are changing CA EEM FIPS mode to off (changing a selected check box to a cleared check box), replace PAM.cer and PAM.key with PAM.p12 and a password.

     Note: For details, see Examples of iGateway Certificate Utility Use (see page 138).
8. Restart the iGateway service.
9. Restart CA EEM with the appropriate FIPS Mode setting.
10. Restart the Orchestrator service on the server with the Domain Orchestrator.
    - Stop the Orchestrator (see page 186).
    - Start the Orchestrator (see page 187).

11. Log in to CA Process Automation and view the FIPS-compliant certificate security setting and related settings as follows:
    a. Log in to CA Process Automation and click the Configuration tab.
    b. Navigate to the level where you want to implement the change and lock it (Domain, Environment, or Orchestrator).
    c. View the FIPS-compliant certificate check box.
    d. If your change was to turn on FIPS Mode for CA EEM, do the following:
        - Verify that FIPS-compliant certificate is selected. If it is not, select it.
        - Enter the key that you generated in the CA EEM Certificate Key field.
    e. If your change was to turn off FIPS Mode for CA EEM, do the following:
        - Verify that the FIPS-compliant certificate is cleared. If it is not, clear it.
        - Enter the password that you generated in the CA EEM Certificate Password field.
    f. Click Save.
    g. Unlock the level, that is, Domain, Environment from the Browser palette or Orchestrator from the Orchestrator palette.
12. Restart CA Process Automation on servers with Orchestrators that are not the Domain Orchestrator.

Examples of iGateway Certificate Utility Use

You can change the CA EEM FIPS Mode security setting from the setting configured at installation. Part of this change process involves using the iGateway Certificate Utility (igwCertUtil). You can find this file in ...\CA\SharedComponents\iTechnology\igwCertUtil.exe.

Note: For details, see Change the CA EEM FIPS Mode Security Setting (see page 135).

The iGateway Certificate Utility includes capabilities described by the following examples:

Example: Create a pem certificate type with PAM.cer and PAM.key files

The following igwCertUtil example creates a pem certificate with a .cer file and a .key file.

```
igwCertUtil -version 4.6.0.0
-create -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
      <subject>CN=PAM</subject>
   </Certificate>"
```

Example: Create a pem certificate type for an issuer

The following igwCertUtil example creates a certificate where the named issuer provided the issuer.cer file and issuer.key file.

```
igwCertUtil -version 4.6.0.0
-create -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
      <subject>CN=PAM</subject>
   </Certificate>"
-issuer
   "<Certificate>
      <certType>pem</certType>
      <certURI>issuer.cer</certURI>
      <keyURI>issuer.key</keyURI>
   </Certificate>"
```

Example: Copy PAM.cer with PAM.key to PAM.p12

In the following example, the igwCertUtil utility copies the pem certificate to the target p12 certificate. The pem certificate includes the name of the .cer file and the .key file. The p12 certificate includes the name and password combination.

```
igwCertUtil -version 4.6.0.0
-copy -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
   </Certificate>"
-target
   "<Certificate>
      <certType>p12/certType>
      <certURI>PAM.p12</certURI>
      <certPW>password</certPW>
   </Certificate>"
```

Example: Convert PAM.cer and PAM.key to PAM.p12 and password

In the following example, the igwCertUtil utility converts the pem certificate type to a p12 certificate type. The utility converts the PAM.cer to PAM.p12 and converts the PAM.key to a password.

```
igwCertUtil -version 4.6.0.0
-conv -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
   </Certificate>"
-target
   "<Certificate>
      <certType>p12/certType>
      <certURI>PAM.p12</certURI>
      <certPW>password</certPW>
   </Certificate>"
```

Configure Domain Properties

The Domain is the root element in the CA Process Automation hierarchy. You can edit some Domain properties, such as the frequency with which agents notify the Domain Orchestrator that they are active. Changing the heartbeat value from 2 to 3, for example, can reduce the network traffic. The setting that you specify at the Domain level can be inherited or overridden at the environment level.

Note: See the *User Interface Reference* for field descriptions.

The Content administrators in the PAMAdmins group can lock the Domain and can edit Domain properties. The Domain_Admin permission in the CA EEM Domain policy grants authorization.

Follow these steps:

1. Click the Configuration tab.

   The Configuration Browser palette opens with the Domain node selected.

2. Click the Properties tab.

3. View the read-only fields, for example:

   a. View the Domain URL entry. This entry is the first part of the URL you use to browse to CA Process Automation. The Domain URL entry can identify either the Domain Orchestrator or the load balancer. The URL can indicate secure or basic communication.

   b. View the Host Name entry. This entry identifies the host where the Domain Orchestrator is installed.

   c. View the Orchestrator Name entry. At the Domain level, this entry is the Domain Orchestrator by default.

   d. View the Status entry. The Domain status can have values such as Active or Locked by *user ID*.

4. With the Domain node selected, click Lock.

   When you lock the Domain, only you can edit the Domain properties.

5. To edit the Heartbeat Interval (minutes) setting, select a new value from the spinner.

   Setting a new value changes how often agents send a heartbeat to the Domain Orchestrator. By default, agents send a heartbeat every 2 minutes. This configuration applies to all agents in the Domain, but you can override this inherited value for any specific agent. Increasing the value reduces network traffic; increasing the interval to every 1 minute lets you identify agent problems more quickly.

6. Consider leaving the default Touchpoint Security setting (Disabled) in place at the Domain level.

   The Enabled setting specifies to verify and enforce user rights on the targets in a given process. The user rights are configured in a custom CA EEM policy that uses the Touchpoint Security resource class. You can grant execute rights to a user or group for a specific environment or touchpoint.

   Note: See Approach to Configuring Touchpoint Security (see page 143).

7. Configure the Host Group targets according to the following guidelines:

   - Disable the Match target in Host Groups only? property if the patterns configured for host groups sometimes match the IP addresses or host names of:
     - Hosts that have installed agents that are associated with touchpoints.
     - Remote hosts that are connected to agents associated with proxy touchpoints.

     Note: In this case, the product disables Lookup DNS when matching target in Host Groups? by default.
   - Enable the Match target in Host Groups only? property if the patterns configured for host groups rarely match the IP addresses or host names of:
     - Hosts that have installed agents that are associated with touchpoints.
     - Remote hosts that are connected to agents associated with proxy touchpoints.
   - Disable the Lookup DNS when matching target in Host Groups? property if content designers typically use the following conventions:
     - They use a host name when the pattern type used in the Host Group configuration is a host name pattern.
     - They use an IP address when the pattern type used in the Host Group configuration is a subnet, IP address range, or IP address list.
   - Enable the Lookup DNS when matching target in Host Groups? property if content designers are aware that Host Groups reference specific hosts in some way, but they do not necessarily know how. Enabling the property ensures that the operator can find a target host. For example, an operator that specifies the host as an IP address can find the target when the Host Group references it with a host name pattern.

8. Specify requirements for purging reporting data that was generated in this Domain. Alternatively, purge reporting data on demand where you specify the date range for when the reports were generated.
    a. Specify whether to purge reporting data daily in the Option to Purge Reporting Data field. If you select Purge Reporting Data Daily, specify the time of day to start the purge. For example, to start the purge at 6:30 PM, specify the military time equivalent, 18:30 in the Start Time to Purge Reporting Data Daily field.
    b. If you specified a purge schedule, indicate the number of days to retain reporting data before it is purged. For example, an entry of 14 in the Number of Days to Keep Reporting Data field specifies to purge all reporting data that is more than two weeks old.
    c. Click the Delete Reporting Data button, specify a date range for the reporting data to delete, and click OK.
9. To generate reporting for processes, select the Enable Process Reporting check box. To disable this capability, clear the Enable Process Reporting check box.
10. To generate reporting data for operators, select the Enable Operator Reporting check box. To disable this capability, clear the Enable Operator Reporting check box.
11. To allow the product to display process logs to content designers in the design environment, select the Enable Process Logs check box. To hide run-time process instance logs at the environment level for the production environment, clear the Enable Process Logs check box.
12. The Agent Configuration Update Interval (minutes) field lets you define the frequency at which the Domain orchestrator checks and, if appropriate, sends configuration updates to agents.
13. To automate the operator recovery, accept the default for the Enable Operator Recovery property.
14. Click Save.
15. Select Domain and click Unlock.

More information:

Lock the Domain (see page 131)
Approach to Configuring Touchpoint Security (see page 143)
Oasis Configuration Properties File (see page 400)

Approach to Configuring Touchpoint Security

Touchpoint Security is a Domain-level property. By default, Touchpoint Security is not enforced. The inherited non-enforcement allows existing processes to run successfully.

Note: If you configure Touchpoint Security as enforced and there are no Touchpoint Security policies in CA EEM, there is no protection.

Typically, mission-critical hosts and hosts that contain highly sensitive data only exist in a production environment. If you have partitioned your CA Process Automation domain into a design environment and a production environment, consider this guideline:

- Design Environment: Accept the Inherited settings, where Touchpoint Security is disabled
- Production Environment: Configure Touchpoint Security to Enabled in Environment properties. Then, create a global Touchpoint Security policy that authorizes the execution of Operators in selected categories to the group or users you specify. Specify the Environment as a filter. Then specify one filter for each Touchpoint mapped to a business critical host.

Alternatively, you can use Touchpoint Security in a development or test environment to restrict who can run processes on your Orchestrator. In that case, you could create a policy and list all members of your staff as Identities. In this policy, you create two filters--one for your Orchestrator as a Touchpoint and another for your Environment.

More information:

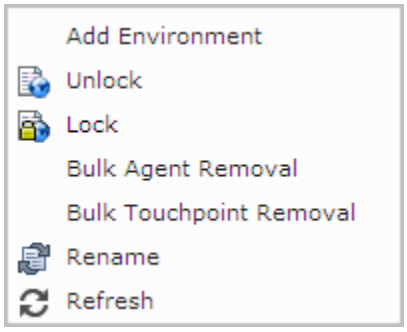
Configure Domain Properties (see page 140)
Create a Touchpoint Security Policy (see page 125)

Maintain the Domain Hierarchy

By default, all administrators assigned to the PAMAdmins group have the Domain_Admin permissions. If you use custom policies and groups, you can restrict the Domain_Admin permissions to selected administrators.

Tasks that only a user with Domain_Admin permissions can perform are those actions that require locking the Domain. See Lock and Unlock the Domain (see page 131).

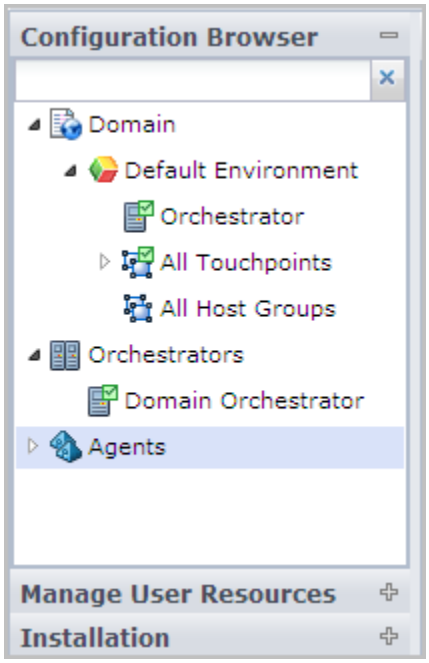
These tasks change the Domain Hierarchy by renaming a node or by adding or removing nodes.



- Add Environment - See Add an Environment to the Domain (see page 147).
- Remove Environment - See Remove an Environment from a Domain (see page 148).
- Bulk Agent Removal - See Remove Selected Agents in Bulk (see page 205).
- Bulk Touchpoint Removal - See Remove Unused Empty Touchpoints in Bulk (see page 235).
- Rename the Domain - See Rename the Domain (see page 149).

About the Domain Hierarchy, Orchestrators, and Agents

The Configuration Browser palette on the Configuration tab contains one root object which the product names Domain during installation. The Domain is the parent element for all configurable elements in the product.



The Configuration Browser displays physical and logical entities.

Physical

A *physical* component is an installed component (an Orchestrator or an agent).

Orchestrators

Domain Orchestrator

Immediately after the installation, the Domain Orchestrator is the only physical component.

Other Orchestrators

Administrators can install other Orchestrators from the Installation palette.

Agents

Administrators can install agents from the Installation palette.

Logical

One or more *logical* entities comprise the Domain hierarchy, which consists of one or more environments. Each environment has one or more Orchestrator touchpoints and can have touchpoints and host groups that are associated with agents.

Domain

The Domain is the Domain hierarchy root node. The product has one Domain.

Default Environment

The Default Environment is the environment that the installation program creates.

Orchestrator (touchpoint)

During the installation, the product displays under Default Environment the Orchestrator touchpoint that associates the Domain Orchestrator with the Default Environment. Each Orchestrator requires a separate touchpoint.

Note: The product associates the environment for a clustered Orchestrator touchpoint with the touchpoint for that cluster. When you use such a touchpoint as an operator target, the load balancer selects the target node.

All Touchpoints

During the installation, the All Touchpoints node is empty. From an installed agent, you can configure a touchpoint at a selected environment. Touchpoints associate agents with environments. The All Touchpoints node under Default Environment contains only touchpoints that are associated with the Default Environment. Multiple touchpoints can map to an agent. A single touchpoint can map to multiple agents.

All Host Groups

During the installation, the All Host Groups node is empty. From an installed agent, you can create a Host Group at a selected environment and you can configure the host group properties. Connectivity from an agent to a group of remote hosts requires a user account on each remote host. The user accounts are configured with the credentials that re defined in the host group properties.

Another Environment

You can add a separate production environment. Each environment requires at least one Orchestrator touchpoint.

Other Orchestrator (touchpoints), other All Touchpoints, other All Host Groups in the new environment

For each installed Orchestrator, you create a touchpoint under a selected environment. The Orchestrator touchpoints appear under the node of the environment you select. All agent touchpoints that you create appear under the All Touchpoints for that environment. All host groups that you create appear under All Host Groups for that environment.

Content administrators automate processes by creating and linking operators. Operators typically target (run on) a specified Orchestrator touchpoint. An operator can target a touchpoint that is associated with multiple agents. In this case, that operator can potentially run on any associated agent host.

Add an Environment to the Domain

Administrators can add an environment to the Domain. Typically, administrators add a Production Environment.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.

   The palette displays the Domain icon with a padlock to indicate that it is locked.

2. Right-click the Domain, and then select Add Environment.

3. On the Add New Environment dialog, enter a name for the environment, and then click OK.

   The Configuration Browser palette displays the new environment name with nodes for adding All Touchpoints and All Host Groups. Initially, the new environment has no Orchestrator.

4. Click Save.

5. Select Domain and click Unlock.

Remove an Environment from the Domain

With the Domain Administrator rights, you can delete an environment from the Domain. If the environment is actively used, take the required steps to preserve library objects and execution targets.

Follow these steps:

1. Click the Configuration tab.
2. Right-click the Domain, and then click Lock.
3. Revise the operators in active processes that target an Orchestrator or touchpoint in the target environment.
4. Reconfigure or remove the touchpoints, proxy touchpoints, host groups, and touchpoint groups that are associated with the target environment. For example, associate agent touchpoints with another environment.
5. Move the Library content to another environment as appropriate.

   Note: The following topics discuss how to move content:

   - Export a Folder (see page 352)
   - Import a Folder (see page 353)
6. Remove each Orchestrator from the environment:

   a. Quarantine the Orchestrator (see page 184).

   b. Remove the Orchestrator from the environment (see page 162).
7. Right-click the environment, and then select Delete.
8. Click Yes on the confirmation message.
9. Click Save.
10. Select Domain and click Unlock.

Rename the Domain

Throughout the documentation and help, we use the name Domain to refer the the CA Process Automation domain. Administrators with Domain_Admin permissions can rename this top node of the domain hierarchy.

Follow these steps:

1. Click the Configuration tab.
2. Select Domain and click Lock.
3. Right-click Domain and select Rename.
4. Enter the new name in the field containing Domain.
5. Click Save.
6. Select Domain and click Unlock.

Chapter 6: Administer Environments

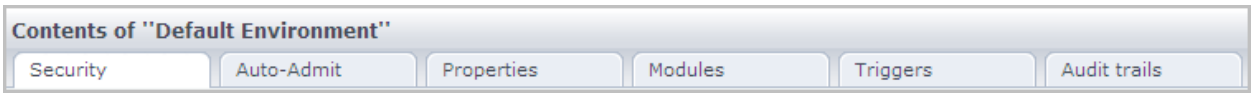
At installation the CA Process Automation Domain has one environment, the Default Environment. Administrators defined in the default PAMAdmins group have all rights. You can create CA EEM policies that grant specific administrator rights to different users. For example:

- An administrator with *Domain Administrator* rights can create additional environments to segment the Domain. Typically, the Default Environment is used for designing automated processes and supporting objects. When one or more processes is ready for use in the existing production environment, the administrator creates an environment in CA Process Automation and names it Production Environment. Other examples include geographic segmentation, life cycle segmentation, and staging. These tasks are addressed in this chapter.
- An administrator with *Environment Content Administrator* rights can add touchpoints, host groups, create touchpoint groups, and remove unused touchpoints in bulk. They also can create new objects, including processes and schedules. See subsequent chapters for details about touchpoints and host groups. See the *Content Designer Guide* for details about using the Library and Designer tabs for content creation and development.
- An administrator with *Environment Configuration Administrator* rights can configure the contents of a selected environment. Administrators can accept or override inherited settings. Configuring the contents of an environment can include editing security settings, setting environment properties, enabling or disabling operator categories, and setting inheritance for triggers.

This section contains the following topics:

Configure the Contents of an Environment

When you select an environment in the Configuration Browser, the following tabs appear under Contents of "<environment name>":



- Security

  See View or Reset Security Settings for a Selected Environment (see page 152).

- Auto-Admit

  See Add Touchpoints for Agents in Bulk (see page 232).

- Properties

  See Configure Environment Properties (see page 153).

- Modules

  See Enable an Operator Category and Override Inherited Settings (see page 156).

- Triggers

  See Specify Trigger Settings for an Environment (see page 157).

- Audit trails

  See View the Audit Trail for an Environment (see page 336).

View or Reset Security Settings for a Selected Environment

Most of the Security tab settings are created during installation or upgrade of the Domain Orchestrator. You can change these read-only settings only by reinstalling the Domain Orchestrator.

Each environment inherits the settings that you establish during the Domain Orchestrator installation. If you clear the Inherit check box, you can update the CA EEM Cache Update Interval (in seconds). When you shorten the update interval, CA Process Automation reflects changes that you make in CA EEM more quickly.

Follow these steps:

1. Click the Configuration tab.
2. Expand Domain in the Configuration Browser palette and select the target environment.

   The Security tab opens.
3. Examine the security settings that were established during the installation process.

4. (Optional) Update the CA EEM Cache Update Interval value.
   a. Click Lock.
   b. Clear the Inherit check box.
   c. Update the value.
   d. Click Save.
   e. Select the environment and click Unlock.

   Note: If you reduced the CA EEM Cache Update Interval, consider suppressing the CA Process Automation permissions cache. See Control Caches of CA EEM Updates (see page 76).

More information:

Configure CA EEM Security Settings for the Domain (see page 133)

Configure Environment Properties

Configure the properties for a selected environment from the Configuration tab. Environment Configuration Administrator rights are required to configure environment properties or override settings at a level that can inherit from the environment.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain node, right-click the appropriate environment name, and then click Lock.
3. Click the Properties tab, and then view or update properties as appropriate.

   Operators Autorecovery

   Specifies whether to automate recovery. Recovery applies to specific operators that fail with a SYSTEM_ERROR and have recoverable processes that are in a BLOCKED, RUNNING, or WAITING state. Select True to begin recovery when the inactive Orchestrator or agent becomes active. Recovery resets operators that were in SYSTEM_ERROR and resumes their processes. The reset operators in a resumed process begin running on the associated targets. The Operator targets can be Orchestrators, touchpoints, hosts that are connected to proxy touchpoints, or hosts in a host group.

   Values: This property has the following values:

   - **Selected** - Automates recovery.
   - **Cleared** - Prevents automated recovery.

   Default: Selected.

Touchpoint Security

Specifies whether to inherit the value that is configured in the Domain properties or to set the value at the environment level.

Values: This property has the following values:

- **Inherit from Domain** - Use the value that is configured for this field in the Domain properties.
- **Enabled** - Enforce the Touchpoint Security policies for this target and allow access only if the user has been granted this permission.
- **Disabled** - Do not verify whether the user running the process has execute rights on the current target.

Default: Inherit from Domain.

Match target in Host Groups only?

Specifies the search scope for an operator target when the Target field entry is an IP address or a host name (FQDN). The operator execution on the target can proceed only when the target is known to CA Process Automation. Select Disabled to allow the broadest search. Select Enabled here and Disabled for the next field for the most restricted search.

Note: A DNS lookup of a specified hostname finds associated IP addresses; a DNS lookup of the IP address finds associated hostnames.

Values: This property has the following values:

- **Inherit from Domain** - Use the value that is configured for this field in the Domain properties.
- **Enabled** - The scope of the search depends on whether the "Lookup DNS when matching target in Host Groups" field is enabled or disabled.

  If a DNS lookup is disabled, searches: Host group reference to a remote host (exact)

  If a DNS lookup is enabled, searches: Host group reference to a remote host (exact or DNS lookup result)
- **Disabled** - Search the Domain components in the following order:

  Touchpoint (exact or a DNS lookup result)

  Orchestrator (exact or a DNS lookup result)

  Agent (exact or a DNS lookup result)

  Proxy touchpoint mapping to a remote host (exact or DNS lookup result)

  Host group reference to a remote host (exact or DNS lookup result)

Default: Inherit from Domain.

Lookup DNS when matching target in Host Groups?

Note: This field is enabled when the "Match target in Host Groups only" is set to Enabled.

Specifies whether to limit the search through Host Group references to the entry type. For example: When the Target field entry type is an FQDN, search only host name patterns. When the Target field entry type is an IP address, search only subnets. When a DNS lookup is included, the search can also accept a host group reference to the other type, as resolved by a DNS lookup.

Values: This property has the following values:

- **Inherit from Domain** - Use the value that is configured for this field in the Domain properties.
- **Enabled** - Search all host group references. Host group references for hostnames are patterns (regular expressions) that can include the specified host name. Host group references for IP addresses are IP address subnets that are expressed in CIDR notation that can include the specified IP address. Extend the search to all host group references. Let the search find either an exact match or a match to the DNS lookup result.
- **Disabled** - Restrict the search to host group references that include an exact match to the Target field entry.

Default: Inherit from Domain.

4. Click Save.
5. Select the environment and click Unlock.

   The environment property updates are active.

More information:

Approach to Configuring Touchpoint Security (see page 143)
Customize Operator Category for a Selected Agent (see page 199)

Enable an Operator Category and Override Inherited Settings

Operator category settings are displayed in an environment as Inherit from Domain by default. When operator category settings are configured at the Domain level, an administrator can accept the inherited settings. Alternatively, an administrator with Environment Configuration Administrator rights can enable any operator category and override inherited settings at the environment level.

To examine the settings for any operator category, you must enable the category.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain, select an environment and click Lock.
3. Click the Modules tab.
4. To view the settings for any operator category, click the Inherit from Domain setting and select Enable from the drop-down list.
5. Right-click the operator category and select Edit.

   The current settings are displayed.
6. Optionally, configure settings for one or more fields.

   Note: See Configuring Operator Categories (see page 270) for field-level details.
7. Click Save.
8. Click Close.
9. Right-click the environment and select Unlock.

More information:

Configure Network Utilities (see page 300)
Configure Web Services (see page 304)
Configure Process Control (see page 301)
Configure File Management (see page 296)
Configure Command Execution: Default Telnet Properties (see page 278)

Specify Trigger Settings for an Environment

Trigger settings are disabled at the environment level by default. If trigger setting have been configured at the domain level, you can specify that you want to inherit these settings. Alternatively, you can enable a trigger and then override the domain-level settings. If needed, you can disable a trigger that is enabled or set to inherit values.

Follow these steps:

1. Click the Configuration tab.
2. Review the Domain-level settings for the trigger:
   a. Click Domain
   b. Click the Triggers tab.
   c. Double-click a trigger.
   d. Determine whether the trigger has been configured, and if so, whether to accept the settings for a given environment.
3. Select an environment and click Lock.
4. Click the Triggers tab.
5. Select a trigger.
6. Select a new value from the drop-down list

   Inherit from Domain

   Specifies that the settings configured at the domain-level are used in the selected environment.

   Disabled

   Specifies that this trigger is not used in this environment.

   Enabled

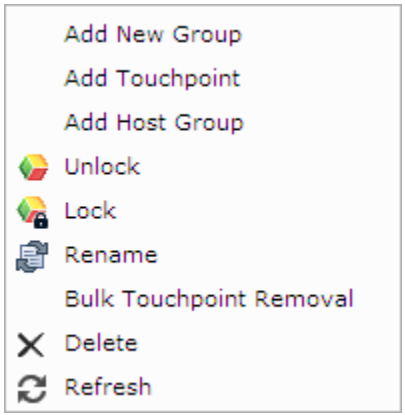
   Specifies that this trigger is to use the settings configured for this environment.
7. If you select Enabled, then right-click the trigger and select Edit. Edit the settings using the following as a guide:
   - Configure File Trigger Properties at the Domain Level (see page 319).
   - Configure Mail Trigger Properties at the Domain Level (see page 320).
   - Configure SNMP Trigger Properties at the Domain Level (see page 323).
   - Configure Catalyst Trigger Properties at the Domain Level (see page 316).
8. Click Save.
9. Click Close.
10. Select the updated environment and click Unlock.

Update an Environment Hierarchy

The Domain hierarchy is composed of one or more environments, where each environment has at least one Orchestrator and one or more touchpoints that associate the environment with an agent. When an operator in a running process targets a touchpoint, that operator runs on the agent or Orchestrator associated with the touchpoint. When an operator targets a touchpoint group, it runs on all of the associated agents and Orchestrators.

To support the running of operators on remote hosts, which are hosts with no agent, an environment can include proxy touchpoints and host groups. A proxy touchpoint associates one remote host with an agent; a host group associates many remote hosts with an agent. In both cases the agent host connects to the remote host with a trusted SSH connection.

An administrator with Environment_Configuration_Admin (Configuration Administrator) permissions can update the hierarchy of a selected environment. The right-click menu options for an environment follow:



Links to topics for the Environment menu options follow:

- Add New Group

  See Group Touchpoints in an Environment. (see page 237)

- Add Touchpoint

  See Add a Touchpoint and Create an Association (see page 230) and other details in the "Administer Touchpoints" and the "Administer Proxy Touchpoints" chapters.

  See also Add an Orchestrator to an Environment (see page 161).

- Add Host Group

  See Create a Host Group (see page 252) and other details in the Administer Host Groups chapter.

- Rename

  See Rename an environment (see page 160).

- Bulk Touchpoint Removal

  See Remove Unused Empty Touchpoints in Bulk (see page 235).

- Delete - Can be used to remove any user-added logical object from the Domain hierarchy, that is:
  - Any environment.
  - Any Orchestrator touchpoint.

    See Delete an Orchestrator Touchpoint (see page 162).
  - Any agent touchpoint.
  - Any touchpoint group.
  - Any host group.

Rename an Environment

Administrators with Environment_Configuration_ Admin (Configuration Administrator) rights can rename an environment.

Follow these steps:

1. Click the Configuration tab.

   The Configuration Browser palette is open.
2. Right-click the Domain, and click Lock.
3. Right-click the environment, and click Lock.
4. Right-click the environment, and select Rename.
5. Enter a new name for the environment.
6. Click Save.
7. Right-click the Domain, and click Unlock.

Add an Orchestrator to an Environment

During the initial installation of CA Process Automation, the Domain Orchestrator is installed in the Default Environment. The Default Environment is typically used for design and testing. Often, administrators create a separate environment for production.

Each environment must have at least one Orchestrator, but any environment can have multiple Orchestrators. Each new Orchestrator involves a separate installation. After you install a separate Orchestrator, add the newly installed Orchestrator to an environment.

Follow these steps:

1. Click the Configuration tab.
2. Right-click the environment to configure, and click Lock.
3. Right-click the environment again, and click Add Touchpoint.

   The Add Touchpoint dialog opens.
4. Next to Touchpoint Name, enter a name for the new Orchestrator.
5. Next to Select Agent/Orchestrator, click Orchestrator.

   The Orchestrator option is unavailable if all the Orchestrators in the Domain are already associated with existing touchpoints.
6. In the list of available Orchestrators, select the Orchestrator that you want to associate with the new touchpoint.
7. Click Save to add the new touchpoint to the environment.
8. Select the Browser palette, right-click the environment, and click Unlock.

   The Unsaved Data dialog prompts you to save changes.
9. Click Yes.

   Note: You can also save it using Save at the top of the screen, or from the File menu without unlocking it.

More information:

Add a Touchpoint for an Orchestrator (see page 170)

Delete an Orchestrator Touchpoint

An Orchestrator touchpoint is a logical entity that associates a selected Orchestrator, or its load balancer, with a specific environment. Deleting an Orchestrator touchpoint removes the association but does not affect the environment or the Orchestrator. However, a physical Orchestrator with no touchpoint cannot be accessed. It cannot accept operator requests or updates to its library.

You can delete an Orchestrator touchpoint in preparation for creating a new touchpoint for that Orchestrator. You can delete an Orchestrator touchpoint in preparation for retiring that Orchestrator.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain node and the environment node with the Orchestrator to remove.
3. Right-click the Domain, and click Lock.
4. Right-click the environment containing the Orchestrator you want to delete, and click Lock.
5. Right-click the Orchestrator you want to delete, and select Delete.
6. Click OK to confirm deletion of the Orchestrator.
7. Right-click the environment and click Unlock.
8. Right-click the Domain and click Unlock.

   The Orchestrator touchpoint is deleted.

More information:

Quarantine an Orchestrator (see page 184)
Disable an Orchestrator Touchpoint (see page 172)

Chapter 7: Administer Orchestrators

You can install as many Orchestrators as are necessary. The first installation creates the Domain Orchestrator. After the Domain Orchestrator is running, you can install additional Orchestrators from the Installation palette on the Configuration tab.

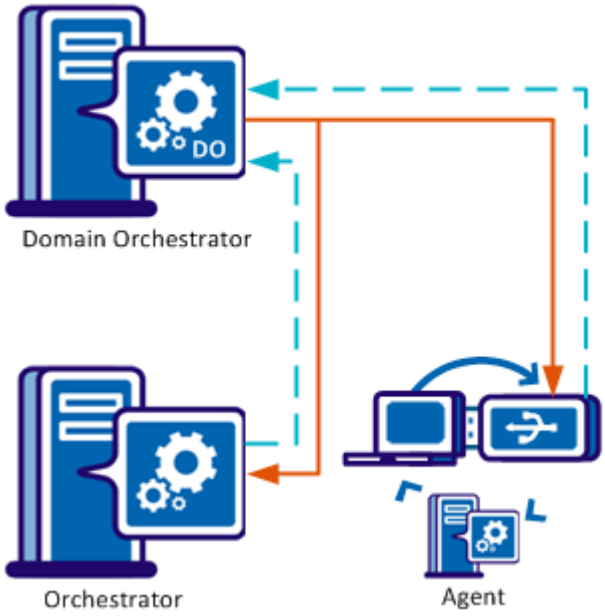
Orchestrators are the "engines" of CA Process Automation; they process the content that is designed with CA Process Automation. All processes run on Orchestrators, which manage and run automation objects. Orchestrators direct agents to perform required actions as part of the process.

This section contains the following topics:

About Orchestrators

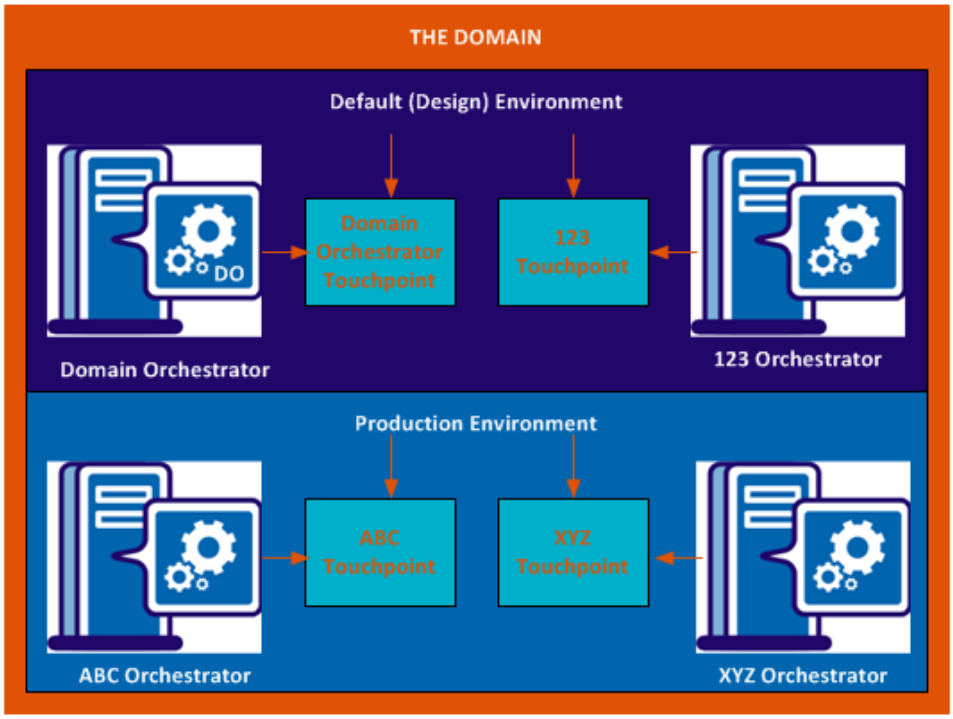
The Domain Orchestrator maintains the configuration and status of all components in the Domain. You can upload updates for Orchestrators or agents to the Domain Orchestrator. The Domain Orchestrator sends the updates you upload to all Orchestrators or agents. All Orchestrators and agents in the Domain send their status to the Domain Orchestrator regularly.

The Domain Orchestrator Maintains Components

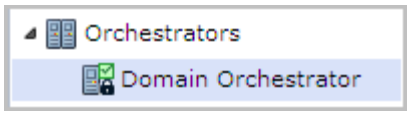


To add an Orchestrator to an environment, configure a touchpoint for the selected Orchestrator at the environment you specify. Each Orchestrator participates in only one CA Process Automation environment. Each Orchestrator is associated with one touchpoint. When an operator is to run on an Orchestrator touchpoint, the Target field is left blank. A blank Target field means run the operator on the Orchestrator where the process started.

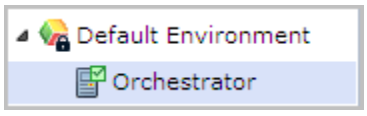
An Orchestrator Touchpoint Associates the Orchestrator with an Environment



You configure host-specific settings and view physical information for an Orchestrator in the Orchestrators node.

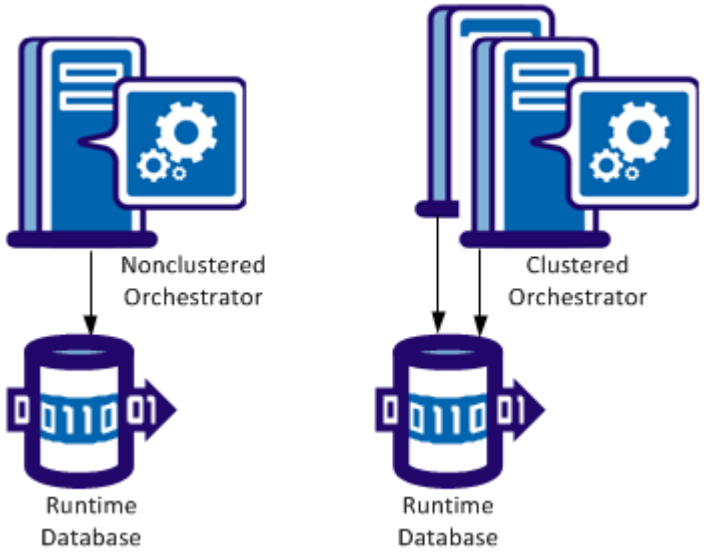


You configure touchpoint-specific settings for the same Orchestrator in the environment node. You can view logical information about an Orchestrator under its environment.



Orchestrators can be *clustered* (with multiple nodes) for high availability and scalability or *nonclustered (*with a single node*)*. A clustered Orchestrator acts as a single Orchestrator. For example, while each nonclustered Orchestrator has its own run-time database, the Orchestrators in a clustered node share a run-time database.

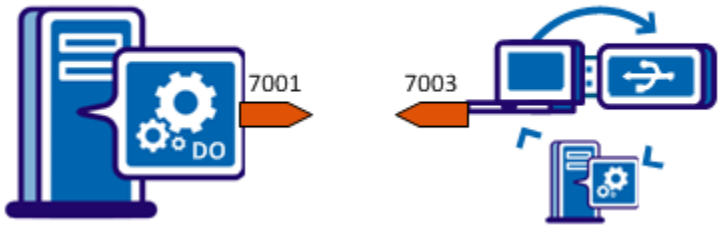
Clustered and Nonclustered Orchestrators Behave Alike



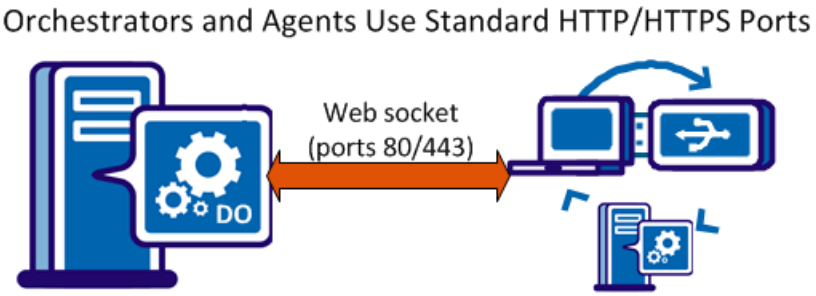
A process that runs on one Orchestrator can run a subprocess on a separate Orchestrator. An agent can perform steps in a process (such as running a script). Orchestrators and agents use a pair of ports to communicate.

With deprecated communications, the default port for Orchestrators is 7001; the default port for agents is 7003. Port 7001 and port 7003 are both bidirectional; that is, these ports both send and receive data.

Orchestrators and Agents Have Default Ports



With simplified communications, agents initiate a persistent web socket connection that the agent and Orchestrator use for communication.



When the Orchestrator requests that an agent complete a step, the agent returns the results to the Orchestrator. In a clustered setup, an Orchestrator node sends a request to an agent. The agent sends the result to any node of the requesting Orchestrator. One of the cluster nodes picks up the agent result from a shared queue.

More information:

Upload Agent Resources (see page 331)
Upload Orchestrator Resources (see page 329)

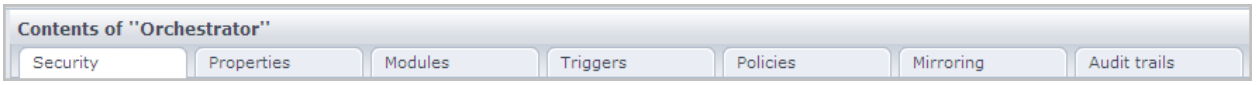
Configure the Contents of an Orchestrator Touchpoint

To configure an Orchestrator touchpoint, select that Orchestrator under an Environment node. All but one of the settings is view-only.

To configure settings that pertain to the Orchestrator host, select the Orchestrator under the Orchestrators node.

Note: For configuration details see, Configure the Contents of an Orchestrator Host (see page 173).

The tabs for Contents of the selected Orchestrator follow:



The only configurable field on this set of tabs is that for Touchpoint Security. On the Properties tab, set Touchpoint Security to True only after you have configured a Touchpoint Security policy.

Topics for the Orchestrator tabs follow:

- Security - Security settings do not apply to the Orchestrator Touchpoint. The fields are read-only from the Orchestrator touchpoint view.
- Properties - You can configure Orchestrator touchpoint properties (see page 168).
- Modules - Operator categories are not configurable from an Orchestrator touchpoint. You can edit settings by selecting the Orchestrator host.
- Triggers - Triggers are not configurable from an Orchestrator touchpoint. You can edit settings by selecting the Orchestrator host.
- Policies - Policies are not configurable from an Orchestrator touchpoint. You can edit settings by selecting the Orchestrator host.
- Mirroring - Mirroring is not configurable from an Orchestrator touchpoint. You can edit the mirroring setting by selecting the corresponding Orchestrator host.
- Audit Trails - Audit trail actions do not apply to Orchestrator touchpoints. You can view audited actions on the corresponding Orchestrator host.

Configure Orchestrator Touchpoint Properties

The Orchestrator touchpoint Properties pane provides information about the touchpoint that is associated with the Orchestrator. You can view status information and you can change the configuration of Touchpoint Security for this Orchestrator touchpoint.

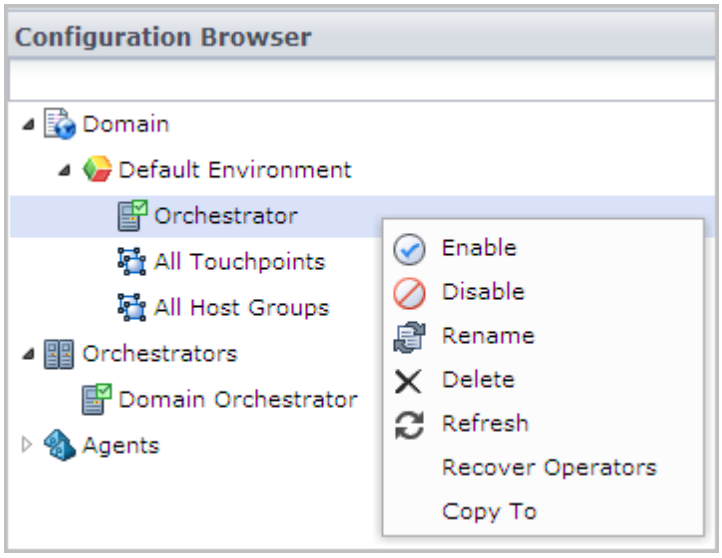
Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain and the environment with the Orchestrator touchpoint.
3. Select the Orchestrator touchpoint to configure and click Lock.
4. Click the Properties tab.
5. (Optional) Configure the Touchpoint Security setting. Specify whether to inherit the setting or set the value at the Orchestrator level. When enabled, processes use the Touchpoint Security policies to authorize users to execute operators in a process.

6. Configure the default settings for how operators process an IP address or host name in the Target field or when referenced by a dataset.
   a. The Match target in Host Groups only? drop-down list selection specifies the search scope for an operator target when the Target field entry is an IP address or a host name (FQDN). The operator execution on the target can proceed only when the target is known to CA Process Automation.
      - Select Disabled to allow the broadest search.
      - Select Enabled here and Disabled for the next field for the most restricted search.
   b. When the Lookup DNS when matching target in Host Groups? drop-down list is enabled, specify whether to limit the search through Host Group references to the entry type.
      - Select Enabled to search all host group references.
      - Select Disabled to restrict the search to host group references that include an exact match to the Target field entry.
7. Click Save.
8. Select the Orchestrator and click Unlock.
9. View the informational properties. For more information, see the tooltips.

Update the Hierarchy of an Orchestrator Touchpoint

When you select an Orchestrator under Domain/Environment, the details you see are relevant to the touchpoint mapped to that Orchestrator.



See the following:

- Enable - Right-click an Orchestrator touchpoint that is disabled and select Enable.
- Disable

  See Disable an Orchestrator Touchpoint (see page 172).
- Rename - Specify a new name for the Orchestrator touchpoint.
- Delete

  See Delete an Orchestrator Touchpoint. (see page 162)
- Recover Operators

  See Recover Operators on the Target Orchestrator (see page 171).
- Copy To

  See Create a Touchpoint Group with Selected Touchpoints (see page 238)

Add a Touchpoint for an Orchestrator

When you add a standalone Orchestrator to an environment, add a touchpoint to the environment and map it to that Orchestrator. Each Orchestrator must be associated with its own touchpoint.

When you add nodes to create a clustered Orchestrator, the load balancer uses the touchpoint that you defined for the first node. The load balancer determines which node handles a request that targets the touchpoint.

Follow these steps:

1. Click the Configuration tab.
2. Right-click the environment at which to add a touchpoint and click Lock.
3. Expand the Orchestrators node.
4. Right-click the target Orchestrator, select Configure touchpoint at, and click the name of the environment you locked.
5. In the Add Orchestrator Touchpoint dialog, enter a name for the new touchpoint and click Add.
6. Right-click the environment where you added the touchpoint and select Unlock.

   The Unsaved Data dialog prompts you to save changes.
7. Click Yes.

   A new Orchestrator touchpoint is added to the selected environment.

