

CA Process Automation

Content Administrator Guide

Service Pack 04.0.01



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

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2012 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>.

CA Process Automation

Documentation Changes

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

- [Browse to CA Process Automation and Log In](#) (see page 18)—This existing topic has been modified to address the the case where a load balancer is used.
- [Configure Command Execution](#) (see page 251)—This existing topic has been modified to include missing fields, previously documented under Network Utilities in the Release 03.1.00 documentation.
- [Permissions by Tab](#) (see page 68)—This existing topic has been modified to address each tab separately.
- [Permission Dependencies](#) (see page 72)—This existing topic has been modified to address dependencies for uploading jars, such as those for JDBC drivers, to Orchestrator Resources and Agent Resources.
- [Customizing Access with CA EEM Policies and Groups](#) (see page 79)—This section contains customization procedures and examples. Functionality has not changed.
- [Add a Touchpoint for an Orchestrator](#) (see page 156)—This existing topic was updated to mention that a touchpoint for a clustered Orchestrator maps the load balancer for that Orchestrator with an environment.
- [Configure SNMP Trigger Properties at the Domain Level](#) (see page 315)—This existing topic has been modified to update screenshots.
- [Update Orchestrator Resources](#) (see page 324)—This new topic describes how to upload jar files for deployment to Orchestrators.
- [Update Agent Resources](#) (see page 326)—This new topic describes how to upload jar files for deployment to agents.

Contents

Chapter 1: Getting Started with CA Process Automation and CA EEM 15

Log In to CA EEM as the EiamAdmin User	16
Create the First CA Process Automation Administrator Account.....	16
Browse to CA Process Automation and Log In	18
Configure User Settings for Date and Time Formats and Language	19
Control Frequency of Updating CA Process Automation with CA EEM Changes	20
Control the Timeout for CA Process Automation.....	21

Chapter 2: Introduction to CA Process Automation Configuration 23

About This Guide.....	23
Administration Task Overview	24
CA Process Automation Tabs	25
Relationships Among CA Process Automation Components	30
Cardinality of Component Associations	33
CA Process Automation Security	36
Securing the CA Process Automation Application	37
Securing Data Transfer Between CA Process Automation and CA EEM	38
Securing Data Transfer Between Orchestrators and Agents	39

Chapter 3: Administer Basic CA EEM Security 41

Determine Process for Achieving Role-Based Access	42
Browse to CA EEM and Log In	43
Change Your Own Password in CA EEM	44
Review Permissions for Default Groups.....	45
PAMAdmins Group Permissions	47
Designers Group Permissions.....	48
Production Users Group Permissions.....	50
PAMUsers Group Permissions	52
Create User Accounts with Default Roles	54
Create User Accounts for Administrators	55
Create User Accounts for Designers	56
Create User Accounts for Production Users	57
Create User Accounts with Basic Access	57
Update User Accounts with Default Roles	58
Manage Access for Referenced User Accounts.....	59
Set Maximum Number of CA EEM Users and Groups.....	61

Search for Identities Matching Specified Criteria	62
Assign an Application Group to a Global User	62
Create a Dynamic User Group Policy	64
Integrate Active Directory with CA EEM	65

Chapter 4: Administer Advanced CA EEM Security 67

Permissions Reference	67
Permissions by Tab.....	68
Permissions Dependencies	72
Filters for Permissions.....	75
Granting Administrators Access to CA EEM	76
Grant CA EEM Access to Selected Administrators	78
Customizing User Access with CA EEM Policies	79
Default Resource Classes and Custom Policies	80
How to Customize Access for a Default Group	83
How to Customize Access with a Custom Group	87
How to Customize Access for a Specified User	91
How to Transition Roles Used in Active Directory to CA EEM.....	98
Create the Custom ConfigAdmin Group	99
Grant Permissions to the Environment Configuration Administrators Group	100
Create User Accounts for Environment Configuration Administrators.....	101
Create the Custom ContentAdmin Group.....	101
Grant Permissions to the Custom ContentAdmin Group.....	102
Create User Accounts for Environment Content Administrators.....	102
Touchpoint Security with CA EEM.....	103
Grant Users CA EEM Access to Define Touchpoint Security Policies	103
About Touchpoint Security	107
Use Cases: When Touchpoint Security is Needed.....	108
Limit Access to Hosts with Sensitive Information	110
Identify the Access Control IDs To Add as Resources	111
Create a Touchpoint Security Policy	112
Example: Secure Critical Touchpoints	114
Example: Secure the Touchpoint for My Host	115
Authorizing Runtime Actions with CA EEM	117
Change Ownership for Automation Objects	118