More information:

Add an Orchestrator to an Environment (see page 161)

Recover Operators on the Target Orchestrator

Manual recovery is always enabled. You can invoke Recover Operators whether the target level Operator Auto Recovery is set to True, False, or Inherit from Environment. Operator recovery is appropriate when a process is in a BLOCKED, RUNNING, or WAITING state and an operator in the process failed with a system error. Operator recovery resets the Operator and then resumes the process.

You can invoke Operators recovery from the Configuration tab when:

- The previously inactive Orchestrator becomes active. An active Orchestrator is displayed as green.
- The target Orchestrator is enabled.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain and an environment in which an Orchestrator has one or more processes that are set to be recoverable.
3. Right-click the Orchestrator and select Refresh.
4. Right-click the Orchestrator and select Recover Operators.

   Operator recovery begins.

Disable an Orchestrator Touchpoint

Disable an Orchestrator touchpoint to prevent processes from running on that Orchestrator touchpoint. Disabling an Orchestrator touchpoint does not affect the Orchestrator library. That is, designers can select an Orchestrator with a disabled touchpoint on the Library tab and can define automation objects.

You disable an Orchestrator touchpoint when affected external objects are unavailable. Consider the example of processes that deal with Service Desk or with an external database. At certain times, those components are down for maintenance. You can prevent the running of processes that interact with components that are temporarily unavailable. When the external components become available, you enable the Orchestrator touchpoint. Then, scheduled processes that use these external components can begin running again.

You can disable the Orchestrator touchpoint that you select on the Domain hierarchy.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain node. Expand the environment node with the Orchestrator touchpoint to disable.
3. Select the environment and click Lock.
4. Select the Orchestrator touchpoint and click Lock.
5. Right-click the Orchestrator touchpoint and select Disable.
6. Click Unlock.
7. Select the locked environment and click Unlock.

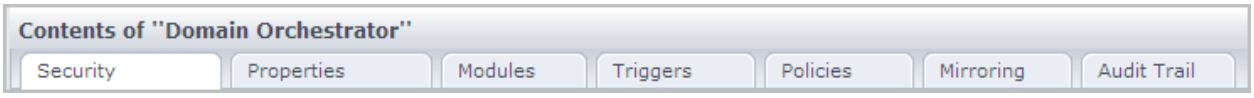
More information:

Quarantine an Orchestrator (see page 184)

Configure the Contents of an Orchestrator Host

Configuration details that are unique to Orchestrators and are not inherited include Policies, and Mirroring, both of which have default values for all fields. Mirroring applies to Orchestrators other than the Domain Orchestrator. Settings for the following are inherited by default: Security, Properties, Modules, and Triggers. The settings that you configure for an Orchestrator host are different from those you configure on the Orchestrator touchpoint.

The tabs for the Orchestrator Host menu follow:



- Security

  See View Orchestrator Security Settings (see page 174).

- Properties

  See Configure Orchestrator Touchpoint Properties (see page 168).

- Modules

  See Override Operator Category Settings Inherited from Environment (see page 178).

- Triggers

  See Activate Triggers for an Orchestrator (see page 179).

- Policies

  See Configure Orchestrator Policies (see page 180).

- Mirroring

  See Configure Orchestrator Mirroring (see page 182).

- Audit Trails

  See View the Audit Trail for an Orchestrator (see page 337).

View Orchestrator Security Settings

Most of the Security tab settings are created during the Domain Orchestrator installation process. You cannot change any of these settings through the UI. You can change these settings by reinstalling the Domain Orchestrator.

The Inherit check box applies only to CA EEM Cache Update Interval (in seconds). You can shorten the update interval when you want CA Process Automation to receive changes that you make in CA EEM more quickly.

Follow these steps:

1. Click the Configuration tab.
2. In the Configuration Browser palette, expand Orchestrators.
3. Select an Orchestrator. You can view security settings on the Security tab.
4. To update the settings:
   a. Click Lock.
   b. Clear the Inherit check box.
   c. Update the EEM Cache Update Interval (in seconds) value.
   d. Click Save.
   e. Click Unlock.

More information:

View or Reset Security Settings for a Selected Environment (see page 152)
Configure CA EEM Security Settings for the Domain (see page 133)

Configure Orchestrator Host Properties

You can configure host properties for a selected Orchestrator and view read-only information.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Orchestrators node.
3. Select the Orchestrator to configure, and then click Lock.

4. Click the Properties tab and view the read-only Orchestrator properties settings:
   - Is Domain
   - Host Name
   - Orchestrator Name
   - Status
5. Configure the following fields:

   Operators Autorecovery

   Specifies whether to automate recovery. Recovery applies to operators that fail with a SYSTEM_ERROR and have recoverable processes in BLOCKED, RUNNING, or WAITING state when the recovery is triggered. If recovery is set to automatic, each Orchestrator in the environment automatically initiates the recovery when the Orchestrator becomes active again. Recovery starts running the affected processes and their operators begin running on this Orchestrator.

   Values: This property has the following values:

   - **Inherit from Environment** - Use the value that is configured for this field in the Environment properties.
   - **True** - Automates recovery.
   - **False** - Prevents automated recovery.

   Default: Inherit from Environment.

Match target in Host Groups only?

Specifies the search scope for an operator target when the Target field entry is an IP address or a host name (FQDN). The operator execution on the target can proceed only when the target is known to CA Process Automation. Select Disabled to allow the broadest search. Select Enabled here and Disabled for the next field for the most restricted search.

Note: A DNS lookup of a specified hostname finds associated IP addresses; a DNS lookup of the IP address finds associated hostnames.

Values: This property has the following values:

- **Inherit from Environment** - Use the value that is configured for this field in the Environment properties.
- **Enabled** - The scope of the search depends on whether the "Lookup DNS when matching target in Host Groups" field is enabled or disabled.

  If a DNS lookup is disabled, searches: Host group reference to a remote host (exact)

  If a DNS lookup is enabled, searches: Host group reference to a remote host (exact or DNS lookup result)
- **Disabled** - Search the Domain components in the following order:

  Touchpoint (exact or a DNS lookup result)

  Orchestrator (exact or a DNS lookup result)

  Agent (exact or a DNS lookup result)

  Proxy touchpoint mapping to a remote host (exact or DNS lookup result)

  Host group reference to a remote host (exact or DNS lookup result)

Default: Inherit from Environment.

Lookup DNS when matching target in Host Groups?

Note: This field is enabled when the "Match target in Host Groups only" is set to Enabled.

Specifies whether to limit the search through Host Group references to the entry type. For example: When the Target field entry type is an FQDN, search only host name patterns. When the Target field entry type is an IP address, search only subnets. When a DNS lookup is included, the search can also accept a host group reference to the other type, as resolved by a DNS lookup.

Values: This property has the following values:

- **Inherit from Environment** - Use the value that is configured for this field in the Environment properties.
- **Enabled** - Search all host group references. Host group references for hostnames are patterns (regular expressions) that can include the specified host name. Host group references for IP addresses are IP address subnets that are expressed in CIDR notation that can include the specified IP address. Extend the search to all host group references. Let the search find either an exact match or a match to the DNS lookup result.
- **Disabled** - Restrict the search to host group references that include an exact match to the Target field entry.

Default: Inherit from Environment.

6. Click Save.
7. Click Unlock.

Override Operator Category Settings Inherited from Environment

Operator category settings are configured on the Modules tab. Operator category settings that have been configured at the Environment level or inherited from settings configured at the Domain level are displayed as Inherit from Environment. An administrator with Environment Configuration Administrator rights can enable any operator category and override inherited settings at the Orchestrator level.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Orchestrators palette.
3. Select the Orchestrator you want to configure, and click Lock.
4. Click the Modules tab.
5. Select an operator category, click Inherit from Environment, and select Enable from the drop-down list.

   Note: You can disable an operator category at the Orchestrator level by selecting Disabled from the drop-down list.
6. Right-click the operator category and select Edit.

   The settings are displayed.
7. Change one or more inherited settings.

   Note: See Configuring Operator Categories (see page 270) for details.
8. Click Save and Close.

   The values configured in the open dialog are saved.
9. Click the Save toolbar button.

   The saved changes are applied to the CA Process Automation configuration.
10. Repeat Steps 5-9 for each operator category to update.
11. Select the Orchestrator you configured, and click Unlock.

More information:

Configure Network Utilities (see page 300)
Configure Web Services (see page 304)
Configure Process Control (see page 301)
Configure File Management (see page 296)
Configure Command Execution: Default Telnet Properties (see page 278)

Activate Triggers for an Orchestrator

An administrator with Environment Configuration rights can manage triggers at the Orchestrator level. You activate a selected trigger by changing its status to Inherit from Environment or by changing its status to Enabled and overriding the displayed settings. To view the current settings of a trigger, you must change the status to Enabled and select Edit. If you accept the settings, configure the trigger to Inherit from Environment. If you do not accept the settings because they are incomplete or not appropriate for this Orchestrator, you can configure the fields and leave the status as Enabled.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Orchestrators palette.
3. Right-click the selected Orchestrator and select Lock.
4. Click the Triggers tab.

   If triggers have not been configured at the Orchestrator level, they are in Disabled status.
5. Right-click the trigger you want to examine and click Edit.

   The fields display with the values that you can use as is or change.
6. If the trigger is fully configured with values you want the selected Orchestrator to use, select Inherit from Environment from the Enable/Disable drop-down list, and click Close.
7. If the trigger is not fully configured or you want to specify difference values for the selected Orchestrator, do the following:
   a. Select Enabled from the Enable/Disable drop-down list.
   b. For field descriptions and other pertinent information about each of the triggers, see Administer Triggers (see page 313).
   c. If the selected trigger is the Mail trigger and the Orchestrator is not the Domain Orchestrator, click Browse and select the default process file.

      The Default Trigger Process field is populated with the correct path for this Orchestrator.
   d. Click Close
8. Click Save.
9. Right-click the Orchestrator you locked and click Unlock.

Configure Orchestrator Policies

The Orchestrator Policies settings specify history settings for processes that run on the Orchestrator. They also specify the default schedule and the default process in the library. You can configure separate policies for separate Orchestrators.

Follow these steps:

1. Click the Configuration tab.
2. From the Configuration Browser, select the Orchestrator to configure, and click Lock.
3. Click the Policies tab.
4. Select whether to allow users to save an edited object as the same version at check-in or to automate object versioning by creating a new version at check-in.
5. If you have defined a process that specifies default process handlers with rules for changing lanes and handling exceptions, navigate to that process and select it.
6. Specify requirements for retaining instances of processes that have run.
   a. Select the minimum number of days to save process instances that ran on a touchpoint or remote host. If you configure one day, the process remains in the library for a minimum of 24 hours before it is archived.
   b. Select the minimum number of failed instances of a process to retain in the history.
   c. Select the minimum number of completed instances of the process object to retain in the history.
   d. Select the maximum number of log messages that can be displayed when the process instance is opened from a process watch.
7. Select the minimum number of days to store an attachment in the CA Process Automation database before deleting it.

   Users can use web services to trigger processes. A user can directly start a process or schedule a Start Request Form. Users can send files as attachments in the web services calls. When a web service call triggers a process, users can access the files in that process. A user can use the SOAP operator to forward an attachment to the outgoing web services call.

8. Specify requirements for purging process instances that were run on the selected Orchestrator and were subsequently archived. Alternatively, purge process instances, which were started within a specified data range, on demand.

   a. Define a policy for purging archived data. Options include:

      Do Not Purge Archived Data

      Archived process instances are retained until manually purged.

      Purge Archived Data Daily

      Purge archived process instances as a scheduled task according to the settings of the following two fields.

      Purge Data Without Archiving

      The Process instances are retained as active for a configured interval. When that interval elapses, the data is purged. No process instances are archived.

   b. Define the time of day (in hh:mm format) at which to purge the archived instances that have been retained for the configured number of days.

   c. Define the number of days to retain archived process instances. After an archived instance is kept for the configured number of days, it is purged at the specified time.

   d. To purge archived instances that were started within a specified age range from the current Orchestrator, click the Delete Archived Instance button, select a date range, and click OK.

9. Specify whether to require authentication when a user tries to access attachments outside of CA Process Automation. If selected, users must supply valid credentials to access attachments.

10. Specify whether to enforce run-time security. If selected, Runtime Security is enabled for processes that are set to Enable or inherit an enabled setting.

    Note: If you select the Enable Runtime Security option here and you select Run as Owner as the Runtime Security option for a process, use Set Owner to establish the ownership of each affected process object. For more information, see the online help or the *Content Designer Guide*.

11. Click Save.

12. Click Unlock.

Configure Orchestrator Mirroring

Orchestrators mirror data and configuration information that is stored on the Domain Orchestrator. The mirroring setting specifies how often an Orchestrator checks for changes on the Domain Orchestrator. Changes to the Domain Orchestrator are applied to the Orchestrator on the local host. You can set the mirroring interval for an Orchestrator.

When you select a clustered Orchestrator, the interval you set applies to the mirroring to all active nodes in the cluster. A cluster node can be inactive when other nodes in the cluster are updated. In this case, mirroring occurs for the inactive node when it starts up.

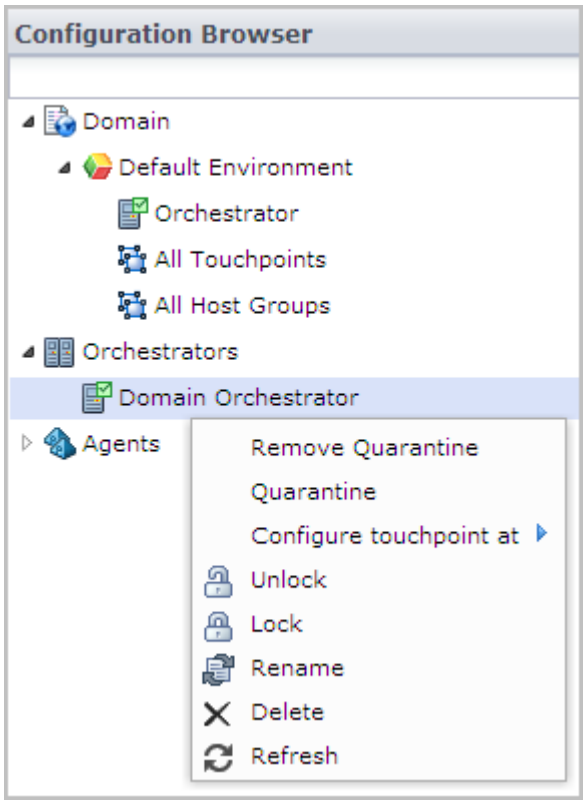
Note: You can upload a JAR file to the Orchestrator Resources folder on the Domain Orchestrator. When you restart the Domain Orchestrator, CA Process Automation deploys the file to the Domain Orchestrator. The Domain Orchestrator mirrors (copies) the file at the configured mirroring interval, after which you restart the other Orchestrators. When the Orchestrators restart, the mirrored file is available for their use.

Follow these steps:

1. Click the Configuration tab.
2. In the Configuration Browser palette, expand Orchestrators.
3. Select the Orchestrator to configure, and click Lock.
4. Click the Mirroring tab.
5. In the Mirroring Interval (Minutes) field, select the interval between the times that the selected Orchestrator requests updates from the Domain Orchestrator. The product mirrors any changes to the selected Orchestrator at the specified interval.
6. Click Save.
7. In the Configuration Browser palette, select the Orchestrator that you configured and click Unlock.

Maintain the Orchestrator Host

When you select an Orchestrator under the Orchestrators node, the details you see are relevant to the host, rather than its touchpoint.



See the following topics associated with the menu options for the Orchestrator host.

- Remove Quarantine

  See Remove the Quarantine from an Orchestrator (see page 185).

- Quarantine

  See Quarantine an Orchestrator (see page 184).

- Configure touchpoint at

  See Configure Orchestrator Touchpoint Properties (see page 168).

- Unlock - Select the Orchestrator and click Unlock.
- Lock - Select the Orchestrator and click Lock.
- Rename - Select the Orchestrator and type a new name.
- Delete - Select the Orchestrator and click Delete. You cannot delete the Domain Orchestrator.
- Refresh - Select the Orchestrator and click Refresh.

Quarantine an Orchestrator

You can quarantine any Orchestrator except the Domain Orchestrator. Quarantining isolates an Orchestrator. Operators cannot be executed on a quarantined Orchestrator. You cannot open the library of a quarantined Orchestrator. Therefore, you cannot create or save library objects on a quarantined Orchestrator.

Follow these steps:

1. Click the Configuration tab.
2. Right-click the Domain and select Lock.
3. Right-click the environment containing the Orchestrator you want to quarantine, and select Lock.
4. Expand the Orchestrators node.
5. Right-click the Orchestrator you want to quarantine, and select Lock.
6. Right-click the Orchestrator again, and select Quarantine.
7. Click Save.
8. Right-click the Orchestrator, and select Unlock.
9. Right-click the locked environment, and select Unlock.
10. Right-click the Domain, and select Unlock.

More information:

Remove the Quarantine from an Orchestrator (see page 185)
Delete an Orchestrator Touchpoint (see page 162)
Disable an Orchestrator Touchpoint (see page 172)

Remove the Quarantine from an Orchestrator

If the quarantine was created for a reason other than removing the Orchestrator, then remove the quarantine from the Orchestrator when the need for quarantine has passed.

To remove the quarantine from an Orchestrator

1. Click the Configuration tab.
2. Expand the Orchestrators palette.
3. Right-click the target quarantined Orchestrator and click Lock.
4. Right-click the Orchestrator again, and click Remove Quarantine.
5. Right-click the Orchestrator, and select Unlock.

   The Unsaved Data dialog opens asking if you would like to save changes.
6. Click Yes.

Stop the Orchestrator

Only administrators with administrator credentials on the server where the Orchestrator is installed can stop the Orchestrator.

Important! If an Orchestrator is not shut down gracefully, the following temporary folder can build up several gigabytes of files. If this happens, you can safely delete the tmp folder:

install_dir/server/c2o/tmp

Follow these steps:

1. Using Administrator credentials, log on to host where the target Orchestrator is installed.
2. If you logged in to a Windows host, you can stop the Orchestrator service from the Start menu, the Services window, or the command line. Complete one of the following actions:
   - Select Programs, CA, CA Process Automation 4.0, and Stop Orchestrator Service from the Start menu.
   - Select Administrative Tools and Services from the Control Panel. Select the following service and click Stop:

     CA Process Automation Orchestrator (C:/Program Files/CA/PAM/server/c2o)
   - Open a command prompt and run the following script:

     install_dir/server/c2o/bin/stopc2osvc.bat
3. If you logged in to a UNIX or Linux host, complete the following steps:
   a. Change directories to ${PAM_HOME}/server/c2o/. For example, change directories to:

      /usr/local/CA/PAM/server/c2o
   b. Run the c2osvrd.sh script with the stop option. For example:

      ./c2osvrd.sh stop

Start the Orchestrator

Only administrators with administrator credentials on the server where the Orchestrator is installed can restart the Orchestrator service.

Follow these steps:

1. Using the Administrator credentials, log on to host where the target Orchestrator is installed.
2. If you logged in to a Windows host, you can restart the Orchestrator service from the Start menu, the Services window, or the command line. Perform one of the following tasks:
   - Select Programs, CA, CA Process Automation, and Start Orchestrator Service from the Start menu.
   - Select Administrative Tools and Services from the Control Panel. Select the following service and click Start:

     `CA Process Automation Orchestrator (C:/Program Files/CA/PAM/server/c2o)`
   - Open a command prompt and run the following script:

     install_dir`/server/c2o/bin/startc2osvc.bat`
3. If you logged in to a UNIX or Linux host, perform the following tasks:
   a. Change directories to ${PAM_HOME}/server/c2o/. For example, change directories to:

      `/usr/local/CA/PAM/server/c2o`

   b. Run the c2osvrd.sh script with the start option. That is, run:

      `./c2osvrd.sh start`

Note: After starting the service for the Domain Orchestrator, start CA Process Automation.

More information:

Configure File Trigger Properties at the Domain Level (see page 319)
Configure SNMP Trigger Properties at the Domain Level (see page 323)
Administer Triggers (see page 313)
Configure Mail Trigger Properties at the Domain Level (see page 320)

Purge Archived Process Instances from an Orchestrator

You can purge on demand the process instances that ran during a date range you specify.

Purge archived process instances from the Runtime database of an Orchestrator in the following situations:

- You need more available space; the accumulation of archived instances is causing the performance to degrade.
- You set the Orchestrator policy to turn off automatic purging.

Follow these steps:

1. Click the Configuration tab and expand the Orchestrators node in the Configuration Browser.

   The expanded node displays all the Orchestrators in the Domain.
2. Right-click the Orchestrator that contains the archived process instances to purge, and click Lock.
3. Click the Policies tab.
4. Click the Delete Archived Instance button at the bottom of the pane.
5. In the Delete Archive Instance dialog, define the date range in which to purge archived instances.
   a. Click the From date calendar button and select Today or a start date that precedes today.
   b. Click the To date calendar button and select Today or an end date that is after today.
   c. Click OK.
6. Click Yes on the confirmation message.

   The purge process deletes all archived instances that ran during the specified date range.
7. Right-click the Orchestrator, and click Unlock.

Chapter 8: Administer Agents

An agent is a component that you install on multiple hosts in each environment. After you install an agent on a host, you configure a touchpoint (a logical entity) that associates the current environment with the agent host.

Agents support the running of processes. Processes are composed of operators. Most operators run on the Orchestrator. When an operator runs on an agent host, it does so at the direction of the Orchestrator and it returns the results to the Orchestrator. The Orchestrator runs the main process.

To ensure that an agent host is always available for processing, you associate multiple agent hosts to a single touchpoint. A touchpoint associates one or more agents with a specified environment. Content designers typically target an agent host by targeting its touchpoint.

To run operators on remote hosts that have no agent, associate an agent with proxy touchpoints or host groups. Operators can run on a remote host with no agent when an SSH connection is configured from the agent host to the target remote host. To run on a remote host, operators target the proxy touchpoint.

For information about how to configure failover (priority settings) or load balancing among agents that are associated with the same touchpoint, see Administer Touchpoints (see page 223).

For information about establishing SSH connections, see Administer Proxy Touchpoints (see page 243) and Administer Host Groups (see page 249).

This section contains the following topics:

Configure Agents to Support Operator Targets

Agent configuration in a design environment is typically limited to configuring a small set of touchpoints, each mapped to a single agent. If hosts are in short supply, you can associate multiple touchpoints to the same agent.

More robust agent configurations are typical of production environments. Six options are first presented separately, then on a summary table for reference. Use these details to plan and implement agent configuration in the production environment.

Operator runs on a specific agent host.

This option is the easiest to implement when running an operator on one host with an agent. This option is acceptable in a development or test environment.

Actual target

Host name or IP address of the target.

Installation requirement

Install an agent on the target host.

Association requirement

Define a touchpoint that associates an agent with the production environment.

Operator target

Enter the touchpoint name. Alternatively, you can enter the agent ID.

Operator runs on the highest priority agent, of several possible agents.

This option lets you specify that the operator run on the most desirable host if it is available, and if not the next most desirable. You decide what makes one host more desirable than another. You can configure a touchpoint so that a given operator always runs on the host with the largest capacity. Or, you can reserve such hosts and only run on them if all other candidates are busy.

Actual target

Unknown. Record the host names of the candidate target hosts, with preference order.

Installation requirement

Install an agent on each candidate target host.

Association requirement

Define a touchpoint and associate it with each of the candidate target hosts. In the touchpoint definition, specify the rank of priority for each.

Operator target

Enter the touchpoint name.

Operator runs on the least busy agent, of several possible agents.

This option takes longer to implement than a touchpoint associated with one agent, but is a robust option when targeting a host with an agent. This option is designed for a production environment where it is important that the process runs at the scheduled time.

Actual target

Unknown. Record the host names of the candidate target hosts.

Installation requirement

Install an agent on each candidate target host.

Association requirement

Define a touchpoint and associate it with each of the candidate target hosts. In the touchpoint definition, enter the same number as the priority for each association. This implementation is for load balancing.

Operator target

Enter the touchpoint name.

Operator runs on multiple agent hosts at once.

Use of the touchpoint group lets you run an operator simultaneously on all hosts that are associated with touchpoints in the group.

Actual targets

Record the host name of each target host.

Installation requirement

Install an agent on each target host.

Association requirement

- Define a separate touchpoint for each of these agents.
- Define a touchpoint group that is composed of these touchpoints.

Operator target

Enter the touchpoint group name.

Operator runs on a specific remote host.

Sometimes, you cannot install an agent on a host you want to target for an operator. In this case, define an agent as the proxy touchpoint. Create an SSH connection from the host with the agent to the target remote host.

Actual target

Record the host name or IP address of the remote host that is the target.

Enabling source host

Record the host name of the source host that can connect to the target with an SSH connection.

Connectivity requirement

Create the SSH connection from the source host to the remote host.

Installation requirement

Install an agent on the source host.

Association requirement

Define a proxy touchpoint on the source host and specify details of connection to the remote target host.

Operator target

Enter the proxy touchpoint name.

Operator runs on a remote host, where the target can be changed each run.

This option lets you decide what remote host to target immediately before runtime, when you specify the target with its host name or IP address. The target must be a member of a host group. A host group is a group with either a common host name pattern or a common IP address pattern. Hosts with a common IP address pattern belong to the same subnet.

Actual target

Unknown. Record the host names of the candidate target remote hosts.

Enabling source host

Record the host name of the source host that can connect to each of the candidate targets with an SSH connection.

Connectivity requirement

Create the SSH connection from the source host to each remote host.

Installation requirement

Install an agent on the source host.

Association requirement

Define a host group on the source host with a pattern that remote hosts have in common.

Operator target

Enter the host name or IP address of the target remote host. Express the operator target in a dataset. You can modify datasets, even when imported with a non-modifiable process.

Use the following table as a guide for creating summary tables for yourself. Documentation in the form of summary tables can help others find this information when you are not available.

Target Type	Agent Association	Other Configuration	Operator Target
A single host	A new touchpoint	N/A	Touchpoint name
One of multiple hosts, in priority order	An existing touchpoint	Specify priority in which to select the target host.	Touchpoint name
One of multiple hosts (no priority)	An existing touchpoint	Assign same priority to each candidate target host.	Touchpoint name
Multiple hosts at once	A new touchpoint	Create a touchpoint group with all touchpoints.	Touchpoint group name
A single remote host	A proxy touchpoint	Create an SSH connection from the agent host to the remote target host.	Proxy touchpoint name

Target Type	Agent Association	Other Configuration	Operator Target
One of multiple remote hosts	A host group	Create an SSH connection from the agent host to each remote target host.	Target host name or IP address

Install an Agent Interactively

Processes can include operators that must run on servers with a target application, database, or system. If possible, install an agent on such a server. If not possible, install the agent on a host that can connect to that server through SSH.

Important! Before you install an agent, verify that the Domain Orchestrator is running.

Follow these steps:

1. Click the Configuration tab.
2. Click the Installation palette.
3. Click Install for Install Agent.

   A dialog appears showing the progress for downloading the application.
4. If you receive a security warning, click Run.

   The Language Selection dialog opens. The language of the host computer is selected by default.
5. Click OK or select another language and click OK.

   The welcome page of the CA Process Automation Agent Setup wizard appears.
6. Click Next.

   The License Agreement opens.
7. Read the license. If you accept the terms, click I accept the terms of the License Agreement. Click Next.

   The Set Java Home Directory page opens.
8. If the displayed Java home directory is not correct, browse to the JRE folder.

   All platforms support jre6; Windows supports jre6 and jre7.

   See the following example path for the Windows platform:

   ```
   C:\Program Files\Java\jdk1.7.0_45
   ```
9. Click Next.

   The Select Destination Directory page opens. On Windows hosts, the default path follows:

   ```
   C:\Program Files\CA\PAM Agent
   ```

10. Click Next to accept the default or enter a destination directory for the new agent, and click Next.

    The Select Start Menu Folder page opens.

11. (Windows only) Click Next to accept CA Process Automation Agent as your Start menu shortcut or type a new name and click Next.

    - (Optional) Create short cuts for all users on this host.
    - (Optional) Do not create a Start menu folder.

12. Examine the Domain URL. This is the URL from which you launched the agent installation. Click Next.

13. If the domain is secured (Support Secure Communication was selected during the installation of the Domain Orchestrator), provide the same Certificate Password that was used to install the Domain Orchestrator (and other Orchestrators).

14. Complete the General Properties page and then click Next.

    a. Enter the agent host name for Agent Host. This name identifies the host from which you started the installation.

    b. Change or accept the default Display Name, the host name.

    c. If you launched the agent installation from a Windows host, select Install as Windows Service.

    d. To force a new connection for each communication from an Orchestrator to an agent, select Use deprecated communication.

       We recommend that you leave this check box *cleared*. Simplified communications, the default, is preferred because it uses one persistent connection.

    e. If you selected Use deprecated communications, accept 7003 as the Agent Port unless this port is used. If the default port is used, enter an unused port number such as 57003 as the port on which the agent listens for communication with Orchestrators.

       Note: If deprecated communication is not used, then Orchestrators use a web-socket connection (established by agents) to communicate to agents. Orchestrators use port 80 to communicate with agents over HTTP. Orchestrators use port 443 to communicate with agents over HTTPS.

    f. Select Start Agent after Installation.

       Starting the agent lets you view the active agent and continue with the agent configuration.

15. Click Next to accept the default temporary directory for executing scripts or enter another path and then click Next.

    Note: An acceptable path contains no spaces.

    The Set PowerShell execution policy page appears.

16. Complete the setting in one of the following ways.
    - To run Windows PowerShell scripts through this agent:
        a. Select the Set PowerShell Execution Policy check box.
        b. Browse to the PowerShell host location if different from the displayed default.
        c. Click Next.
    - If you do not use Windows PowerShell, click Next.

    The Agent installation starts.
17. Click Finish.
18. (Windows only) Start the agent service. Click Start, Programs, CA, CA Process Automation Agent, Start Agent service.
19. Click the Configuration Browser palette on the Configuration tab.
20. Click Refresh. (Or, log out and log back in.)
21. Expand Agents and verify that your agent name is listed.

    Note: To use the agent host as a target, configure a touchpoint. To use the agent host as a gateway to a remote host, configure a proxy touchpoint.

More Information

About Agent Communication (see page 219)

Add an Agent Touchpoint

When you install an agent on a host, the agent display name appears under the Agents node. For an operator to be able to target that host, you configure a touchpoint that references the host.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Agents node.
3. Right-click the agent and select Configure touchpoint at, then select the *environment*.

   A prompt to lock the selected environment appears.
4. Click Yes to lock the selected environment.

   The Add Agent Touchpoint dialog appears.

5. Enter a name for the new touchpoint that is different from the host name, and click OK.

   The new touchpoint appears under the All Touchpoints node for the associated environment.

6. Click Save.

7. Select the locked environment and click Unlock.

More information:

Administer Touchpoints (see page 223)
Administer Proxy Touchpoints (see page 243)

Add an Agent Host Group

If an operator must target remote hosts directly (with an IP address or host name), you can:

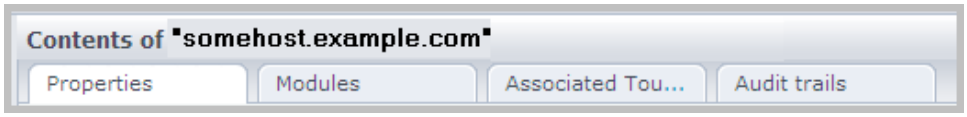
1. Create a host group (see page 252).
2. Configure host group properties (see page 253). You can add specific remote hosts or you can enter patterns that include the hosts that you want to target.
3. Create SSH credentials on hosts in a host group (see page 258). That is, create a user account on each remote host with the credentials entered in the host group properties.

More information:

Administer Host Groups (see page 249)

Configure the Contents of a Selected Agent

Many Properties settings are retrieved during the agent installation. Associated touchpoints are configuration details that are unique to agents and are not inherited. Settings for operator settings on the Modules tab are inherited by default. The settings that you configure for an agent are different from the settings that you configure for the agent touchpoint.



The Agent menu has the following tabs:

Properties

See Configure Agent Properties (see page 198).

Modules

See Customize Agent Settings for Operator Categories (see page 199).

Associated Touchpoints and Host Groups

See View the Touchpoints and Host Groups for a Selected Agent (see page 201).

Audit Trails

See View the Audit Trail for an Agent (see page 338).

Configure Agent Properties

You can set the agent properties in the Configuration Browser.

Follow these steps:

1. Click the Configuration tab and expand Agents on the Configuration Browser palette.
2. Select the agent to configure and click Lock.
3. Select the Properties tab for the selected agent.
4. (Optional) Review the following read-only properties:
   - Status - Locked or Quarantined.
   - Agent Name - name configured as Display Name at installation.
   - Host Name - name configured as Agent Host at installation.
   - Host Address
5. (Optional) Update the following properties:
   - Mirroring Interval (Minutes)
   - Use Deprecated Communication
6. Select the agent and click Unlock.
7. Click Yes on the Unsaved Data dialog to save the changes.

Customize Operator Category for a Selected Agent

All environments, Orchestrators, and agents inherit settings that you configured on the Modules tab for the Domain. Administrators can edit the configuration at lower levels of the Domain hierarchy. Administrators can also enable categories of operators on any agent and can edit the configurations as necessary.

Follow these steps:

1. Click the Configuration tab.
2. Expand agents, right-click the agent to customize, then select Lock.
3. Click the Modules tab.
4. Select Enabled from the Enable/Disable drop-down list for the operator category to edit.
5. Right-click the same category, then select Edit.
6. Change the property settings of the selected category for the selected agent. For more information, see the following Domain-level field descriptions:
   - Configure Catalyst (see page 272).
   - Configure Command Execution (see page 278).
   - Configure Databases: Oracle properties (see page 284).
   - Configure Databases: MSSQL Server properties (see page 286).
   - Configure Databases: MySQL properties (see page 288).
   - Configure Databases: Sybase properties (see page 289).
   - Configure Directory Services (see page 291).
   - Configure Email.
   - Configure File Management (see page 296).
   - Configure File Transfer (see page 298).
   - Configure Network Utilities (see page 300).
   - Configure Process Control (see page 301).
   - Configure Utilities (see page 302).
   - Configure Web Services (see page 304).
7. Click Save and click OK on the verification message.
8. Right-click the locked agent, then select Unlock.

Disable an Operator Category on a Selected Agent

From the Modules tab for a selected agent, you can disable one or more operator categories for that agent.

Follow these steps:

1. Click the Configuration tab and expand Agents on the Configuration Browser palette.
2. Select the agent to configure and click Lock.
3. Click the Modules tab.
4. Select an operator category for which Enable/Disable is set for Enable or Inherit from Environment.
5. Select Disable from the Enable/Disable drop-down list.
6. Click Save.
7. Click Unlock.

   The product disables the selected operator category on the selected agent.

Configure a Selected Touchpoint or Host Group

A touchpoint is an association between an agent (or Orchestrator) and an environment. A proxy touchpoint is an association between an agent, a remote host, and an environment. A host group is an association between an agent, a group of remote hosts, and an environment.

When you add a touchpoint or proxy touchpoint to an agent, that touchpoint appears under All Touchpoints.

When you add a host group to an agent, that host group name appears under All Host Groups.

See the following topics for configuration details:

- Administer Touchpoints (see page 223).
- Administer Proxy Touchpoints (see page 243).
- Administer Host Groups (see page 249).

View the Touchpoints and Host Groups for a Selected Agent

You can view the touchpoints and host groups for a selected agent on the Associated Touchpoint tab.

Follow these steps:

1. Click the Configuration tab and expand Agents on the Configuration Browser palette.
2. Select the agent for which to view touchpoints and host groups.
3. Click the Associated Touchpoint tab.

   The names of the touchpoints or host groups and the hierarchy (where Domain is the root node) are displayed.

Quarantine an Agent

Quarantining isolates an agent from incoming or outgoing network traffic from CA Process Automation. Operators cannot be executed on a quarantined agent. Quarantine an agent whenever you want to prevent it from being a CA Process Automation operator target.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Agents node.
3. Select the agent you want to quarantine and click Lock.
4. Right-click the agent and select Quarantine. The quarantine modifier is added to the locked agent base icon.

5. Click Unlock.

   The Unsaved Data dialog opens asking if you would like to save changes.

6. Click Yes.

   The quarantine modifier is displayed for the touchpoint or host group associated with the quarantined agent.

Remove Quarantine from an Agent

Once the quarantine period is over, remove the quarantine from the agent.

Follow these steps:

1. Click the Configuration tab and expand the Agents node.
2. Click the quarantine agent for which you want to remove the quarantine, and click Lock.
3. Right-click the agent, and click Remove Quarantine.
4. Click Unlock.

   The Unsaved Data dialog opens asking if you would like to save changes.
5. Click Yes.

   The lock modifier for the agent base icon is removed. The quarantine modifiers for the agent and associated touchpoint or host group base icons are replaced with the active icon modifier.

Rename an Agent

The name for an agent defaults to the host name during the agent installation process. You can rename the agent. For example, you could replace the FQDN for the host with Agent-*host_name*.

Follow these steps:

1. Click the Configuration tab and expand Agents on the Configuration Browser palette.
2. Select the agent to rename and click Lock.
3. Right-click the agent and select Rename.
4. Type the new name.
5. Click Save.
6. Select the agent and click Unlock.

Identify the Installation Path of an Agent

You can identify the path where an agent is installed. The default path for a Windows 7 operating system is:

```
C:\Program Files (x86)\CA\Pam Agent\PAMAgent
```

Follow this step:

Use the following script to identify the agent installation path:

```
echo %C2OHOME%
```

The script returns the full installation path of the CA Process Automation agent.

Note: This script assumes that you have defined C2OHOME as an environment variable.

Manage the Decommissioning of a Host with an Agent

When you are notified that your company plans to replace hardware on which you have installed agents, consider the following process to minimize the impact. This process reassigns the original touchpoints to agents installed on new hardware. The reassignment allows processes that rely on these touchpoints to continue to run without modification.

Two common situations follow:

- The old hosts are removed and then the new hosts are added. This practice is common when IP addresses are reassigned.
- The new host is added and then the old host is removed.

In the case where the plan is to remove old hosts before deploying new ones, consider the following approach:

1. Do the following before a host is removed from the network:
    a. Identify the agent name in CA Process Automation for the host that is being decommissioned.

       The Agents palette in the Configuration Browser lists all agents with their status.

    b. Identify the touchpoints associated with the agent targeted for deletion.

       On the Agents palette in the Configuration Browser, select the agent, and click the Associated Touchpoints tab to view the list of touchpoints to evaluate for reassignment.

    c. Uninstall the agent software from the host being decommissioned or repurposed.

2. Install the agent software on the host that replaces the decommissioned host.
3. Associate the impacted touchpoint with the new agent.
4. Remove the agent for the decommissioned host from CA Process Automation.

   On the Agents palette in the Configuration Browser, right-click the agent, select Lock, and then right-click and select Delete.

In the case where the new hosts are brought into the network before the old hosts are taken out, consider the following approach:

1. Install an agent on each new host.
2. Associate the impacted touchpoints with new agents.
3. Use Bulk Agent Removal to remove the agents that have been replaced.

More information:

Remove Selected Agents in Bulk (see page 205)
Remove Unused Empty Touchpoints in Bulk (see page 235)
Associate a Touchpoint with a Different Agent (see page 234)

Delete an Agent

When you no longer want an agent that you have installed, uninstall that agent from the host. Then, delete that agent from the Agents palette.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Expand Agents and verify that the target agent is unlocked and not quarantined.
3. Select the target agent and click Delete.

   A confirmation dialog appears.
4. Click OK.
5. Click Save.
6. Select Domain and click Unlock.

Remove Selected Agents in Bulk

When servers used for agents are decommissioned, you can remove the CA Process Automation references to these inactive agents in bulk. Then you can remove, in bulk, the associated empty touchpoints.

When replacement of servers is done a subnet at a time, you can select the associated agents for removal by specifying a CIDR-based search. If the servers being decommissioned have a common pattern in their host names, you can select agents for removal based on a specified pattern matching criteria.

Follow these steps:

1. Click the Configuration tab.
2. Right-click Domain and select Lock.
3. Right-click Domain and select Bulk Agent Removal.
4. Enter search criteria in one of the following ways:
   - Select Search for IP address pattern and enter a subnet in CIDR format that contains the target IP addresses.
   - Select Search by host name pattern and enter a search expression that includes the domain name, for example, *.*mycompany*.com.
   - Select one of the patterns but leave the search field blank.
5. Click Search.

   The Agents table displays all agents that match the search criteria, but only inactive agents can be selected for removal.
6. From the inactive agents displayed, select the agents to remove and click Delete.

   A confirmation message that states the number of agents selected asks whether to continue or cancel.
7. Select Continue.

   The selected agents are removed from the domain and the change to the domain is automatically saved.
8. Right-click Domain and select Unlock.

More information:

Remove Unused Empty Touchpoints in Bulk (see page 235)
Lock the Domain (see page 131)
Manage the Decommissioning of a Host with an Agent (see page 203)

Start an Agent

Use the agent start or restart method for the operating system on the host containing the agent.

Start or restart an agent on a Microsoft Windows host

The following steps apply to any agent in your CA Process Automation domain that resides on a host with a Windows operating system.

Follow these steps:

1. Log on to Windows host on which an agent is installed.
2. From the Start menu, select Programs, CA, CA Process Automation Agent, Start Agent Service.
3. Log off the host.

Start or restart an agent on a Linux host

The following steps apply to any agent in your CA Process Automation domain that resides on a host with a UNIX or Linux operating system.

Follow these steps:

1. Log on to the UNIX or Linux host on which an agent is installed.
2. Change directories to:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Run the following command:

   ```
   ./c2oagtd.sh start
   ```

   The agent restarts.

Stop an Agent

You can stop a CA Process Automation agent running on a UNIX or Linux host.

Stop an agent on a Microsoft Windows host

The following steps apply to any agent in your CA Process Automation domain that resides on a host with a Windows operating system.

Follow these steps:

1. Log on to Windows host on which an agent is installed.
2. From the Start menu, select Programs, CA, CA Process Automation Agent, Stop Agent Service.
3. Log off the host.

Stop an agent on a Linux host

The following steps apply to any agent in your CA Process Automation domain that resides on a host with a UNIX or Linux operating system.

Follow these steps:

1. Log on to the UNIX or Linux host on which an agent is installed.
2. Change directories to:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```
3. Run the following command:

   ```
   ./c2oagtd.sh stop
   ```

   The agent stops running.

Agent Management Console

The Agent Management console lets the administrators in the PAMAdmins group view the list of available agents in a domain. They can then select a single agent or multiple agents from the console to obtain the status for the selected agents. The status of the agent helps administrators identify whether the agent is able to run PAM operators.

Irrespective of the communication mode (Simplified or Deprecated), all agents are displayed in the Agent Management console. Also, the Active or Inactive status is reflected on the Agent icon.

Note: For more information about user roles and permissions, see the Role-Based Access to Configuration (see page 47), Permissions Reference (see page 98), and Grant Permissions to the Environment Configuration Administrators Group (see page 113).

Obtain the Status for an Agent

You can use the Agent Management console to obtain the status for a single agent or multiple agents. The status of an agent enables you to determine whether the agent is able to run PAM operators.

Follow these steps:

1. Click the Agent Console button from the toolbar of the Configuration browser to access the Agent Management console.

   The console is populated with the following columns for the available agents:

   Agent Name

   Indicates the configured name during installation.

   Agent Hostname

   Indicates the host name of the server where the agent is installed.

   IP Address

   Indicates the IP address of the server where the agent is installed.

   Status

   Indicates whether the agent is active or inactive. Default value is blank.

   Status Updated

   Indicates the date and time when the status for the particular agent was last obtained. Default value is blank.

2. Select one or multiple agents or enter the agent name, hostname, or IP address in the Search field, click Search, and select the required agents.

3. Click the Get Status button from the toolbar.

   The console is populated with the following information:

   - The Status column displays the agent status as Active or Inactive.
   - The Status Updated column is updated with the latest date and timestamp.

   Note: For quarantined agents, the status is displayed as Inactive in the Status column.

4. Click Reload. The information in the Status and Status Updated columns from the console are cleared. Also, the new agents that are installed display in the console.

   Note: Based on the number of agents that are selected, the Status and Status Updated columns can take more time to populate the information.

How to automatically Upgrade Agents through CA Process Automation Content

As an administrator in the PAMAdmins group, you can upgrade agents from the following versions to CA Process Automation 4.2 Service Pack (SP) 2:

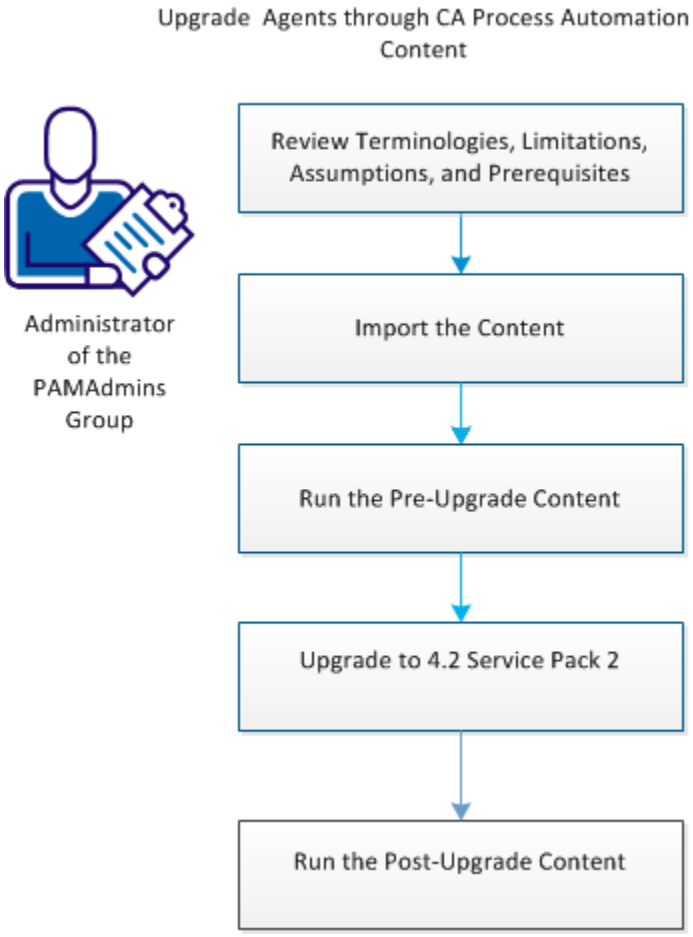
- 3.1 Service Pack 1 CP 12
- 4.0 and 4.0 Service Pack 1
- 4.1 and 4.1 Service Pack 1

Important! Run the content before you upgrade the domain orchestrator to a new version.

The content enables you to upgrade agents to CA Process Automation 4.2 SP2 automatically without using the following approaches:

- Manual reinstallation of the agent.
- Using an external code or patch management tool.

The following diagram describes how an administrator in the PAMAdmins group can upgrade the pre-4.2 agents to the 4.2 SP2 release:



Review Terminologies, Limitations, Assumptions and Prerequisites

Review the following terminologies before you run the content:

- Active agents

  Indicates the agents for which the pre-upgrade content obtains the details.

- Inactive agents

  Indicates the agents for which the pre-upgrade content does not obtain the details.

- Content

  CA Process Automation content that is designed using automation objects for automatically upgrading agents.

Note: The following steps are optional:

- View the Output after content execution:

  After the content is run, the results are saved in the datasets. Whenever required, you can verify the output using the datasets.

- Verify the upgraded agents after the post-upgrade content is executed:

  The IsReinstalled field in the Agent Details dataset is set to 'True' for the agents that are successfully upgraded.

Review the following prerequisite before you run the content:

- Create touchpoints for the agents you want to upgrade before you run the pre-upgrade content. For more information about creating touchpoints, see Administer Touchpoints in the *CA Process Automation Content Administration Guide*.

Review the following limitations before you run the content:

- The content is not supported when domain orchestrator runs on non-windows platform, that is, Linux, Solaris.
- You cannot use the content to upgrade from the CA Process Automation 4.2 version to 4.2 SP2 version.
- Agents that run in console mode can fail to upgrade.
- The Certificate Password field in the Upgrade Agents form is plain text instead of a password field.
- No support for agents that run on Windows 2003 Server R2 and Windows XP.

Review the following assumptions before you run the content:

- Orchestrator and agents run in service mode.
- Domain orchestrator is installed on the Windows platform.
- By default, FTP/SFTP and SSH are enabled for non-windows agents.

Import the Content

The installation media contains content (CA PAM Upgrade Agents.xml) that enables you to upgrade the agents automatically.

Follow these steps:

1. Import the content to any folder as follows:
   - For the CA Process Automation 3.1 version:
     a. Log in to PAM and click CA Process Automation Client.

        The previously installed agents are listed in the Configuration browser.

     b. Access the Library folder, right-click the folder, select the content, and click Import.
   - For CA Process Automation 4.0 and 4.1 versions:

   1. Log in to CA Process Automation.
   2. Access the Library tab, right-click the folder, select Import, select the Content, and click Open.

   After the content is imported successfully, a folder with the name, CA PAM Upgrade Agents is created in the left pane.
2. Verify the following folders in the CA PAM Upgrade Agents folder:
   - Pre-Upgrade content
   - Post-Upgrade content

   Important! Do not modify to the objects in the Core Content and Output folder.

Run the Pre-Upgrade Content

The pre-upgrade content enables you to obtain the details of the agents in the existing environment. The steps that are involved in obtaining the details for agents are as follows:

1. Obtain the details of the active agents (see page 214)
2. View the output of content execution (see page 216)

Obtain the Details of the Agents

To obtain the details of the agents in the existing environment, run the pre-upgrade content. The pre-upgrade content uses the details of the agents to upgrade the agents to the current release.

Important! Run the content before you upgrade the domain orchestrator to a new version.

Follow these steps:

1. Start the SRF Get Agents details from the Pre-Upgrade Process Watch.
2. Enter the SOAP URL in the SOAP_URL field and click Finish.

   The content starts obtaining details of the agents in your environment and is run for both windows and non-windows agents.
3. Monitor the Get Agents Details process using the Pre-Upgrade Process Watch until the process instance changes to the Waiting state.

   Based on the number of agents in your environment, the 'Results for Get Agents Details' task can take more time to populate.
4. Navigate to the Group Tasks tab of the Tasks pane to view the 'Results for Get Agents Details' task.
5. Right-click the 'Results for Get Agents Details' task and select Reply to view the results.

   If there are no inactive agents, a success message displays in the task. However, agents can fail due to many reasons and a list of inactive agents is displayed for the same.

   You can decide to resolve the problems with the inactive agents and rerun the SRF Get Agents Details as follows:

   a. Start the inactive agents in the InactiveAgentsList dataset.

      Note: For more information, see Start the Agent in the *CA Process Automation Installation Guide*.

   b. Follow steps 2 through 5.

   c. Verify the output (see page 216).

      The content updates the details of the agents in the Agent Details and Inactive AgentList datasets. Information regarding the inactive agents that are activated is appended to the Agent Details dataset and the Totalnumberofactiveagents field is increased.

      Similarly, the information regarding the inactive agents that are activated is removed from the InactiveAgentList dataset. You can run the content until the Totalnumberofinactiveagents field changes to zero.
6. Click Finish.

The content is run successfully and the status of the 'Results for Get Agents Details' task changes to Completed. Also, the state of the Get Agents Details instance changes to Completed.

Notes:

- You can reset the details in the datasets and can rerun the SRF Get Agents details to obtain a new set of details for the agents. All the details in the datasets that are related to the pre-upgrade content in the Core Content and Output folder are cleared. To repopulate the details in the datasets, follow these steps:

  a. Manually delete the details from all the datasets that are related to the pre-upgrade content in the Core Content and Output folder

  b. Change the Totalnumberofinactiveagents field to 0.

  c. Rerun the SRF Get Agents details to populate the details in the datasets.

- During the pre-upgrade content execution, the operators can cause an Echo Off error.

  Symptom:

  During operator execution in CA Process Automation, when the operator is unable to find the c2oHome location of the agent or the orchestrator, the Echo Off error displays in the Operator Runtime dataset.

  Solution:

  To mitigate the issue, follow these steps:

a. Select My Computer > System Properties > Advanced > Environment Variables.

b. Add the c2oHome variable.

   - For the CA Process Automation agent, provide the location where the agent is installed.
   - For the domain orchestrator, provide the location for c2oHome. For example, C:\Program Files\CA\PAM\server\c2o.

View the Output after Content Execution

To ensure that the content ran successfully, verify the information for active and inactive agents in the following datasets in the Output folder:

- Agent Details

  Contains the information for active agents.

- Inactive Agent List

  Contains the list of inactive agents.

Follow these steps:

1. Double-click the Agent Details dataset and verify the following information for each agent:

   Name

   Indicates the configured name during installation.

   User

   Indicates the username of the agent. Default value is blank.

   Password

   Indicates the password of the agent. Default value is blank.

   JavaHome

   Defines the JavaHome that the agent uses during installation.

   Installed Location

   Location where the agent is installed.

   is Windows

   True if the agent is installed on Windows server.

   Hostname

   Indicates the host name of the server where the agent is installed.

   UUID

   Indicates the UUID of the agent.

   AgentInstaller Type

   Defines wrapper_32/wrapper_64 for Windows and blank for non-Windows.

   totalNoofActiveAgents

   Contains the total number of active agents.

   IsReinstalled

   Indicates if the agent is reinstalled and upgraded successfully.

2. Double-click the Inactive Agent List and verify the following information for each inactive agent:

   Hostname

   Indicates the host name of the server where the agent is installed.

   UUID

   Indicates the UUID of the agent.

   totalNoofInactiveAgents

   Indicates the total number of inactive agents.

   Note: You must rerun the SRF Get Agents details to upgrade the inactive agents to the higher version.

Upgrade to 4.2 Service Pack 2 Release

Upgrade your current release of CA Process Automation to the CA Process Automation 4.2 SP2 release. After you upgrade to CA Process Automation 4.2 Service Pack 2, run the content after upgrade to upgrade the active agents to 4.2 Service Pack 2.

Note: For more information on how to upgrade to the 4.2 Service Pack 2 release, see Upgrade to the Current Release and Upgrade Examples in the *CA Process Automation Installation Guide*.

Run the Post-Upgrade Content

The post-upgrade content enables you to upgrade the active agents in the AgentDetails dataset to the CA Process Automation 4.2 SP2 release. The steps involved in upgrading the active agents to the CA Process Automation 4.2 SP 2 release are as follows:

1. Upgrade the agents to the CA Process Automation 4.2 Service Pack 2 release (see page 218)
2. View the output of content execution (see page 219)

Upgrade the Agents to the 4.2 Service Pack 2 Release

When you run the post-upgrade content, the active agents in the AgentDetails dataset are upgraded to the 4.2 SP 2 release.

Follow these steps:

1. Log in to CA Process Automation 4.2 Service Pack 2 version and navigate to the Library tab.
2. Navigate to the folder where the content is imported.
3. Start the SRF Upgrade Agents from the Operations tab.
4. Enter the following information in the Upgrade Agents form:

   Certificate Password

   Enter the certificate password for the domain orchestrator.

   Note: The entered password displays in plain text.

   Username and password

   Enter the username and password for each orchestrator node in the cluster setup.

   Important: The Operating system account credentials (username and password) are assumed to be same across the nodes.
5. Click Finish.

   The content runs for both Windows and non-windows agents. The 'Select Agents to Upgrade' task displays with the Pending status in the Group Tasks tab of the Tasks pane.
6. Right-click the 'Select Agents to Upgrade' task and select Reply. The 'Select Agents to Upgrade' task displays the list of non-upgraded agents.
7. Select the agents that use the same user name and password to access their host machines from the 'Select Agents to Upgrade' task, then click Finish.

   The status of the 'Select Agents to Upgrade' task changes to Completed. The 'Results for Upgrade Agents' task can take more time to populate in the Tasks > Group Tasks pane, based on the number of agents that are selected.

   The resultant task displays a success message for successful upgrade. However, agents can fail to upgrade for many reasons and you can decide to resolve the problems associated with the agents and rerun the SRF Upgrade Agents as follows:

   a. Follow steps 2 through 6.

   b. Verify the output after content execution (see page 219).

      Until all agents are upgraded, you can rerun the content for the agents that fail to upgrade. The details of the agents that fail to upgrade are saved in the Failed Agent List dataset.

View the Output after Content Execution

After the post-upgrade content is run successfully, the following datasets are updated:

- Agent Details dataset in Pre-Upgrade Content folder

  Contains information regarding agents that are successfully upgraded.

  Note: The IsReinstalled field in the Agent Details dataset is set to 'true' for the agents that are successfully upgraded.

- Failed Agent List dataset in Output folder under Post-Upgrade Content

  Contains the agents that failed to upgrade.

  Note: If there are no failed agents, then the Failed Agent List dataset is not displayed.

Follow these steps:

1. Double-click the Agent Details dataset from the PostUpgrade Process Watch and verify the details for the agents that are successfully upgraded.
2. Double-click the Failed Agent List dataset and verify the details for the agents that failed to upgrade.

About Agent Communication

You configure agent communications when you install an agent. You can reconfigure this setting without reinstalling the agent.

Simplified Communication

The simplified communication uses web sockets and HTTP to produce a one way, persistent connection from the agent to the Orchestrator. CA Process Automation uses a standard port (80 or 443) that provides a fast connection between the components.

Deprecated Communication

The deprecated communication, which uses multiple ports, is not as firewall-friendly or NAT router-friendly as simplified communication. The Orchestrator-initiated connections used in deprecated communication is not as efficient as the persistent connections used in simplified communication.

Note: For recommendations on load balancers and the corresponding agent communication, see "Load Balancers and Communication" in the *Installation Guide*.

Configure Agents to Use Simplified Communication

You can configure agents to use simplified communication.

Follow these steps:

1. Click the Configuration tab and expand Agents on the Configuration Browser palette.
2. Select the agent for which to switch communication and click Lock.
3. Select the Properties tab for the selected agent.
4. Clear the Use Deprecated Communication check box.
5. Select the agent and click Unlock.
6. Click Yes on the Unsaved Data dialog to save the changes.

   The agent creates web socket connections and sends connection details to all Orchestrator nodes. Orchestrators use the persisted web socket connection to send requests or updates to the agent as needed.

Configure Agent to Use Deprecated Communication

Agents installed from CA Process Automation 4.2 use deprecated communication by default. If you previously switched the communication method to use simplified communication, you can switch agent communication back to deprecated communication.

If you have a firewall-enabled environment, reconfigure the firewall port usage before switching from simplified communication to deprecated communication. The Jetty ports used for simplified communication are the standard 80 and 443 for HTTP and HTTPS, respectively. The tomcat ports used in deprecated communication use 8080 and 8443. For more details about agent ports, see the "Ports Used by an Agent" topic in the *Installation Guide*.

Follow these steps:

1. Ensure that the agent is running.

   If the Agents palette displays a CA Process Automation agent as inactive, you can start the agent. See Start an Agent (see page 206).
2. Click the Configuration tab and expand Agents on the Configuration Browser palette.
3. Select the agent for which to switch communication and click Lock.
4. Select the Properties tab for the selected agent.
5. Select the Use Deprecated Communication check box.

6. Select the agent and click Unlock.
7. Click Yes on the Unsaved Data dialog to save the changes.

The agent terminates the web socket connection. After the web socket connection is terminated, the agent uses deprecated communication.

Chapter 9: Administer Touchpoints

Touchpoints map symbolic names to Orchestrators and agents. Touchpoints are used to identify the Orchestrator or agent within an environment. A layer is provided between CA Process Automation and the network topology, allowing CA Process Automation operators to be configured without explicitly specifying host information.

The category configuration for an operator specifies the touchpoint on which to run the operator. A user configuring a CA Process Automation operator selects a name from a list of touchpoints that are configured to run the operators in the same category as the referenced operator. This indirection allows you to substitute hosts at runtime. Indirection also allows you to define multiple CA Process Automation environments in which the same touchpoints are mapped to different real hosts.

This section contains the following topics:

Touchpoint Implementation Strategy

A *touchpoint* is an environment-specific logical representation of one or more managed resources. A *managed resource* is an agent or Orchestrator on which operators of a process run. To run an operator on a specific agent or a failover of that agent, specify the target as the touchpoint that is mapped to them.

Content administrators create touchpoints for process targets in the design environment after completing the process plans but before the design process starts. Content designers create the process, where operators target the touchpoints you created. Content designers test the process and then package it for transitioning to the production environment.

Before you transition the process, you create similar touchpoints that associate production agents with the production environment. That is, you create the same touchpoint names or proxy touchpoint names in the production environment that you used in the design environment. Creating these touchpoints enables the operators in the transitioned process to continue to use the same touchpoints as operator targets.

Consider the following process:

1. Get a test version of the external system or activity that you plan to target.

   Examples of external entities include a Service Desk application, a production database, or a backup system.

2. Install an agent on the host with the test version of the entity that you plan to target.

   If this approach is not possible, create an SSH connection from an agent host to the host with the target then create a proxy touchpoint.

3. Map a touchpoint (or proxy touchpoint) to the agent in the design environment that runs the test copy of the targeted external system.

4. Designers run and test the process, where operators in the process target the touchpoint for testing.

5. During the transitioning of a process to the production environment, complete the following procedure for each target that is an agent touchpoint:

   a. Identify one or more hosts that are running the application, database, or system to target.

   b. Install an agent on each identified host.

   c. Create a touchpoint that associates each agent that is a potential target with the production environment. Name the touchpoint with the same name used in the design environment.

6. During the transitioning of a process, complete the following procedure for each target that is a proxy touchpoint:

   a. Identity the remote host that is running the application, database, or system to target.

   b. Install an agent on an available host.

   c. Create an SSH connection from the agent host to the remote host.

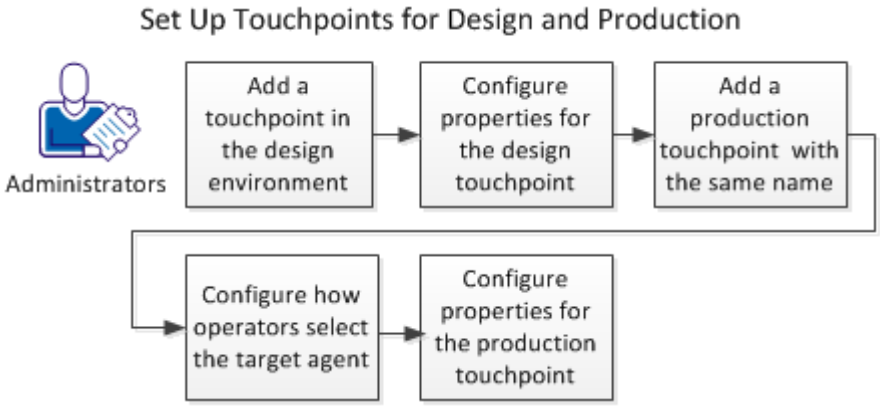
   d. Create a proxy touchpoint that associates the agent host with the production environment. Name the proxy touchpoint with the same name used for the proxy touchpoint in the design environment.

Set up Touchpoints for Design and Production

An operator that targets a touchpoint can run in both the design environment and in the production environment with no changes to the operator Target field. To make this possible, you define the same touchpoint name in each environment.

You can set up touchpoints for design and production as you finish these prerequisites:

- Install agents on hosts that the process is to target in the design environment.
- Install agents on hosts that the process is to target in the production environment.



Follow these steps:

1. Add a touchpoint in the design environment (see page 226).
2. Configure properties for the design touchpoint (see page 226).
3. Add a production touchpoint with the same name (see page 227).
4. Configure how operators select the target agent (see page 228).
5. Configure properties for the production touchpoint (see page 229).

More information:

Example: How Touchpoints Enable Content Portability (see page 33)

Add a Touchpoint in the Design Environment

A touchpoint associates an agent with an environment. You can add a touchpoint and associate it with an agent that is installed on a host that you want to target during design and testing.

Follow these steps:

1. Click the Configuration tab.
2. Expand Domain on the Configuration Browser.
3. Select the environment you use for design, and then click Lock.
4. Right-click the environment, and then click Add Touchpoint.
5. Enter a name for the new touchpoint in the Touchpoint Name field on the Add Touchpoint:*environment* dialog.
6. Select the agent that is installed on the host that you want to target with this touchpoint.
7. Click Add, click Save in the menu bar, and then right-click the environment and select Unlock.
8. View the touchpoint you added in the All Touchpoints node for the design environment. View the additional row in the Touchpoint Data tab.

More information:

Configure Properties for the Design Touchpoint (see page 226)
Configure Proxy Touchpoint Properties (see page 246)

Configure Properties for the Design Touchpoint

You configure properties for a touchpoint based on the environment. For touchpoints associated with a design environment, you have the option of recovering operators manually. This setting provides you with the better opportunity for troubleshooting. Touchpoint security typically targets mission critical hosts and is typically not applicable to any agent host used during design.

Follow these steps:

1. Click the Configuration tab.
2. Right-click the environment with the touchpoints to configure, and then select Lock.
3. Expand the environment, and then expand All Touchpoints.
4. Select the touchpoint to configure, and then click the Properties tab.

5. Set the Autorecovery of Operators property to allow you to recover operators manually. This setting gives you optimal control over recovering operators when required.
6. If an active Touchpoint Security policy protects this touchpoint, enable the Touchpoint Security property.

   Enabling the property enforces the applicable policy that specifies the users that are allowed to run operators on the current target.
7. Click Save.
8. Right-click the environment, and then select Unlock.

Add a Production Touchpoint with the Same Name

When content designers enter touchpoint names in the Target field for operators, the operator runs on the agent associated with the touchpoint in the design environment.

A touchpoint name must be unique within an environment. Two environments can have different touchpoints with the same name. The following scenario is valid, where there are two distinct touchpoints named TP-125.

- TP-125 associated with agent-1 and the design environment
- TP-125 associated with agent-2 and the production environment

Agents are not environment-specific.You can associate two touchpoints, with the same names, in different environments to the same agent.

When a process is transitioned to another environment, each operator must run on an agent used in the import environment. To prepare for the use of an imported process, do the following:

1. Identify each touchpoint targeted by an operator in a process that runs in the design environment. The process can be in the planning stage or it can be ready for export.
2. For each identified touchpoint, identify two appropriate agents used in the production environment on which the operator can run. Associating two agents rather than one is recommended for high availability.
3. In the production environment, create a touchpoint with the same name as the identified touchpoint. Associate it to the appropriate agents used in the production environment. The following procedure describes this step.

Follow these steps:

1. Click the Configuration tab.
2. Right-click the production environment in the Configuration Browser palette, and then click Lock.

3. Right-click the production environment, and then click Add Touchpoint.
4. Enter the same touchpoint name as the one used in the design environment. Enter the name in the Touchpoint Name field on the Add Touchpoint:*productionEvironment* dialog.
5. Select the two previously identified agents that can be targeted with this touchpoint.
6. Click Add, click Save in the menu bar, and then right-click the environment and select Unlock.
7. View the touchpoint you added in the All Touchpoints node for the design environment. View the additional row in the Touchpoint Data tab.

Note: If you associated multiple agents with the touchpoint in the target environment, you must configure how operators select the target agent.

More information:

Configure How Operators Select the Target Agent (see page 228)

Configure How Operators Select the Target Agent

You can associate multiple agents to the same touchpoint. When an operator targets such a touchpoint, the operator can either select a specific agent or select an agent randomly. By default, the operator selects the first agent that you associated with the touchpoint.

You can configure how operators select the agent on which to run.

- To instruct operators to select your preferred agent, assign that agent priority 1. Assign priority 2 to the backup agent.
- To instruct operators to select the agent randomly, assign priority 1 to all agents.

You can configure how operators select the target host by assigning priorities to the associated agents.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain, select environment to configure, and click Lock.
3. Expand the environment. Under All Touchpoints, click the agent touchpoint that you want to configure.

   The Agents tab displays the list of agents that are mapped to the selected touchpoint. Each agent is listed with a priority number that reflects the order in which it was added.

4. Examine the displayed priority settings and take one of the following actions:
   - For load balancing, assign the same number to each agent that can potentially be the active agent. For example, assign 1.
   - For backup, assign 1 to the agent to target with the touchpoint. Assign 2 to the backup agent that is to take over the operation only if the high priority agent becomes inactive.
   - For both, assign 1 to agents that are to participate in load balancing and assign a higher number to the agent or agents that are to serve as backups.
5. Click Save.
6. Select the environment and click Unlock.

Configure Properties for the Production Touchpoint

You can configure properties for a touchpoint based on the associated environment. In a production environment, enabling Operators Autorecovery reduces the time it takes to restore the running of a process when an operator with recoverable processes fails. Touchpoint Security is applicable only to high-valued hosts in the production environment. Therefore, set this property based on whether you have a Touchpoint Security policy that protects the agents associated with this touchpoint.

Follow these steps:

1. Click the Configuration tab.
2. Right-click the environment with the touchpoints to configure, and then select Lock.
3. Expand the environment, and then expand All Touchpoints.
4. Select the touchpoint to configure, and then click the Properties tab.
5. Set the Operators Auto Recovery property to recover operators automatically.

   This setting lessens the impact of network problems on production users.
6. If the production agents associated with this touchpoint are defined in a Touchpoint Security policy, enable the Touchpoint Security property.

   Enabling the property enforces the applicable policy that specifies the users that are allowed to run operators on these agents.
7. Click Save.
8. Right-click the environment, and then select Unlock.

Add One or More Touchpoints

You can add touchpoints one at a time.

Follow these steps:

1. Click the Configuration tab.
2. Expand Domain on the Configuration Browser.
3. Right-click the environment to configure, and then click Lock.
4. Right-click the environment, and then click Add Touchpoint.
5. Enter a name for the new touchpoint in the Touchpoint Name field on the Add Touchpoint:*environment* dialog.
6. Select an object to associate with the touchpoint from the drop-down list. Select:
   - An Orchestrator
   - An agent
   - Multiple agents
7. Click Add, click Save in the menu bar, and then right-click the environment and select Unlock.
8. View the added touchpoints in the All Touchpoints node for the selected environment. View the additional row in the Touchpoint Data tab.

More information:

Configure Properties for the Design Touchpoint (see page 226)
Configure Proxy Touchpoint Properties (see page 246)

Add One or More Agents to an Existing Touchpoint

You can add one or more agents to an existing touchpoint. We recommend that you add more than one agent to each touchpoint that you associate with your production environment. If one agent is unavailable, an operator that targets the touchpoint can run on another associated agent.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain node in the Configuration Browser palette, select an environment, and then click Lock.

3. If a touchpoint does not exist, create one:
   a. Expand the Agents node.
   b. Identify an agent that runs in the locked environment. Right-click the agent, select Configure Touchpoint At, and then select the locked environment.

      The Add Agent Touchpoint dialog appears.
   c. Enter the name of the respective touchpoint and click OK.
4. To add one or more agents to an existing touchpoint:
   a. Expand All Touchpoints for the selected environment, select the target touchpoint, and then click Add.
   b. Select one or more active agents that run in the locked environment, and then click Add. (The active agents are displayed in green.)

      The new agents to be associated with the selected touchpoint appears on the list in the Agents tab.
   c. Click Save.

      The selected touchpoint is now associated with the additional agents.
5. Right-click the locked environment, and then select Unlock.
6. Click Yes to the prompt to save changes.

Note: If you associated multiple agents with the touchpoint in the target environment, configure how operators select the target agent.

More information:

Configure How Operators Select the Target Agent (see page 228)

Add Touchpoints for Agents in Bulk

You can add touchpoints to new agents in bulk by specifying patterns for agent host names or IP addresses. Every agent with a host name or IP address that matches a specified pattern is automatically configured with a touchpoint. The touchpoint name is the same as the agent display name. An *auto-admit pattern* is a host name pattern expressed as a regular expression or an IP address subnet expressed in CIDR notation.

You can configure different auto-admit patterns for each environment or you can configure the same or overlapping auto-admit patterns across environments. Touchpoints are environment-specific. Agents are not environment-specific.

Follow these steps:

1. Click the Configuration tab.
2. Expand Domain in the Configuration Browser.
3. Right-click the environment you want to configure, and click Lock.
4. Click the Auto-Admit tab.
5. For each IP address pattern, take the following steps. Then use the up and down arrows to order the search list.
   a. Click Add in the IP Address Patterns area.

      An entry field appears.

   b. Enter an IPv4 subnet using CIDR notation.

      Note: CA Process Automation uses CIDR pattern matching for auto admit requirements. For example, the CIDR pattern 155.32.45.0/24 matches IP addresses in the range 155.32.45.0 through 155.32.45.255.
6. For each host name pattern, take the following steps. Then use the up and down arrows to order the search list.
   a. Click Add in the Host Name Patterns area.

   b. Enter a host name pattern.

      Note: The host name of the Orchestrator/agent is compared to the regular expressions specified. For example, if the pattern specified is ca\.com$, then all agents/Orchestrators whose host names end with ca.com are added.

7. Right-click the environment, and click Unlock.
8. Repeat this procedure for each environment.

   The Domain searches for a new Orchestrator and new agents with IP addresses or host names that match the auto-admit patterns for one or more environments.

   When the Domain discovers such new agents, the Domain creates a touchpoint for each match and automatically adds it to each environment. The name of the touchpoint is the display name of the agent.

   When the Domain discovers such an Orchestrator, the Domain creates one touchpoint for that Orchestrator and adds it to the first matching environment. An Orchestrator has only one touchpoint.

Example of touchpoints added to environments based on agent auto-admit patterns

In the following example, overlapping auto-admit patterns are defined for two environments. Two agents are installed, where the IP address of one matches the auto-admit pattern in one environment and the IP address of the other matches the auto-admit patterns in both environments. The result is that three touchpoints are automatically added.

- Environment1 has an auto-admit pattern of 155.32.45.0/24 (155.32.45.0 - 155.32.45.255)
- Environment2 has an auto-admit pattern of 155.32.45.32/27 (155.32.45.32 - 155.32.45.63)
- New agents with these addresses are installed:
  - 155.32.45.5 with display name of host1.mycompany.com
  - 155.32.45.50 with display name of host2.mycompany.com

The following touchpoints are automatically added based on the auto-admit patterns:

- Touchpoint name: host1.mycompany.com in Environment1
- Touchpoint name: host2.mycompany.com in Environment1
- Touchpoint name: host2.mycompany.com in Environment2

Associate a Touchpoint with a Different Agent

Associate an existing touchpoint with a different agent in cases such as the following:

- A process regularly runs on a host slated for removal from the network.

  Here, the touchpoint is associated with only one agent and that agent is installed on a host scheduled for decommission. If a touchpoint is associated with multiple agents, no action is needed.

- A process that has been running in one data center now must run in a different data center.

  Here, the process references a touchpoint that must be associated with an agent installed on a host in the new data center.

Changing the agent association for a selected touchpoint involves deleting the current agent association and then adding a new agent association. To run a tested process on multiple hosts, associate the same referenced touchpoint to the agent that runs on each target host.

You can replace the agent association for a given touchpoint.

Follow these steps:

1. Click the Configuration tab.
2. Expand the tree to display All Touchpoints and select the target touchpoint.

   The Agents tab in the main pane lists the agent or agents currently associated with the selected touchpoint.
3. Select the agent with which you want to break the association and click Delete.
4. When the delete confirmation message appears, click OK.

   The agent touchpoint is removed from the list.
5. Click Add.

   The Add agent reference to: *touchpointName* appears with a list of all agents. Active agents are displayed in Green.
6. Select one or more active agents and click Add.

   The new agent to be associated with the selected touchpoint appears on the list in the Agents tab.
7. Click Save.

   The selected touchpoint is now associated with a different agent.

More information:

Manage the Decommissioning of a Host with an Agent (see page 203)

Delete a Touchpoint

You can delete a touchpoint.

Follow these steps:

1. Click the Configuration tab.
2. Expand Domain and expand the environment with the touchpoint.
3. Right-click the environment with the touchpoint and click Lock.
4. Expand All Touchpoints and select the touchpoint to delete.

   The Agents tab opens and lists the agents that are associated with the touchpoint.
5. Select all agents that are associated with the touchpoint, and then click Delete.

   A confirmation message appears.
6. Click Yes.

   The deleted touchpoint is removed from the All Touchpoints list and from the Touchpoint Data tab.
7. Select Domain and click Unlock.

Remove Unused Empty Touchpoints in Bulk

Performing bulk agent removal can create multiple empty touchpoints. If these touchpoints are used in active processes, reassign them to other agents.

You can remove touchpoints at two levels:

- To remove selected touchpoints across environments, initiate the removal from the Domain right-click menu.

  You must have Content Administrator and Domain Administrator rights.
- To remove selected touchpoints within an environment, initiate the removal from the Environment right-click menu.

  You must have Content Administrator rights for the selected environment to remove its touchpoints.

Follow these steps:

1. Click the Configuration tab.
2. Lock the Domain or the target environment. If already locked with unsaved changes, save the changes.
3. Right-click the Domain or target environment and select Bulk Touchpoint Removal.

   The Bulk Touchpoint Removal dialog appears.
4. Click Search or enter a touchpoint name search expression and then click Search.

   The returned list includes only the names and states of empty touchpoints matching your search criteria. If you initiated the removal at the Domain level, the environment for each touchpoint is also shown.
5. Select the touchpoints to delete from the displayed list of touchpoints that are not mapped to agents, then click Delete.

   A confirmation states the number of touchpoints targeted for deletion.
6. Evaluate the message.
   - If the number displayed reflects the number you intended to select, click Continue to remove those touchpoints.
   - If there was a selection mistake, click Cancel and repeat Steps 4 and 5.

More information:

Remove Selected Agents in Bulk (see page 205)

Rename a Touchpoint

Renaming a touchpoint has prerequisites only when the Run Program operator or the Run Script operator runs on the touchpoint.

Important! The Run Program operator and the Run Script operator in the Command Execution category reference touchpoints directly by name. Therefore, update references to the touchpoint in the Run Program operator and the Run Script operator before you rename the touchpoint.

Follow these steps:

1. Click the Configuration tab and expand Domain in the Configuration Browser palette.
2. Select the appropriate environment, and then click Lock.
3. Expand All Touchpoints.
4. Right-click the appropriate touchpoint, and then click Rename.

5. Enter the new agent touchpoint name.

   Note: The unsaved data icon to the left of your entry reminds you to save the changes. Click Save now or wait for the text prompt.

6. Select the environment that you locked, and then click Unlock.

   The Unsaved Data dialog prompts you to save changes.

7. Click Yes.

Manage Touchpoint Groups

Every touchpoint is a member of the default group named All Touchpoints. Additionally, you can create your own named groups to group touchpoints functionally or logically. Logically, touchpoint groups allow you to organize related touchpoints and browse more easily among touchpoints in an environment.

Functionally, touchpoint groups allow commands and operators to operate on all touchpoints in the group:

- The Reload command that is executed on a touchpoint group updates the touchpoint list for all touchpoints within the group.
- The Refresh command that is executed on a touchpoint group updates property settings for all touchpoints in the group.
- An operator that is configured to execute on a group at run time executes on every touchpoint in the group.

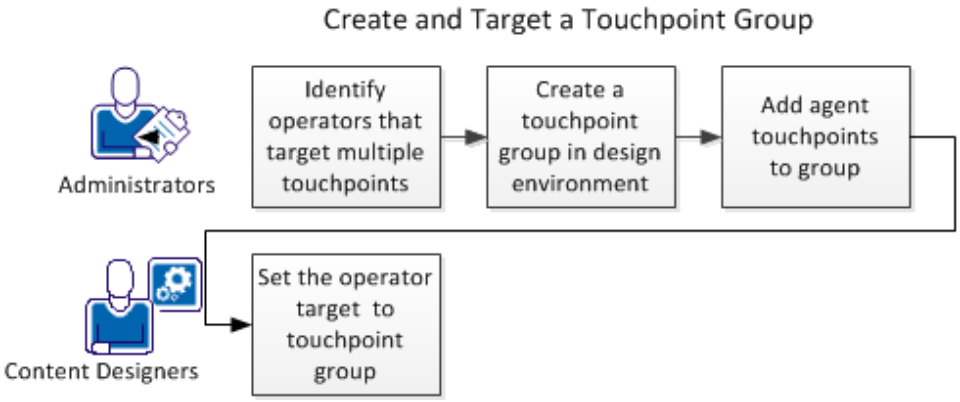
A touchpoint group is active if at least one touchpoint in the group is active. A touchpoint group is inactive if all touchpoints in the group are inactive. If all the Touchpoints in a group are active, the touchpoint group icon is green. If some touchpoints are active, the touchpoint group icon is yellow.

If all the touchpoints in a group are inactive, the touchpoint group icon is red.

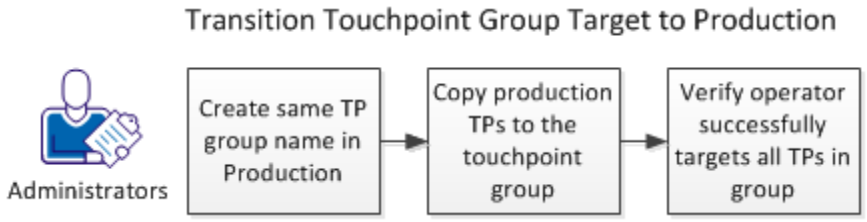
A user must have Environment Administrator permissions to create a touchpoint group in an environment.

About Touchpoint Groups

When a given operator must target multiple touchpoints at once, administrators create a touchpoint group that can serve as an operator target. For example:



When administrators transition a touchpoint group target to the production environment, they create a touchpoint group in the production environment. The touchpoint name duplicates the name used in the design environment. Administrators associate the production agents and Orchestrators to the touchpoint group. When they test the process, one of the things they verify is that operators that target a touchpoint group actually run on each Orchestrator and agent represented by a touchpoint in that group. For example:



Create a Touchpoint Group with Selected Touchpoints

Create a touchpoint group that can serve as an operator target when a given operator must target multiple touchpoints at once. You add a Touchpoint Group at the environment level. Select each touchpoint for the group from the Domain hierarchy. You can select an Orchestrator touchpoint or an agent touchpoint, then use the Copy To option to copy the selected touchpoint to a touchpoint group.

Follow these steps:

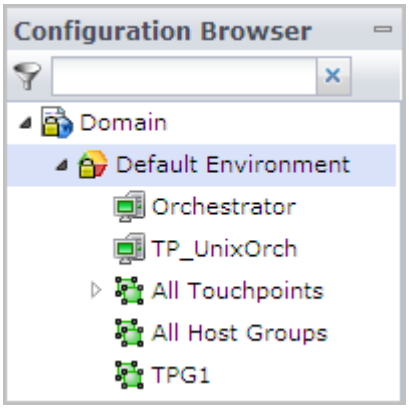
1. Click the Configuration tab.
2. Expand the Domain, select the environment to configure, and click Lock.

3. Create a touchpoint group:

   a. Right-click an environment, then select Add New Group.

   b. On the Add Touchpoint Group dialog, enter a name for the touchpoint group and click OK.

      For example, if you entered TPG1 for the name, the new group name appears under the selected environment below All Host Groups.



   c. Click Save.

      Note: You cannot successfully add an Orchestrator to an unsaved touchpoint group.

4. Copy Orchestrator touchpoints and agent touchpoints to the touchpoint group. For example:

   a. Right-click an Orchestrator, then select Copy To, *group_name*.

      The selected Orchestrator appears in the hierarchy under the selected touchpoint group name.

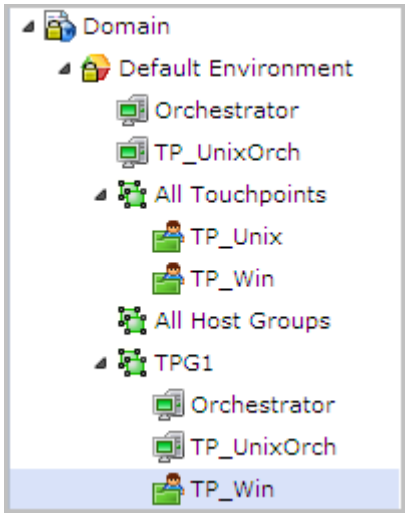
   b. Click Save.

   c. Right-click another Orchestrator, select Copy To, then select the same *group_name*.

   d. Click Save.

   e. Expand All Touchpoints, right-click an agent touchpoint, select Copy To, then select the same *group_name*.

   The TPG1 touchpoint group in the following example displays contents of two Orchestrator touchpoints and one agent touchpoint:



5. Select the environment, and select Unlock.

   The Unsaved Data dialog prompts you to save changes.

6. Click Yes.

More information:

Manage Touchpoint Groups (see page 237)

Delete a Touchpoint from a Touchpoint Group

Deleting a touchpoint from a touchpoint group only removes the touchpoint from that group. Deleting a touchpoint from the All Touchpoints group removes the touchpoint from the environment and from any touchpoint groups to which it was added. Content administrators can delete a touchpoint from a touchpoint group.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain, select the environment to configure, and click Lock..
3. Expand the touchpoint group to configure.
4. Select the touchpoint to remove from the group and click Delete.
5. Select the environment and click Unlock.

   The Unsaved Data dialog prompts you to save changes.
6. Click Yes.

Delete a Touchpoint Group

Content administrators can delete a user-created touchpoint group and all its touchpoint from an environment. This procedure does not delete the touchpoint from any other group in the environment. You cannot delete the All Touchpoints group.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain, select the environment to configure, and click Lock.
3. Right-click the touchpoint group that you want to remove from the environment, and then click Delete.
4. Select the environment and click Unlock.

   The Unsaved Data dialog prompts you to save changes.
5. Click Yes.

Chapter 10: Administer Proxy Touchpoints

When an operator targets a proxy touchpoint, the operator executes on the remote host to which the proxy touchpoint host has an SSH connection. No agent software is installed on the remote host. Operators can execute on any device running the Windows or UNIX operating system. A proxy touchpoint does sacrifice some performance, but it is useful when the agent software cannot be installed on a target host.

To use a proxy touchpoint, you configure a CA Process Automation touchpoint to point to a remote target and create an SSH user on the target computer.

This section contains the following topics:

Proxy Touchpoint Prerequisites

Proxy touchpoints can be created by configuring an existing touchpoint to run as a proxy touchpoint for a remote computer or other device. A touchpoint can be configured as a proxy touchpoint for a host with either a UNIX or a Windows operating environment. Proxy touchpoints use SSH to execute actions on target computers.

Proxy touchpoint usage prerequisites follow:

- Java Virtual Machine (JVM) version 1.6+ or later is required on the host with the touchpoint to be configured as a proxy touchpoint.
- When the target for a proxy touchpoint is a UNIX computer, the Korn shell (ksh) must be installed on the target computer. If missing from the target, either install the Korn shell or link it to from the Bash shell.
- An SSH user account must be specified on the remote computer targeted by a proxy touchpoint.
- (Optional) To use public key authentication, a trust relationship must be created from the proxy touchpoint host to the target remote computer.

  Important! If you do this step, be sure to adhere to guidelines documented in CA Process Automation-Specific Requirements for SSH Connectivity.
- In CA Process Automation, the proxy touchpoint must be configured with authentication information and other specifications for the remote host.

More information:

CA Process Automation-Specific Requirements for SSH Connectivity (see page 244)
Create an SSH Trust Relationship to the Remote Host (see page 245)
Configure Proxy Touchpoint Properties (see page 246)
Create the SSH User Account on the Remote Host of the Proxy Touchpoint (see page 245)

CA Process Automation-Specific Requirements for SSH Connectivity

SSH connectivity can be achieved by creating an SSH user account on each target host. If you create the optional trust relationship between an agent host and a remote host, certain CA Process Automation-specific configuration requirements apply.

When a request to a remote host is processed, the following properties are read:

- Remote User Name.
- Remote Password.
- SSH Keys Path, if configured.

CA Process Automation attempts an SSH connection from the agent host to the remote host specified in the request. The first access attempt is made with the configured credentials of the user account. If this attempt fails, a second attempt is made using key-based authentication. To use SSH public key authentication with CA Process Automation, the name of the private key file must match the name on the user account. If a passphrase is specified when creating the keys, the passphrase must match the password on the user account. Thus, the following two fields serve double duty.

Remote User Name

Is the user name for the user account that is used when authentication is based on SSH credentials.

Is also the name of the key file that stores the SSH private key at the path configured as SSH Keys Path, when configured.

Remote Password

Is the password for the user account that is used when SSH credentials are used for authentication.

Is also the passphrase that is used when the SSH public key is used for authentication.

Follow these guidelines when creating a trust relationship from the local host to the remote host:

- Enter the Remote User Name for *user_name* when you enter the following command:

  ```
  ssh-keygen -t dsa -b 1024 -f user_name
  ```

- Enter the Remote Password as the passphrase.

Create the SSH User Account on the Remote Host of the Proxy Touchpoint

The proxy touchpoint configuration specifies the Remote User Name and Remote Password of the SSH user account used to access the remote host. The SSH user account must have administrator-level permissions required to run CA Process Automation Operators on the target computer. Consider defining the same user account for all similarly configured computers that are accessed as remote hosts. For example, add the account *pamuser*, with the same password, to each remote host.

When a proxy touchpoint initiates a connection to the remote host, it creates a temporary directory named c2otmp on the target computer. On a UNIX computer, this directory is created in the /home directory of the SSH user.

Create an SSH Trust Relationship to the Remote Host

If you want to make public key authentication available for use, create a trust relationship from the proxy touchpoint host to the target remote host. Then, test SSH connectivity from the computer running the proxy touchpoint to the target computer. A trust relationship is created between two host computers.