Chapter 5: Administer the CA Process Automation Domain 119

Lock and Unlock the Domain.....	119
Configure the Contents of the Domain	119
About Configuration Inheritance	121
Configure CA EEM Security Settings for the Domain	122

Configure Domain Properties.....	129
Maintain the Domain Hierarchy.....	132
About the Domain Hierarchy, Orchestrators, and Agents	133
Add an Environment to the Domain	136
Remove an Environment from the Domain	137
Rename the Domain	138

Chapter 6: Administer Environments **139**

Configure the Contents of an Environment	139
View or Reset Security Settings for a Selected Environment.....	140
Configure Environment Properties	142
Enable an Operator Category and Override Inherited Settings	144
Specify Trigger Settings for an Environment.....	145
Update an Environment Hierarchy.....	146
Rename an Environment.....	148
Add an Orchestrator to an Environment.....	149
Delete an Orchestrator Touchpoint	150

Chapter 7: Administer Orchestrators **151**

About Orchestrators.....	151
Configure the Contents of an Orchestrator Touchpoint	152
Configure Orchestrator Touchpoint Properties	153
Update the Hierarchy of an Orchestrator Touchpoint.....	155
Add a Touchpoint for an Orchestrator.....	156
Recover Operators on the Target Orchestrator	157
Disable an Orchestrator Touchpoint	158
Configure the Contents of an Orchestrator Host	159
View Orchestrator Security Settings	159
Configure Orchestrator Host Properties	162
Override Operator Category Settings Inherited from Environment	164
Activate Triggers for an Orchestrator	165
Configure Orchestrator Policies	166
Configure Orchestrator Mirroring.....	168
Maintain the Orchestrator Host.....	169
Quarantine an Orchestrator.....	170
Remove the Quarantine from an Orchestrator	171
Stop the Orchestrator	172
Start the Orchestrator.....	173

Chapter 8: Administer Agents 175

Configure Agents to Support Operator Targets	176
Install an Agent Interactively.....	180
Add an Agent Touchpoint.....	182
Add an Agent Host Group	183
Configure the Contents of a Selected Agent	183
Configure Agent Properties.....	184
Customize Agent Settings for Operator Categories	186
Disable an Operator Category on a Selected Agent	187
Configure a Selected Touchpoint or Host Group	188
View the Touchpoints and Host Groups for a Selected Agent	188
Quarantine an Agent	189
Remove Quarantine from an Agent	189
Rename an Agent	190
Manage the Decommissioning of a Host with an Agent	190
Remove an Agent	192
Remove Selected Agents in Bulk.....	192
How to Start or Stop an Agent	193
Start CA Process Automation Agent on a UNIX or Linux Host.....	194
Stop CA Process Automation Agent on a UNIX or Linux Host	194

Chapter 9: Administer Touchpoints 195

Touchpoint Implementation Strategy	196
Add a Touchpoint to a Selected Environment.....	197
Add an Agent to an Existing Touchpoint	198
Add Touchpoints for Agents in Bulk	198
Configure How Operators Select the Target Agent.....	200
Configure Touchpoint Properties	201
Rename a Touchpoint	203
Associate a Touchpoint with a Different Agent.....	204
Remove Unused Empty Touchpoints in Bulk	205
Manage Touchpoint Groups.....	207
About Touchpoint Groups.....	207
Create a Touchpoint Group with Selected Touchpoints	209
Create a Touchpoint Group.....	211
Rename a Touchpoint Group	211
Add a Touchpoint to a Touchpoint Group	212
Delete a Touchpoint from a Touchpoint Group	212
Delete a Touchpoint Group.....	213

Chapter 10: Administer Proxy Touchpoints **215**

Proxy Touchpoint Prerequisites	215
CA Process Automation-Specific Requirements for SSH Connectivity	216
Create the SSH User Account on the Remote Host of the Proxy Touchpoint	217
Create an SSH Trust Relationship to the Remote Host	217
Configure Proxy Touchpoint Properties	218
Use a Proxy Touchpoint	221