CA Process Automation uses the public key authentication that you configure only if user/password authentication fails.

To create a trust relationship, use the ssh-keygen program to generate the private and public key pair. The private key stays on the host with the agent. Copy the public key to the target remote host that has no agent.

Follow these steps:

1. Generate a key pair. Use the following command, where *user_name* is the user name on the SSH user account you created on the target computer.

   ```
   ssh-keygen -t dsa -b 1024 -f user_name
   ```

   You are prompted for a passphrase to use later as a password.

2. Specify the pass phase in response to the prompt.

   The private key file named *user_name* and the public key file named <user_name>.pub are created.

3. Place the private key file named *user_name* in either of the following locations:
   - The private keys directory specified in the proxy configuration.

     The key is accessed from this directory with any host for which there is no *target_host_name*/*user_name* file.
   - The SshKeys/*target_host_name* directory, a subdirectory of the private keys directory specified in the proxy configuration. The private key is accessed from this directory when attempting to connect with *user_name* to *target_host_name*.

     The SSH Keys Path option specifies the location for the private keys directory in the proxy touchpoint properties dialog.
4. Transfer the public key file (*user_name*.pub) to the target host and place it where the SSH daemon can find it.

   Different SSH daemons follow different conventions. Examine the ssh-keygen options for details such as formatting requirements for the public key file.
5. For OpenSSH, concatenate the public file to the file which contains authorized keys for the user_name. Run the following cat command on the proxy target SSH host:

   `cat user_name.pub >> ~user_name/.ssh/authorized_keys`

More information:

CA Process Automation-Specific Requirements for SSH Connectivity (see page 244)

Configure Proxy Touchpoint Properties

You can create a proxy touchpoint by reconfiguring an existing agent touchpoint to target a specified remote computer.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain node, select the environment to configure, and click Lock.
3. Under All Touchpoints, select the agent touchpoint to make a proxy touchpoint.

4. Verify that the following properties are set:
   - Operators Auto Recovery
   - Touchpoint Security

   If these properties are not set, see Configure Touchpoint Properties (see page 226).
5. Select the Proxy Touchpoint check box.

   Selection indicates that this touchpoint is a proxy touchpoint. A proxy touchpoint is mapped to a remote host. A remote host typically has no installed agent.
6. Configure the remote host and values for SSH authentication. Complete the following steps:
   a. Enter the absolute or relative path on the agent host at which the private key file is stored in the SSH Keys Path field.

      The names of the private key file, <user_name>, and public key file, <user_name>.pub, match the Remote User Name of the user account.
   b. Identify the remote host with its fully qualified domain name or its IP address in the Remote Host field.

      Note: See Syntax for DNS Host Names (see page 397).
   c. Enter the user name with which a connection is made to the SSH Daemon on the target host in the Remote User Name field.

      The SSH user account must have sufficient permissions to perform administrative tasks on the target computer.
   d. Enter the password for the user account that is associated with the remote user name.

      This value is also used as the passphrase if connectivity is established through SSH public key authentication.
   e. Enter the maximum concurrent connections that the proxy touchpoint can open on the target remote host in the Maximum Number of Active Processes field.

      An SSH connection remains open while a program or script runs on the target host. If set to 20 and you attempt to run 40 scripts on the remote host concurrently, only 20 scripts start running. Scripts that are not started wait in a queue until others finish; then they start.
   f. Select the operating system of the target remote host.
7. Click Save.
8. Right-click the environment, and then select Unlock.

More information:

Configure Properties for the Design Touchpoint (see page 226)
Add One or More Touchpoints (see page 230)

Use a Proxy Touchpoint

When a process is run, operators in the process perform operations on target hosts. To execute an operator on a remote host that has no agent, first create an SSH connection from an agent host to the remote host. When you create a touchpoint and select an agent with a connection to a remote host, that touchpoint becomes a proxy touchpoint. When an operator specifies a proxy touchpoint as the target, the operation affects the remote host.

To perform an operation across many similarly configured proxy touchpoints, you can group the proxy touchpoints in a touchpoint group. Then, specify the touchpoint group as the target when configuring the operator properties. At runtime, the operator runs on all proxy touchpoints in the group.

More information:

Manage Touchpoint Groups (see page 237)

Chapter 11: Administer Host Groups

CA Process Automation can run operators on a target that has no agent or touchpoint when you reference that target in a host group. Content designers can specify such a target by its IP address or fully qualified domain name (FQDN).

Note: See Syntax for DNS Host Names (see page 397).

When the same host group resides on multiple agents, the agent selected to run the operator depends on the priority of the agent.

This section contains the following topics:

About Host Groups

A *host group* represents a group of hosts, typically with similar names or IP addresses, each of which can be specified in an operator with its FQDN or IP address. A host group references hosts as subnets of IP addresses, host name patterns, or a list of specific IP addresses and FQDNs.

Host groups provide direct access, that is, the ability to specify an IP address or FQDN in an operator, as opposed to a touchpoint or proxy touchpoint name. Hosts referenced in a host group do not need agents or proxy touchpoint associations. Avoid including a host that belongs to a clustered Orchestrator in a host group. Content designers cannot target such a host by its IP address or FQDN.

You can define multiple host groups on the same agent. A given agent could have one host group for variants of a Windows operating system and another for variants of a UNIX operating system.

You can define the same host group on one or more agents. When the same host group resides on multiple agents, the agent selected to run the operator depends on the priority of the agent.

To execute CA Process Automation operators on a remote host, a local host with a CA Process Automation agent that is mapped to a host group must gain access to the target host. The agent uses SSH to gain access to a target remote host and run operators on it. You define SSH access from the agent host to each target host represented by the host group with an SSH user account and, optionally, a trusted SSH relationship.

Properties for a host group include a setting for the maximum number of SSH connections. SSHD servers typically have limits in default configurations. The SSH connection remains open while the program or script is running on the target host. CA Process Automation implements internal queuing, by destination. If you set the value to 20, and then you run 40 scripts simultaneously on the same target host, only 20 run concurrently. New scripts start as others finish. With host groups, where the same agent is a proxy for multiple remote hosts, each remote host has a specific limit. So, this setting does not affect the number of hosts in the host group. The limit for the number of hosts is the maximum number of concurrent TCP connections that the operating system for the agent supports. Some operating systems support a high number of current TCP connections.

Important! Although a host group could include remote hosts with agents, do not create a host group of hosts with agents as a means of allowing them to be referenced directly. Reference by Touchpoint and proxy touchpoint is highly preferred for its flexibility and processing speed.

Host Group Implementation Process

You can configure a host group on any existing agent. An agent does not need to be configured as a touchpoint to host a host group. The agent host for the host group uses SSH to access and execute actions on a remote host. Part of host group preparation is to enable SSH authentication. When content designers target a member of a host group in an operator definition, they reference the target host by its IP address or FQDN.

Prepare to use a host group by performing the following tasks and procedures. Topics providing procedural details follow this process overview.

1. Create a Host Group (see page 252).
2. Configure the Host Group Properties (see page 253). That is, specify values for all settings except SSH Keys Path.
   - For help on entering patterns, see How to Define Remote Host Name Patterns Using Regular Expressions (see page 255).
   - (Optional) For public key authentication, configure SSH Keys Path.

     Note: CA Process Automation gains access with public key authentication only when access fails with the user account credentials.
3. From the agent host for the host group, verify that Java Virtual Machine (JVM) version 1.7 or 1.6 (no later than version 1.6.0_45) is installed. JVM comes with the JRE or JDK. Both 32-bit JVM and 64-bit JVM are supported for agents that are installed on hosts with Windows operating systems. Use the following command to verify that your Java version is a valid version. An example follows:

   ```
   java -version
   ```

   Example response:

   ```
   Java version "1.6.0_x", a valid version
   ```
4. Create SSH credentials on hosts in a host group (see page 258). Define a user account with the SSH credentials that are specified in the host group properties for Remote User Name and Remote Password.
5. From each remote UNIX host that the host group references, verify that the Korn shell is installed. If the Korn shell is not installed, take one of the following actions:
   - Install the Korn shell.
   - Create a soft link from an existing Bash shell to the Korn shell using the returned location. For example:

   ```
   ln –s  /bin/bash /bin/ksh
   ```
6. Take the following steps to complete the configuration for public key authentication. These steps apply to an SSH Keys Path specification.
   - Verify that the path you entered for SSH Keys Path in the host group configuration exists on the agent host. If it does not, create it. For example:

     Windows: C:\PAM\Sshkeys

UNIX: /home/PAM/Sshkeys

- Verify that you have the ssh-keygen utility or download it. On a Windows system, the ssh-keygen.exe appears in the C:\Program Files\OpenSSH\bin directory. The bin directory also contains other files that enable you to use UNIX commands.

  You use this utility to generate the private/public key pair.

- Verify that you can copy a file from one host to another. If needed, download a copy utility such as scp or Winscp.

  You copy the public key from the agent host to each remote host.

- Create the destination directory and destination file for the public key (see page 259).

- Create a trust relationship to a remote host referenced by a host group (see page 260).

  Important! Follow these instructions carefully. Steps include CA Process Automation-specific requirements that vary from the standard implementation of DSA key pairs.

More information:

CA Process Automation-Specific Requirements for SSH Connectivity (see page 244)

Create a Host Group

You can add a host group to a selected environment and then select the agent. Or, you can configure a host group on an agent and then select the environment. The combination of the agent name and the host group name must be unique within an environment.

Follow these steps:

1. Click the Configuration tab.
2. Select the environment to configure, and then click Lock.
3. To add a host group to a selected environment, follow these steps:
   a. Right-click the locked environment, and then select Add Host Group.

      The Add Host Group: *environment* appears.

   b. Enter the host group name.

   c. Select a displayed agent, and then click Add.

4. To add a host group to a selected agent, follow these steps:
   a. Expand the Agents node.
   b. Right-click the desired agent, select Configure Host Group at, and select the desired environment.

      The Add Agent Host Group dialog appears.
   c. Enter the host group name in the Host Group Name field and click OK.

      If you enter the name of an existing host group, the selected agent is mapped to that existing host group.
5. View the host group name as follows:
   - Expand the All Host Groups node for the environment where you created the host group.
   - Expand Agents and select the agent with the host group. The new host group is listed on the Associated Touchpoints and Host Groups tab with the domain hierarchy path.

More information:

Host Group Implementation Process (see page 251)

Configure Host Group Properties

You can configure properties of a host group within the Configuration tab. You establish connectivity between the agent and each remote host in the host group with third-party products.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain.
3. Expand the environment with the host group.
4. Expand All Host Groups.
5. Select the host group to configure, and then click the Properties tab.

6. Set the properties of the selected host group.
    a. Set Operators Autorecovery and Touchpoint Security as required or accept the default, Inherit from Environment.
    b. For SSH Keys Path, indicate the target path that you created on the agent for storing the private ky file.

        If the agent host has a Windows operating system, enter:
        `C:\PAM\SshKeys`

        If the agent host has a UNIX or Linux operating system, enter:
        `/home/PAM/Sshkeys`

        Important! Create the target path on the agent host.
    c. For each remote host name pattern, click the Add Parameter button, and define a host name pattern.

        See How to Define Remote Host Name Patterns using Regular Expressions (see page 255).
    d. Enter the credentials of the user account you did create or plan to create on each remote host referenced by this host group.

        Note: If you configure public key authentication, this value must be specified as the *user-name* in the command to generate key files. If using public key authentication with a passphrase, enter the passphrase for Remote Password.
    e. Complete the remaining intuitive fields.
7. Click Save.
8. Right-click the locked environment, and then select Unlock.

    Configuring properties is part of the total configuration. You must create a user account on each remote host with the credentials you configured here. This provides SSH access from the agent to each remote host in the host group. Establishing a trust relationship with public and private keys is optional.

More information:

Host Group Implementation Process (see page 251)

How to Define Remote Host Name Patterns Using Regular Expressions

When you configure host groups, you specify host name patterns and IP address patterns or both. Regular expression operators that you can apply when defining Remote Host Patterns for Host Groups follow:

- ^ (caret) means starts with.
- \ (escape) means interpret the operator character that immediately follows as a literal.
- . (dot) within an expression means any character. The expression a.b matches any string of three characters starting with “a” and ending with “b”.
- .* (dot asterisk) means accept any character any number of times. The expression a.*b matches a string of any length starting with "a" and ending with "b".
- $ (dollar sign) means ends with.

Think of the regular expression as a way to express anything in the FQDN, including:

- a start pattern (^String)
- a middle pattern (String)
- an end pattern (String$)
- a precise pattern (^StringWithEscapedDots$)

The following table contains examples designed to help you enter host name patterns in a way that helps ensure efficient processing. If you enter an FQDN or subdomain without operators, the FQDN or group you intend to map is found, but processing is not as efficient. As a best practice, include the following regular expression combinations in the host name patterns you enter for Remote Host Patterns.

Common Combinations	Description	Example FQDN and Example Host Group
^<hostname>	The caret as the first character means that the pattern starts with the text that follows the caret.	**FQDN:** ^host1\.ca\.com$ matches only host1.ca.com (But, host1\.ca\.com$ without the preceding caret searches for every host with a name that ends with host1.ca.com, such as aaaahost1.ca.com) **Group:** ca\.com$ without the preceding caret matches every FQDN in the ca.com subdomain.

Common Combinations	Description	Example FQDN and Example Host Group
\.	The escape dot combination (\.) means to interpret the dot as a literal.	**FQDN:** ^host1\.ca\.com$ matches only host1.ca.com (But, ^host.ca.com$ without an escape before each dot could match: host1Mca0com) **Group:** ^host.\.ca\.com$ with a dot after host could match hosts named {host0, host1, ...hostZ} in the ca.com domain.
.*<domain>	The dot asterisk combination (.*) allows everything to match.	**Group:** .*\.ca\.com$, a domain preceded by .* matches all hosts in the Domain.
<domain name>$	The dollar sign following a domain name means that the pattern ends with the specified domain.	**FQDN:** ^host1\.ca\.com$ matches only host1.ca.com (But ^host1\.ca\.com without the ending $ operator could match: host1.ca.comaaaaaaaa)

Examples

Remote IP Address Patterns

Specifies any combination of the following, where IP addresses are static rather than dynamic. Click Add to create each row.

- A list of IPv4 IP addresses.
- One or more IPv4 subnets using CIDR notation.

Remote Host Name Patterns

Specifies a group of remote hosts with a list of fully qualified domain names (FQDN) or regular expression patterns for a subdomain. Select Add to create a row for each pattern entry.

For example:

- abc\.mycompany\.com
- .*pam-lnx\.mycompany\.com$

  This pattern matches any hostname that ends in pam-lnx in your company domain, where mycompany is replaced with your company name.
- ^machine1\.mycompany\.com$

  Specifically, ^machine1\.mycompany\.com$ expresses a Fully Qualified Domain Name (FQDN) as a regular expression. This pattern matches only the FQDN that meets all of these criteria:

  starts with *machine1.*

  ends with *com.*

  contains *machine1*, then a *dot*, then *mycompany*, then a *dot*, and then *com*.

Create SSH Credentials on Hosts in a Host Group

A host group configuration specifies the SSH credentials as follows.

- Remote User Name
- Remote Password

Log on to each host that the host group references. Create a user account with these SSH credentials. This SSH user account must have sufficient permissions for the following tasks:

- To perform administrative tasks.
- To run CA Process Automation operators on each target computer.

The agent uses the user name of the SSH user account to connect to the SSH Daemon on the target remote host. The target host can be any host that matches the Remote Host Name Patterns or the Remote IP Address Patterns in the host group configuration.

The agent host of the host group initiates a connection to the remote host as follows:

1. Logs in to the remote host with the specified credentials.
2. Creates a temporary directory named c2otmp.

   This directory is created in the /home directory of the SSH user if the target host is a UNIX computer. For example:

   ```
   /home/<user_name>/c20tmp
   ```

More information:

Host Group Implementation Process (see page 251)

Create the Destination Directory and File for the Public Key

If you decide to create the optional trust relationship to remote hosts referenced by the host group, first verify the existence of the following directory and file on each remote host. If the directory or file does not exist, create it.

The following are required on each remote host before you create the trust relationship from the host with the host group.

- The .ssh directory under /home/<user_name>, the target directory for <user_name>.pub
- An authorized_keys file, to which the public key contained in <user_name>.pub can be appended. The ~/.ssh/authorized_keys is the default file that lists the public keys that are permitted for DSA authentication.

You can create the .ssh directory and authorized_keys file on a UNIX or Linux remote host

Follow these steps:

1. Use ssh to access a remote host and log in with the Remote User Name and Remote Password configured for the host group.
2. Verify the current directory is your home directory. Enter:

   pwd

   The response is:

   /home/*user_name*
3. Create the .ssh directory in this path and navigate to the new directory.

   ```
   mkdir .ssh
   cd .ssh
   ```
4. Create authorized_keys in the .ssh directory.

   ```
   cat > authorized_keys
   ```

   An empty authorized_keys file is created in the /home/*user_name*/.ssh directory.

To create the .ssh directory and authorized_keys file on a Windows remote host

1. Use remote desktop to access the remote host and log in with the Remote User Name and Remote Password configured for the host group.
2. Navigate to your home folder. For example, \Users*user_name.*
3. If a folder named .ssh does not exist, create a new folder and name it .ssh.
4. In the following folder, create a file named authorized_keys with no extension.

   \Users*user_name*\.ssh

   The following empty file is created.

```
\Users\user_name\.ssh\authorized_keys
```

Create a Trust Relationship to a Remote Host Referenced by a Host Group

A *remote host* is a host that a host group references. The host group is configured on a host with an agent; the remote host typically has no agent. Targeting a remote host requires that a process operator has SSH connectivity between an agent host and the referenced remote host.

Establish an SSH connection with one of the following methods:

- Create a trust relationship between the agent host and the remote host. This method creates a public key/private key pair.
- Create a user account on the remote host. This method creates credentials.

When you create a user account *and* a trust relationship, the product uses the trust relationship as the backup mechanism. If the authentication fails for the configured credentials, the product authenticates with the key pair.

Generate a key pair with the SSH-keygen program. Save the private key to the configured SSH Keys Path, and then copy the public key to each remote host that the host group references. Put the public key file where the SSH daemon can find it. The OpenSSH daemon, sshd, looks for the key in /home/*user_name*/.ssh/authorized_keys.

You can create a trust relationship to a remote host that a host group references.

Follow these steps:

1. Log in to the host that contains the agent where the host group is defined.
2. Open a command prompt and change directories to a path from which to generate the key pair.

   For example, if you downloaded OpenSSH on a Windows system, change to the C:\Program Files\OpenSSH\bin directory that contains the ssh-keygen program.
3. Generate a key pair with the following command:

   ```
   ssh-keygen -t dsa -b 1024 -f user_name
   ```

   user_name

   Defines the value that you configured as Remote User Name in the Host Group.

   The following message and prompt are displayed:

   ```
   Generating the public/private dsa key pair.
   Enter passphrase <empty for no passphrase>:
   ```

4. Enter the value that you configured as Remote Password in the Host Group. This value is required.

   The following prompt is displayed:

   ```
   Enter same passphrase again:
   ```

5. Enter the Remote Password value again.

   The following messages are displayed:

   ```
   Your identification has been saved in user_name.
   Your public key file has been saved in user_name.pub.
   The key fingerprint is:
       fingerprint_string login_name@host_name
   ```

   The product creates the private key file named *user_name* and the public key file named *user_name*.pub. The passphrase for the key file is the same as the password on the user account that is used for SSH access.

6. Move the private key file named *user_name* to the location that is configured as SSH Keys Path in the host group. For example:

   - **Windows:** C:\PAM\Sshkeys
   - **UNIX:** /home/PAM/Sshkeys

7. Transfer the public key file *(user_name*.pub) to each host that the host group references and put it where the SSH daemon can find it.

   Different SSH daemons follow different conventions. Examine the ssh-keygen options for public key file formatting requirements.

8. For OpenSSH, append the public key from *user_name*.pub to the file that contains all authorized keys that the host uses. The OpenSSH SSH daemon (sshd) searches the authorized_keys file. The authorized_keys file must be in the .ssh directory in the home directory path.

   a. Run the following command on each host that the host group references:

      ```
      cat user_name.pub >> home/user_name/.ssh/authorized_keys
      ```

   b. Switch users to root and restart the ssh service:

      ```
      su root
      service sshd restart
      ```

9. Verify that access is established. Log in to the host with the agent and ssh to the remote host. If the login succeeds, the trust relationship is established. Enter the following command from the agent host:

   ```
   ssh user_name@remote_host
   ```

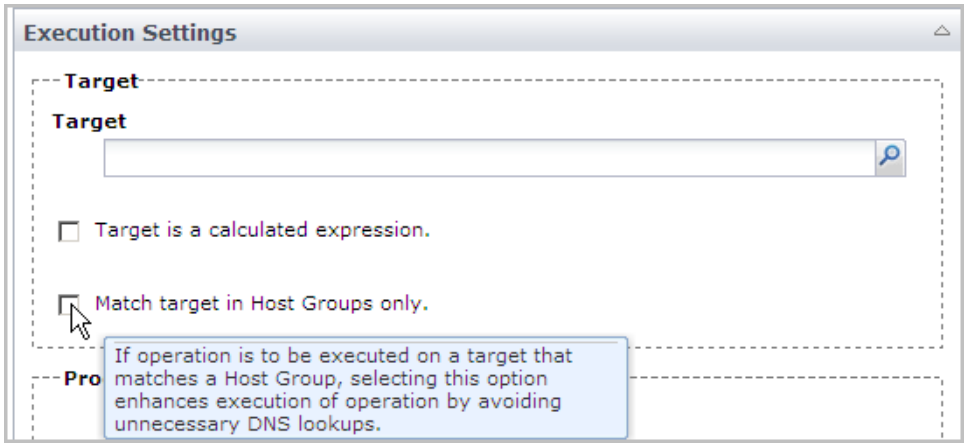
More information:

Host Group Implementation Process (see page 251)
CA Process Automation-Specific Requirements for SSH Connectivity (see page 244)

Ensuring Efficient Processing of Host Group References

This topic, which is relevant to content designers, is for administrator information.

During process design, content designers specify execution settings for each operator. The following example shows a partial dialog with the Target field and the Match target in Host Groups only check box.



When the Target field contains a touchpoint name, a proxy touchpoint name, or an agent ID, clear the Match target in Host Groups only check box.

When the Target field contains an IP address of a specific host, select the Match target in Host Groups only. Specifying an IP address or a host name in the Target field is valid only if a host group in the current environment references the corresponding host.

Important! If a process is destined for export in a folder as a content package, do not enter an IP address in the Target field. Rather, enter a dataset name that contains the IP address. Also:

- Select Target is a calculated expression.
- Select the Match target in Host Groups only. A dataset that references an IP address is valid if a host group in the current environment references the corresponding host.

To understand the purpose of this check box, consider the case where:

- The Target field has the entry *some_host,* where the entry is the host name of a host in a host group.
- The Match target in Host Groups only check box is cleared.

The runtime processing evaluates and processes the Target entry in the following sequence:

1. If the entry is a touchpoint name, runs on the host with the agent associated with the touchpoint.
2. If the entry is a proxy touchpoint name, runs on the host with the SSH connection to the agent associated with the proxy touchpoint.
3. If the entry is an agent ID, runs on the host with this agent ID.
4. If the entry is an IP address or a host name that a host group references, runs on that host.

   Note: The operator fails if you select the Match target in Host Groups only check box when the specified target is *not* part of a host group. The operator fails even if the target is a valid touchpoint name, proxy touchpoint name, or agent ID.

When to Avoid Using Host Group References as Targets

When a process is exported in a folder as a content package:

- Processes *cannot* be modified in the import environment.
- Datasets *can* be modified in the import environment.

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

The recommendation for redistributable content is to use datasets for the configuration parameters. The content designer creates 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 with an IP address value that a host group in the import environment references.

How Host Groups Compare to Proxy Touchpoints

Host groups and proxy touchpoints are alike in the following ways:

- Both run on agents.
- Both access remote hosts through SSH.
- Both support the same CA Process Automation operators that can be executed on remote hosts through SSH.
- The configured categories for the required operators must be running on the agent host on which the proxy touchpoint or host group is configured.

Host groups differ from proxy touchpoints in the following ways:

- The relationship between a host group and potential target hosts is one to many, whereas the relationship between a proxy touchpoint and the target host is one to one.
- Content designers can target multiple hosts with associated proxy touchpoints by specifying a touchpoint group. Content designers cannot target multiple hosts that have only a host group reference.
- Content designers specify a remote host as a target by its touchpoint name when the remote host has an associated proxy touchpoint. Content designers specify a remote host as a target by its IP address or FQDN when the remote host has a host group reference.

Chapter 12: Administer Operator Categories and Custom Operator Groups

This chapter describes concepts and procedures relevant to configuring common default settings for operators at the category level. This chapter also addresses configuring values for variables that can be defined for custom operator groups.

Note: You do not need to configure modules (operator categories). The recommended best practice is for the content designer to create global datasets for the module settings. The content designer then uses expressions that reference the dataset variables in the operator properties.

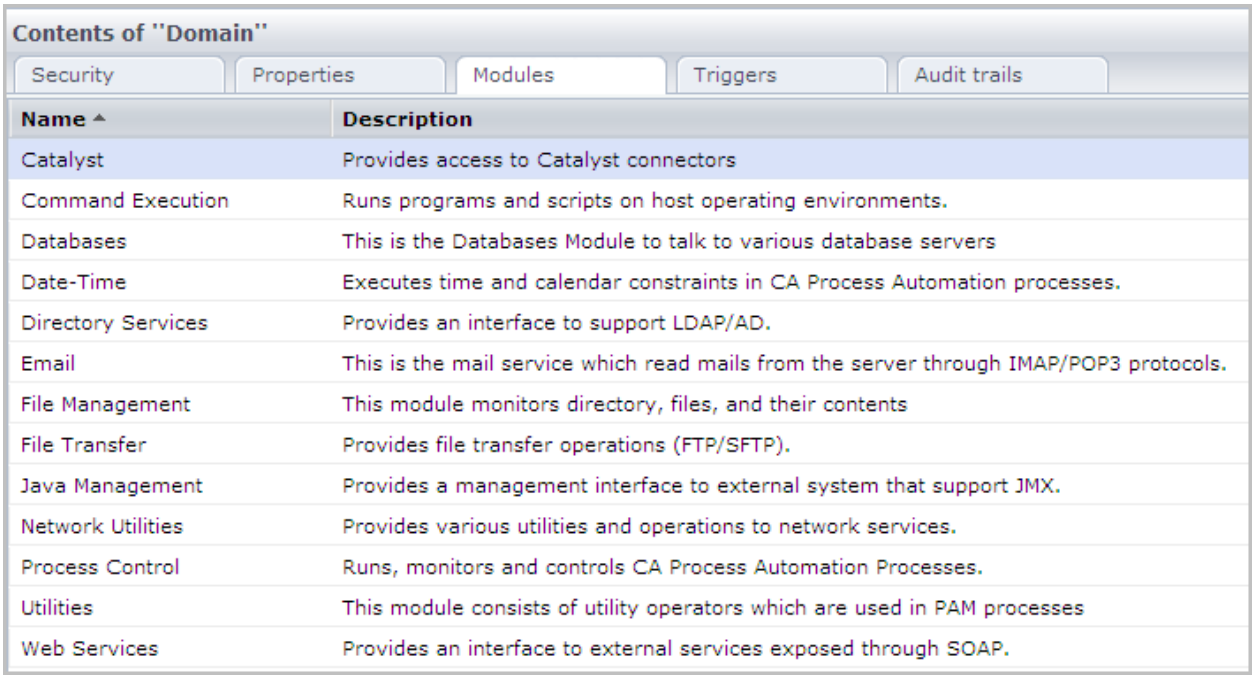
This section contains the following topics:

Operator Categories and Operator Folders

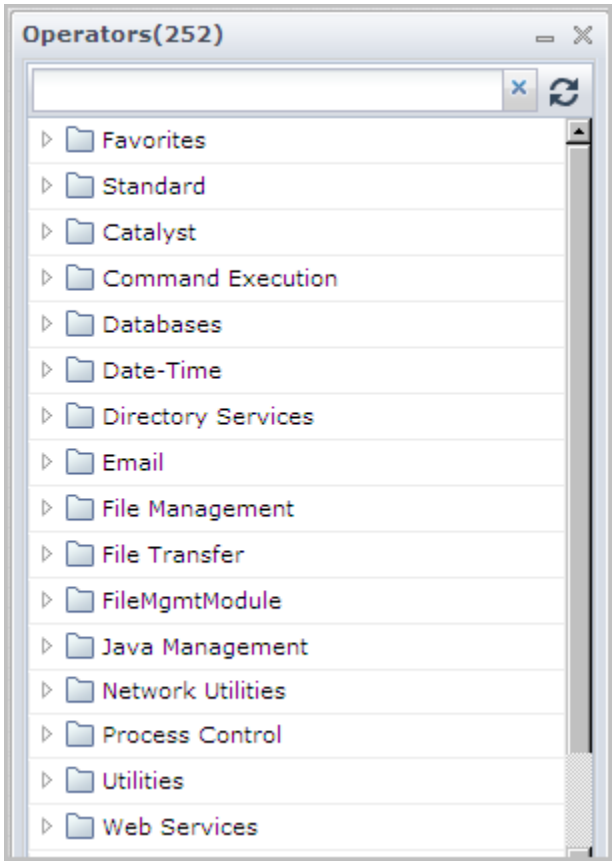
Operator categories correspond to operator folders. Administrators configure operator categories on the Modules tab, starting at the Domain level. Content designers expand operator folders to display a group of operators in the named category. The Operators palette in the Designer tab displays Operator folders.

Click the Configuration tab, select Domain, and click the Modules tab to list the operator categories under Name.

Note: The Name list can also include published groups that are created for custom operators. Content designers can expand these group folders to display a group of custom operators in the named configuration group. Configuration group folders that are displayed here for custom operators are also displayed in the Operators palette in the Designer tab.



Click the Designer tab, click View, and select Operators to display the folder names that reflect the same operator grouping as the operator categories you configure.



Content designers select operators from the Operators palette to create automated processes. Each operator performs a specific operation. To assist designers in quickly locating the appropriate operator, CA Process Automation groups the operators in categories that represent common use. For example, all of the operators that are used for file transfer with FTP are grouped together in a folder named File Transfer.

You configure the operator category values at the Domain level. The values are inherited at the environment level, and then at the Orchestrator or agent touchpoint level. You can override inherited values at any level. The operators then inherit the operator category default values. Content designers can accept or override these values.

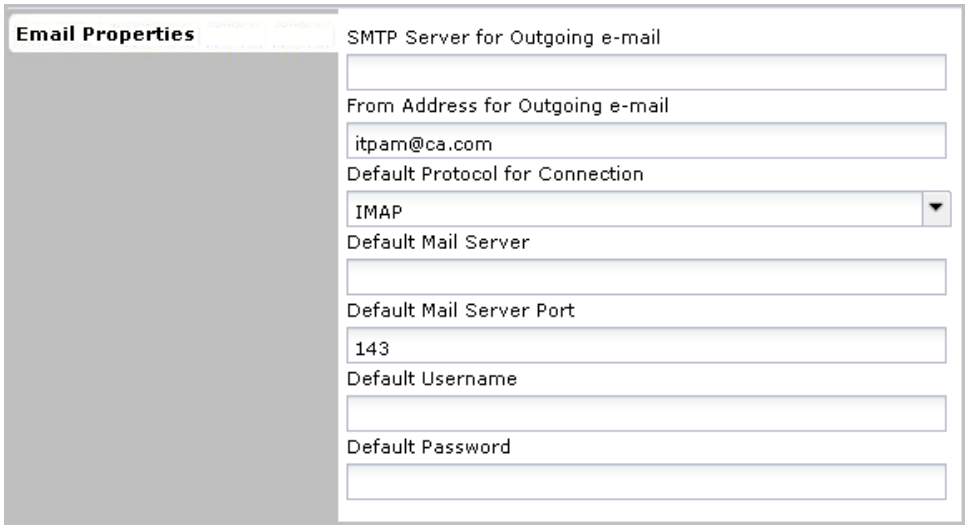
More information:

Category Configuration and Operator Inheritance (see page 306)

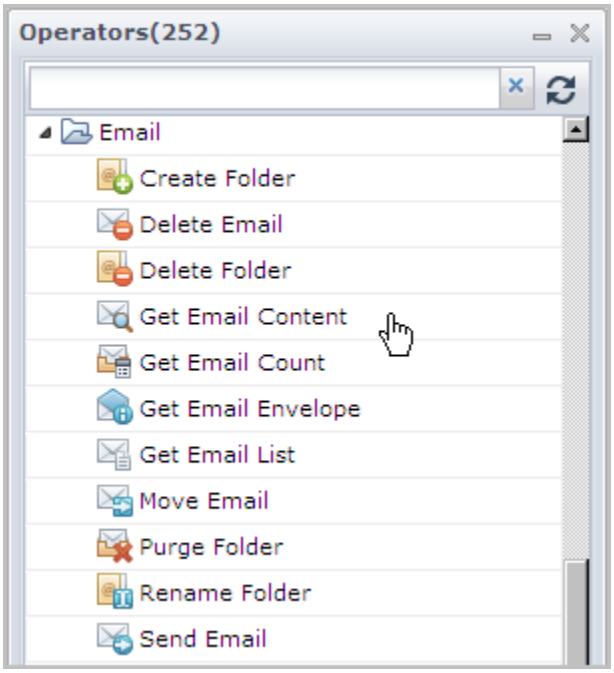
Example: Category Settings Used by Operator

When you configure Domain level settings for each category on the Modules tab, consider the values that are typically used by operators. If you configure settings based on the most used case, then configuration at lower levels is done only for exceptions.

Consider the configuration in Email Properties, where the Default Protocol for Connection is set to IMAP and the Default Mail Server Port is set to 143. You configure the default mail server, default user name, and default password.



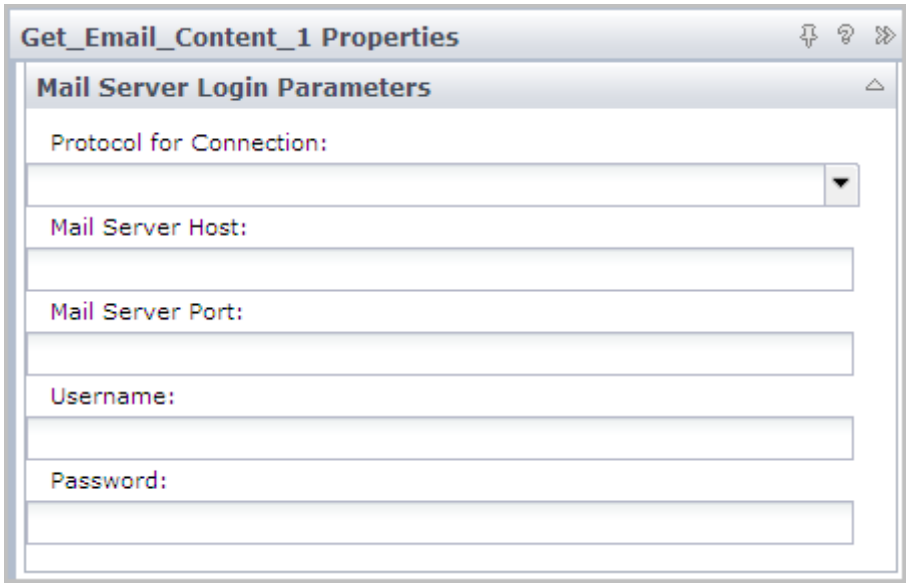
When a content designer automates a process for email, one of the operators available for use is Get Email Content.



When a content designer drags the Get Email Content operator to the canvas, the Get_Email_Content_1 Properties appear. Notice the similarity between Email Properties configured on the Modules tab in the Configuration tab and the Mail Server Login Parameters for Get_Email_Content_1 Properties displayed in the Designer tab.

The Get Email Content operator inherits values for these Mail Server Login Parameters	**from values configured in the Email module setting for Email Properties**
Protocol for Connection	Default Protocol for Connection
Mail Server Host	Default Mail Server Host
Mail Serve Port	Default Mail Server Port
Username	Default Username
Password	Default Password

The content designer can configure process-specific values and override previously configured default values. Or, the content designer can leave the field blank to inherit the default values. In this example, a blank Protocol for Connection uses IMAP and a blank Mail Server Port uses port 143.



Configuring Operator Categories

Administrators who can lock the Domain can configure or change default settings for operator categories at the Domain level. These configurations are inherited. You can edit these settings at the environment, Orchestrator, and agent levels. For details, see Override Settings Inherited by a Category of Operators (see page 308).

Default values for all operator category fields can be overridden at the operator level. The values you enter for any operator category are all default values. When an operator is configured with a blank field, that operator inherits the default value of the corresponding field from the category setting. When you make a selection of a value in the Module tab, nothing gets enabled or disabled. You can specify all of the defaults, at your discretion. (When you configure these same options at the operator level, selection of one option disables the others.)

Note: For more details, see the *Content Designer Reference* for the operator configuration of these same fields.

To expand a field for an entry that is longer than the space provided, right-click the field and select Expand. A dialog with a text box opens.

About Catalyst

Catalyst is configured with the following settings:

- Catalyst Property settings.
- Catalyst Security settings.

The Unified Service Model (USM) is a schema of common object types and properties to which data from all connectors is converted. The USM schema enables analysis of data from all Domain managers. You can analyze data in a common interface with identical formatting across Domain managers.

The Catalyst operators let you use Catalyst connectors in automated processes. The Catalyst operators support the following interfaces:

- Create, read, update, delete (CRUD)
- Execute
- Event subscription

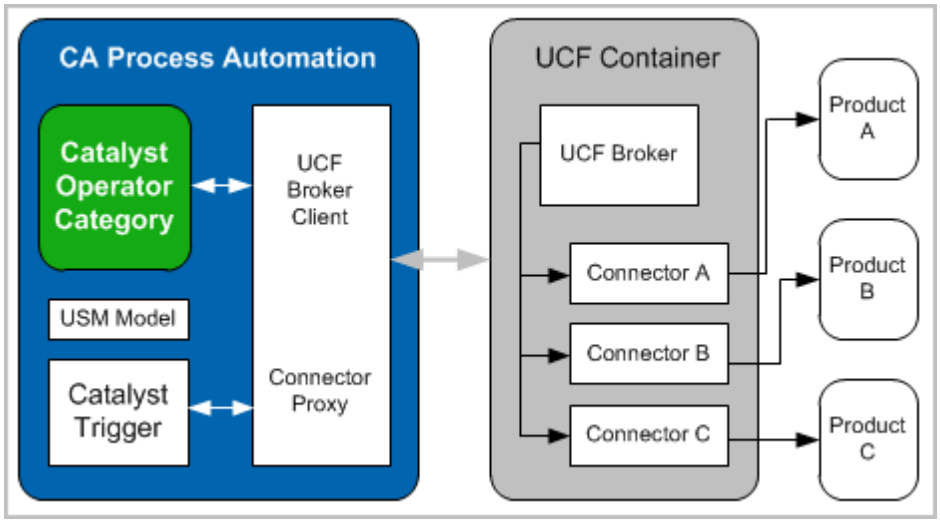
The operators expose USM object types and properties.

Using the common USM and standard UCF interfaces provides Catalyst compatibility with all UCF connectors and containers.

CA Process Automation embeds the following UCF-USM components:

- Catalyst Operator Category
- Catalyst Trigger

The Catalyst operator category and the Catalyst Trigger are remote UCF connector clients. They use the UCF Broker and Connector proxy interfaces, as the following illustration shows:



Configure Catalyst Defaults

You can configure the Catalyst defaults by completing the following tabs:

- Default Catalyst Properties
- Default Catalyst Security
- Default Catalyst Claims
- Default Catalyst Password Claims

Note: The password values are encrypted.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Catalyst, and select Edit.

   The Default Catalyst Properties tab opens.

3. Configure the default Catalyst properties.
    a. Type the appropriate default URL in the UCF Broker URL field. The associated operator inherits this setting. Examples of URLs for basic and secure communication follow:

        `http://hostname:7000/ucf/BrokerService`

        `https://hostname:7443/ucf/BrokerService`

    b. Type the appropriate name in the Product property configuration file name field. This file is used to customize the properties that the generic Create operator shows.
4. Click the Default Catalyst Security tab and type the default Catalyst user ID and password.
5. Click the Default Catalyst Claims tab and complete the configuration.
    a. Click Add Parameter and enter the first claim name with its value.
    b. Repeat this step for each default claim.
    c. Use the up and down arrows to sequence the claims as needed.
6. Click the Default Catalyst Password Claims tab and complete the configuration.
    a. Click Add Parameter and enter the first claim name with its value.
    b. Repeat this step for each default password claim.
    c. Use the up and down arrows to sequence the claims as needed.
7. Click Save and Close.
8. Click Save.
9. Select Domain and click Unlock.

More information:

Override Settings Inherited by a Category of Operators (see page 308)
Category Configuration and Operator Inheritance (see page 306)
About Catalyst (see page 271)
Configuring Operator Categories (see page 270)

Load Catalyst Descriptors

A Catalyst connector descriptor specifies the connector capabilities, including the operations that it supports. Each operation further specifies the associated parameters. You can load descriptors into CA Process Automation. The Execute operator, an operator n the Catalyst operator category, uses the descriptors. The product displays the loaded descriptors at various levels:

- Operation Categories (drop down)
- Operation (drop down)
- Parameters (editor values)

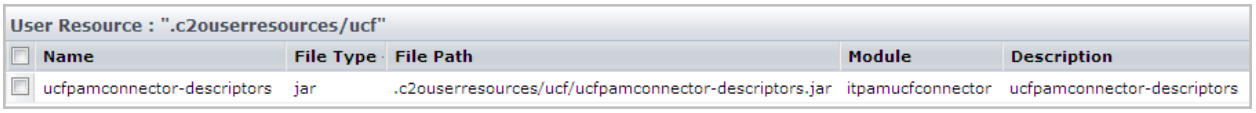
You can load a Catalyst descriptor from your local host to the remote Domain Orchestrator as a user resource. The product replicates all resources to each new Orchestrator.

Follow these steps:

1. Click the Configuration tab.
2. Expand Manage User Resources in the left pane.
3. Expand the Repository folder, expand the User Resource folder, and then select the ucf folder. If
4. Click New.
5. Complete the fields in the Add New Resource pane as appropriate.

   Note: Leave the Resource Subfolders Path field blank; Step 3 defined the ucf subfolder path.
6. Click Save.

   The user resources list displays the descriptor.



User Resource : ".c2ouserresources/ucf"

Name	File Type	File Path	Module	Description
ucfpamconnector-descriptors	jar	.c2ouserresources/ucf/ucfpamconnector-descriptors.jar	itpamucfconnector	ucfpamconnector-descriptors

Note: The descriptor is available in the Execute operator after you restart the Orchestrator. For more information about the Execute operator in the Catalyst category, see the *Content Designer Reference*.

More information:

Add a Resource to User Resources (see page 332)

About Command Execution

Command Execution operators let you run shell scripts or executable programs on any agent or Orchestrator. This category provides data and resource access to network devices that support the Telnet and SSH (Secure Shell) interface protocols.

The list of operators follows:

- Run Program
- Run Script
- Run SSH Command
- Run SSH Script
- Run Telnet Command
- Run Telnet Script

If you are running scripts, follow the Windows or UNIX operating system conventions to make them executable. In CA Process Automation, scripts return result as CA Process Automation dataset variables.

- For UNIX systems, the first line of the script specifies the full path to the desired interpreter. For example:

  `#!/bin/sh`

  Specifies to execute using sh, the Bourne shell on systems such as Oracle Solaris. On Linux systems, this entry is a link to another shell, such as bash. A Script operator can execute any script for which the target host has an interpreter.

  Wrap Shell commands such as *cp* or *dir* in an executable script file.

  `#!/usr/bin/perl`

  When placed at the top of a Perl script, tells the web server where to find the Perl executable.

- For Windows systems, the filename extension defines the scripting interpreter. For Windows, define file associations to run the scripts automatically. The following extensions are supported:

  `*.ps1`

  A Windows PowerShell file.

  `*.exe`

  An executable file that installs and runs programs and routines.

  `*.cmd`

  A batch file that is composed of a sequence of commands; similar to a .BAT file, but run by the CMD.exe program rather than the COMMAND.com program.

  `*.vbs`

  VBScript file.

  `*.wsh`

  A Windows Script Host text file with parameters for a script such as a .vbs file; requires Microsoft WScript or Microsoft CScript to open the file.

More information:

Configure Command Execution: Default Telnet Properties (see page 278)

Configure Command Execution: Default SSH Properties

When you configure the default SSH properties, you configure the following items:

- The terminal type specifications
- The authentication details for logging on to a remote host
- (Optional) Whether to switch users after login

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Command Execution, and select Edit.
3. Select the Default SSH Properties tab.
4. Select the default pseudo terminal type to request on the SSH connection.

   Note: VT100 typically works with Linux hosts; VT400 typically works with Windows hosts.
5. Select the default port with which to connect to the remote host.

   Note: Port 22 is the system TCP/UDP port for the Secure Shell (SSH) Protocol.

6. Enter the default for the user name with which to log in to the remote host.
7. Specify the private key defaults:
   a. Indicate whether to use a private key to log in.

      Note: The alternative is to use the password information.

   b. Enter the default password with which to log in to the remote host.
   c. Click Browse (...) and retrieve the private key content (that is, the content of a default private key with which to log in to the remote host).
   d. Enter the path to a default private key with which to log in to the remote host.
   e. Enter the passphrase with which to unlock the content of the default private key.

      Note: The passphrase is required if the default private key was created with a passphrase.
8. Specify the defaults for running the script or specified commands as a different user.
   a. Indicate whether to run the script or the specified commands as a different user.
   b. Enter the operating system-specific command to switch the user on the remote host. The command "su -root" switches users to the root user. For example:

      ```
      su - <username>
      ```

      ```
      sudo su - <username>
      ```

   c. Enter a regular expression for the default text prompt if the remote host requires a password to switch users.

      The text prompt is typically "Password: " or "password: ". The regular expression, ".*assword: " matches any input (including new lines) and an uppercase "P" or lowercase "p" followed by “assword: “.

   d. Enter the default password to enter at the text prompt if the remote host requires a password to switch users.
   e. Enter a regular expression for the command prompt that indicates that the remote host is ready for commands as the switched user.

      Typical command prompts are # (hash), > (greater than), and ? (question mark). The entry .*[$>?:#] matches any input (including new lines) that is followed by a #, >, ?, $ (dollar symbol), or : (colon). Consider the following examples:

      ```
      .*[$]
      ```

      ```
      .*[$>?:#]
      ```

      Note: When you use a dollar symbol in a regular expression, enclose it in square brackets. A dollar symbol without brackets has a special meaning in regular expressions.

9. Click Save and Close.
10. Click Save.
11. Select Domain and click Unlock.

More information:

About Command Execution (see page 275)
Override Settings Inherited by a Category of Operators (see page 308)
Category Configuration and Operator Inheritance (see page 306)
Configuring Operator Categories (see page 270)

Configure Command Execution: Default Telnet Properties

Configuration of the default Telnet properties includes the following tasks:

- Configure the connectivity
- Specify the login scheme and related details
- Specify whether to switch users after logging in to the remote host
- Define the switching details

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Command Execution, and select Edit.
3. On the Default Telnet Properties tab, select the default pseudo terminal to request on the Telnet connection.
4. Select the default port with which to connect to the remote host.

   Note: Port 23 is the system TCP/UDP port for Telnet.
5. For Connection Timeout (sec), use the spinner to select the interval (in seconds) the connection waits before timing out.
6. Select a default login scheme from the drop-down list.
7. Define the default login prompts and values:
   a. Enter a regular expression for the login prompt (for example, enter .*ogin.*:).
   b. Enter the user name with which to log in to the remote host.
   c. Enter a regular expression for the default text prompt that indicates that the remote host requires a password for the user logging in (for example, enter .*assword.*:).
   d. Enter the default password to use for logging in to the remote host.

8. Enter a regular expression for the command prompt that indicates that the remote host is ready for commands (for example, enter .*[$>?:#]).

   Note: To use a dollar symbol in a regular expression, enclose it in square brackets. For example, [$].

9. Select the interval (in seconds) that the connection waits for the prompt to send the commands.

10. Define the default values for switching users:

    a. Specify whether to switch users before running the script or the specified commands.

    b. Enter the operating system-specific command with which to switch the user on the remote host.

       Note: The "su -root" command switches the user to the root user.

       Consider the following examples:

       ```
       su - <username>
       ```

       ```
       sudo su - <username>
       ```

    c. Enter a regular expression for the default text prompt for the switch user password (for example, enter .*assword.*:).

    d. Enter the default password to enter at the password text prompt.

    e. Enter a regular expression for the prompt that indicates that the remote host is ready for commands as the switched user.

       Note: Hash (#), greater than (>), and question mark (?) are the typical command prompts. Enter .*[$>?:#] to match any input (including new lines) that a #, >, ?, $ (dollar sign), or : (colon) follows.

       Consider the following examples:

       ```
       .*[$]
       ```

       ```
       .*[$>?:#]
       ```

       Note: To use a dollar symbol in a regular expression, enclose it in square brackets. For example, [$].

11. Click Save and Close.

12. Click Save.

13. Select Domain and click Unlock.

Configure Command Execution: Default UNIX Command Execution Properties

You can configure default run properties for the UNIX commands.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Command Execution, and select Edit.
3. Select the Default UNIX Command Execution Properties tab.
4. Enter one of the following Shell command interpreters to use as the default for the profile and for shell commands:

   `/bin/bash`

   `/bin/csh`

   `/bin/ksh`
5. Enter the name of the default shell script file to interpret before starting a user process for which no profile is specified.

   The profile can contain any noninteractive command that the shell interpreter understands.
6. Specify the user credential defaults.
   a. Select one of the following values to specify that the Process operators use the selected option when user credentials are not specified:
      - (Default) Defaults to the user under which touchpoint is run.

        The Process operators use the user credentials under which the agent or Orchestrator process is running.
      - Defaults to the specified Default user.

        The Process operators use the user credentials that are configured as the Default user and Default password.
      - No default.

        The Process operators use the user credentials that are supplied at run time.

   b. Consider the implications of specifying defaults for user ID and password:
      - To prevent users from defining and starting processes through CA Process Automation to which they otherwise have no access, specify a user ID with only necessary permissions.
      - Leave the user ID and password blank to force users to enter those values when they start processes through CA Process Automation.

   c. If appropriate, enter the default shell account to use when starting user processes that lack a user name and a password.

d. If appropriate, enter the password for the Shell user account.

   Note: Passwords that are part of the Command Execution configurations are protected and cannot be modified through a program, referenced, or passed to external methods.

e. Reenter the Default password to confirm it.

7. Consider the implications of specifying defaults for user ID and password:
   - To prevent users from defining and starting processes through CA Process Automation to which they otherwise have no access, specify a user ID with only necessary permissions.
   - Leave the user ID and password blank to force users to enter those values when they start processes through CA Process Automation.
8. If appropriate, enter the default shell account to use when starting user processes that lack a user name and a password.
9. If appropriate, enter the password for the Shell user account.

   Note: Passwords that are part of the Command Execution configurations are protected and cannot be modified through a program, referenced, or passed to external methods.
10. Reenter the Default password to confirm it.
11. Indicate whether to load the user profile that is associated with the specified default user and password.
12. Indicate whether to disable password checking.
13. Click Save and Close.
14. Click Save.
15. Select Domain and click Unlock.

More information:

About Command Execution (see page 275)
Override Settings Inherited by a Category of Operators (see page 308)
Category Configuration and Operator Inheritance (see page 306)
Configuring Operator Categories (see page 270)

Configure Command Execution: Default Windows Command Execution Properties

You can configure default run properties for the Windows commands.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Command Execution, and select Edit.
3. Select the Default Windows Command Execution Properties tab.
4. Enter the default shell command interpreter to use for the profile and for shell commands. For example:

   `cmd.exe`

   Note: Do not enter Command.exe.
5. Enter the name of the default shell script file to interpret before starting a user process for which no profile is specified.

   The command interpreter that the Shell program specifies interprets the profile file. The profile can contain any noninteractive command that the shell interpreter understands.
6. Specify the user credential defaults.
   a. Select one of the following values to specify that the Process operators use the selected option when user credentials are not specified:
      - (Default) Defaults to the user under which touchpoint is run.

        The Process operators use the user credentials under which the agent or Orchestrator process is running.
      - Defaults to the specified Default user.

        The Process operators use the user credentials that are configured as the Default user and Default password.
      - No default.

        The Process operators use the user credentials that are supplied at run time.

   b. Consider the implications of specifying defaults for user ID and password:
      - To prevent users from defining and starting processes through CA Process Automation to which they otherwise have no access, specify a user ID with only necessary permissions.
      - Leave the user ID and password blank to force users to enter those values when they start processes through CA Process Automation.

   c. If appropriate, enter the default shell account to use when starting user processes that lack a user name and a password.

d. If appropriate, enter the password for the Shell user account.

Note: Passwords that are part of the Command Execution configurations are protected and cannot be modified through a program, referenced, or passed to external methods.

e. Reenter the Default password to confirm it.

7. Consider the implications of specifying defaults for user ID and password:
   - To prevent users from defining and starting processes through CA Process Automation to which they otherwise have no access, specify a user ID with only necessary permissions.
   - Leave the user ID and password blank to force users to enter those values when they start processes through CA Process Automation.
8. If appropriate, enter the default shell account to use when starting user processes that lack a user name and a password.
9. If appropriate, enter the password for the Shell user account.

   Note: Passwords that are part of the Command Execution configurations are protected and cannot be modified through a program, referenced, or passed to external methods.
10. Reenter the Default password to confirm it.
11. Indicate whether to load the user profile that is associated with the specified default user and password.
12. Click Save and Close.
13. Click Save.
14. Select Domain and click Unlock.

More information:

About Command Execution (see page 275)
Override Settings Inherited by a Category of Operators (see page 308)
Category Configuration and Operator Inheritance (see page 306)
Configuring Operator Categories (see page 270)

About Databases

The Databases category of operators leverages the Java Database Connectivity (JDBC) technology. JDBC technology supports connectivity in a heterogeneous environment between the Java programming language and databases such as Microsoft SQL Server. The Databases category does not support administrative operations such as stopping a database server. The connection information can be supplied with the server, port and the system identifier (SID), or with a TNSNAMES entry in tnsnames.ora. The tnsnames.ora file is the Oracle Service name configuration file.

The Databases category includes settings for the following databases:

- Oracle
- MSSQL
- MySQL
- Sybase

To use the Databases category of operators with an RDBMS from a vendor other than the ones that CA Process Automation uses, install the appropriate driver.

Note: See “Install JDBC Drivers for JDBC Connectors” in the *Installation Guide* for details.

More information:

Enable Windows Integrated Security for the JDBC Module for MSSQL Server (see page 287)

Configure Databases: Default Oracle Properties

You can configure the Databases category of operators for Oracle.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Databases, and select Edit.

3. On the Default Oracle Properties tab, select one of the following values as the default Oracle JDBC driver type. Use a JDBC version that matches the Java Development Kit (JDK) version.

   thin

   The Thin Driver type is used on the client side with no Oracle installation. The Thin driver connects to the Oracle database with Java sockets.

   oci

   The OCI Driver type is used on the client side with Oracle installed. The OCI drivers use the Oracle Call Interface (OCI) to interact with the Oracle database.

   kprb

   The KPRB Driver type is used to write Java database stored procedures and triggers.

4. Accept the default driver entry (oracle.jdbc.OracleDriver), or change the driver entry.
5. Enter the location of the Oracle server and login credentials:
   a. Enter the server host where the Oracle database is running.
   b. Enter the default port for the Oracle database.
   c. Enter the default user name for the Oracle database user.
   d. Enter the password that is associated with the specified user name.
6. Enter the Oracle Service ID.
7. Enter the source of the contents of tnsnames.ora in the Oracle directory.

   The Oracle TNS Names file translates a local database alias to information that enables the connectivity to the database. This information includes the IP address, the port, and the database Service ID.
8. Accept the default maximum number of rows to retrieve (10), or select another value up to 512.

9. Enter the default data encryption method. Consider entering one of the following values, where RCA_128 and RCA_256 are for domestic editions only:
   - RC4_40
   - RC4_56
   - RC4_128
   - RC4_256
   - DES40C
   - DES56C
   - 3DES112
   - 3DES168
   - SSL
   - AES128
   - AES256
   - AES192
10. Enter the default from the checksums that Oracle supports. See your Oracle documentation.
11. Click Save and Close.
12. Click Save.
13. Select Domain and click Unlock.

More information:

Category Configuration and Operator Inheritance (see page 306)
About Databases (see page 284)
Configuring Operator Categories (see page 270)

Configure Databases: Default MSSQL Server Properties

You can configure the Databases category of operators for MSSQL Server.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Databases, and select Edit.
3. Click the Default MSSQL Server Properties tab.
4. Accept com.microsoft.sqlserver.jdbc.SQLServerDriver as the default driver for MSSQL Server.

5. Enter the host name or IP address of the host where the MSSQL Server is running, to use as the default.
6. Enter the default MSSQL Server port (typically 1433).
7. Specify default credentials for the MSSQL database user.
   - Enter a user name.
   - Enter the password that is associated with the specified user name.
8. Accept the default maximum number of rows to retrieve (10), or select another value up to 512.
9. Enter the default MSSQL database name.
10. Enter the default MSSQL instance name.
11. Click Save and Close.
12. Click Save.
13. Select Domain and click Unlock.

More information:

Override Settings Inherited by a Category of Operators (see page 308)
Category Configuration and Operator Inheritance (see page 306)
About Databases (see page 284)
Configuring Operator Categories (see page 270)

Enable Windows Integrated Security for the JDBC Module for MSSQL Server

You can enable operators in the Databases category for the Microsoft SQL Server (MSSQL) to use integrated security. These operators can use integrated security when connecting to touchpoints on hosts running on Windows operating systems.

A Databases operator is an operator in the Databases category. Target hosts are hosts with an agent or Orchestrator. For each target host that a Databases operator can access, copy sqljdbc_auth.dll to the system path of that host. This process configures the Databases category for MSSQL so it uses integrated security with Windows Authentication.

You can enable Windows integrated security for the Databases category for MSSQL Server.

Follow these steps:

1. If you use the Microsoft SQL Server driver version that is packaged with CA Process Automation, download version 3.0 of the driver from the Microsoft website. Otherwise, locate (or download again) the complete version of the driver.
2. Locate the packaged or downloaded sqljdbc_auth.dll that corresponds to the hardware where the agent or Orchestrator is running.
3. Copy sqljdbc_auth.dll to a folder on the system path of each CA Process Automation agent or Orchestrator that is running in a Windows operating environment.

   To determine the system path, take *one* of the following actions:

   - Enter the following command at a command prompt:

     echo %PATH%

     The system path displays.

   - Go to Start, Settings, Control Panel, System, Advanced (Advanced System Settings), Environment Variables. The system path displays in the PATH variable.
4. Restart the agent or Orchestrator.

Notes:

- When you create a connection URL without integrated security, you specify the user name and password. To use integrated security, do not specify the user name and password.
- Append ;integratedSecurity=true to the Connection URL. For example:

  ```
  jdbc:sqlserver://localhost ... ;integratedSecurity=true
  ```

Configure Databases: Default MySQL Properties

You can configure the Databases category of operators for the MySQL Server.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Databases, and select Edit.
3. Click the Default MySQL Server Properties tab.
4. Accept com.mysql.jdbc.Driver as the default driver for MySQL.
5. Identify the host where the MySQL database is running.
6. Enter the default MySQL database port, for example, 3306.

7. Enter the default login credentials for the default MySQL database.
   a. Enter the default user name for the MySQL database user.
   b. Enter the password that is associated with the specified user name.
8. Accept the default maximum number of rows to retrieve (10), or select another value up to 512.
9. Enter the default MySQL database name.
10. Click Save and Close.
11. Click Save.
12. Select Domain and click Unlock.

More information:

Override Settings Inherited by a Category of Operators (see page 308)
Category Configuration and Operator Inheritance (see page 306)
About Databases (see page 284)
Configuring Operator Categories (see page 270)

Configure Databases: Default Sybase Properties

You can configure the Databases category of operators for Sybase.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Databases, and select Edit.
3. Click the Default Sybase Properties tab.
4. Select one of the following values for the default Sybase relational database system:
   - Adaptive Server Anywhere (ASA)
   - Adaptive Server Enterprise (ASE)
5. Accept Tds or enter a different default connection protocol.
6. Accept com.sybase.jdbc2.jdbc.SybDriver or enter a different default driver.
7. Specify the location of the Sybase database.
   a. Identify the server host.
   b. Enter the default port.

8. Enter the default login credentials for the default Sybase database.
   a. Enter the default user name.
   b. Enter the password that is associated with the specified UserName.
9. Accept 10 as the default maximum number of rows to retrieve, or select another value up to 512.
10. Specify the amount of memory that the driver uses to cache insensitive result set data in one of the following ways:

    -1

    All data is cached.

    0

    Up to 2 GB of data is cached.

    n

    Defines the buffer size in KB, where the value is a power of 2 (an even number). When the specified limit is reached, the data is cached.
11. Indicate whether to use the JDBC v3.0 compliant mechanism as the default batch performance workaround.

    Note: If not selected, the native batch mechanism is used.
12. Click Save and Close.
13. Click Save.
14. Select Domain and click Unlock.

More information:

Override Settings Inherited by a Category of Operators (see page 308)
Category Configuration and Operator Inheritance (see page 306)
About Databases (see page 284)
Configuring Operator Categories (see page 270)

About Date-Time

Operators in the Date-Time category can run on Orchestrators. The Date-Time category supports date and time options for operators in other categories and conditional operators for executing branches in a process. Examples follow:

- Compare the current date and time with a specified date and time.
- Test whether the current date falls within a calendar rule.
- Wait for a specified date and time.

The Date-Time category of operators has no configurable properties.

About Directory Services

The Directory Services category of operators provides an interface to support Lightweight Directory Access Protocol (LDAP). Directory Services operators can execute on an Orchestrator or an agent.

Configure Directory Services Defaults

You can configure Directory Services. The Directory Services operator category provides an interface to support LDAP/AD.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Directory Services, and select Edit.
3. Specify a batch size default for returning operation results to help the server optimize performance and usage of resources. Either select a value from 1 through 1000 or enter 0 to let the server determine the batch size.
4. Select a value for the maximum number of objects to return when executing the Get Object or Get User operators.
5. Specify the following factory class names:
    a. Accept the default, com.sun.jndi.ldap.LdapCtxFactory, as the fully qualified class name of the factory class that creates an initial context.
    b. Enter a colon-separated list of fully qualified state factory class names that can get the state of a specified object. Leave this field blank to use the default state factory classes.
    c. Enter a colon-separated list of the fully qualified class names of factory classes that create an object from information about the object. Leave this field blank to use the default object factory classes.

6. Enter a colon-separated list of language tags, where tags are defined in RFC 1766. Leave blank to let the LDAP server determine the language preference.
7. Select one of the following values to specify how the LDAP server handles referrals.

   Ignore

   Ignore the referrals.

   Follow

   Follow the referrals.

   Throw

   Return the first referral that the server encounters and stop the search.
8. Specify the authentication mechanism for the LDAP server to use with one of the following entries:

   None

   Use no authentication (anonymous).

   Simple

   Use weak authentication (clear-text password). Select this option when you set Security Protocol to SSL.

   Space-separated SASL mechanism list

   Let LDAP support any type of authentication agreed upon by the LDAP client and server.
9. Indicate the security protocol in one of the following ways:
   - Enter **ssl** to specify the protocol that permits LDAP server connections through a secure socket.

     Important! If connecting to Active Directory (AD), type **ssl** in *lowercase*. AD rejects the value SSL.
   - Leave blank to use basic connectivity.
10. Select a value to indicate the connection timeout value in seconds or enter 0 (zero) for no timeout.
11. Enter the location of the default LDAP Server and the default login credentials.
    a. Enter the host name or IP address.
    b. Enter the default port for the LDAP Server. Consider the following ports:
       - 389 - The ldap port for Lightweight Directory Access Protocol (LDAP).
       - 636 - The ldaps port for the ldap protocol over TLS/SSL.

c. Enter the User ID of the default LDAP User. Operators can use this default or can override it.

d. Enter the default Password for LDAP User. Operators can use this default or can override it.

12. Enter the default base distinguished name (DN). Operators can use this default or can override it.
13. Enter either **uid** or **cn** as the default user prefix.
14. Click Save and Close.
15. Click Save.
16. Select Domain and click Unlock.

More information:

Override Settings Inherited by a Category of Operators (see page 308)
Category Configuration and Operator Inheritance (see page 306)
About Directory Services (see page 291)
Configuring Operator Categories (see page 270)

About Email

The Email category of operators allows you to work with messages and folders on an email server. Email operators communicate with your mail server remotely using one of the following protocols:

- Post Office Protocol version 3 (POP3)
- POP3-SSL
- Internet Message Access Protocol (IMAP)
- IMAP-SSL

Some operators, such as those that act on folders, are supported only when using the IMAP protocol.

Note: See the *Content Designer Reference* for details on the protocol each Email operator supports.

Configure Default Email Properties

You can configure default settings for the Email operators.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Email, and select Edit.

   The Email page appears. Configure the following information:

   - Default Outgoing Email Properties (see page 294)
   - Default Incoming Email Properties (see page 295)
3. Click Save.
4. Select Domain and click Unlock.

Default Outgoing Email Properties

You can configure the default outgoing Email properties.

Follow these steps:

1. Enter the host name of the SMTP Server for Outgoing e-mail.
2. Select the Protocol for Outgoing Email.
   - SMTP Unsecure
   - SMTP STARTTLS
   - SMTP SSL
3. Enter the port number of the SMTP server.

   Note: For CA Process Automation r4.2.2 and above, we recommend you to edit the SMTP server port number in the SMTP Server Port field only (instead of Oasisconfig.properties file).
4. Enter the email address to display in the sender field of outgoing Java e-mail alerts. Fully configure this account. For example:*username*@*company-name*.com
5. Specify default credentials for the email user as follows, or leave this value blank if it is always specified at the operator level.
   a. Enter a user name.
   b. Enter the associated password.
6. Click Save and Close.

Default Incoming Email Properties

You can configure the default incoming Email properties.

Follow these steps:

1. Select the default protocol with which to receive emails from a remote server or remote web server.
   - IMAP
   - POP3
   - IMAP-SSL
   - POP3-SSL
2. Identify the default mail server from which email is retrieved.
3. Enter the default port of the default mail server for inbound emails. Consider the following ports:

   143

   The IMAP port for an unsecured connection.

   110

   The POP3 port for an unsecured connection.

   993

   The IMAP-SSL port for a secured connection.

   995

   The POP3-SSL port for a secured connection.
4. Specify default credentials for the email user as follows, or leave this value blank if it is always specified at the operator level.
   a. Enter a user name.
   b. Enter the associated password.
5. Click Save and Close.

About File Management

The File Management category of operators can run on either an agent or an Orchestrator. File Management operators monitor the existence or status of a file or directory. Additionally, File Management operators look for specific patterns within the contents of a file. POSIX rules govern the patterns on text pattern matching. This function can be used to determine further processing in a Process. For example, the File Management operators can wait for an XML file that contains patterns that require processing. File Management can look for error messages in the contents of log files.

The File Management category of operators watches for files or monitors the contents of a file on the target. The files can be on another computer or network drive, but they have to be visible to the operators. All File Management operators (such as building directory paths or scanning file contents) are performed as Administrator or as the user that started the touchpoint.

Specific conditions to test or wait for include:

- The appearance of a file.
- The absence of a file.
- Conditions on the size of a file.
- The last modification date/time.
- The existence of a string or a pattern in a file (based on POSIX masks).

More information:

Configure File Management (see page 296)

Configure File Management

You can configure default settings for operators in the File Management category. Unless noted, the referenced fields apply to both UNIX or Linux and Microsoft Windows operating systems.

Note: To expand a field for a File Management window entry that exceeds the provided space, right-click the field and then select Expand.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click File Management, and select Edit.

3. Complete the following steps on the File Management window:
   a. Click Default Windows File Management Properties or Default UNIX File Management Properties as appropriate for the operating system you are configuring.
   b. Complete the following fields if you set the Require user credentials field to Defaults to User Specified Below:
      - User
      - Password
      - Confirm password
   c. (UNIX) Define the operator system shell. For example, enter one of the following values for Shell:
      - /bin/bash
      - /bin/csh/
      - /bin/ksh
   d. (UNIX) Select or clear the Disable Password Check check box, depending on whether the product is to verify the user password when it switches users.
   e. Enter the command that compresses a file or directory in the Compression Utility field. For example:

      ```
      WZZIP -P -r {0} {1}
      ```

      ```
      gzip -qrf {0}
      ```

      - {0} defines the output compressed file name.
      - {1} defines the name of the source file to compress.
   f. Enter the command that extracts a compressed file or directory in the Uncompress Utility field. For example:

      ```
      WZUNZIP -d -o -yO {0}
      ```

      ```
      gunzip -qrf {0}
      ```

      {0} defines the name of the compressed file to extract.
4. Click Save and Close.
5. Click Save.
6. Select Domain and click Unlock.

More information:

Override Settings Inherited by a Category of Operators (see page 308)
About File Management (see page 296)
Configuring Operator Categories (see page 270)

About File Transfer

The File Transfer category acts as a File Transfer Protocol (FTP) client that supports remote file operators in a process. Operators in the File Transfer category can be executed on either Orchestrator or agent touchpoints. The File Transfer category supports all commands that standard FTP supports, including:

- File transfers to/from a remote host supporting FTP.
- Getting file/directory information from a remote host.
- Deleting a file/directory.
- Renaming a file/directory.

No prerequisites are required for FTP-based operators using standard FTP and standard FTP servers. For SFTP transfers, use SSH2 and prearrange for the touchpoint to communicate with the SFTP server computer based on user name and password credentials.

Establish an SSH connection and set up the certificates with an SSH client, before using SFTP. CA Technologies delivers a test SSH client for Windows so that you can establish that initial connection. Most UNIX computers already have it. The advantage of SFTP is that it is secure. With SFTP, data goes through an encrypted tunnel and passwords are authenticated.

Configure File Transfer

You can configure default settings for all operators in the File Transfer category. In all cases, the values you configure can be overridden at the operator level. For more information, see Category Configuration and Operator Inheritance (see page 306).

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click File Transfer, and select Edit.
3. On the File Transfer window, complete the Default UDP Port for Trivial FTP field (port 69 is the typical value).
4. Click Save and Close.
5. Click Save.
6. Select Domain and click Unlock.

More information:

Override Settings Inherited by a Category of Operators (see page 308)

About Java Management

Java Management operators can run on either an agent or an Orchestrator. These operators perform various tasks on Java ManagedBeans (MBeans) resources using Java Management Extensions (JMX) technology. The operators use a specified username and password to connect to a JMX Service URL or a JMX Server on a specified host and port.

Specific operators perform the following tasks:

- Retrieve MBeans attributes.
- Invoke MBeans methods using specified parameters.
- Set MBeans attributes values.

The Java Management category has no configurable properties.

About Network Utilities

Operators in the Network Utilities category can run on both Orchestrators and agents and can interact with SNMP devices or SNMP managers (such as network managers). Network Utilities operators determine the state of a configuration element of an IP device.

Network Utilities operators generate SNMP-based Alerts (traps) to either devices or network managers. Network Utilities is designed to influence a Process, not to implement a full-fledged network monitor.

Users can invoke operators from Network Utilities to:

- Get the value of remote MIB (Management Information Base) variables and use their values in the Process (for example, as parameters or as conditions).
- Wait for conditions on the value of remote MIB variables.
- Set remote MIB variables to affect the behavior of external devices.
- Send SNMP traps to report errors and special conditions to SNMP management platforms (for example, Tivoli, HP OpenView, or ISM).

Network Utilities operators are available on hosts with UNIX and Windows operating systems. Network Utilities identify remote MIB variables by their Object IDs (OIDs).

More information:

Configure Network Utilities (see page 300)

Configure Network Utilities

You can configure the Network Utilities category of operators.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click File Transfer, and select Edit.
3. Right-click Network Utilities and select Edit.
4. In the Poll frequency (secs) field, specify how often a Network Utilities operator synchronously obtains the device object identifier (SNMP OID) for an SNMP variable.
5. Click Save and Close.
6. Click Save.

   The configuration process applies the module-level changes to the product configuration.
7. Select Domain and click Unlock.

More information:

Override Settings Inherited by a Category of Operators (see page 308)
Category Configuration and Operator Inheritance (see page 306)
About Network Utilities (see page 299)
Configuring Operator Categories (see page 270)

About Process Control

Operators in the Process Control category can run only on Orchestrator touchpoints. Process Control operators have the following functions:

- Start and interpret CA Process Automation processes
- Invoke other categories to run operators in a process object instance
- Enforce dependencies
- Monitor category invocations and base how subsequent process branches run on the invocation results

When a process starts, the product makes a copy (instance) of the process. Changes to the copy do not affect other copies or the original process. You can start a process in any of the following ways:

- With the Form Designer.
- From a schedule.
- From another process.
- From an external application that uses a CA Process Automation trigger.
- From an external application that uses SOAP calls. See the *Web Services API Reference*.

If highly decentralized architectures, consider defining logical groups of operator categories in an environment and configure Process Control on a selected touchpoint in each group. In such a configuration, the product starts processes on the touchpoint that runs the Process Control operators for a group. You configure a touchpoint specifically to run multigroup processes. Running the processes in a decentralized architecture has the following benefits:

- It reduces the load on individual computers
- It reduces the impact of potential incidents
- It reduces the amount of data that is exchanged on remote hosts

More information:

Configure Process Control (see page 301)

Configure Process Control

You can configure the default setting for operators in the Process Control category.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Process Control, and select Edit.
3. On the Process Control window, complete the Time to keep completed user interactions (mins) field.
4. Click Save and Close.
5. Click Save.
6. Select Domain and click Unlock.

More information:

Override Settings Inherited by a Category of Operators (see page 308)
Category Configuration and Operator Inheritance (see page 306)
About Process Control (see page 300)
Configuring Operator Categories (see page 270)

About Utilities

The Utilities category in the Modules tab contains fields that pertain to the Invoke Java operator.

Important! The Invoke Java operator only runs on an agent and cannot be configured for an Orchestrator.

The Utilities category lets you specify:

- Paths to the external jars to load by default for all Invoke Java operators.
- Default logging.

Each jar that is specified becomes available to the Java code that the Invoke Java operators execute. The classes defined in the operator level jars override the same classes specified in the jars for the Utilities category.

If configured, designers can use the logger in the context of the code. For example:

```
logger.debug()
logger.info()
```

You can elect to configure logging, where logged data does not include info.

Configure Utilities

You can configure default settings for the Invoke Java operator in the Utilities category only if the operator runs on an agent. Otherwise, this operator category requires no configuration. The Invoke Java operator is not permitted to run on Orchestrators.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click Utilities, and select Edit.

   The Default Invoke Java Operator Properties tab opens
3. Select the Use Strict Java Mode check box to enforce typed variable declarations, method arguments, and return types in the main method code at runtime.

4. Click Add Parameter  and define the external JAR files as appropriate.
5. To remove a selected JAR file, select an item from the External Jars list, and then click Delete.
6. Complete the remaining fields on the Utilities window as appropriate.
7. Click Save and Close.
8. Click Save.
9. Select Domain and click Unlock.

More information:

Category Configuration and Operator Inheritance (see page 306)
Configuring Operator Categories (see page 270)

About Web Services

Web Services operators run on both Orchestrators and agents. Two of the operators provide an interface to remote services exposed through SOAP. These operators:

- Builds a SOAP request.

  The data can be extracted at run time from existing CA Process Automation Datasets and variables or from external sources.
- Sends the SOAP request to the appropriate Web Services operator category specified at design or run time.
- Retrieves response handling error conditions as appropriate.
- Parses the incoming response and stores the results into CA Process Automation Datasets that subsequent Operators in a Process access.
- An asynchronous call sends the request and, after receiving an acknowledgment, waits for a response from remote destination. Asynchronous calls use a more complex send and receive than synchronous calls. Subsequent Operators in a Process access the returned data.

Web Services also provides the ability to automate data management facilities over a network using HTTP. For example, content designers can develop processes that automate RESTful services through HTTP Operators. When an HTTP operator is configured with a blank field, that operator inherits the default value of the corresponding field from the parent category setting. Therefore, when you make a selection for an operator category field, nothing gets enabled or disabled. You can specify all of the defaults, at your discretion. When you configure these same options at the operator level, selection of one option disables the others.

More information:

Configure Web Services (see page 304)

Configure Web Services

You can configure default settings for operators in the Web Services category.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click WebServices, and select Edit.
3. On the Web Services window, click Default Web Services Properties, and then review or update the fields as appropriate.
4. Click Default Web Services HTTP Properties, and then review or update the fields as appropriate.
5. Click Save and Close.
6. Click Save.
7. Select Domain and click Unlock.

More information:

Operator Categories and Where Operators Run (see page 311)
Override Settings Inherited by a Category of Operators (see page 308)
About Web Services (see page 303)
Configuring Operator Categories (see page 270)

Configure Values for a Custom Operator Group

You can configure values for the variables that you defined for a selected custom operator group. You define custom operator groups in the Group Configuration tab of a custom operator editor.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Modules tab, right-click a custom operator group, and select Edit.

   The selected custom operator group opens. The product initially displays the pages and variables without values.

3. For each displayed field or array, add the value to use as the default.

   The default values can be overridden at the environment level and at the operator level.

4. Click Save and Close.

5. Click Save.

6. When you finish configuring the operator categories and custom operator groups on the Modules tab, select Domain, and click Unlock.

Note: When you delete a variable or you change the variable data type, the product does not publish the changes to the Domain or the associated environments.

Delete a Custom Operator Group Configuration

Administrators can use the Modules tab in the Configuration Browser to delete the published custom operator group from the Domain and its environments.

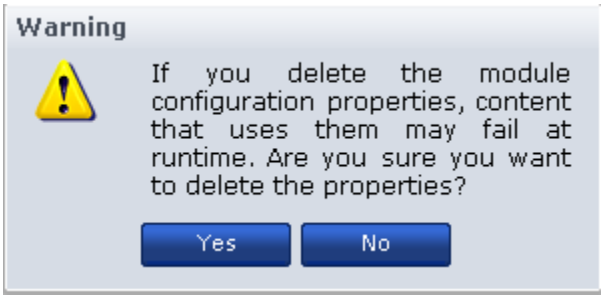
Follow these steps:

1. Click the Configuration tab

2. Right-click the Domain and select Lock.

3. Right-click the custom operator group and select Delete.

   The following warning appears:



4. Click Yes to confirm the deletion.

   CA Process Automation deletes the custom operator group configuration module from the Domain. If a process is using the custom operator group configuration module, the process fails to run.

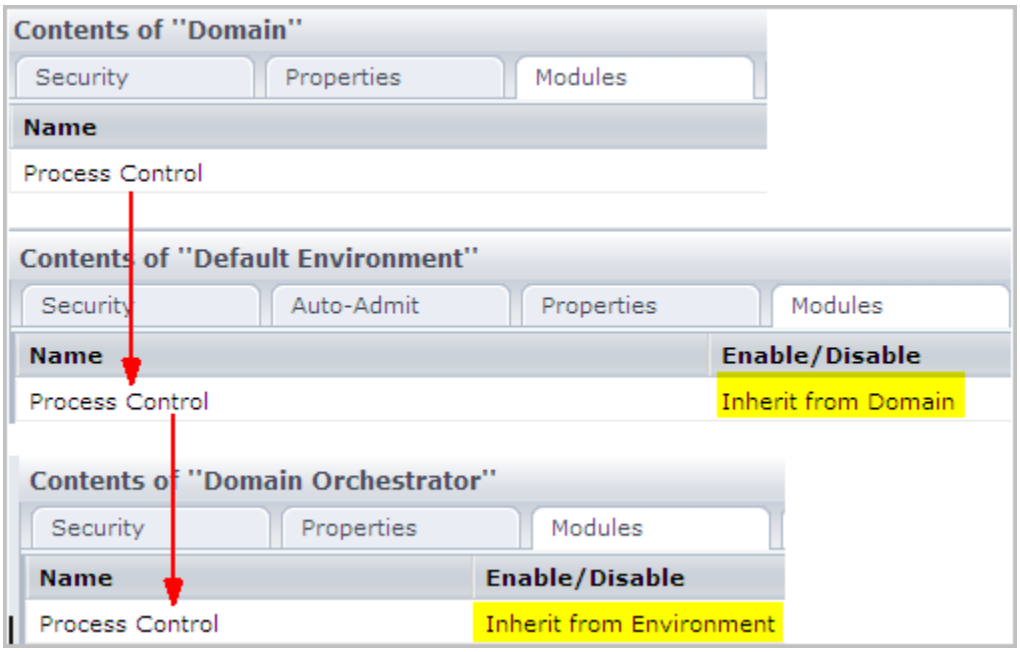
5. Click Save.

   The custom operator group configuration is deleted from the Domain and its environment.

Category Configuration and Operator Inheritance

Operator categories, such as Email or File Transfer, have configurable settings with predefined defaults. Administrators can edit a category from the Modules tab at various levels of the Domain hierarchy. At installation, the default settings for each operator category begin at the Domain level. These settings are marked Inherit from Domain at the environment level. At the Orchestrator level, these settings are marked Inherit from Environment.

As the following illustration shows, operator category settings are inherited from the Domain to each environment, and from each environment to Orchestrators in that environment. You can override settings at the Domain level, the environment level, and at the Orchestrator level.



Operators that target an Orchestrator inherit their operator category settings from that Orchestrator. Content designers override these inherited settings at the operator level as needed.

Agents inherit settings configured at the Domain level, but operators do not use these settings. When a touchpoint is associated with an agent, the association includes an environment. At run time, operators that target a touchpoint use the properties configured for the environment associated with the touchpoint.

Note: For user-defined custom operator groups, settings are inherited from the Domain level to the environment level. Administrators can override settings at the environment level that were defined at the Domain level. These settings are not available for override at the Orchestrator or agent levels.

More information:

Operator Categories and Operator Folders (see page 266)

Enable or Disable an Operator Category

Operator category settings are typically configured at the Domain level. By default, operator category settings for environments are Inherit from Domain. By default, operator category settings for Orchestrators and agents are set to Inherit from Environment.

Access the Modules tab for an environment, Orchestrator, or agent to:

- Enable one or more operator categories.
- Disable one or more operator categories.
- Configure one or more enabled categories.

Follow these steps:

1. Click the Configuration tab.

   The Configuration Browser opens.
2. Take one of the following actions to place a lock at the desired level:
   - Expand the Domain node, select the target environment and click Lock.
   - Expand the Orchestrators node, select the target Orchestrator and click Lock.
   - Expand the Agents node, select the target agent and click Lock.
3. Click the Modules tab.
4. Select an operator category, click the Enable/Disable column, and select either Enabled or Disabled.
5. Click Save.
6. Click Unlock.

Enable or Disable a Custom Operator Group

Custom operator group settings are typically configured at the Domain level. By default, custom operator group settings for environments are Inherit from Domain.

Access the Modules tab for an environment to:

- Enable one or more custom operator groups.
- Disable one or more custom operator groups.
- Override settings on one or more enabled groups.

Follow these steps:

1. Click the Configuration tab.

   The Configuration Browser opens.
2. Expand the Domain node, select the target environment and click Lock.
3. Click the Modules tab.
4. Select a custom operator group, click the Enable/Disable column, and select either Enabled or Disabled.
5. Click Save.
6. Click Unlock.

Override Settings Inherited by a Category of Operators

An administrator with Domain Administrator rights configures categories for operators at the Domain level. An administrator with Environment Configuration Administrator rights can override inherited settings at any of the following levels:

- Environment
- Orchestrator
- Agent

Operator category settings that have been configured at the Domain level are displayed as Inherit from Domain. This setting is in a drop-down list, where other valid choices are Enabled and Disabled. Select Enabled to edit the inherited settings. Select Disabled to disable operators in the selected category.

You can override inherited settings for any category of operators at one or more levels.

Follow these steps:

1. Click the Configuration tab.
2. (Optional) Override selected settings at the environment level as follows:
   a. Right-click the selected environment and select Lock.
   b. Click the Modules tab.
   c. Select a category, click the drop-down list for Enable/Disable and select Enabled.
   d. Right-click the category and select Edit.

      The properties of the selected category are displayed in a scrollable list.
   e. Change one or more inherited settings.
   f. Click Save.
   g. Right-click the environment and select Unlock.
3. (Optional) Override selected settings at the Orchestrator level as follows:
   a. Expand Orchestrators, select an Orchestrator, and click Lock.
   b. Click the Modules tab.
   c. Select a category, click the drop-down list for Enable/Disable and select Enabled.
   d. Right-click the category and select Edit.

      The properties of the selected category are displayed in a scrollable list.
   e. Change one or more inherited settings.
   f. Click Save.
   g. Click Unlock.
4. (Optional) Override selected settings at the agent level as follows:
   a. Expand the Agents node, select an agent, and click Lock.
   b. Click the Modules tab.
   c. Select a category, click the drop-down list for Enable/Disable and select Enabled.
   d. Right-click the category and select Edit.

      The properties of the selected category are displayed in a scrollable list.
   e. Change one or more inherited settings.
   f. Click Save.
   g. Click Unlock.

Override Inherited Values for a Custom Operator Group

An administrator with Domain Administrator rights configures custom operator groups at the Domain level. An administrator with Environment Configuration Administrator rights can override inherited settings at the environment level.

Note: Unlike operator categories, you cannot override values for custom operator groups at the Orchestrator or agent level.

Custom operator group settings that have been configured at the Domain level are displayed as Inherit from Domain. This setting is in a drop-down list, where other valid choices are Enabled and Disabled. Select Enabled to edit the inherited settings. Select Disabled to disable custom operators in the selected group.

You can override settings that the selected environment inherits from the Domain.

Follow these steps:

1. Click the Configuration tab.
2. Right-click the selected environment, then select Lock.
3. Click the Modules tab.
4. Select a category, click the drop-down list for Enable/Disable, and select Enabled.
5. Right-click the category, then select Edit.

   The properties of the selected category are displayed in a scrollable list.
6. Change one or more inherited settings.
7. Click Save.
8. Right-click the environment, then select Unlock.

More information:

Configure Network Utilities (see page 300)
Configure Web Services (see page 304)
Configure Process Control (see page 301)
Configure File Management (see page 296)
Configure Command Execution: Default Telnet Properties (see page 278)

Operator Categories and Where Operators Run

Some operators run only on Orchestrators, but not on touchpoints associated with agents. Other operators run on Orchestrators and agent touchpoints, but not on remote hosts targeted by proxy touchpoints or host groups. Several operators can run on any target type. Some operators within an operator category can run on Orchestrators but not on agent touchpoints. Other operators within the same category can run on both Orchestrators and agent touchpoints. The ability to run on a given target type is not perfectly mapped to operator category.

Note: See "Where Operators Can Run" in the *Content Designer Reference* for information on valid targets for each operator.

More information:

Use a Proxy Touchpoint (see page 248)
Enable or Disable an Operator Category (see page 307)

Chapter 13: Administer Triggers

Applications that cannot make SOAP calls can use triggers as an alternative. Use of SOAP calls is recommended over triggers because it is more robust.

Triggers allow external applications to start a process in CA Process Automation. A trigger invokes the CA Process Automation process that is defined in XML content or in an SNMP trap. The XML content can be delivered to the configured file location or to the configured email address. SNMP trap content is sent in an OID matching a configured regular expression. CA Process Automation listens for incoming SNMP traps on the configured SNMP trap port, 162 by default.

This section contains the following topics:

How to Configure and Use Triggers

For external applications that cannot issue SOAP calls to start CA Process Automation processes, CA Process Automation provides four predefined triggers. You can configure triggers to enable the initiation of processes from any of the following:

- An event from a Catalyst connector
- A received file
- An email
- An SNMP trap

After you configure a file trigger or a mail trigger, you can create XML contents. The XML contents start configured CA Process Automation processes with parameters from the external applications. The XML content can be put in a file and placed in the configured directory or sent as an email to the configured account. The trigger invokes the process specified in the XML content when specified criteria are met. The process instance invoked by the trigger also populates process datasets with the values specified in the XML content.

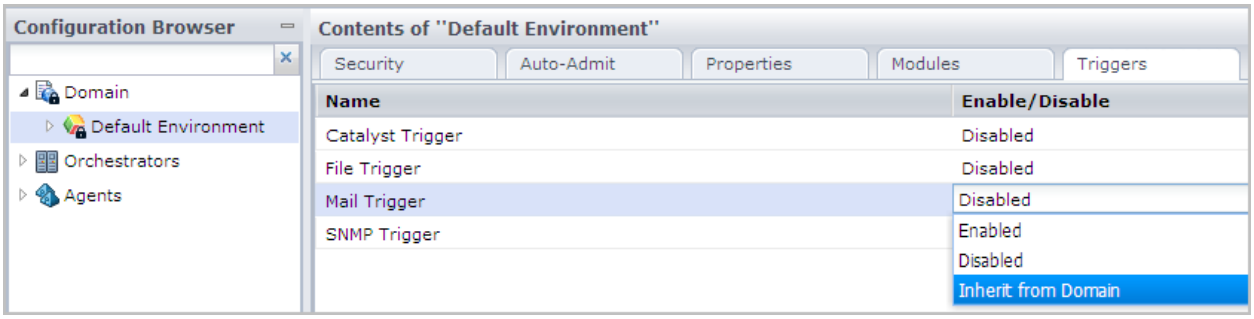
After you configure an SNMP trap trigger in CA Process Automation, external applications can send SNMP traps to CA Process Automation. When CA Process Automation receives an SNMP trap that matches object IDs (OIDs) and the payload values filter, the configured process starts. The dataset of the triggered process receives the trap information.