Chapter 11: Administer Host Groups **223**

How a Target Host Can Be Specified in an Operator	223
About Host Groups	224
How Host Groups Compare to Proxy Touchpoints	225
Host Group Implementation Process	226
Create a Host Group	227
Configure Host Group Properties	229
Create SSH Credentials on Hosts in a Host Group	234
Create the Destination Directory and File for the Public Key	235
Create a Trust Relationship to a Remote Host Referenced by a Host Group	236
View Details about All Host Groups	238

Chapter 12: Administer Operators By Category **239**

Operator Categories and Operator Folders	240
Example: Category Settings Used by Operator	242
Configuring Operator Categories	244
About Catalyst	245
Configure Catalyst	246
Load Catalyst Descriptors	247
About Command Execution	249
Configure Command Execution	251
About Databases	260
Configure Databases: Oracle Properties	261
Configure Databases: MSSQL Server Properties	263
Configure Databases: MySQL Properties	264
Configure Databases: Sybase Properties	266
About Date-Time	268
About Directory Services	268
Configure Directory Services	268
About Email	272
Configure Email	273
About File Management	275

Configure File Management.....	275
About File Transfer.....	278
Configure File Transfer.....	278
About Java Management.....	279
About Network Utilities.....	280
Configure Network Utilities.....	280
About Process Control.....	282
Configure Process Control.....	282
About Utilities.....	283
Configure Utilities.....	284
About Web Services.....	287
Configure Web Services.....	287
Category Configuration and Operator Inheritance.....	294
Enable or Disable an Operator Category.....	295
Override Settings Inherited by a Category of Operators.....	296
Operator Categories and Where Operators Run.....	298

Chapter 13: Administer Triggers **299**

How to Configure and Use Triggers.....	300
Configure Catalyst Trigger Properties at the Domain Level.....	302
Configure File Trigger Properties at the Domain Level.....	308
Configure Mail Trigger Properties at the Domain Level.....	311
Configure SNMP Trigger Properties at the Domain Level.....	315
Change the SNMP Traps Listener Port.....	318

Chapter 14: Manage User Resources **319**

About User Resources Management.....	320
How to Deploy JDBC Drivers for Database Operators.....	321
Upload User Resources.....	321
Add a Resource to User Resources.....	322
Delete a Resource from User Resources.....	323
Modify a Resource in User Resources.....	323
Upload Orchestrator Resources.....	324
Upload Agent Resources.....	326

Chapter 15: Audit User Actions **329**

View the Audit Trail for the Domain.....	329
View the Audit Trail for an Environment.....	331
View the Audit Trail for an Orchestrator.....	332
View the Audit Trail for an Agent.....	334

View the Audit Trail for a Touchpoint, Touchpoint Group, or Host Group	335
View the Audit Trail for a Library Folder	336
View the Audit Trail for an Open Automation Object	338

Appendix A: FIPS 140-2 Support **341**

When CA Process Automation Uses Encryption	341
Cryptographic Module Validated to FIPS 140-2	342
User Authentication and Authorization in FIPS Mode	342
How Authentication and Authorization Work.....	344

Appendix B: Maintaining the Domain **347**

Build Out the Domain.....	347
Back up the Domain	348
Restore the Domain from Backups	349
Manage Certificates	350
How CA Process Automation Protects Passwords	350
About the CA Process Automation Certificate	351
Install the Predefined CA Process Automation Certificate	351
Create and Implement Your Own Certificate for CA Process Automation	352
Implement Your Third-Party Trusted SSL Certificate for CA Process Automation	355
Maintain IP Addresses.....	357
Maintain the DNS Host Name	358
Syntax for DNS Host Names	358
Deploy the Catalyst Process Automation Connector	359

Index **361**

Chapter 1: Getting Started with CA Process Automation and CA EEM

CA Process Automation is installed with the default administrator user with the following credentials:

- User name: pamadmin
- Password: pamadmin

You can browse to a freshly installed CA Process Automation and log in with these credentials. A better approach is to create your own user account in CA EEM during your first session. Then you can browse to CA Process Automation and log in with your own credentials.

After you log in, configure the settings that will help you when administering security and configuring the Domain.