After you configure a Catalyst event subscription, external Catalyst Connectors can send events to CA Process Automation. When CA Process Automation receives a Catalyst event that matches the filter, the configured process starts with the event properties available in the process dataset.

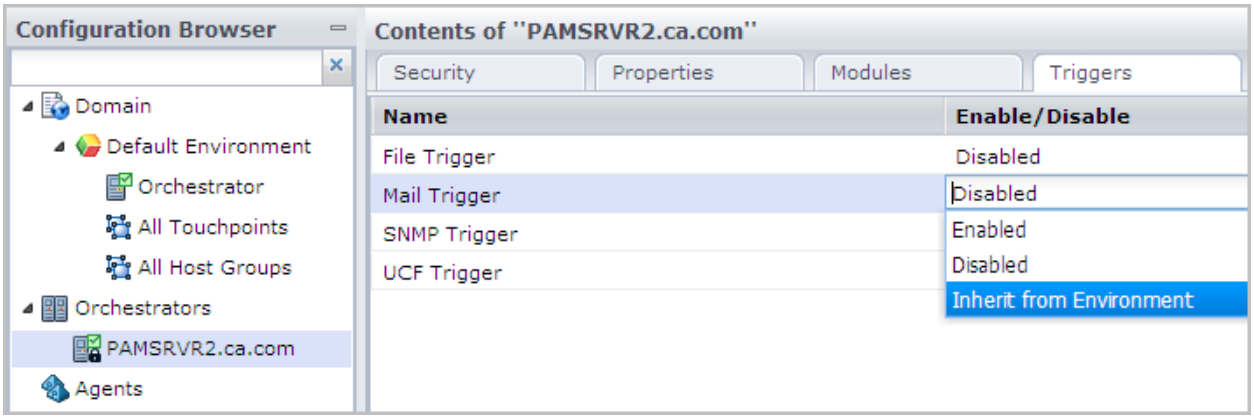
Unlike settings that the environment inherits from the Domain by default, triggers are disabled at both the environment level and Orchestrator levels by default. To enable CA Process Automation triggers that are set at Domain level, set inheritance from the Domain at the environment level. Then, set inheritance from the environment at the Orchestrator level. Alternatively, you can override inherited values and configure trigger values at the environment and Orchestrator levels.

Use the following approach to implement triggers:

1. Configure triggers at the Domain level. These configurations are not inherited by default. Configure triggers only if you plan to accept process initiation from external applications and only for the trigger types you plan to receive.
2. At the environment level, where the trigger status is Disabled, take one of the following actions:
   - Leave disabled for trigger types that are not applicable.
   - Change the status to Inherit from the Domain for Environments where Domain configuration is applicable.



   - Change the status to Enabled and configure the triggers at this level, where needed.
3. At the Orchestrator level, where the trigger status is Disabled, take one of the following actions:
   - Leave disabled for trigger types that are not applicable.
   - Change the status to Inherit from Environment. If you select this option, values are picked up from the environment at runtime if the triggers are defined at the environment level. Otherwise, the values defined at the Domain level are used.



   - Change the status to Enabled and edit the properties.

4. CA Process Automation searches the configured directory, the configured email account, and the configured port for content that matches the corresponding trigger criteria.
   - External applications create the input for configured triggers:
     - For a file trigger or mail trigger, they create valid XML content. XML content specifies the path to the starting process, the credentials, the time to start, and the initialization parameter values.
     - For an SNMP trap trigger, they send a valid SNMP trap to port 162 with values that match the configured criteria.
   - External applications send triggers to CA Process Automation as part of automation processing.
5. CA Process Automation processes new content and starts the configured CA Process Automation process with the values passed by the external application.
6. Monitor the process instance invoked by the trigger sent from the external process. You can monitor the running process through process watch. You can view the values passed by the trigger in the page containing dataset variables for the associated trigger type.

Configure Catalyst Trigger Properties at the Domain Level

The Domain Administrator rights let you configure Catalyst Trigger properties at the Domain level. With the inherited Catalyst Trigger properties, the product can start processes when it receives a Catalyst event.

The Catalyst Trigger supports a list of subscriptions, each referencing a Catalyst Connector with a filter. When the product receives a matching event from the Catalyst Connector, it starts the specified process is started.

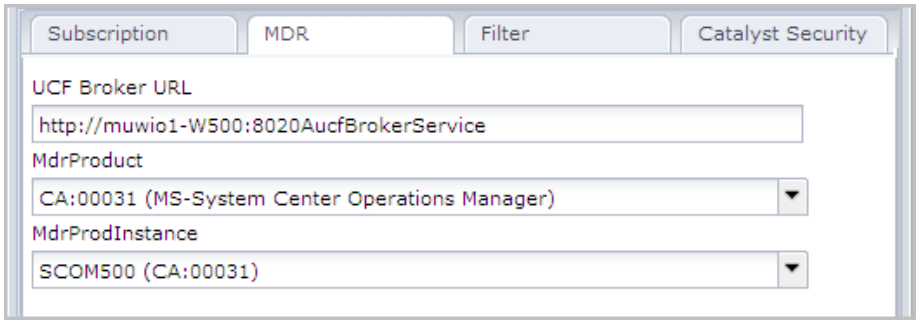
You can configure the Catalyst Trigger properties at the Domain level.

Note: This procedure shows examples of setting a Catalyst trigger to start a process when the Microsoft System Center Operations Manager creates or updates an Alert object. The Alert object properties are available as process variables.

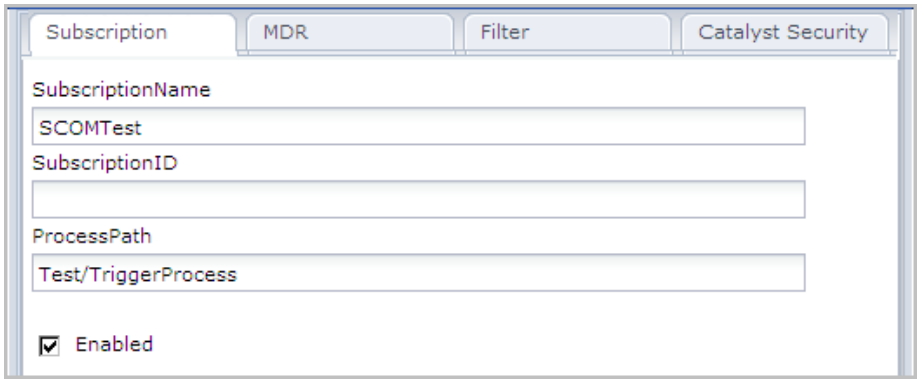
Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Triggers tab.
3. Right-click Catalyst Trigger, and then click Edit.
4. On the Catalyst Trigger dialog, click Add Parameter  .

5. On the Catalyst Subscriptions window, click the MDR tab, and then complete the fields as appropriate.
6. Verify that your entries resemble the following example:

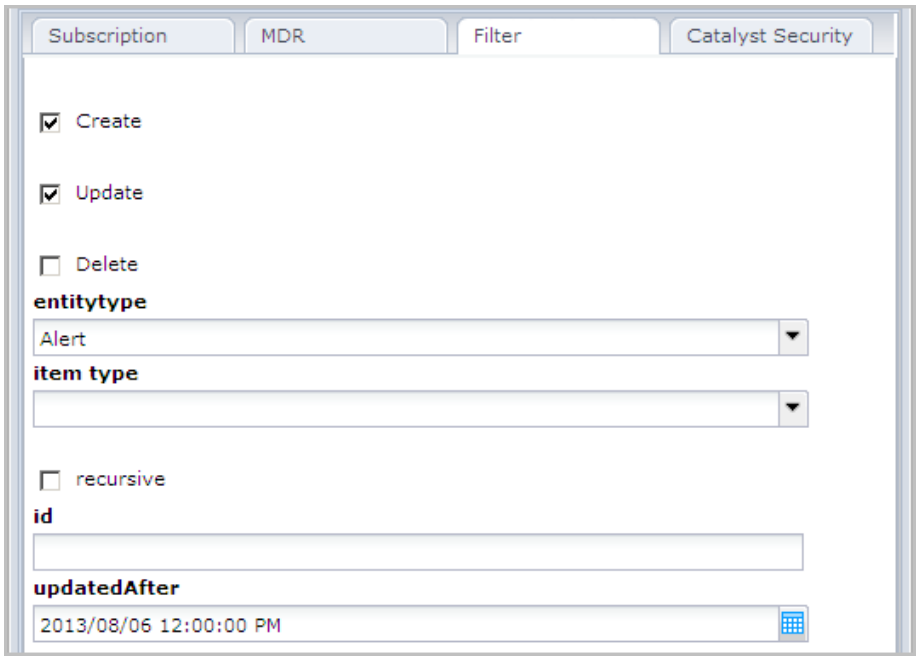


7. Click the Subscription tab, and then complete the fields as appropriate.
8. Verify that your entries resemble the following example:



9. Click the Filter tab, and then complete the fields as appropriate.

10. Verify that your entries resemble the following example:



11. Click the Catalyst Security tab.
12. Enter the credentials in the Username and Password fields.
13. For each claim to add, click the Add Parameter button under Claims, and then complete the Claim Name and Claim Value fields.
14. For each password claim to add, click the Add Parameter button under Password Claims, and then complete the Claim Name and Claim Value fields.
15. Click Save and Close.

    The product adds the subscription that you defined to the Subscription list. To edit the definition, highlight the entry and then click Edit.
16. Click Save.
17. Select Domain and click Unlock.

Configure File Trigger Properties at the Domain Level

The Domain Administrator rights let you configure File Trigger properties at the Domain level. Inheritance is *not* the default. Therefore, to use settings you configured at the Domain level, configure Inherit from Domain at the environment level and configure inherit from environment at the Orchestrator level.

When you use File Triggers to start processes, the Orchestrator searches the specified input directory for new files at the configured intervals. The product parses the content of each file that matches the specified input file name pattern and triggers the specified process. After it triggers the process, the product moves the file to the specified Processed directory. If the product cannot start the process, it moves the triggering file and an .err file to the specified Error directory. The .err file describes why the trigger failed.

Note: If a new file has the same name as an existing file, it replaces the older file.

Before you configure the File Trigger properties, create the following directories:

- An Input directory with the write permissions that are required to accept trigger files. To allow remote triggering, consider associating the directory with an FTP folder.
- A Processed directory to receive the successfully processed output.
- An Error directory for output that cannot be processed.

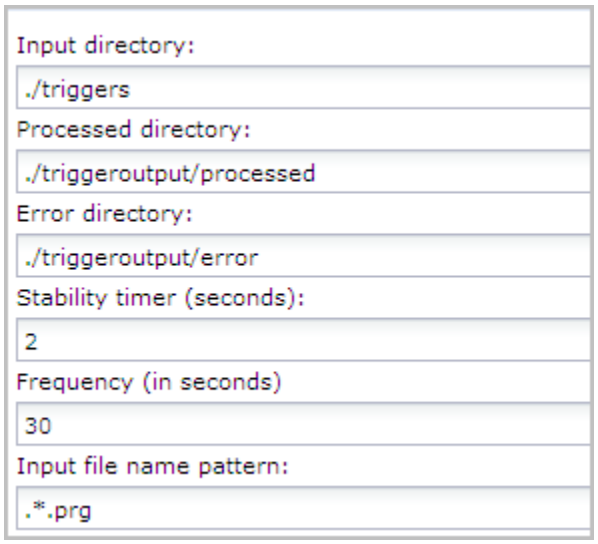
If they do not exist, the product creates the directories.

You can configure the File Trigger properties at the Domain level.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Triggers tab, right-click File Trigger, and click Edit.
3. On the File Trigger dialog, complete the fields as appropriate.

4. Verify that your entries are valid. The following example contains valid entries.



5. Click Save and Close.
6. Click Save.
7. Select Domain and click Unlock.

Configure Mail Trigger Properties at the Domain Level

The Domain Administrator rights let you configure Mail Trigger properties at the Domain level. Mail Trigger properties only enable the triggering of processes when they are inherited or configured at lower levels. To achieve the inheritance, configure Inherit from Domain at the environment level and configure Inherit from the Environment at the Orchestrator level.

When active, the Mail trigger searches the email account (configured as User Name and Password) for emails. If the email body or an attachment contains valid XML content, the product processes it. The parameters that the product creates in the triggered process instance depend on whether the email contains valid XML content.

Before you configure the Mail Trigger properties, complete the following tasks:

- Create an email account that is dedicated to receiving emails that trigger processes.
- Verify that the IMAP service is enabled on the mail server you identify as the Incoming mail server.

  If your corporate mail server restricts enabling the IMAP service, create a proxy mail server with IMAP enabled. Specify the proxy server as the Incoming mail server. Then, configure your corporate mail server to forward the emails that are addressed to the configured user account to the proxy mail server.
- (Optional) Create a default Domain Orchestrator process and save it to the Default Process handler path. The product uses the default process only then the email does not contain valid XML content. In this case, the default process starts and populates the following variables in the SMTP page in the process dataset:

  senderAdd

  Identifies the email address of the sender.

  senderTime

  Identifies the email server time when the email was sent.

  MailBody

  Contains the complete content of the email.

  The default process determines any further action.

You can configure the Mail Trigger properties at the Domain level.

Follow these steps:

1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Triggers tab, right-click Mail Trigger, and then click Edit.
3. On the Mail Trigger dialog, General Properties tab, complete the fields as appropriate.

   Default Trigger Process (Orchestrator only)

   Specifies how to handle emails that have invalid XML content in the message body or attachment.

   Values:

   - **Blank** - Ignore the emails with no valid XML trigger content.
   - The full path of the process that the Domain Orchestrator is to start. (One default process can be defined for each Orchestrator.)

IMAP Mail Server

Specifies the hostname or IP address of the mail server that receives incoming emails. The Inbox folder for the configured email account is searched for new emails. This server must have the IMAP protocol enabled. The Mail Trigger does not support POP3.

IMAP Server Port

If the default TCP port for an IMAP server is used, enter 143. If a nondefault port is used or secure communication is set up on a different port, obtain the correct port to enter from an administrator.

User Name

Specifies the user name with which to connect to the incoming mail server. Observe the requirements of your IMAP server when determining whether to enter the full email address or the alias as the user name. The user name pamadmin@ca.com is an example of a full address; pamadmin is the alias.

Note: Microsoft Exchange Server accepts both the full email address or the alias.

Password

Specifies the password that is associated with the specified user name.

Mail Processing Interval (seconds)

Frequency is seconds with which CA Process Automation searches the IMAP server for new incoming emails into the specified account. The user name and password specify the account.

Default:

2

Save mail attachments to database

Specifies whether to save attachments of mails that trigger CA Process Automation processes in the database.

- Selected: CA Process Automation saves attachments of mails to the CA Process Automation database and populates the data set of the process being started with relevant information of the attachments.
- Cleared: CA Process Automation does not save email attachments.

Outgoing SMTP Mail Server

Specifies the server name for the outgoing SMTP mail server. When a triggering email with valid XML content is received in the configured account of the IMAP mail server, an acknowledgment email is returned. The acknowledgment email is returned to the sender through the outgoing SMTP server.

SMTP Server Port

Specifies the port of the outgoing mail server.

Default:

25

Use secure SMTP connection

Specifies whether to process over a secure connection to the SMTP mail server.

- **Selected** - The mail server allows a secure connection to the SMTP mail server.
- **Cleared** - The mail server does not allow a secure connection.

Default:

Cleared

4. Click Save and Close.
5. Click Save.
6. Select Domain and click Unlock.

Configure SNMP Trigger Properties at the Domain Level

An administrator with Domain Administrator rights can configure SNMP Trigger properties at the Domain level. When inherited, the SNMP Trigger properties enable Processes to be triggered upon the receipt of an SNMP trap.

Before you begin configuring the SNMP Trigger properties, verify that port 162 is accessible to CA Process Automation. Modify the SNMP traps listening port in the CA Process Automation properties file if you use an alternative port.

Follow these steps:

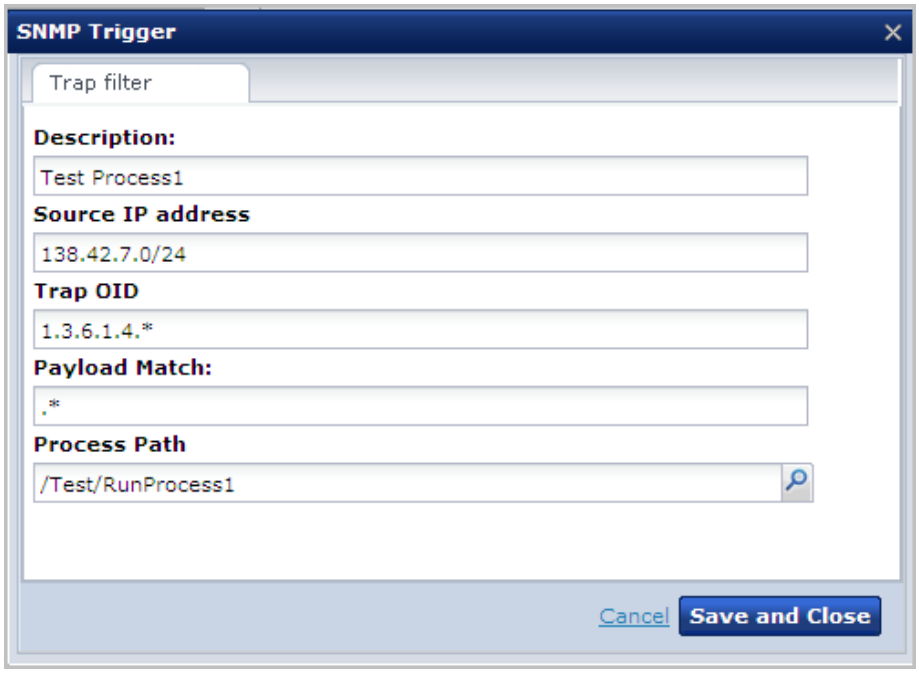
1. Click the Configuration tab, select Domain, and click Lock.
2. Click the Triggers tab, right-click SNMP Trigger, and then click Edit.
3. Click Add Parameter  .
4. On the SNMP Trigger window, complete the Trap filter fields as appropriate.

5. Verify that your entries are valid.

   The following example filter accepts SNMP traps from any host that have the following characteristics:

   - An IP address between 138.42.7.1 and 138.42.7.254 with an OID that begins with 1.3.6.1.4.1.[x.x.x.x.x]
   - At least one payload value that matches the literal string "Test Payload for trigger."

   When the product receives an SNMP trap matching these criteria, it triggers the process RunProcess1 in the path /Test.



6. Click the Move Up and Move Down buttons as appropriate to sequence the list by precedence. Each filter has precedence over the filters that are listed below it.

7. Click Save.
8. Select Domain and click Unlock.

More information:

Change the SNMP Traps Listener Port (see page 325)

Change the SNMP Traps Listener Port

By default, CA Process Automation listens on port 162 for SNMP traps designed to start CA Process Automation processes. If you have closed port 162 at your site and configured an alternative port, change the CA Process Automation configuration for this port in the OasisConfig.properties file. Then restart the Orchestrator service.

You can change the port on which CA Process Automation listens for SNMP traps.

Follow these steps:

1. Log on to the server on which the Domain Orchestrator is configured.
2. Navigate to the following folder or directory:

   install_dir`/server/c2o/.config/`
3. Open the OasisConfig.properties file.
4. Change the value in the following line from 162 to the port number you are using for SNMP traps.

   `oasis.snmptrigger.service.port=162`
5. Save the file.
6. Restart the Orchestrator service.
   a. Stop the Orchestrator (see page 186).
   b. Start the Orchestrator (see page 187).

   As soon as the service restarts, CA Process Automation begins listening on the port you configured. CA Process Automation listens for new SNMP traps that meet the criteria configured in the SNMP trigger.

More information:

Oasis Configuration Properties File (see page 400)

Chapter 14: Manage User Resources

You can manage resources for users, Orchestrators, and agents from the Manage User Resources palette of the Configuration tab.

The Manage User Resources palette contains three folders under Repository:

- Agent Resources
- Orchestrator Resources
- User Resources, which includes the subfolder, VBS_Resources.

  Note: You can add subfolders only under the User Resource folder.

Users who are granted the Configuration_User_Resources permission in the Configuration Browser policy in CA EEM can manage resources under the User Resources folder. However, only users who are also granted the Domain_Administrator permissions of the Domain policy can access folders for the Orchestrator Resources and Agent Resources. Members of the PAMAdmins default group have both of these permissions.

This section contains the following topics:

About User Resources Management

Resource Management requires specific permissions for various activities. Users that belong to the default PAMAdmins group (the group with full permissions) can perform any Resource Management activity.

Users in custom groups that have custom policies must have basic access and one or both of the following permissions:

PAM40 Environment Policy: Environment_Configuration_Admin (Configuration Administrator)

Users with Environment_Configuration_Admin (Configuration Administrator) permissions can upload, modify, or delete any type of file to User Resources. For example:

- A JAR file for use with the Invoke Java operator
- A script for use with the Run Script operator
- An image

PAM40 Domain Policy: Domain_Admin (Administrator)

Users with Domain_Admin (Administrator) permissions can perform the following tasks:

- Add resources to the Orchestrator Resources folder or the Agent Resources folder
- Edit the content of a resource and readd it; update descriptive fields
- Delete a previously uploaded Orchestrator Resource or Agent Resource

Note: The procedures for editing and deleting Orchestrator Resources and Agent Resources are similar to procedures for editing and deleting User Resources.

Differences between User Resources and Agent or Orchestrator Resources are as follows:

User Resources

- After a restart, the agent or Orchestrator classpath does not include resources that were uploaded to User Resources.
- You can create subfolders in the User Resources folder.
- You do not need Domain_Admin (Administrator) rights.

Agent Resources and Orchestrator Resources

- After a restart, the agent or Orchestrator classpath includes resources that were uploaded to Agent Resources and Orchestrator Resources.
- You cannot create subfolders in the Agent Resources and Orchestrator Resources folders.
- You need Domain_Admin (Administrator) rights.

How to Deploy JDBC Drivers for Database Operators

You can install JDBC drivers for Database operators either during installation or after CA Process Automation is installed. Only processes with Database operators require a JDBC driver.

During installation, the JDBC drivers uploaded in the Third-Party Software installation are displayed but not selected. You can select the JDBC drivers for MySQL, Microsoft SQL Server, and Oracle. You can also add other JAR files that you copied to a local directory.

After installation, you can upload JAR files that contain JDBC drivers for Database operators using the Manage User Resources palette in the Configuration tab. CA Process Automation deploys the uploaded JAR files to either Orchestrators or agents, depending on the folder you select when doing the upload. See the following topics for more information:

- Upload Orchestrator Resources (see page 329).
- Upload Agent Resources (see page 331).

Upload Orchestrator Resources

After installation, the Orchestrator Resources folder displays only the JDBC JAR files that were added during installation. After you use the Manage User Resources palette to update the Orchestrator Resources folder, the Orchestrator Resources folder also displays the uploaded JAR files.

You can upload a JAR file to the Orchestrator Resources folder on the Domain Orchestrator. When you restart the Domain Orchestrator, CA Process Automation deploys the file to the Domain Orchestrator. The Domain Orchestrator mirrors (copies) the file at the configured mirroring interval, after which you restart the other Orchestrators. When the Orchestrators restart, the mirrored file is available for their use.

Note: Mirroring applies to all Orchestrators in the domain. For clustered Orchestrators, mirroring applies to all nodes in each cluster.

Follow these steps:

1. Click the Configuration tab.
2. Click the Manage User Resources palette and expand the Repository folder.
3. Select the Orchestrator Resources folder.
4. Click New.

   The Add New Resource: "Untitled" pane opens.

5. Provide upload details in the following fields as appropriate:

   a. Enter the name of the resource in the Resource Name field.

      The following example is a reasonable way to specify the resource name if you are uploading a JDBC driver:

      database_name Driver

      database_name

      Defines the name of the RDBMS. For example, Oracle Driver, MySQL Driver, or Sybase Driver.

   b. Click Browse, navigate to the location where you saved the JAR file, and select the target file. This populates the Resource File field.

   c. Select a user-specified module name from the Module Name drop-down list.

   d. (Optional) Enter a description of the resource in the Resource Description field.

6. Verify your entry, and then click Save.

   A line with your entry displays.

   CA Process Automation copies the uploaded resource to the following paths:

   install_dir/server/c2o/ext-lib

   install_dir/server/c2o/.c2orepository/.c2oserverresources/lib

   install_dir

   Defines the directory on the server where the Domain Orchestrator was installed.

7. Restart the Domain Orchestrator. (Stop the Domain Orchestrator (see page 186) and then start the Domain Orchestrator (see page 187).)

   When the Domain Orchestrator restarts, the system deploys all jars that you uploaded to the Domain Orchestrator Resources. That is, CA Process Automation puts the jars in the classpath of the Domain Orchestrator.

8. After mirroring occurs, restart all other Orchestrators.

   The system deploys all uploaded jars to all Orchestrators. That is, the system puts the jars in the classpaths of the Orchestrators.

   Note: For clustered Orchestrators, restart each node.

Upload Agent Resources

Users with Domain Administrator permissions can upload resources to the Agent Resources folder on the Domain Orchestrator. The uploaded resource can be a jar file, for example, a JDBC driver. The uploaded agent resources are mirrored at the configured mirroring interval. After mirroring occurs, you restart the agents. Restarted agents can use the uploaded agent resources.

Follow these steps:

1. Browse to CA Process Automation and log in (see page 18).
2. Click the Configuration tab.
3. Click the Manage User Resources palette and expand the Repository folder.
4. Select the Agent Resources folder and click New.

   The Add New Resource: "Untitled" pane opens
5. Provide upload details, using the following field descriptions as needed.
   a. Enter the name of the resource in the Resource Name field.

      If you are uploading a JDBC driver, type *database_name* Driver; where *database_name* is the RDBMS. For example, Oracle Driver, MySQL Driver, or Sybase Driver.

   b. Click Browse, navigate to the location where you saved the jar file, and select the target file.

      This populates the Resource File field with the file and its path.

   c. (Optional) Select a user-defined module name from the Module Name drop-down list.

   d. (Optional) Enter a meaningful description in the Resource Description field.
6. Verify your entry. Then, click Save.

   A line with your entry displays.

   CA Process Automation copies the uploaded resources, for example, a JDBC driver, to the following path, where *install_dir* is the directory on the server where the Domain Orchestrator was installed.

   install_dir`/server/c2o/.c2orepository/.c2oagentresources/lib/drivers/jars`
7. After mirroring completes, restart the agents where you need the uploaded jar files. The jar files are put in the classpath of the restarted agents.

   Note: See How to Start or Stop an Agent for details on restarting agents.

Upload User Resources

Uploading involves creating a folder under the User Resources folder and browsing to the resource to upload. CA Process Automation adds the resource to the User Resources tree structure and uploads the resource.

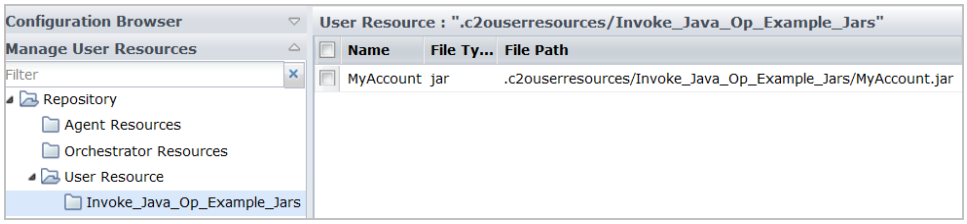
See the following procedures:

- Add a resource to User Resources (see page 332).
- Delete a resource from User Resources (see page 333).
- Modify a resource in User Resources (see page 334).

Note: To modify the resource path, delete the resource and add it again under a different path.

Resource for Running Invoke Java Operator Example

The installation process adds one resource to the User Resource folder under Repository in the Manage User Resources palette on the Configuration tab. The JAR file, MyAccount.jar, is located in the Invoke_Java_Op_Example_jars folder. You can use the MyAccount.jar file to run the Java example that is provided in the Required Main Method field of the Invoke Java operator.



Add a Resource to User Resources

Users with administrative-level permissions can add scripts to the User Resources folder in the global Repository. The product mirrors uploaded user resources at the configured interval to other Orchestrators and agents in the Domain. Orchestrators and agents can access user resources by reference.

Follow these steps:

1. Click the Configuration tab.
2. Click the Manage User Resources palette.
3. Expand the Repository folder, and then expand the User Resource folder.
4. Select the User Resource folder or a subfolder and click New.

5. Complete the fields on the Add New Resource pane as appropriate.
6. Verify your entries, and then click Save.

   The list in the User Resource pane displays the name, type, path, module, and description of the uploaded file.

The product copies the uploaded user resources to the following path:

install_dir/server/c2o/.c2orepository/.c2ouserresources/...

install_dir

Defines the directory on the server where the Domain Orchestrator was installed.

The product creates subfolders as necessary to maintain the path from the User Resources folder to the resource.

More information:

Load Catalyst Descriptors (see page 274)

Delete a Resource from User Resources

You can delete a resource, such as a script or jar file, that you added to the User Resources folder.

Follow these steps:

1. Click the Configuration tab.
2. Click the Manage User Resources palette.
3. Expand the Repository folder. Expand the User Resources folder.
4. Click the folder where the resource resides.
5. Select the row displaying the name of the resource to delete, and then click Delete.

Note: When you delete the last resource from a subfolder of User Resources, that subfolder is also deleted.

Modify a Resource in User Resources

You can modify a resource in the following ways:

- You can change text in any displayed field except Resource Path. This action is possible whether you select Replace File or not.
- You can upload an edited resource (such as a script or JAR file) that you previously added to User Resources. This action is possible only if you select Replace File.

Follow these steps:

1. Click the Configuration tab.
2. Click the Manage User Resources palette.
3. Expand the Repository folder, then expand the User Resources folder.
4. Click the folder in which the resource resides.
5. Right-click the row that displays the name of the resource to modify and select Edit.

   The Resource page opens.
6. (Optional) Modify the resource information. You can edit the following fields:
   - Resource Name
   - Module Name
   - Resource Description
7. Set the Replace File check box as follows:
   - If your *only* changes to the resource are updated fields on the Resource page, clear the Replace File check box and click Save.
   - If you updated your local copy of the Resource File and you want to upload your updates:
     a. Select Replace File.
     b. Click Browse.
     c. Navigate to the updated file and click Open.
     d. Click Save.

   The User Resources folder now contains the updated file. The Resources page includes text for any fields you modified.

Chapter 15: Audit User Actions

CA Process Automation provides audit trails to trace and record activity for configuration objects (Domain, Environments, Agents, and Orchestrators), and Library objects (folders and automation objects). A Domain administrator can view the audit trail for the Domain. An Environment configuration administrator can view the audit trail for an Environment. An end user with Environment user permission can view the audit trail for an object.

This section contains the following topics:

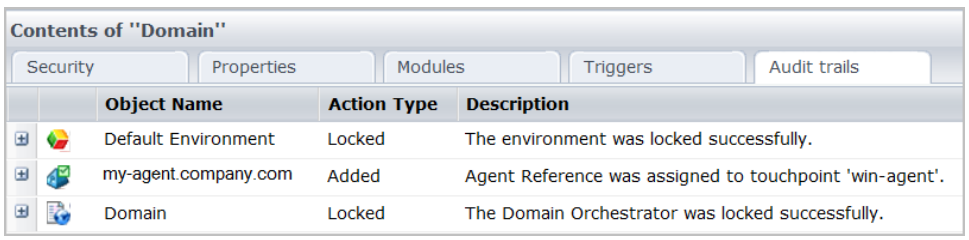
View the Audit Trail for the Domain

Administrators can view the Domain audit trail.

The Domain audit trail monitors the following actions:

- Domain is locked or unlocked.
- Domain property is changed.
- Domain Orchestrator is changed.
- Environment is created, deleted, locked, unlocked, or renamed.
- Orchestrator is added, deleted, or renamed.
- Agent is added, deleted, or renamed.
- Agent Reference was assigned to touchpoint 'touchpoint-name'.

The following example shows the audit trail for assigning a touchpoint to an agent. Two of the columns are hidden.



Follow these steps:

1. Select the Configuration tab.
2. On the Configuration Browser palette, select the Domain node.
3. In the Contents pane, click the Audit trails tab.

   The Audit Trails tab displays the following information for all records:

   - Object Name
   - Last Updated
   - Username
   - Action Type
   - Description
4. (Optional) To sort the audit trails by a specific column, select Sort Ascending or Sort Descending from the target column drop-down list.

   For example, to audit a specific user, select a sort option from the Username column drop-down list, and then scroll to the appropriate record.
5. (Optional) To change the number of records that the product displays on a page, select a value from the Rows On Each Page drop-down list.
6. Examine the records in the audit trail.

   If the audit records comprise multiple pages, use the toolbar navigation buttons to display the first page, previous page, next page, or last page.

View the Audit Trail for an Environment

With Configuration Administrator access rights, you can view the Environment audit trail.

The Environment audit trail monitors the following actions:

- Environment is locked or unlocked.Environment property is changed.
- Environment is created or deleted.
- Environment or object in the Environment is renamed.
- Touchpoint is added, deleted, or renamed.
- Touchpoint Group is added or deleted.
- Host Group is added or deleted.

Follow these steps:

1. Click the Configuration tab.
2. On the Configuration Browser palette, expand the Domain node and select the Environment to audit (for example, the Default Environment).
3. In the Contents pane, click the Audit trails tab.

   The Audit Trails tab displays the following information for all records:

   - Object Name
   - Last Updated
   - Username
   - Action Type
   - Description
4. (Optional) To sort the audit trails by a specific column, select Sort Ascending or Sort Descending from the target column drop-down list.

   For example, to audit a specific user, select a sort option from the Username column drop-down list, and then scroll to the appropriate record.
5. (Optional) To change the number of records that the product displays on a page, select a value from the Rows On Each Page drop-down list.
6. Examine the records in the audit trail.

   If the audit records comprise multiple pages, use the toolbar navigation buttons to display the first page, previous page, next page, or last page.

View the Audit Trail for an Orchestrator

With read permissions on a configuration object, you can view the associated audit trail. Viewing the audit trail for configuration objects requires access rights that include Environment User and View Configuration Browser.

The Orchestrator audit trail monitors the following actions:

- Orchestrator is locked or unlocked.
- Orchestrator property is changed.
- Orchestrator is quarantined or not quarantined.
- Orchestrator is mapped to a Touchpoint or is unmapped from a Touchpoint.
- Orchestrator is renamed.

Follow these steps:

1. Click the Configuration tab.
2. On the Configuration Browser palette, expand the Orchestrators node and select the target Orchestrator.
3. In the Contents pane, click the Audit trails tab.

   The Audit Trails tab displays the following information for all records:

   - Object Name
   - Last Updated
   - Username
   - Action Type
   - Description
4. (Optional) To sort the audit trails by a specific column, select Sort Ascending or Sort Descending from the target column drop-down list.

   For example, to audit a specific user, select a sort option from the Username column drop-down list, and then scroll to the appropriate record.
5. (Optional) To change the number of records that the product displays on a page, select a value from the Rows On Each Page drop-down list.
6. Examine the records in the audit trail.

   If the audit records comprise multiple pages, use the toolbar navigation buttons to display the first page, previous page, next page, or last page.

View the Audit Trail for an Agent

With read permissions on a configuration object, you can view the associated audit trail. Viewing the audit trail for configuration objects requires CA EEM access rights that include Environment User and View Configuration Browser.

The agent audit trail monitors the following actions:

- Operator category is enabled on the Modules tab and changing a configured value.
- Agent is quarantined or not quarantined.
- Agent is locked or unlocked.

Follow these steps:

1. Click the Configuration tab.
2. On the Configuration Browser palette, expand the Agents node and select the target agent.

3. In the Contents pane, click the Audit trails tab.

   The Audit Trails tab displays the following information for all records:

   - Object Name
   - Last Updated
   - Username
   - Action Type
   - Description

4. (Optional) To sort the audit trails by a specific column, select Sort Ascending or Sort Descending from the target column drop-down list.

   For example, to audit a specific user, select a sort option from the Username column drop-down list, and then scroll to the appropriate record.

5. (Optional) To change the number of records that the product displays on a page, select a value from the Rows On Each Page drop-down list.

6. Examine the records in the audit trail.

   If the audit records comprise multiple pages, use the toolbar navigation buttons to display the first page, previous page, next page, or last page.

View the Audit Trail for a Touchpoint, Touchpoint Group, or Host Group

With read permissions on a configuration object, you can view the associated audit trail. Viewing the audit trail for configuration objects requires access rights that include Environment User and View Configuration Browser.

The Touchpoint, Touchpoint Group, and Host Group audit trails monitor the following actions:

- Touchpoint is created
- Agent is assigned to Touchpoint
- Touchpoint group is created
- Touchpoint is added to a group
- Touchpoint group is renamed
- Host Group is created

Follow these steps:

1. Click the Configuration tab.
2. On the Configuration Browser palette, expand the Domain node. Then, expand the Environment node that contains the target touchpoint, touchpoint group, or host group.
3. Expand the appropriate node (All Touchpoints, All Touchpoint Groups, or All Host Groups), and select the target touchpoint, touchpoint group, or host group.
4. In the Contents pane, click the Audit trails tab.

   The Audit Trails tab displays the following information for all records:

   - Object Name
   - Last Updated
   - Username
   - Action Type
   - Description
5. (Optional) To sort the audit trails by a specific column, select Sort Ascending or Sort Descending from the target column drop-down list.

   For example, to audit a specific user, select a sort option from the Username column drop-down list, and then scroll to the appropriate record.
6. (Optional) To change the number of records that the product displays on a page, select a value from the Rows On Each Page drop-down list.
7. Examine the records in the audit trail.

   If the audit records comprise multiple pages, use the toolbar navigation buttons to display the first page, previous page, next page, or last page.

View the Audit Trail for a Library Folder

Administrators can view the audit trail for any selected folder in the Library. The product logs the following actions for folders in a Library:

- Created
- Renamed
- Deleted
- Create or delete an automation object
- Retrieve an automation object or folder from the Recycle Bin
- Change permissions on a folder, including links to the old and new ACLs

Follow these steps:

1. Click the Library tab and select an Orchestrator from the Orchestrator drop-down list.
2. Navigate to the folder that contains the folder to audit.
3. In the Contents pane, right-click the folder to audit, and then select Properties.
4. In the Properties pane, click the Audit Trails tab.

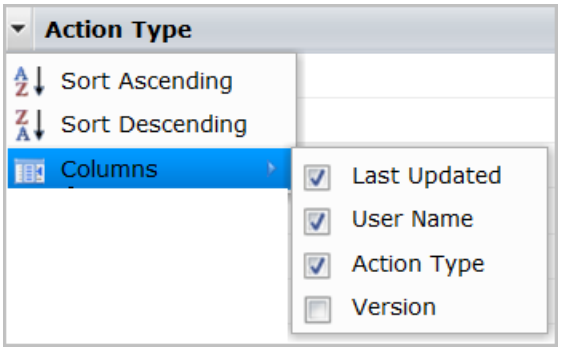
   The Audit Trails tab displays the following information for all records:

   - Last Updated
   - User Name
   - Action Type
5. (Optional) To sort the audit trails by a specific column, select Sort Ascending or Sort Descending from the target column drop-down list.
6. (Optional) Define which columns the product displays:

   a. Select Columns from the drop-down list from any column header.

   b. Clear (hide) or select (show) the column check boxes as appropriate.

   For example, to display the Version column, select the Version check box from the Columns menu.



7. Examine the records in the audit trail.

View the Audit Trail for an Open Automation Object

Administrators can view the audit trail for an open automation object. The product logs the following actions for automation objects:

- Create
- Delete
- Check in and check out
- Rename
- Export and import
- Change automation object permissions, including links to the old and new ACLs
- Retrieve an automation object from the Recycle Bin
- Change the designated current version
- Create or update the release version
- Add a release version property
- Update an automation object (for example, a schedule) without checking it out
- Make a custom Operator object available or unavailable
- Activate or deactivate a schedule

Follow these steps:

1. Click the Library tab and select an Orchestrator from the Orchestrator drop-down list.
2. Navigate to the folder that contains the automation object instance to audit.
3. In the Contents pane, right-click the target automation object instance, and then select Properties.
4. In the Properties pane, click the Audit Trail tab.

   The Audit Trail tab displays the following information for all records:

   - Last Updated
   - User Name
   - Action Type

   Note: The Version column is also available, but is not displayed by default. For more information, see Step 5.

5. (Optional) To sort the audit trails by a specific column, select Sort Ascending or Sort Descending from the target column drop-down list.

   For example, to audit a specific user, select a sort option from the User Name column drop-down list, and then scroll to the appropriate record.

6. (Optional) Define which columns the product displays:

   a. Select Columns from a column drop-down list.

   b. Clear (hide) or select (show) the column check boxes as appropriate.

   For example, to display the Version column, select the Version check box from the Columns menu.

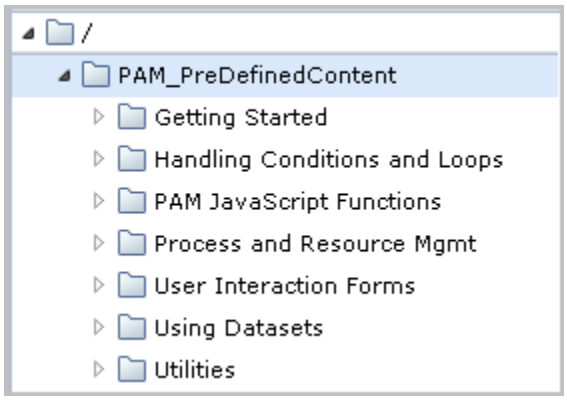
7. Examine the records in the audit trail.

Chapter 16: Administer Library Objects

This section contains the following topics:

Create and Manage Folders

The library of a newly installed CA Process Automation Domain Orchestrator contains no folders in the navigation panel of the Library tab. Installing the Out-of-the-Box Content from the Home page creates folders in the library for predefined content.



Typically, an administrator sets up the folder structure for content created by content designers. Designers save all automation objects in the Library folders. (By default, members of the Designers group can create folders.)

Note: For an upgraded CA Process Automation, all folders are migrated in their previous structure with their contents.

Set Up Folders for Design

You can use the following process to set up folders:

1. Plan the folder structure (see page 346).
2. Create folders (see page 347).
3. Grant folder access (see page 347).

Plan the Folder Structure

One of your first decisions as a new CA Process Automation administrator is how to organize and use folders in the Library tab. The folder structure can be as deep as you find practical.

To ease the task of preparing for export, set up a folder structure similar to this one before design work begins. That is, at the root level of the Library, create a folder for each process you plan to automate. Under each process-level folder, create a release-level folder using your own naming conventions for the first release version. If you create updates to a process, you can add new folders for the subsequent release versions.

```
/ (root folder)
Automated Process1
   Release Version 1
   Release Version 2
Automated Process 2
   Release Version 1
   Release Version 2
```

When you deploy the first release version of the first process you automate, you export the release version folder, which contains all of the objects contained in that release.

Consider the following approaches to creating a folder structure:

- Create the export structure from the start and use the release version folder as the working folder. Content designers then create, update, and test objects within the release version folder or one of its subfolders. Whatever folder structure is created here and exported is reproduced in the production environment upon import.
- Create working folders. Then, when the first release version of a process is ready for deployment, create the export folder and populate it with the objects that are part of the release version.
- Hybrid approach. Create the export structure and use the export folder for the upcoming release version as the working folder but keep objects that are shared across processes in a different root-level folder. For example, multiple processes can share named datasets and specific subprocesses. Calendars can be shared across schedules. Global schedules can be shared. Then, as part of preparation for export, copy the required objects from the shared objects folder to the export folder.

Note: If you export a folder with absolute paths, the complete folder structure of the export folder is replicated in the production environment when contents are imported.

Create Folders

You create a folder in the left pane of the Library tab. The left pane is the navigation pane for the library. A folder contains the content that content designers design from automation objects. All objects that support a specific automated process must be in the same folder or same folder structure for export. It is convenient to create a root-level folder for each project.

Within a process-level folder, you can create subfolders. At export time, the folder that you export as a content package cannot contain any unused or obsolete objects. The folder structure that you establish for a project in the design environment is replicated in the production environment upon import.

Follow these steps:

1. Decide on the level where you want the folder.

   You can create a folder under the root node or under an existing folder.

2. Right-click the parent node for the folder and select New Object, Folder.

   The folder path appears in the main pane with a field for the name. The default name is displayed as Folder.

3. Click the Name field, delete the default folder name and enter a name for this new folder.

How to Grant Folder Access

Administrators (members of the PAMAdmins group), have access to all folders and to the contents of all folders.

You can grant folder access to users who are not administrators in the following ways:

- Set folder ownership (see page 348).

  The individual who creates the folder (or the automation object) is the first owner. If you (as an administrator) create all of the folders, Set Owner is the easiest way to grant users who are not administrators folder access.

- Create a policy for each content designer (see page 348).

  You can grant specific folder access to content designers (members of PAMUsers or a custom group) that do not have Content Administrator rights.

Set Folder Ownership

Only a content administrator or the folder owner can change the ownership of a folder. By default, the creator of the folder owns the folder. The owner has unlimited permissions on the folder. As the content administrator, you can create a folder and then transfer the folder ownership to the appropriate user ID. For example, content designers could have their own folders, but the folder that is used to export a release version as a content package could be assigned to an administrator.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the appropriate *Orchestrator:environment*.
3. Select a folder.
4. Click Set Owner.
5. Enter the User ID of the user to set as the owner and click Search.

   Note: The search results include all users with a user ID or user name that contains the string you enter.
6. Select the user from the displayed list.
7. Click Save and Close.

Note: Ownership of a folder grants access to the folder, including the ability to export it individually or as a content package. With a CA EEM policy, you have more control over the actions that a content designer can take on a folder.

Create a Policy for Each Content Designer

Once your folder structure is in place and your content designers have user accounts, you can grant folder access to those designers. Folder access specifies the folder in which a user or application group can create and control automation objects. This procedure assumes that you are assigning a separate folder to each content designer and that these folders are directly under the root folder.

A custom policy based on Object lets you grant folder access to specified users or groups. Available access rights to folders include List, Read, Edit, Delete, and Admin. After you create the first policy, you can use that policy as a template for creating other policies.

Follow these steps:

1. Browse to CA EEM and log in (see page 45).
2. Click the Manage Access Policies tab.
3. Click New Access Policy  for Object.

   A New Access Policy appears where the Resource Class Name is Object.
4. Enter a name for this policy that provides folder access to a specific content designer.
5. Click the Search Identities link and click Search.
6. Select the name of the content developer and click the right arrow.

   The name appears in the Selected Identities list prefaced by [User].
7. Enter the path and name of the folder you created for this content designer in the Add resource field and click Add resource. 

   Your entry appears in the Resources list
8. Select each permission to grant to this content designer. For example, grant all actions except Object_Admin.
9. Click Save.

   The saved policy resembles the following:

Name/Description	ResourceClassName	Identities	Actions	Resources
Folder Access for Content Designer 1 Grants Content Designer 1 access to the /ContentDesigner1 folder.	Object	content designer 1	Object_List Object_Read Object_Edit Object_Delete	/ContentDesigner1

10. Test access.
    a. Log in to CA Process Automation with the credentials for this user.
    b. Verify that the only folder you can use is the one to which you granted access.
11. Create a policy for each additional content designer in one of the following ways:
    - Repeat steps 2-10.
    - Open the saved policy, click Save As, enter a new name and edit.

Note: To grant read access to all folders, create a policy with Object to which you add all content designers. Select Object_List and Object_Read for the root folder.

How to Manage Folders

To manage folders, use any combination of the following procedures:

- Back up all folders and their content (see page 356).
- Delete a folder (see page 357).
- Export a folder (see page 352).
- Import a folder (see page 353).
- Move a folder (see page 351).
- Search the folder structure (see page 350).
- Show the contents of a folder (see page 351).

Notes:

- See How to Prepare the Production Environment for a New Release (see page 359) for details about exporting a folder as a content package.
- See Use the Recycle Bin (see page 373) for details about purging and restoring deleted folders.

Search the Folder Structure

You can query for folders with a folder name that begins with the string or partial string you specify. The search field is at the top of the left pane in the Library.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the appropriate *Orchestrator:environment*.
3. Type the name or partial name for a folder or set of folders in the search field.
4. Examine the filtered list. Notice that the folder at the end of every path in the displayed list meets your search criteria.

Show the Contents of a Folder

Select a folder to display its contents.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the appropriate *Orchestrator:environment*.
3. Navigate the folder tree, expanding folders as needed. Or, enter search criteria in the search field to filter the displayed list to folders beginning with the name you entered.
4. When the target folder is displayed, select it.

   The folder contents are displayed in table format on the main pane.
5. (Optional) Display the data in the desired order. Click the header of the column on which you want to sort and select Ascending or Descending.

Move a Folder

You can move folders in an Orchestrator library.

Note: To move a folder from one Orchestrator library to another, export the folder (see page 352).

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the *Orchestrator:environment* with the library that contains the source folder.
3. Navigate the folder tree, expanding folders as needed.

   Note: Enter the partial folder name to display folders with names that begin with the string you entered.
4. When the target folder is displayed, select it and click Cut.
5. Navigate to the destination folder, then click Paste.

   One of the following results occurs:

   - If the destination folder name differs from the source folder name, the Orchestrator adds the source folder as a subfolder of the destination folder.
   - If the destination and source folders have the same name, the Orchestrator adds the source folder contents to the destination folder. That is, the Orchestrator merges the contents of the two folders.

Export a Folder

When you export one of the following items, the product creates an XML file that you can import:

- An object.
- A folder that contains multiple objects that are needed in the target Orchestrator. The objects can be unrelated to each other, perhaps for different processes. The Release Version value is not applicable.
- A folder that contains all objects that compose a release version of a process. Before export, you define a Release Version for the folder and each object in the folder.

  Note: For more information, see Scenario: Prepare a Folder for Export as a Content Package.

Content administrators and content designers can export a folder from the Library Browser to an export file on the local host. The export file preserves the path to the folder and the hierarchical structure of objects and subordinate folders.

Administrators can export a folder in the following ways:

Export, {Absolute Paths | Relative Paths}

The modifiable export lets the recipients in the target environment update the exported object versions in the folder.

Export as Content Package {Absolute Paths | Relative Paths}

The nonmodifiable export does not let the recipients in the target environment update the exported object versions or the Release Version label.

Note: You cannot export objects that reside in multiple folders as shortcuts in a package. Instead, create an export folder and then assemble all of the objects for export in that folder. For more information, see the *Content Designer Guide*.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator, and then select the appropriate *Orchestrator:environment*.
3. Navigate to the folder to export, right-click it, and then select one of the following options:
   - Export, Absolute Paths
   - Export, Relative Paths
4. To save the XML file, click Save on the File Download dialog.

   Note: The default file name is *folder-name*.xml.
5. On your local drive, navigate to the location at which to save the XML file.

6. Define the name with which to save the file.

   For example, append _RP to the file name to denote a relative path or _AP to denote an absolute path.

   *folder-name*_RP.xml

   *folder-name*_AP.xml

7. Click Save.

   The product exports the folder and its contents.

More information:

Scenario: Export and Import Objects in a Content Package (see page 361)
About Release Versions (see page 363)

Import a Folder

Content administrators can import the XML file that represents an exported folder and the objects it contains. If the folder was exported with the absolute path, the hierarchical structure of objects and subordinate folders is preserved in the export file. If the folder was exported with the relative path, the structure from the export folder is created in the import folder.

The import process is the same regardless of how the content was exported. The options that are applicable are based on the content contained in the export file.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the target *Orchestrator*:*environment*.
3. Navigate to the destination folder for the import.
4. Right-click the folder, then select Import.
5. Complete the following actions on the Import dialog:
   a. Click Browse and navigate to the location on your local drive where you saved the exported file.
   b. Select the exported XML file and click Open.

c. Select how to import an object that has the same name as an existing object in the same path, based on your knowledge of the objects existing in the import folder.

Import

Treat the imported version of the object as a new version of the existing object. Select this option if the purpose of this import is an upgrade and you want to keep the history of previous versions. If the imported object has the same release version, the existing release version is overridden with the release version of the imported object.

Overrides the release version of the imported object if a similar object exists with the same release version.

Do Not Import

Stop the import of the object and keep the existing object. If you select this option, the import process lists the objects with conflicting names. If there are conflicts, you can import again to an empty folder. Alternatively, you can rename the object in the source environment and then repeat the export and import. This option is a good choice when the objects being imported are new objects instead of new versions of existing objects.

Import and Replace

Delete the existing object and import the new version of the object as version 0.

d. Select whether to set the version of objects in the import folder to current. The current version of the process is the version that runs when the process starts. This version becomes active after the import. Other processes can also use the objects that this process uses. If the imported versions are already set to current, they are immediately available for use. For more information, see Determining Whether to Import as Current (see page 366).

e. Select whether to make Custom Operators available.

f. Select whether to publish the custom operator group to the Modules tab for the Domain.

Note: Do not publish a custom operator group unless the folder you are importing is from a different Domain.

6. Click Submit to start the import process.

7. Click OK on the verification of successful import message.
8. Review the imported folder and its contents in the currently displayed folder. Notice the following results:
   - If you exported the folder as a content package:
     - You cannot modify the Release Version attribute value for any object or for the content package.
     - You cannot modify the imported version of any object. Objects are baselined during the import.
   - If you selected to make custom operators available during the import, the imported custom operators are available for use.
   - If you published the custom operator group to the Modules tab, configure values for the custom operator group (see page 304).

More information:

Scenario: Export and Import Objects in a Content Package (see page 361)
About Release Versions (see page 363)

Back Up All Folders and Their Content

You can back up a library of folders and their content to protect against loss. Invoke an export at the root level of the folder structure. The export process creates an XML file with all of the information needed to recreate the library folders and their content upon import. The best security practice is to store this XML file off-site. If you ever lose your library, you can always reconstruct it by importing the XML file into the root directory of a new Orchestrator.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the appropriate *Orchestrator:environment*.
3. Right-click the root folder and select Export.
4. Determine whether to include the full path for the exported objects or the path relative to a folder containing the object.
5. Click Export and select one of the following path types:
   - Absolute Paths.
   - Relative Paths.

   On Windows hosts, the File Download dialog opens. You can select whether to open or save the file.
6. Select Save.

   On Windows hosts, the Save As dialog opens.
7. Specify the filename with which to save the XML file and the path. For example, librarybackup_*date*.xml
8. Click Save.

Delete a Folder

You can delete any folder that you no longer need.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the appropriate *Orchestrator:environment*.
3. Take one of the following actions:
   - Right-click the folder and select Delete.
   - Select the folder and click the Delete toolbar button.

   A confirmation message for the delete appears.
4. Click Yes.

   The folder is deleted.

   Note: The Recycle Bin contains both deleted automation objects and deleted folders. When an automation object is restored, the deleted folders in the original folder path are also restored.

How to Manage Automation Objects

Administrators use the library to manage automation objects within a folder structure. Maintenance tasks follow:

- Set a new owner for automation objects (see page 358).
- Add tags to use in object searches.
- Manage object versions.
- Delete automation objects from a folder structure.
- Move an object to another folder.
- Copy one or more object to an Orchestrator in the same environment.

  See Export a Single Object and Import a Single Object.

  See Export a Folder (see page 352) and Import a Folder (see page 353).
- Copy objects to another environment, for example, from a design environment to a production environment.

  See Export a Folder as a Content Package (see page 364) and Import a Content Package (see page 368).

More information:

Create and Manage Folders (see page 345)

Set a New Owner for Automation Objects

Only a content administrator or the owner of an automation object can change the ownership of an automation object. By default, the owner of an automation object is the login User ID of the individual who creates the object. The owner of an object has unlimited permissions on that object. As the owner of an automation object or content administrator, you can transfer the ownership to another CA Process Automation user. You can also set a new owner for multiple objects you own.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the appropriate *Orchestrator:environment*.
3. Select the folder containing the target automation objects.
4. Select one or more rows on the grid for the target objects.
5. Click Set Owner.
6. Specify the CA Process Automation user ID of the new owner.

How to Prepare the Production Environment for a New Release

Content designers prepare a folder for export as a content package.

Content administrators verify that the touchpoints set as targets for operators are mapped to the Orchestrator or agents in the production environment. If content administrators complete their verification before the import, then objects can be imported as current. If they do not complete verification until after the import, the objects are not imported as current.

The user that performs the export and import verifies that the process works as designed in the production environment. Then, production users can begin using the new release.

Transitioning consists of the following steps:

1. Export and import objects in a content package (see page 361).
2. Configure production targets for the new process.
3. Verify that the process works as designed (see page 372).
4. Hand off the new process to production users.

   Note: The hand-off occurs outside the CA Process Automation application.

About Exporting and Importing a Content Package

A content package is created from a folder that contains automation objects for a specific release. Typically, the folder contains the following objects:

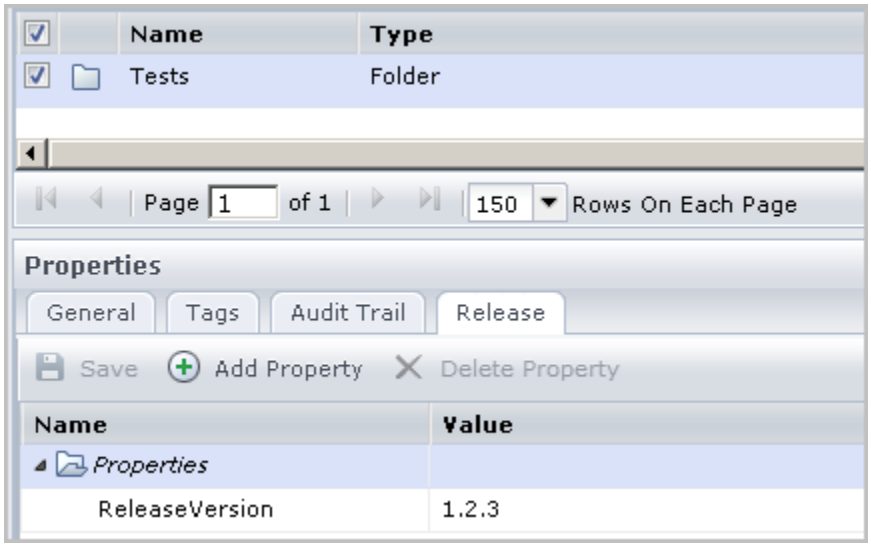
- A process, either the first release or a later release.
- All of the objects the process uses.
- All of the objects necessary for users to run the process.

Prior to export, you add a unique release version value to the the folder and to each object and verify that each object is baselined. Baselining provides you with a static version in the design environment of each object as it existed for this release.

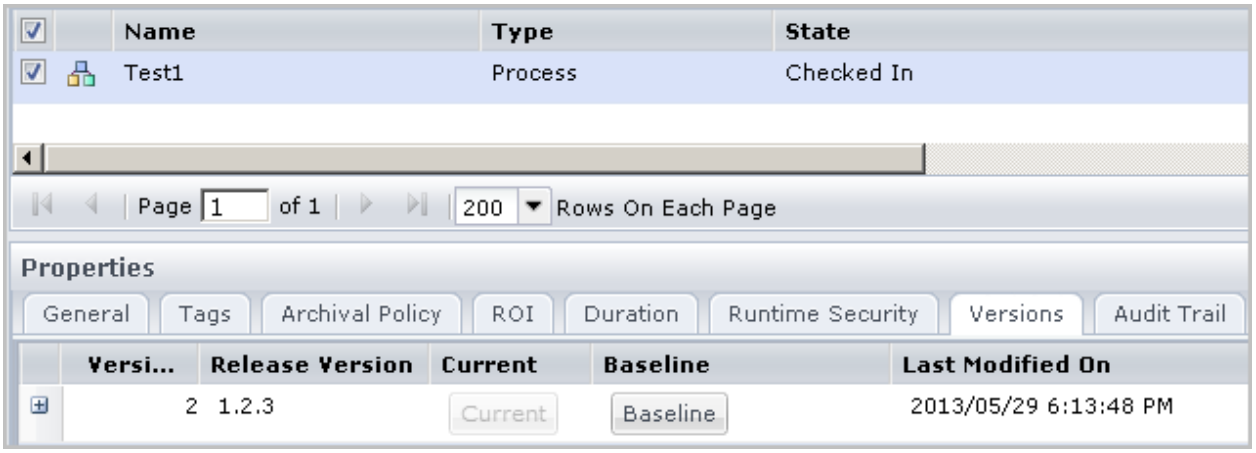
When you export a folder as a content package, CA Process Automation automatically baselines all objects in the content package at import. Content packages and the objects they contain are not modifiable in the new environment. (To make an object modifiable in the import environment, you save the baselined version as a new version.)

Example Release Versions

The following Release tab for a folder shows a ReleaseVersion property. In the example, the Value is 1.2.3.



The following example is for a Versions tab for a process, where the added Release Version value matches that added for the folder.

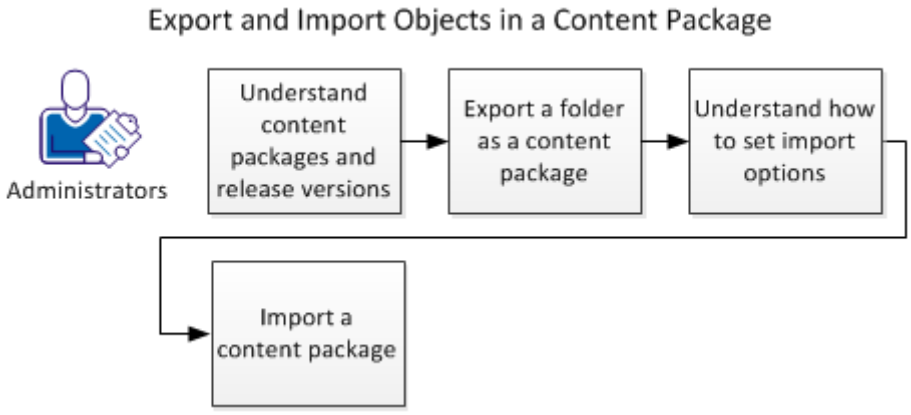


Notice that the Release Version is not Baselined; the Baseline button is enabled. When you notice an object targeted for release that is not baselined in the source environment, set the version that is be released as a baseline version.

Note: It is possible to export multiple processes at once in a folder as a content package and use the Release Version attribute to describe the folder contents.

Scenario: Export and Import Objects in a Content Package

Use a content package to export and import a set of related objects that compose a release version from one Orchestrator to another Orchestrator. In most cases, the source and target Orchestrators are in different environments. When you export a folder as a content package, the export process creates an XML file on your local drive. When you import into a different Orchestrator, you select this XML file from your local drive. The imported result is the content package.



Follow these steps:

1. Understand the purpose of content packages and release versions. See the following topics:
   - About Content Packages (see page 362)
   - About Release Versions (see page 363)
2. Export a Folder as a Content Package (see page 364).
3. Understand the impact of setting different import options. See the following topics:
   - Determining Whether to Import as Current (see page 366)
   - How to Set Import Options (see page 366)
4. Import a Content Package (see page 368).

More information:

Example: Export and Import a Content Package (see page 370)

About Content Packages

Objects can be exported in the following forms:

- A single object
- A folder
- A folder as a content package

Exporting a folder as a content package is different from exporting a folder in the following ways:

- The release version value of any object that is exported in a *folder as a content package* cannot be modified after import. (Objects that are exported in a *folder* do not require a release version value.)
- The release version value of an object that is exported in a folder as a content package cannot be modified after import.

Export a folder when there is no need for assigning a release version to its objects. For example, exporting objects from one design Orchestrator to another design Orchestrator in a folder.

Export a folder as a content package when exporting objects from a design environment to a production environment. Typically, the objects included in a content package represent a release of an automated process. In this case, there is a need to preserve the version of each object as it existed at the time of the release. The content package includes:

- The release version of the process object.
- All objects that the process uses.
- All objects that production users use to start or interact with the process.

A content package is a self-contained unit. A content package contains a folder of objects that are bundled together for export. Before the export, the version of each object being exported is tagged with a Release Version value. This same value is assigned as the Release Version of the folder.

The import process deploys all the objects in the content package to the Library. When imported as current, the object is available for use. Users in the import environment cannot create or change values for Release Version.

The import process for a content package baselines each object. The intent is for the release version of the objects to be used as is. However, it is possible to save an imported object as a new version, change the object, and save the changed object as the current version. In such a case, the baselined version with the Release Version value stays intact. This safeguards those objects from being altered in a potentially harmful way. To reverse any unwanted changes, make the baselined version the current version. The content designers who do troubleshooting can identify the nonmodifiable object versions that were imported to the production environment.

If you import an object from a third-party provider into a design environment that you want to change, make a copy of that object. Then, you can update the object copy and you can assign a different release version.

About Release Versions

Before you export a folder as a content package that contains a process and its component objects, the content designer takes the following actions:

- Sets the release version of each object(s)
- Sets the release version of the folder containing the object(s)

After import, objects have the same release version values you exported. When you export a folder as a content package, the imported content package is in nonmodifiable mode. The target users cannot modify the Release Version value that you set for this release. The Release Version value helps content designers, who work in the design environment, identify a specific version of an object in the production environment.

Note: CA Process Automation sets the Release Version attribute lock on both the object and the released version of the object. Therefore, users cannot modify the release version value for the imported object version or set release version values for new versions of the object.

Users cannot change nonmodifiable release version values after import. Consider the need for release versions based on what you are doing with the objects. For example:

- If you export from one *design* environment to another, (optionally) set Release Version attribute values and export the folder.
- If you export from a design environment to a *production environment*, then content designers are required to set Release Version attribute values for each object and the folder they are contained in. Designers then export that folder as a content package.

The following rules govern the export and import of Release Versions:

- If either of the following statements is true, Release Versions are nonmodifiable at import:
  - The objects are contained in a content package.
  - The object Release Version was nonmodifiable before export.
- CA Process Automation baselines imported versions when objects are imported as a content package (with nonmodifiable release versions).

  Note: If an object is imported again with the same release version, then that object is overwritten.

The following rules govern the copy and paste of imported objects:

- The first version of the object copy maintains the Release Version value and whether it is modifiable.
- If the current version of the original object is baselined and the object Release Version attribute is nonmodifiable, the object copy is also baselined.

Export a Folder as a Content Package

Content designers prepare objects associated with the same release version for export. Then a content designer or an administrator exports the content package. The following procedure addresses both the preparation and the export step.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the source *Orchestrator*:*environment*.
3. Navigate to the target folder. Verify that the folder contains all of the objects that you want to export. Verify that the folder contains only the objects that you want to export.
4. Add the release version to the target folder:
   a. In the navigation pane, select the folder containing the folder to export.
   b. In the main pane, right-click the folder to export and select Properties.
   c. Click the Release tab.
   d. Double-click the Value column in the ReleaseVersion row.
   e. Enter the release version in the Value dialog and click OK.
   f. Click Save.

5. Add the release version to the selected version of each object in the target folder and verify that the selected version is Baselined.
   a. Select the target folder containing the objects to export.
   b. Right-click an object and select Properties.
   c. Select the Release tab.
   d. Right-click the row for the version to export, select Set Release Version, and enter the same release version value that you assigned to the folder, and click OK.
   e. If the Baseline value for the selected row is No, click the Versions tab, and click Baseline. Click Yes to confirm Baselining.

      Note: It is important to Baseline objects before export so that you always have a saved image in the design environment of each object at release time. (All objects are automatically baselined during the import process.)
   f. Click OK.
   g. Repeat these steps for each object in the folder.
6. In the navigation pane, right-click the folder, then select one of the following options:
   - Export as Content Package, Absolute Paths

     Includes the full path for the selected folder.
   - Export as Content Package, Relative Paths

     Includes the path relative to the folder that contains the selected folder.
7. Save the file of the exported package.
   a. Click Save to save the XML file.
   b. Navigate to a folder on your local drive and click Save.
   c. When the Download Complete dialog appears, click Close.

   CA Process Automation exports the content package as an XML file. The content package is ready to import to another Orchestrator. The *folder-name*.xml file is encrypted.

Determining Whether to Import as Current

During an import, you specify whether to import objects as current. Import objects as current when both of the following statements are true:

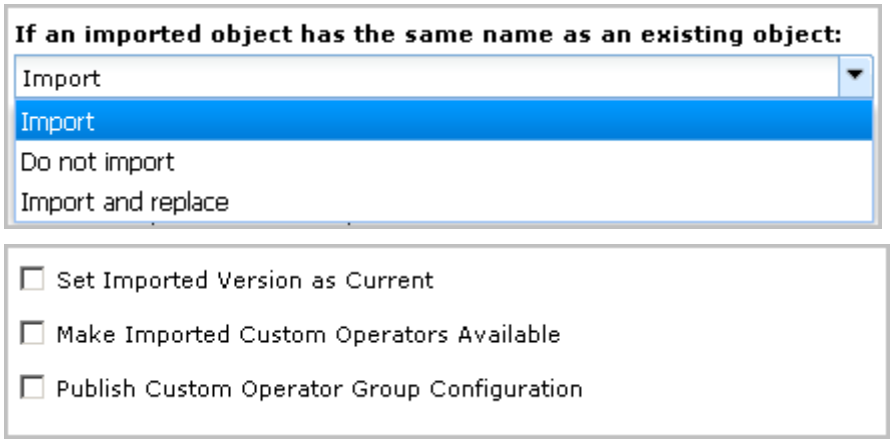
- All targets are defined as a touchpoint, a proxy touchpoint, or a touchpoint group.
- You configured production targets for the new process.

Note: You can import a process as current where the targets are expressions that point to variables in a dataset. When you import, you can modify the variables in the dataset to reference production touchpoints.

CA Process Automation requires you to wait until after import to map operator targets to production hosts only if you defined a target as an agent ID, IP address, or host name. In this case, do not import objects as current. Instead, update the targets in the operators after import, then mark the imported version as current.

How to Set Import Options

CA Process Automation provides you with some flexibility in how to import objects.



If your import includes custom operator, select Make Imported Custom Operators Available.

If the custom operators are new and they belong to a new custom group, take the action appropriate to your environment.

- Do not select Publish Custom Operator Group Configuration if the import environment is in the same Domain as the export environment. In this case, the custom operator group configuration is already published.
- Select Publish Custom Operator Group Configuration if the import environment is in a different Domain than the export environment

Consider the import content when you configure Set Imported Version as Current and select how to handle duplicate names.

- To activate the imported objects, with the ability to revert to a previous version of an imported object, if needed:
  - Select: Import
  - Select: Set Imported Version as Current

  Note: These options are best when you are importing an upgrade release version and all operator targets are set to hosts in the import environment. You can expect to be notified of duplicate names because objects of the last release are located in the destination folder.
- To import without activating the upgraded objects, where the previous version retains its current version status:
  - Select: Import
  - Clear: Set Imported Version as Current

  Note: These options are best when the import includes operators that target hosts that are not yet defined with their touchpoint name in the import environment. With this setting, you can make objects current after ensuring that the process targets are available in the import environment.
- To defer the import of any object with a duplicate name and to opt for making the objects current manually:
  - Select: Do not import
  - Clear: Set Imported Version as Current
  - **Note:** These options are best when you are importing new objects into a populated folder. These options avoid making an import object a new version of an object with the same name but a different function. These options also let you make the objects current after you test and verify their use in the new environment.

    If you receive alerts, consider these actions:
    - Record the duplicate names in the alert message and inform an administrator in the source environment. Perhaps those objects can be renamed and exported again.
    - Import again, but import to an empty folder.
- To activate the imported objects without the ability to revert the action for objects with duplicate names:
  - Select: Import and replace
  - Select: Set Imported Version as Current
  - **Note:** These options are best when you are reimporting fixes to objects in the destination folder. In this case, you would never need to revert to the replaced version.

Import a Content Package

Administrators select the Orchestrator, select the target folder, and then invoke the import. If the import result is a content package, it contains a set of baselined objects for the same release. You cannot modify the release version values of objects in an imported content package.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the target *Orchestrator:environment*.
3. Right-click the destination folder and select Import.
4. Click Browse and navigate to the location on your local drive where you saved the exported file. Select the exported XML file and click Open.
5. Select how to import an object that has the same name as an existing object in the same path.
   - Select Import to import each object as a new version of the existing object.

     This option is appropriate for an upgrade when you want to keep the history of previous versions.

     Note: If an existing object has the same release version as the imported object, the imported object replaces the duplicated version.
   - Select Do Not Import to stop the import of the object and keeps the existing object.

     If you select this option, the import process lists the objects with conflicting names. If there are conflicts, you can import again to an empty folder. Alternatively, you can rename the object in the source environment and then repeat the export and import. This option is a good choice when the objects being imported are new objects instead of new versions of existing objects.
   - Select Import and Replace to delete the existing object and import the new version of the object as version 0.
6. Select whether to set the version of objects in the import folder to current.
   - Select Set Imported Version as Current to activate the imported version immediately upon import. If the imported object is an upgrade, existing processes that used the previous version of objects now use the imported version. The imported objects can include a process with the operator targets configured in the import environment. In this case, you can verify the updated process without resetting versions.
   - Clear Set Imported Version as Current to defer the setting as current to a manual process. For example, clear this option if the import contains a process where the targets of its operators are not yet defined in this environment.

7. Select whether to make imported Custom Operators available.
   - Select Make Imported Custom Operators Available to automate the setting as available for all imported custom operators.
   - Clear Make Imported Custom Operators Available to retain an unavailable status for imported custom operators and make them available manually one by one.
8. Select whether to publish a custom operator group to the Modules tab.
   - Select Publish Custom Operator Group Configuration if the import includes new custom operators and a new custom operator group and you are importing to a different Domain than the export Domain.
   - Clear Publish Custom Operator Group Configuration in the following cases:
     - The import environment is in the same Domain as the export environment.
     - The imported custom operators are new releases of existing custom operators. In this case, the custom operator groups exist.
     - You prefer that an administrator publish any new custom operator group configurations manually.
9. Click Submit to start the import process.
10. Click OK on the verification of successful import message.

    The package successfully imports to the selected folder. The package also appears in the Content Packages palette in the Operations tab. When you select a content package from the palette, the properties display. The displayed property is the ReleaseVersion value that was set for the folder before it was exported as a Content Package.

Example: Export and Import a Content Package

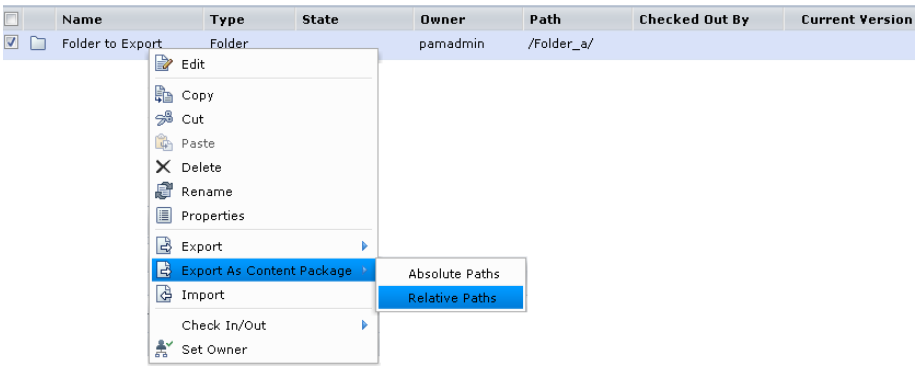
Export a folder as a content package from the Library in the source (design) environment and save the resulting XML file. Import a content package to the Library of the target (production) environment by browsing for the XML file and specifying import options.

Export as a Content Package

1. Click the Library tab for the *Orchestrator*:*environment* that contains the folder that contains the objects to transition.
2. Right-click the folder, then select Export As Content Package, Relative Paths.

   This selection copies the package to a folder other than root.

Equation 1: The right-click options for a folder include Export and also Export As Content Package. Both export options include a choice of Absolute Paths and Relative Paths.



3. Save the file to a folder on your local drive or on a mapped drive.
4. Click Open Folder. The folder in which you saved the XML file of the export opens when the download completes.

Import a Content Package

1. Click the Library tab and select the *Orchestrator*:*Environment* that is the target for the export and import process.
2. Navigate to the folder in which to import the XML file, right-click it, and select Import.

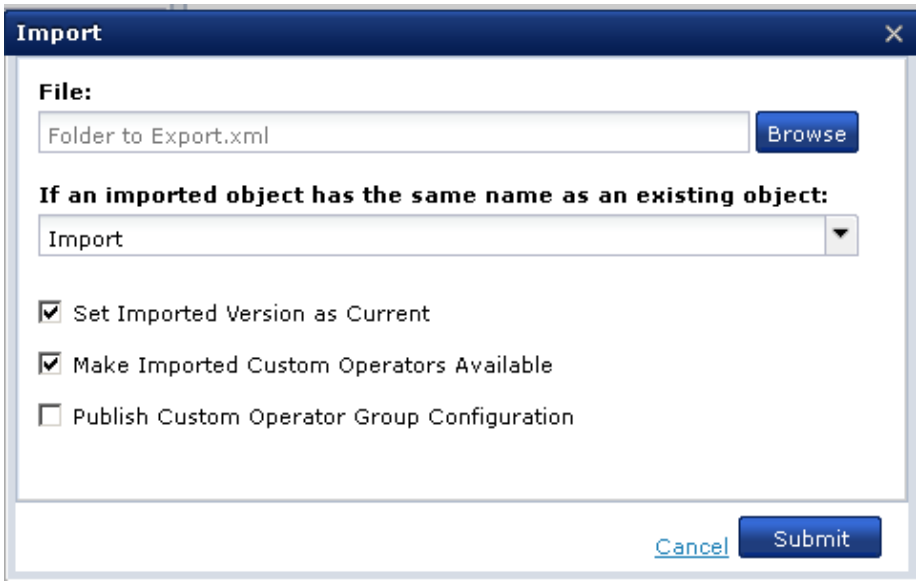
3. Click Browse, navigate to the location where you exported the file, and click Open.

   In this example, select the following options:

   - Import
   - Set Imported Version as Current
   - Make Imported Custom Operators Available

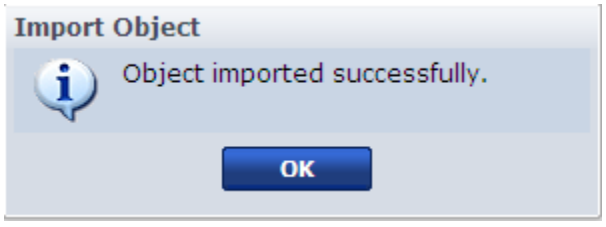
     Note: If you do not select this option, CA Process Automation imports custom operators as unavailable.

     Note: Do not select Publish Custom Operator Group Configuration when the import package contains one or more custom operators for which a new custom operator group was published to the Domain to which the import environment belongs. The published group already exists in the Modules tab in the Configuration Browser when exporting and importing between environments in the same Domain.



4. Click Submit.

5. Click OK on the confirmation message.



The imported content package appears in the import folder you selected. You can also find content packages under the Content Packages palette on the Operations tab. If you click the content package in the left-hand pane, its properties display in the right-hand pane.

6. From the import folder, select the imported content package and click Properties.
7. Click the Release tab.

   The content package Release Version data is the same as at export. If you point to the Release Version field, the tooltip indicates that you cannot modify the Release Version value.
8. Double-click the content package and notice the following:
   - All imported objects appear in the same destination folder.
   - All imported objects are baselined.
   - All imported objects have the release version text that was set for the object before export.

Verify that the Process Works as Designed

Before turning over the contents of an imported content package for production use, the administrator runs the process and monitors the results. A successful run implies that the import of the content package provided all required objects components and that all targets are correctly configured.

The verification step can include verifying that the automated start mechanism is working, whether a schedule, forms, or triggers. Activate triggers, if needed.

In its simplest form, the verification process can be summarized as follows.

Follow these steps:

1. Click the Library tab and select the **Orchestrator**:*environment* of the import target.
2. Click the Operations tab.
3. Start the process through the planned start mechanism.
4. Monitor the running process until it completes. Reply to any forms so that the process can continue.
5. If the process does not run successfully, return it to the content designer for troubleshooting.
6. If the process contains branches, create the cases to test the branches. Then, start the process and monitor it.
7. Take one of the following actions:
   - If the process does not run successfully, return it to the content designer for troubleshooting.
   - If the process runs successfully, hand it off to the production administrator.

8. If you identify any object that needs additional design work, use the following process:
   a. A content designer fixes the problem and tests it to verify that it works.
   b. Content designers prepare a new folder for export as a content package. This involves setting a new release version for the folder and all objects comprising the release. See Scenario: Prepare a Folder for Export as a Content Package.
   c. Re-export and re-import this folder as a content package. See Scenario: Export and Import Objects in a Content Package (see page 361).
   d. Re-verify that the automated process works as designed.

More information:

How to Prepare the Production Environment for a New Release (see page 359)

Use the Recycle Bin

The Recycle Bin contains folders and objects that you and other users have deleted from the library.

The *purge* action permanently deletes the selected objects or folders from the library.

The *restore* action restores the selected objects or folders. The restore includes any previously deleted folders in the path of restored objects.

For details, select the action you want to perform:

- Search the Recycle Bin (see page 374)
- Restore objects and folders (see page 375)
- Purge objects and folders (see page 376)

Search the Recycle Bin

You can query the Recycle Bin with a basic search or an advanced search. The basic search filters on the name when the entry is the whole name or a string that begins like certain names. The Advanced Search provides many search criteria.

Follow these steps:

1. Click the Library tab, contract the root folder, and select the Recycle Bin.

   All currently deleted automation objects and folders appear in the main pane.

2. Enter a string and an asterisk (*) in the search field and click Search to perform a basic search. For example, enter Custom* to limit the display to objects beginning with the string Custom.

   Folders and automation objects with names matching your entry appear in the filtered list.

3. Click Advanced Search to display attributes on which to search. You can enter one or more types of search criteria.

   - Keywords - Enter one or more keywords to find objects or folders that are assigned the specified keywords. If you specify more than one keyword, use the comma (,) as a delimiter.
     - To filter for objects that are tagged with any of the keywords you specify, select OR, the default.
     - To filter for objects that are tagged with all the keywords you specify, select AND.
   - Name - Name of the folder or automation object.
   - Owner - User ID of the object or folder owner. The default owner is the user who created the object. A new owner can be specified with Set Owner.
   - Type - Select an automation object type from the drop-down list.
   - State - Select a state from the drop-down list.
   - Modification Date - Use the calendars to select the date range during which the items you want displayed were modified.
   - Creation Date - Use the calendars to select the date range during which the items you want displayed were created.

4. Click Search.
5. Take the purge or restore action on the result set.
6. Click Reset to clear the search criteria if you want to do another search right away.

Restore Objects and Folders

When you delete an object or folder from the library, it moves to the Recycle Bin. From the Recycle Bin, you can restore an object or folder that you deleted. The restore process restores the object or folder and any other folders in the deleted path. You can specify whether to overwrite objects in the target path that have the same name as selected objects.

Follow these steps:

1. Click the Library tab, contract the root folder in the left pane, and select the Recycle Bin.

   The main grid refreshes to display all automation objects and folders that currently reside in the Recycle Bin.

2. Select one or more objects or folders and click Restore Selected.

3. Click Yes on the confirmation message for restoring.

   - If the target path contains no object with the same name as a selected object, the product restores the selected object to the target location.
   - If an object in the target path has the same name as an object selected for a restoration, a warning appears. Take one of the following actions:
     - Select the object and click OK to continue the restore process.

       The product moves the object from the Recycle Bin to the target path and overwrites the object that exists in the target path.
     - Click Cancel to stop the restore process for the object.

       The product does not overwrite the object in the target path. In this case, consider moving or renaming the object with the duplicate name and then retrying the restore process.

   The restore process restores the selected objects and, if necessary, their folder paths.

Purge Objects and Folders

The Recycle Bin is intended to be a temporary container for deleted objects, such that content designers can restore objects that they inadvertently delete.

Purging obsolete objects regularly results in a tidy Recycle Bin. As an administrator, you can purge selected automation objects and folders. Alternatively, you can purge the contents of the Recycle Bin in a single step. A purged object cannot be retrieved or restored.

Follow these steps:

1. Click the Library tab.
2. Click Orchestrator and select the appropriate *Orchestrator:environment*.
3. If the Recycle Bin is not visible, contract the root folder.
4. Click the Recycle Bin.

   All automation objects and folders that are deleted from the library appear in the main pane grid.
5. Take one of the following actions:
   - Select specific objects, and then click Purge selected.
   - Click Purge all.
6. If you initiated the purge for selected objects, a confirmation message appears.
   - Click No to cancel the purge, restore the required objects to the Library, restart the purge.
   - Click Yes to continue with the purge process.
7. If you initiated a purge all process where the contents of the recycle bin include checked out objects, a dialog appears that lists these objects. Evaluate the list and then take one of the following actions:
   - Click No to cancel the purge, restore the required objects to the Library, restart the purge.
   - Click Yes to continue with the purge process.

Appendix A: FIPS 140-2 Support

The Federal Information Processing Standard (FIPS) 140-2 publication, *Security Requirements for Cryptographic Modules,* defines a set of requirements for products that encrypt sensitive data. The standard provides four levels of security intended to cover a wide range of potential applications and environments. The Security Management and Assurance (SMA) division of NIST validates cryptographic modules and cryptographic algorithm implementations. When validated, SMA publishes the vendor and validation certificate numbers with modules names.

In support of FIPS 140-2, CA Process Automation uses validated cryptographic modules from the RSA BSAFE® Crypto-J libraries. RSA is the Security Division of EMC.

This section contains the following topics:

When CA Process Automation Uses Encryption

CA Process Automation encrypts communication and encrypts its data stores. CA Process Automation uses modules validated to FIPS 140-2 as needed for security.

For example:

- When transferring data between the Orchestrator and agents, the data is encrypted.
- When transferring data from the Orchestrator to the CA Process Automation Client, sensitive data is encrypted.
- When transferring data between CA EEM and CA Process Automation, the data is encrypted. (Release 03.1.00 and later).
- When transferring a System composed of automation objects using export and import, all Password objects in the System are encrypted.
- When any sensitive data, such as passwords, is stored in file systems, that data is encrypted.

Cryptographic Module Validated to FIPS 140-2

CA Process Automation uses an embedded cryptographic module validated to FIPS 140-2 with these specifications:

- Cert#: 1048
- Vendor: RSA, The Security Division of EMC
- Cryptographic Module: RSA BSAFE® Crypto-J JCE Provider Module (Software Version: 4.0)
- Module Type: Software
- Validation Dates: 10/27/2008; 01/26/2009; 09/07/2010
- Level/Description: Overall Level 1
- FIPS-approved algorithm: RSA (Cert. #311)

For details, use a search engine to find the *RSA BSAFE Crypto-J JCE Provider Module Security Policy*. This policy lists the platforms on which the algorithms are compliant, including platforms from Microsoft, Linux, Oracle (Solaris), HP, and IBM. This document also includes details on Crypto-J FIPS-approved algorithms.

In FIPS-only mode, CA EEM uses the following algorithms:

- SHA1, SHA256, SHA384—For managing client-server communication.
- SHA512—For storing user passwords.

  Note: CA EEM applies SHA512 to the password digest only if you update the password digest. Until you update, CA EEM accepts the existing password in the password digest.
- SHA256—For managing application certificates.
- TLS v1.0—For communication with external LDAP directories if the LDAP connection is over TLS.

User Authentication and Authorization in FIPS Mode

CA EEM can be configured to use FIPS mode. This is an option. When CA EEM is configured to use FIPS, CA Process Automation must be configured to use FIPS. This is achieved by selecting the Use FIPS-Compliant Certificate check box during installation of the Domain Orchestrator.

Whether FIPS mode is set to on or off, the data transferred between CA EEM and CA Process Automation is encrypted. The difference is in the algorithms used for encryption.

When users log in, CA Process Automation transfers the user name and password to CA EEM. CA EEM returns authentication data and authorization data to CA Process Automation.

- When FIPS mode is on:
  - Transferred data is encrypted with the SHA1 algorithm supported by FIPS.
  - A PAM.cer certificate is used.
- When FIPS mode is off:
  - Transferred data is encrypted with the MD5 algorithm.
  - A PAM.p12 certificate is used.

Appendix B: Maintaining the Domain

Maintaining the Domain involves some tasks that you perform outside of the Configuration tab.

This section contains the following topics:

Build Out the Domain

Building out a system includes both physical and logical changes. You build out your physical system through installation. You build out your logical system within CA Process Automation.

- If additional capacity is needed in the design environment, add a node to the Domain Orchestrator.
- If additional capacity is needed in the production environment, add a node to the Orchestrator used for production. Add a software or hardware load balancer.

  Note: See the *Installation Guide* for details.
- If a server on which an Orchestrator is installed is being taken out of service, export the root node of the library and import it into a new Orchestrator.
- When new users are needed or new roles are added, update CA EEM with changes to user accounts and policies.

Back up the Domain

Back up CA Process Automation with the backup tool that you use at your site.

Follow these steps:

1. Back up each occurrence of the following three CA Process Automation databases:
   - Repository
   - Runtime
   - Reporting
2. Back up the following folder:

   install_dir/server/c2o/.config
3. Back up the library contents by exporting the root folder in the Library tab.

Restore the Domain from Backups

CA Process Automation can fail due to data corruption, misconfiguration, or loss of storage on a clustered Domain Orchestrator. You can recover from such a failure and restore your data to CA Process Automation.

You can restore your use of CA Process Automation after a failure. The approach is to perform a fresh install of the Domain Orchestrator, which you shut down as soon as it is installed. You replace the empty databases with your database backups and restore your configuration file from a backup. Then you start CA Process Automation and verify that the restored data is in place.

Follow these steps:

1. Prepare for installation. Refer to the *Installation Guide* as you complete the following preparation:
   - Verify that the hardware, operating system, and database engine are installed.
   - Verify that the required third-party components are installed.
   - Install and configure CA EEM.
2. Perform a fresh install of CA Process Automation as described in the *Installation Guide*.
3. Add nodes as needed to reflect the original cluster. See the *Installation Guide* for details.
4. Stop CA Process Automation.
5. Restore your system from backups.
   a. Replace the repository database, runtime database, and reporting database with their respective database backups.
   b. Rename the current .config folder in:

      `install_dir/server/c2o/.config`

   c. Restore the following from the backup:

      `install_dir/server/c2o/.config`
6. Start CA Process Automation.
7. Verify that your configuration has been restored.
8. Verify that your database data is intact.

Maintain IP Addresses

The need to maintain IP addresses and or names can arise. Examples follow:

- Change IP address and name of an Orchestrator.

  Modify the name and IP address combination wherever they appear in the following files.

  install_dir/server/c2o/.config/OasisConfig.properties

  install_dir/server/c2o/.config/Domain.xml

  Note: To continue to use an unchanged host name in all references in CA Process Automation, modify the DNS with the new IP address.

- If you install agents using IP addresses that change, reconfigure the agent by updating the following file:

  install_dir/PAM Agent/PAMAgent/.config/OasisConfig.properties

  Change the value of the following property:

  oasis.jxta.host

- Use multiple IP addresses for CA Process Automation when you have two NICs, one internal, another external.

  To get CA Process Automation to bind at the external IP address, add the following property to OasisConfig.properties:

  jboss.bind.address=*xxx.xxx.xxx.xxx*

More information:

Oasis Configuration Properties File (see page 400)

Manage Certificates

Managing certificates involve the following procedures:

- Install the predefined CA Process Automation certificate (see page 386).
- Create and implement your own certificates for CA Process Automation (see page 388).
- Implement your third-party trusted SSL certificate for CA Process Automation (see page 394).

How CA Process Automation Protects Passwords

User account credentials, user name and password, are used to gain access to various systems and features. The password value must be protected for security reasons. Although passwords are strings, they are treated differently than other values of this data type. CA Process Automation protects passwords at the UI level in the following ways:

- Users cannot pass Passwords from place to place.
- Users cannot write a CA Process Automation process that says process.v = process.Password, because v is visible.
- Manipulations such as appending a password with the letter "t" and then later moving the "t" are disabled using JavaScript.
- Users cannot concatenate passwords with a + operator. No action that would reveal the Password value is permitted.
- Users cannot enable detection of password contents. For example, they cannot make what is hidden viewable.

In summary, CA Process Automation helps ensure password privacy as long as the password is within CA Process Automation. Passwords that are part of operator category configurations are protected. They cannot be modified or referenced or passed to external methods.

When a password that is not part of an operator category configuration is passed to an external method, it can be returned in clear text. Take precautions to protect passwords that are passed to external programs. The best solution is to use certificates or an alternative.

You can export the contents of definitions stored in a database and then import them to a database within the same domain or in a different domain. Importing datasets into another domain nulls out passwords since passwords are encrypted. This is by design; different domains use different encryption keys.

About the CA Process Automation Certificate

Research the differences between using a self-signed certificate and a Trusted SSL certificate in light of your security needs for CA Process Automation.

CA Process Automation provides a self-signed certificate that is preconfigured for use. You can manage the CA Process Automation certificate in any of the following ways:

- Use the certificate provided with CA Process Automation. Install this certificate from each browser from which you access the URL to the CA Process Automation Domain Orchestrator.
- Create your own self-signed certificate with a provided utility, encrypt the password with a provided utility, update the properties file with the keystore location, encrypted password, and keystore alias.
- Obtain a certificate from a recognized Certificate Authority. Update the properties file with the keystore location, encrypted password, and keystore alias.

Important! Do not remove the default keystore or the self-signed certificate provided with CA Process Automation. This certificate is required even when you configure CA Process Automation to use your own self-signed certificate or one you obtain from a CA.

Install the Predefined CA Process Automation Certificate

If you access CA Process Automation with a URL that uses the HTTPS protocol, the browser checks for a certificate issued by a Certificate Authority (CA). If you are using the CA Technologies self-signed certificate when you launch the CA Process Automation, the browser displays a warning that the certificate is not trusted.

To install the predefined certificate for CA Process Automation

1. Open a browser, enter the URL for the CA Process Automation, and log in.
2. If a Security Alert appears, click View Certificate.
3. Click Install Certificate and click OK.
4. Finish the wizard.

   The next time you log in, no Security Alert is presented.

About Creating a Self-Signed Certificate

You can replace the self-signed certificate that comes with CA Process Automation. The predefined certificate is configured in the OasisConfig.properties file. When you create your own self-signed certificate, update this properties file and run a batch file to sign the Jar files (or Java ARchive).

Before you create your own certificate, plan values for the keystore path and keystore alias. You enter these values when you run the keytool and when you update the properties file.

You use the following files and utilities to implement your own self-signed certificates:

- keytool utility

  Note: For details about this Java Sun utility, browse for keytool - Key and Certificate Management Tool.

- PasswordEncryption.bat
- SignC2OJars.bat
- OasisConfig.properties file, specifically, the following three parameters
  - itpam.web.keystorepath=

    Default:

    install_dir/server/c2o/.config/c2okeystore

    Note: The default is the self-signed keystore path,
  - itpam.web.keystore.password=

    The default points to encrypted DomainID. (Run the PasswordEncryption.bat file, enter the keystore password. The batch program generates the encrypted password on the console, which you specify here as the new value.)
  - itpam.web.keystorealias=

    Default: ITPAM

More information:

Oasis Configuration Properties File (see page 400)

Create and Implement Your Own Self-Signed Certificate

You can create your own self-signed certificate to replace the self-signed certificate that comes with CA Process Automation.

Follow these steps:

1. Using administrator credentials, log on to host where the target Orchestrator is installed.
2. Stop the Orchestrator (see page 186).
3. If you plan to reuse the current alias name for the keystore, remove this alias before continuing.
4. Run the following command to generate a keystore with the Java tool, keytool. Specify your own values for aliasname and for keystore_name. The default value for aliasname is ITPAM. If you do not enter a path for keystore, the current path is used.

   ```
   keytool -genkey -alias "aliasname" -keyalg RSA -keystore
   "keystore_path.keystore"
   ```

   For example, accept the default keystore path and enter:

   ```
   keytool -genkey -alias "PAM" -keyalg RSA
   ```

   Prompts to enter and confirm a keystore password appear.
5. Enter the same keystore password in response to both prompts. (Remember this password for later entry into an encryption utility.)

   A series of prompts appear followed by a confirmation prompt.
6. Respond to prompts with the requested distinguished name information as follows:
   a. Enter your first and last name.
   b. Enter the name of your organizational unit.
   c. Enter your organization name.
   d. Enter the name of your city or locality.
   e. Enter the name of your state or province.
   f. Enter the two-letter country code for your organizational unit.

   A confirmation of your entries appears in the format, Is CN=value, OU=value, O=value, L=value, ST=value, C=value correct?

7. Review the entries and if correct, enter yes. (If incorrect, enter no and respond to the prompts again.)
8. Respond to the prompt for the key password for *aliasname* in one of the following ways. The recommended option lets you avoid entering the certificate password as each jar is signed in Step 13.
   - Enter a unique key password for *aliasname*.
   - (Recommended) Press Enter to use the keystore password as the alias password.

   A new keystore is created in the current directory.
9. (Optional) Move this keystore to another path.
10. Encrypt the keystore password you entered in Step 5.
    a. Change directories to the *install_dir*/server/c2o directory.
    b. Run PasswordEncryption.bat.
    c. Enter the keystore password in response to the prompt.

    The utility encrypts the entered keystore password and saves the results on the console.
11. Back up the OasisConfig.properties file. (*install_dir*/server/c2o/.config/OasisConfig.properties)
12. Update the OasisConfiguration properties file as follows:
    a. For itpam.web.keystorepath=, enter the absolute path to the keystore, using "/" rather than "\", for example, C:/*keystore_path*/keystore.
    b. For itpam.web.keystore.password=, copy and paste the encrypted keystore password generated in Step 9.
    c. For itpam.web.keystore.alias=, enter the alias name specified in the keytool command in Step 4.
13. Execute SignC2OJars.bat to sign the Jars.

    This step is required after updating the certificate or keystore.
14. Start the Orchestrator (see page 187).

More information:

Oasis Configuration Properties File (see page 400)

About Using a Certificate Issued by a Third-Party Certificate Authority

CA Process Automation supports third-party security certificates for HTTPS web access and signing of jars. Use your own resources to obtain a trusted SSL certificate from the Certificate Authority of your choice. This procedure is beyond to scope of this guide.

The use of third-party security certificates requires the use of third-party tools. The set-up process also requires manual changes to the OasisConfig properties file (*install_dir*/server/c2o/.config/OasisConfig.properties). Before you begin, become familiar with the basic concepts of security certificates and keystores and the keytool utility provided with the Java JDK.

Implementing third-party security certificates requires updating values for three parameters in the OasisConfig properties file:

- "itpam.web.keystorepath"

  The default value is the keystore path for the self-signed certificate:

  install_dir`/server/c2o/.config/c2okeystore`

- "itpam.web.keystore.password"

  The default value is the encrypted "DOMAINID".

- "itpam.web.keystorealias"

  The default value is ITPAM.

  Note: A keystore can have more than one alias. To use a keystore alias that duplicates an existing alias, remove the existing alias before adding a new instance.

More information:

Oasis Configuration Properties File (see page 400)

Configure JBoss Web Server for custom SSL certificates prohibiting jar signing

Some third-party Certificate Authorities provide a trusted SSL certificate that is exclusive to the CA Process Automation JBoss Web Server but does not allow for jar signing. This restriction on jar signing produces an error in the customer environment.

Configuring the JBoss Web Server through the following procedure allows you to:

- Avoid a new certificate request
- Use the certificate while using an auto-generated, self-signed keystore for signing jars

Important! Repeat this procedure after a major upgrade, such as applying service packs or a version upgrade. This server configuration is preserved through a patch or a Hotfix installation.

Note: Skip steps 1-4 to generate a PKCS keystore if you already have the keystore. Ensure that your PKCS keystore has a private key and corresponding certificate that can be imported into a JKS keystore for use with CA Process Automation.

Follow these steps:

1. Use openssl to create a private key.

   openssl genrsa -out automation.key 2048

2. Create a CSR.

   The information that you enter through the command line is incorporated into your certificate request. Collectively, the identification fields you populate are referred to as Distinguished Name (DN) fields. Some fields contain a default value and others are left blank. To leave a field blank, enter '.'.

   openssl req -new -key automation.key -out automation.csr

   Country Name (2 letter code) [GB]:

   State or Province Name (full name) [Berkshire]:

   Locality Name (eg, city) [Newbury]:

   Organization Name (eg, company) [My Company Ltd]:

   Organizational Unit Name (eg, section) []:

   Common Name (eg, your name or your server's hostname) []:

   Email Address []:

   Please enter the following 'extra' attributes

   to be sent with your certificate request

   A challenge password []:

   An optional company name []:

Note: Do not enter a challenge password or an optional company name. Press Enter to keep them empty. The Common Name is the fully qualified domain name of the ITPAM server. If a load balancer is used, the Common Name is the fully qualified domain name of the load balancer.

3. Send automation.csr to your Certificate Authority and save the resulting server certificate, such as automation.cer.
4. To create a PKCS keystore, use the server private key and the public certificate.

   openssl pkcs12 -export -in automation.cer -inkey automation.key -out automation.p12 -name automation

   Note: The -name switch is used in step 5 for importing into jks keystore using the -srcalias switch. The password is required to create JKS keystore to be used with CA Process Automation as well.
5. Use keytool from the JDK bin directory to import the PKCS keystore to the JKS keystore.

   Keytool -importkeystore -srckeystore automation.p12 -destkeystore automation.jks -srcstoretype pkcs12 -srcalias automation -destalias automation

   Note: Optionally, enter the following command to list the contents to view the alias of your pkcs12 certificate. This parameter is required for -srcalias.

   keytool -v -list -storetype pkcs12 -keystore automation.p12

   To list the contents of JKS keystore:

   keytool -v -list -keystore automation.jks

   Important! Ensure that the source and destination passwords are the same. Use the same password for the new JKS keystore as was used to create PKCS keystore from step 4.
6. Stop the CA Process Automation Orchestrator. Stop all nodes if in a clustered environment.
7. Backup current server\c2o\deploy\jbossweb.sar\server.xml file outside of the CA Process Automation installation directory.

   Important! Do not make a backup copy in the same folder. Instead, copy and paste server.xml in a temporary backup directory.
8. Edit the Connector element to use non-default properties. The following example has the word custom added to out-of-the-box properties.

```
   <Connector
protocol="org.apache.coyote.http11.Http11Protocol"
SSLEnabled="true"
     port="${tomcat.secure.port}"
address="${jboss.bind.address}"
     maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
     emptySessionPath="true"
```

```
scheme="https" secure="true" clientAuth="false"
keystoreFile="${itpam.custom.web.keystorepath}"
keyAlias="${itpam.custom.web.keystorealias}"
keystorePass="${itpam.custom.web.keystore.password}"
sslProtocol = "${SSL_PROTOCOL}" algorithm =
"${X509_ALGORITHM}" ciphers="${jboss.ssl.ciphers}"
useBodyEncodingForURI="true" maxPostSize="12582912"/>
```

9. Encrypt the password that is used for automation.jks using PasswordEncryption utility in server\c2o folder. For example, in Windows create a new file with encrypted password by running the following command:

   PasswordEncryption.bat passwordUsedForJKSKeystore > automation-pass.txt

   Note: If necessary, return the utility to the command prompt by pressing Enter.

10. Copy automation.jks to the <pam_dir>/server/c2o/.config/ folder.

11. Back up current server\c2o\.config\OasisConfig.properties file and add the following parameters. These parameters are based on server.xml parameters from step 8.

```
itpam.web.keystorepath=<pam_dir>/server/c2o/.config/c2okeystore

itpam.custom.web.keystorepath=<pam_dir>/server/c2o/.config/auto
mation.jks
itpam.web.keystore.password=<leave_default>

itpam.custom.keystore.password=<encrypted_password_from_step_9>
itpam.web.keystorealias=ITPAM
itpam.custom.web.keystorealias=automation
```

12. Start the PAM Orchestrator.

13. Repeat this procedure for any other nodes of the cluster.

Implement Your Third-Party Trusted SSL Certificate

CA Process Automation supports third-party security certificates for HTTPS web access and signing of jars. You can obtain such certificates from a third-party Certificate Authority.

Follow these steps:

1. Decide on a certificate password and obtain a security certificate from a Certification Authority.
2. Using the instructions provided by the Certification Authority, import the certificate into a keystore.

   Generally you use a command similar to keytool –import –alias *myalias* –file certfile –keystore "path_and_file_specification_for_keystore".
3. For the keystore password, enter the certificate password provided by the Certificate Authority.
4. Obtain an encrypted version of the keystore password.
   a. Navigate to *install_dir*/server/c2o.
   b. Locate the PasswordEncryption script (PasswordEncryption.bat for Windows, PasswordEncryption.sh for UNIX or Linux).
   c. Run PasswordEncryption passwordtoencrypt.
   d. Save the long encrypted value returned for entry in the properties file.
5. Stop the Orchestrator (see page 186).
6. Back up and edit the Oasis Configuration properties file to add or update the following:
   a. itpam.web.keystorepath to the location of the keystore using the fully qualified path and file name for the keystore file.
   b. itpam.web.keystore.password with the encrypted keystore password (do not surround encrypted password value with quotes)
   c. itpam.web.keystorealias to the alias used to reference the certificate in the keystore (myalias in the examples).
7. Sign the jars by running SignC2OJars (SignC2OJars.bat for Windows, SignC2OJars.sh for UNIX or Linux) included with CA Process Automation in *install_dir*/server/c2o. Run SignC2oJars without parameters to sign the jars. If the keystore password you entered does not match the certificate password, enter the certificate password as each jar is signed.

   Note: On AIX, there is a known problem when re-signing a jar file using SignC2OJars. To work around this problem, manually "unsign" the jars by removing the *.SF and *.RSA files in the META-INF folder for each Java Archive before running SignC2OJars.

8. If the keystore contains more than one alias, modify the connector entry in server.xml. The server.xm. is located in <install_dir>\server\c2o\deploy\jbossweb-tomcat55.sar\server.xml. Add the line in bold:

```
<Connector port="${tomcat.secure.port}"
address="${jboss.bind.address}"
    maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
    emptySessionPath="true"
    scheme="https" secure="true" clientAuth="false"
    keystoreFile="${itpam.web.keystorepath}"
    keyAlias="${itpam.web.keystorealias}"
    keystorePass="${itpam.web.keystore.password}" sslProtocol =
    "${SSL_PROTOCOL}" algorithm = "${X509_ALGORITHM}"
    useBodyEncodingForURI="true"/>
```

9. Start the Orchestrator (see page 187).
10. Repeat this procedure for each Orchestrator that is to use the new certificate.

More information:

Oasis Configuration Properties File (see page 400)

Maintain the DNS Host Name

You can modify the host name for an Orchestrator. For example, if the host name does not conform to the supported syntax, you can update it. If you installed CA Process Automation using an invalid DNS host name containing restricted characters such as underscores, create an alias that conforms to DNS standards. Then, manually replace the invalid host name with this alias in your OasisConfig.properties file.

Follow these steps:

1. Create an alias. See Enable DNS to resolve an invalid host name.
2. Log in as an administrator to the server where the Domain Orchestrator is installed.
3. Navigate to the following folder, where install_dir refers to the path where the Domain Orchestrator is installed:

   install_dir`/server/c2o/.config`
4. Open the OasisConfig.properties file with an editor.
5. Use Find to locate the following property:

   `oasis.local.hostname`
6. Change the value for the property oasis.local.hostname=.
7. Save the file and exit.
8. Restart the Orchestrator service.
   a. Stop the Orchestrator (see page 186).
   b. Start the Orchestrator (see page 187).

More information:

Oasis Configuration Properties File (see page 400)

Syntax for DNS Host Names

There are many places where you can enter a FQDN or an IP address. If your DNS host names include an underscore or in any way do not conform to the required syntax, specify the IP address.

Valid DNS host names:

- Begin with an alpha character.
- End with an alphanumeric character.
- Contain 2-24 alphanumeric characters.
- Can contain the special character (-) minus sign.

  Important! The minus sign (-) is the only valid special character permitted in DNS host names.

Disable the Catalyst Process Automation Services

The Catalyst Process Automation Services is enabled by default. You can disable it by changing a property value in the OasisConfig.properties file.

Follow these steps:

1. Log in as an administrator to the server where the Domain Orchestrator is installed.
2. Stop the Orchestrator (see page 186).
3. Navigate to the following folder:

   install_dir/server/c2o/.config
4. Open the OasisConfig.properties file.
5. Scroll to the UCF embedded connector in the jboss-service.xml section of the OasisConfig.properties file.
6. Change the ucf.connector.enabled value to false. For example:

   ```
   ucf.connector.enabled=false
   ```
7. Save the file and exit.
8. Start the Orchestrator (see page 187).

More information:

Oasis Configuration Properties File (see page 400)

Appendix C: OasisConfig.Properties Reference

This section contains the following topic:

The OasisConfig.properties text file controls CA Process Automation. The selections that the installer makes when installing the Domain Orchestrator, its prerequisites, and its objects are stored as parameter values in the OasisConfig.properties file.

Important! Restrict the updating of OasisConfig.properties to a trusted administrator.

This guide includes the following topics on updating the OasisConfig.properties file:

- Control Caches of CA EEM Updates (see page 76).
- Change the SNMP Traps Listener Port (see page 325).
- Configure Domain Properties (see page 140).
- Control the Timeout for CA Process Automation (see page 20).
- Create and Implement Your Own Certificate for CA Process Automation (see page 388).
- Disable the Catalyst Process Automation Services (see page 397).
- Implement Your Third-Party Trusted SSL Certificate for CA Process Automation (see page 394).
- Maintain the DNS Host Name (see page 396).
- Maintain IP Addresses (see page 384).
- Set Maximum Number of CA EEM Users and Groups (see page 61).

The *Installation Guide* includes the following topics on updating the OasisConfig.properties file:

- Enable Logout in CA Process Automation for SSO
- Enable NTLM Pass-Through Authentication After Installation
- Generate SSL Certificate Files
- Maintain the DNS Host Name
- Port Planning Prerequisites
- Resolve Port Conflict for an Agent

The *Content Designer Reference* includes the following topic on updating the OasisConfig.properties file:

- Operator Ports

The *Web Services Reference* includes the following topics on updating the OasisConfig.properties file:

- Communications
- executePendingInteraction

Oasis Configuration Properties File

The Oasis Configuration properties file (OasisConfig.properties) contains the property settings for all aspects of CA Process Automation. The file is located in the *install_dir*/server/c2o/.config folder. All users with access to the CA Process Automation installation location can modify the files. Consider restricting access to this location. Some values must *not* be edited.

Settings include:

USE_DEPRECATED_COMMS_V1

(For agents only) Determines during the start of an agent whether it uses the new mode of communication or deprecated mode of communication. This is a boolean value.

When the Use Deprecated Communications check box in an agent's properties is selected, this value is set to true. CA Process Automation:

- Terminates the web socket connection from the agent, then passes that information to all of the Orchestrators before termination.
- Cleans the server map where these connection details are stored.

When the Use Deprecated Communications check box in an agent's properties is not selected, this value is set to false.

- The agent creates a new web socket connection and sends connection details for the Orchestrator.
- The Orchestrator saves these connection details in a server map.

See About Agent Communication (see page 219) for more information.

DOMAINID

Defines the unique ID for the Domain.

Example

```
ac04f945-f08b-4308-aa9c-c3fd95964f4d
```

CLUSTERNODEID

Determines a node uniquely in a cluster.

Example

```
8d11558a-3bf7-43d9-b394-4c055229e9ae
```

KEYSTOREID

Defines the password of the keystore.

Example

```
ac04f945-f08b-4308-aa9c-c3fd95964f4d
```

itpam.web.keystorepath

Defines the path of the keystore that is used for signing jars.

Example

```
C:/Program
Files/CA/PAMcert_Java7_Node2/server/c2o/.config/c2okeystore
```

itpam.web.keystore.password

Defines the password of the keystore that is used for signing jars.

Example

```
LQotQj55Y8dPGRRXkrF4yTyk/IwzTcT0rLY+pWeGrGHaRKnlcXHL3fr7pYI
zjVhoGdrnRxSO4Prl70rIxqs3fCGIgFVIAnOzICQ9ct4qXIBIPnxQcgflrF
0WDdaIjCS6ubKwe9Wxhn0xjnmctvkLnMC1L74b48yQd9yhWSMAgpLAPLPJi
Mz/VoIzcFVylqLS44KdM+wH6b6xkqVJECSH1GolBG2QUj/2
```

itpam.web.keystorealias

Defines the alias name of the certificate in the keystore that is used for signing jars.

Example

```
ITPAM
```

CERTPASSWORD

Defines the password that is used to control access to the keystore that is used to encrypt passwords and other critical data.

Example

```
XNASLujiOdl6POYm8CwjBTHnFUlbXQLcPqd+xc7oJkPF5X3cq8UHbEYL4iH
+01b1EmwHhw9uPXqDABcJqIJ+ECmODDAMn7rytSWqli+oxKp+e5scp1fnHj
F1ENCKZNasYy6nF6vPozT9qLmB7DhzuFAvg8Av9J/U4ngYrZ5AMdU1sFP5D
df3nw==
```

oasis.database.username

Defines the user name for the Library database server.

Example

```
sa
```

oasis.database.password

Defines the password that is associated with the specified library database server user.

Example

```
SSb28pTxSL4fxuv+8IV8zLz+S6jwleU4mpQTDTM1xmwQ037qmAjDO74Y569
W3LIP0vBUEkJ30raf3/RsodMLdL3L51cnz8Gus4mJfGJla7WdTtzx0ts0Bu
UFPxZ1pOpHOUUljFHn73243Iv7/pXIQe+O8lrHB00XotDicrleXavs+8sXS
IPqKyX3gmjy6LUZ
```

oasis.database.dbhostname

Defines the host name of the library database server.

Example

```
lodivsa205
```

oasis.database.dbport

Defines the Library database server connection port number.

Example

```
1433
```

oasis.database.connectionurl

Defines the Library database JDBC connection URL.

Example

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

oasis.database.databasetype

Defines the type of library database.

Example

```
MSSQLServer2005
```

oasis.database.dialect

Defines the user-defined dialect class of the library database.

Example

```
com.optinuity.c2o.persistence.MSQLServerDialect
```

oasis.database.genericdialect

Defines the dialect class of the library database.

Example

```
org.hibernate.dialect.SQLServerDialect
```

oasis.database.driver

Defines the fully qualified name of the JDBC driver class.

Example

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

oasis.database.typemapping

Defines the type mapping for the datasource.

Example

```
MS SQLSERVER2000
```

oasis.database.exceptionsorter

Defines a class that implements the org.jboss.resource.adapter.jdbc.ExceptionSorter interface. The interface examines database exceptions to determine whether they indicate a connection error.

Example

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorter
```

oasis.database.validConnectionChecker

Defines a class that implements the org.jboss.resource.adapter.jdbc.ValidConnectionChecker interface. The interface provides a SQLException isValidConnection(Connection e) mode. The application calls the mode with a connection that is returned from the pool to test its validity.

Example

```
org.jboss.jca.adapters.jdbc.extensions.mssql.MSSQLValidConnectionChecker
```

oasis.database.datasource.class

Defines the datasource class.

Example

```
com.microsoft.sqlserver.jdbc.SQLServerXADataSource
```

oasis.database.additionalparamurl

Defines parameters that are used to create the database connection.

Example

```
responseBuffering=full;SelectMethod=cursor;
```

oasis.database.lib.dbname

Defines the name of the library database.

Example

```
pamgacert_cluster_JDK7_rep
```

oasis.database.queues.dbname

Defines the name of queues database.

Example

```
pamgacert_cluster_JDK7_run
```

oasis.reporting.database.databasetype

Defines the type of reporting database.

Example

```
MSSQLServer2005
```

oasis.reporting.database.username

Defines the user name for the reporting database server.

Example

```
sa
```

oasis.reporting.database.password

Defines the password that is associated with the specified user for the reporting database server.

Example

```
oIzz9oH5OU4XRkOaeLblNqEYDsaXNGiMg9LSy2P7gsVLG0ea32nBlUIvXgE
XhiKfGzIbCmYFgYoFg0sVBlnY/k1sAeZ21z20sw5Yr9HC2B3+IRoyy5LXCm
ByMUMc7Ywq/BocPnw4e1DBDDfGqCQL/6ciK4CT1C7hU/V3Y4Ktrc9IsPK1a
XeNRM1qvpVwBAtG
```

oasis.reporting.database.dbhostname

Defines the host name of the reporting database server.

Example

```
lodivsa205
```

oasis.reporting.database.dbport

Defines the reporting database server connection port number.

Example

```
1433
```

oasis.reporting.database.genericdialect

Defines the dialect class of the reporting database.

Example

```
org.hibernate.dialect.SQLServerDialect
```

oasis.reporting.database.driver

Defines the fully qualified name of the JDBC driver class.

Example

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

oasis.reporting.database.typemapping

Defines the type mapping for the data source.

Example

```
MS SQLSERVER2000
```

oasis.reporting.database.dialect

Defines the user-defined dialect class of the reporting database.

Example

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

oasis.reporting.database.ValidConnectionQuery

Defines an SQL statement to run on a connection before it returns from the pool to verify its validity to test for stale pool connections. For example: select count(*) from x.

Example

```
select 1
```

oasis.reporting.database.connectionurl

Defines the reporting database JDBC connection URL.

Example

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

oasis.reporting.database.additionalparamurl

Defines the additional parameters to use for creating the database connection.

Example

```
;responseBuffering=full;SelectMethod=cursor;
```

FIPS_COMPLIANT

Specifies whether the CA Process Automation server is FIPS-compliant.

Example

```
true
```

oasis.reporting.database.dbname

Defines the name of the reporting database.

Example

```
pamgacert_cluster_JDK7_rpt
```

oasis.runtime.database.dbtype

Defines the runtime database type.

Example

```
MSSQLServer2005
```

oasis.runtime.database.username

Defines the user name for the runtime database server.

Example

```
sa
```

oasis.runtime.database.password

Defines the password that is associated with the specified user for the runtime database server.

Example

```
SOIjQ79jp66tm5E7ZYxLV2yqtVV54HRVs+xvNksG7p1pzTZOoOXahwS0XOc
VoMl8MznkgQgVOllCIU/YBx6lT3ZAxnzOMY2xBQnIp5xTxw0Dv5eqqTvpOn
m6P2vPOS1RzYGA6GRt3VdASiTZwZs/BkIX/sY+6C52V/x5Eg7l4hff6/6gS
6wvRHdJG/sXU6D6
```

oasis.rntime.database.dbhostname

Defines the host name of the runtime database server.

Example

```
lodivsa205
```

oasis.runtime.database.port

Defines the runtime database server connection port number.

Example

```
1433
```

oasis.runtime.database.dialect

Defines the user-defined dialect class of the runtime database.

Example

```
com.optinuity.c2o.persistence.MSQLServerDialect
```

oasis.runtime.database.genericdialect

Defines the dialect class of the runtime database.

Example

```
org.hibernate.dialect.SQLServerDialect
```

oasis.runtime.database.driver

Defines the fully qualified name of the JDBC driver class.

Example

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

oasis.runtime.database.typemapping

Defines the type mapping for the data source.

Example

```
MS SQLSERVER2000
```

oasis.runtime.database.exceptionsorter

Defines a class that implements the org.jboss.resource.adapter.jdbc.ExceptionSorter interface to examine database exceptions to determine whether the exception indicates a connection error.

Example

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

oasis.runtime.database.ValidConnectionQuery

Defines an SQL statement to run on a connection before it returns from the pool to verify its validity to test for stale pool connections. For example: select count(*) from x.

Example

```
select 1
```

oasis.runtime.database.validConnectionChecker

Defines a class that implements the org.jboss.resource.adapter.jdbc.ValidConnectionChecker interface to provide a SQLException isValidConnection(Connection e) method. A connection that returns from the pool calls this method to test its validity.

Example

```
org.jboss.jca.adapters.jdbc.extensions.mssql.MSSQLValidConn
ectionChecker
```

oasis.runtime.database.datasource.class

Defines the data source class.

Example

```
com.microsoft.sqlserver.jdbc.SQLServerXADataSource
```

oasis.runtime.properties.table.create.stmt

Defines the SQL statement to use to create the properties table if it is not present. The user is not expected to modify this statement because the application configures the correct value for the relevant database by default.

Example

```
create table properties (propkey varchar(255) NOT
NULL,propvalue NVARCHAR(MAX),PRIMARY KEY (propkey))
```

oasis.runtime.database.connectionurl

Defines the runtime database JDBC connection URL.

Example

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

oasis.runtime.database.additionalparamurl

Defines the additional parameters that are used to create the database connection.

Example

```
;responseBuffering=full;SelectMethod=cursor;
```

oasis.runtime.database.driver.name

Defines the runtime database driver name.

Example

```
com.microsoft.sqlserver.jdbc.SQLServerDriver (for a MSSQL
database)
```

oasis.runtime.database.dbname

Defines the name of the runtime database.

Example

```
pamgacert_cluster_JDK7_run
```

oasis.security.server.type

Defines the type of security server that is used for authentication and authorization.

Example

```
EEM
```

oasis.policy.type

Defines the type of login policy.

Example

```
EEM
```

certificatefolderFullpath

Defines the path of the folder that contains the security certificate. The path is relative to the c2o folder.

Example

install_dir/server/c2o/.c2orepository/public/certification/

oasis.eem.backend.server.location

Defines the host name of the computer that hosts the EEM security server.

Example

```
lodivsa205
```

oasis.eem.application.name

Defines the application name in the EEM server on which the policies are defined for the current CA Process Automation instance.

Example

```
pamgacert_cluster_JDK7
```

isFipsMode

Specifies whether the EEM server is running in FIPS mode.

Example

```
false
```

oasis.eem.certificate.path

Defines the name of the security certificate.

Example

```
PAM.p12
```

eiamCertKeyPath

Defines the name of the security certificate key file that is used for authentication. This property is only applicable if isFipsMode=true.

Example

```
PAM.key
```

oasis.eem.certificate.password

Defines the password that is associated with the EEM security certificate. This property is only applicable if isFipsMode=false.

Example

```
dD65vFTVmbn8aaZxjot9QCUIfPEey1H8/KGtNShgrronJk0rMtqliDMrNo2
VE+xoAUDcfmT9IPCQsAe497w1xUBkHg8PbZNjWVkPpFYw496eFiwiq7AoyB
8WCoUrx8wVnkMjoGs1BqDND+kjHcnUt9HLljYgxatT7Q2FpbTA7+Qag0W9g
Sv2oH4iBsUjVs22
```

ntlm.enabled

Specifies whether NTLM authentication is enabled. When changing this port, remove the .c2o folder in the ${Installation Dir}/server/c2o/.system folder, if it exists.

oasis.jxta.port

Defines the port to use for communication with other Orchestrators or agents.

Example

```
7001
```

oasis.jxta.host

Defines the host name of the computer that is used for communication with the Orchestrator or agent.

Example

```
name03-I40136.ca.com
```

oasis.local.hostname

Defines the host name of the computer where CA Process Automation is installed.

Example

*name*03-I40136.ca.com

oasis.server.isCluster

Specifies whether this CA Process Automation instance is clustered.

Example

true

loadbalancer.worker.node

Defines the name of this node in the cluster. This property is applicable only if it is a part of cluster.

Example

node2

oasis.snmptrigger.service.port

Defines the listening port for SNMP triggers.

Example

162

oasis.transport.secure

Specifies whether communication is secure.

Example

true

AcceptAllSSLCertificates

Specifies whether to accept all certificates in secure communication.

Example

true

oasis.reject.unnecessary.approval

Specifies whether to reject an interaction form which has not been configured for approval.

Example

true

managementconsole.timeout

Defines the timeout (in minutes) for CA Process Automation. The timeout is the interval CA Process Automation can be idle, after which the session expires.

Example

30

eem.connection.retries

Defines the number of retries for authentication when the security server is EEM.

Example

3

SSL_PROTOCOL

Defines the SSL protocol type. If the Java vendor is IBM Corporation, SSL protocol is used. Otherwise, TLS is used.

Example

TLS

X509_ALGORITHM

Defines the algorithm that is used for SSL certificates. If the Java vendor is IBM Corporation, the algorithm that is used is IbmX509. Otherwise, SunX509 is used.

Example

SunX509

oasis.publisher.name

Defines the name under which this CA Process Automation instance is licensed.

Example

CA

jboss.partition.udpgroup

Defines the multicast address for this cluster node.

Example

228.1.46.192

jboss.rmi.port

Defines the port of the RMI naming service.

Example

1098

jboss.jndi.port

Defines the listening port for the bootstrap JNP(JNDI Provider) service.

Example

1099

jboss.rmi.classloader.webservice.port

Defines the port that is used for the simple HTTP service that supports requests for classes for RMI dynamic class loading, org.jboss.web.WebService.

Example

8083

jboss.rmi.object.port

Defines the RMI server socket listening port to which RMI clients connect when communicating through the proxy interface.

Example

```
4444
```

jboss.pooledinvoker.serverbind.port

Defines the pooled invoker server bind port.

Example

```
4445
```

remoting.transport.connector.port

Defines the remoting server bind port.

Example

```
4448
```

jboss.ha.jndi.port

Defines the port on which the HA-JNDI stub is made available.

Example

```
1100
```

jboss.ha.jndi.rmi.port

Defines the RMI port that the HA-JNDI service uses when bound.

Example

```
1101
```

jboss.ha.rmi.object.port

Defines the RMI object port that JRMPInvokerHA uses.

Example

```
4447
```

jboss.ha.pooledinvoker.serverbind.port

Defines the pooled invoker HA server bind port.

Example

```
4446
```

jboss.mcast.jndi.autodiscovery.port

Defines the multicast group port that is used for JNDI autodiscovery. This port is defined in cluster-service.xml and hajndi-jms-ds.xml in deploy/jms.

Example

```
1102
```

jboss.mcast.ha.partition.port

Defines the multicast UDP port for HAPartition. This port is defined in cluster-service.xml and jmx-console.war/WEB-INF/web.xml.

Example

```
45566
```

jboss.mcast.http.sessionreplication.port

Defines the multicast UDP port for HttpSession replication. This port is defined in tc5-cluster-service.xml.

Example

```
45567
```

tomcat.connector.http.port

Defines the port for the connector component that supports the HTTP/1.1 protocol. This property enables Catalina to function as a stand-alone web server, in addition to its ability to run servlets and JSP pages. The Port is also configured in jboss-ws4ee.sar/META-INF/jboss-service.xml for Axis SService.

Example

```
8080
```

tomcat.connector.ajp.port

Defines the port for the connector component that communicates with a web connector through the AJP protocol.

Example

```
8009
```

tomcat.secure.port

Defines the secure port that the SSL connector uses. This port is unused. This port is the same port that is configured as:

- redirectPort for the AJP connector in server.xml
- WebServiceSecurePort for Axis Service in jboss-ws4ee.sar/META-INF/jboss-service.xml

The port is of use only if the SSL connector is enabled.

Example

```
8443
```

jboss.uil.serverbind.port

Defines the port to which Unified Invocation Layer (UIL) service clients connect when they establish a connection to the JBossMQ server.

Example

```
8093
```

oasis.protection.level

Specifies the CA Process Automation protection level. In secure mode, the protection level is set to CONFIDENTIAL, otherwise it is set to NONE.

Values: NONE, INTEGRAL, or CONFIDENTIAL.

itpam.initialperiodicheartbeatfrequency

Defines the initial heartbeat frequency (in minutes).

Example

2

system.encoding

Defines the encoding of this system.

Example

Cp1252

eem.max.search.size

Defines the maximum number of records to search simultaneously in EEM.

Example

10000

jboss.remoting.transport.Connector.port

Defines a JBoss-related port.

Example

3873

OAPort

Defines a JBoss-related port.

Example

3528

OASSLPort

Defines a JBoss-related port.

Example

3529

scripts.tmpDir

Defines the value of the temporary directory that runs scripts.

Example:

C:/Users/ADMINI~1/AppData/Local/Temp/2

oasis.powershell.setexecutionpolicy

Specifies whether the user selected an option to change the PowerShell run policy during installation.

Example

```
false
```

oasis.powershell.path

Defines the PowerShell path on the host computer.

Example

```
C:/Windows/System32/WindowsPowerShell/v1.0
```

override.jvm.tmpdir

Specifies whether to override the java.io.tmpdir system variable. The default value (true) lets the server refer the system variable to c2oHome/tmp. Set this property to false if you do not want the server to refer the system variable to c2oHome/tmp..

Example

```
true
```

jboss.default.jgroups.stack

Defines the default stack type being set up for use by JGroups for the application to run on.

Example

```
tcp
```

jboss.jgroups.tcp.tcp_port

Defines the TCP port for TCP-based clustering in JBoss.

Example

```
7600
```

jboss.jgroups.tcp_sync.tcp_port

Defines the TCP sync port for TCP-based clustering in JBoss.

Example

```
7650
```

jboss.messaging.datachanneltcpport

Defines the TCP-based messaging datachannel port.

Example

```
7900
```

jboss.messaging.controlchanneltcpport

Defines the TCP-based messaging control channel port.

Example

```
7901
```

jts.default.tx.reaper.timeout

Defines a nonnegative integer that the JBoss Transaction Service requires.

Example

```
120000
```

jboss.transaction.timeout

Defines the time when the reaper starts timing out the ongoing transactions after timeout a timeout occurs. JBoss requires this property.

Example

```
300
```

jboss.service.binding.port

Defines the File Ref deploy/messaging/remoting-bisocket-service.xml. JBoss Messaging requires this property.

Example

```
4457
```

jboss.remoting.port

Defines the File Ref deploy/jmx-remoting.sar. JBoss Remoting requires this property.

Example

```
1090
```

jboss.jbm2.port

Defines the communication transport to JBoss Messaging. JBoss Messaging 2 Netty requires this property.

Example

```
5445
```

jboss.hbm2.netty.ssl.port

The JBoss. SSL version of Netty requires this property.

Example

```
5446
```

jboss.tx.recovery.manager.port

Defines the File Ref deploy/transaction-jboss-beans.xml. JBossTS Recovery Manager requires this property.

Example

```
4712
```

jboss.tx.status.manager

Defines the File Ref deploy/transaction-jboss-beans.xml. JBossTS Transaction Status Manager requires this property.

Example

```
4713
```

jboss.tx.manager.sock.pid.port

Defines the File Ref deploy/transaction-jboss-beans.xml. JBossTS requires this property.

Example

```
4714
```

ucf.payload.file

Defines the name of the file that contains the Catalyst container payload.

Example

```
catalyst.installer.payload.zip
```

catalyst.container.name

Defines the name of the Catalyst container.

Example

```
node0
```

ucf.connector.enabled

Specifies whether the Catalyst Process Automation Services is enabled.

Example

```
false
```

ucf.payload.override

Specifies whether to override the payload (if the payload is present).

Example

```
false
```

ucf.pax.web.http.port

Defines the /container/etc/org.ops4j.pax.web.cfg port.

Example

```
8181
```

ucf.bus.hostname

Defines the host name of the Catalyst bus in /registry/topology/physical/node0/catalyst-bus/bus.properties.

Example

```
localhost
```

ucf.bus.port

Defines the port of the Catalyst bus in /registry/topology/physical/node0/catalyst-bus/bus.properties.

Example

```
61616
```

ucf.bus.http.port

Defines the HTTP port of the Catalyst bus in /registry/topology/physical/node0/catalyst-bus/bus.properties.

Example

```
61617
```

ucf.max.archive.query.results

Defines the maximum archive query results.

Example

```
30
```

use.catalyst.claims.credentials

Specifies whether to use the Catalyst claims for credentials.

Example

```
false
```

org.apache.commons.logging.Log

Defines a factory class for instantiating Loggers for Commons Logging.

Example

```
org.apache.commons.logging.impl.Log4JLogger
```

org.apache.commons.logging.LogFactory

Defines a factory class for instantiating Loggers for Commons Logging.

Example

```
org.apache.commons.logging.impl.Log4jFactory
```

eem.cache.timeout

This user-added parameter defines the maximum age (in seconds) of the cache that stores user credentials with the associated permissions profile. If set to zero, this CA Process Automation authorization cache is turned off and CA Process Automation sends a request to CA EEM each time user permissions are needed. When this parameter is missing, CA Process Automation uses 30 seconds as the refresh rate for the secondary cache.

Note: See Control the Refresh Rate of Caches of CA EEM Updates (see page 76) for details about the two CA EEM caches.

Example

30

mail.attachment.buffer.size

Lets you download an email with a specified amount of buffer.

K is the unit of measure. For example, if you specify 256, CA Process Automation defines it as 256K.

Example

mail.attachment.buffer.size=256

mail.imap.fetchsize

This property is specific to IMAP protocol and is not introduced for CA Process Automation. This property lets you more quickly download large mail attachments.

Specify this property in bytes.

Example

To specify 800k, multiply 800*1024.

mail.imap.fetchsize=819200

jts.allow.multi.last.rsrc

Specifies the property that Jboss Transaction Service uses. If XA resources are involved in multiple transactions, this property is false.

jsse.enableSNIExtension

Enables or Disables the SNI Host Name Matching.

org.apache.activemq.managementcontext.port

Defines the activeMQ Management Context port.

org.apache.activemq.minheapsize

Defines the activeMQ Min JVM Heap.

org.apache.activemq.tcp.port

Defines the tcp port of the activeMQ.

org.apache.activemq.maxheapsize

Defines the activeMQ Max JVM Heap.

Index

A

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U