This section contains the following topics:

[Log In to CA EEM as the EiamAdmin User](#) (see page 16)

[Create the First CA Process Automation Administrator Account](#) (see page 16)

[Browse to CA Process Automation and Log In](#) (see page 18)

[Configure User Settings for Date and Time Formats and Language](#) (see page 19)

[Control Frequency of Updating CA Process Automation with CA EEM Changes](#) (see page 20)

[Control the Timeout for CA Process Automation](#) (see page 21)

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 CA EEM that CA Process Automation uses. The URL follows, where *hostname* is the host name or IP address of the server where CA EEM is installed.
`https://hostname:5250/spin/eiam`
The CA Embedded Entitlements Manager dialog opens.
2. Select **Process Automation** from the Application drop-down list.
If you assigned another name to the CA Process Automation application, select the name you assigned.
3. Type **EiamAdmin** and the password that was established at installation for the EiamAdmin user.
4. Click Log In.

Create the First CA Process Automation 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:

[Grant CA EEM Access to Selected Administrators](#) (see page 78)

[Change Your Own Password in CA EEM](#) (see page 44)

Browse to CA Process Automation and Log In

Browse to CA Process Automation. Enter either the fully qualified domain name (FQDN) or the IP address of the correct server.

Follow these steps:

1. Launch the URL where *server* refers to the server where the Domain Orchestrator is installed, if unclustered. For a clustered Domain Orchestrator, *server* refers to the server with the load balancer.

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

Examples:

`https://domainOrchestrator_host:8443/itpam`
`https://loadBalancer_host:443/itpam`

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

Examples:

`http://domainOrchestrator_host:8080/itpam`
`http://loadBalancer_host:80/itpam`

The CA Process Automation login page opens.

2. Enter the user ID and password from the default administrator account or from your user account.
3. Click Log In.

CA Process Automation opens. The Home tab displays.

Configure User Settings for Date and Time Formats and Language

By default, date and time data corresponds to the time zone of the local host. During your first login session, you can set your preferred date and time formats and preferred language.

Follow these steps:

1. Browse to CA Process Automation and log in, if not already logged in.

2. Click your login name in the toolbar.

The User Settings dialog appears.

3. Select the preferred formats for the date and time from the drop-down lists.

4. Verify the language setting and change, if needed.

5. Click Save and Close.

A message advises you to log out and log back in to view the changed settings.

6. Click OK.

7. Apply your changes as follows:

a. Click Log Out to log out from CA Process Automation.

b. Browse to CA Process Automation and log in.

All data is displayed in the language, time, and date formats you selected.

Control Frequency of Updating CA Process Automation with CA EEM Changes

When you modify policies in CA EEM, it takes time for CA Process Automation to honor the changes. CA Process Automation maintains a cache of the policies defined in CA EEM. Reduce the cache refresh interval to update CA Process Automation with CA EEM changes more frequently. When you are not updating CA EEM, increase this value back to the default. The default value reduces network traffic.

Follow these steps:

1. Click the Configuration tab.

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

2. Click Lock.
3. Edit the following setting. For example, replace the default value of 1800 seconds (30 minutes) with 300 to apply CA EEM updates every 5 minutes.

CA EEM Cache Update Interval (in seconds)

Specifies the frequency in seconds that CA EEM updates CA Process Automation with CA EEM changes, where the minimum value is 60 seconds.

Default: 1800 seconds

4. Click Save.
5. With the Domain selected, click Unlock.
6. Restart the Domain Orchestrator.
 - a. [Stop the Orchestrator](#) (see page 172).
 - b. [Start the Orchestrator](#) (see page 173).

More information:

[Configure CA EEM Security Settings for the Domain](#) (see page 122)

Control the Timeout for CA Process Automation

The CA Process Automation timeout interval is 15 minutes, by default. CA Process Automation automatically logs off after 15 minutes of inactivity. You can extend the timeout period.

You can control the timeout value for CA Process Automation.

Follow these steps:

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

`install_dir/server/c2o/.config`
3. Open the `OasisConfig.properties` file with an editor.
4. Use Find to locate the following property:

`managementconsole.timeout`
5. Change the value for the property `managementconsole.timeout`.
6. Save the file and exit.
7. Restart the Orchestrator service.
 - a. [Stop the Orchestrator](#) (see page 172).
 - b. [Start the Orchestrator](#) (see page 173).

Chapter 2: Introduction to CA Process Automation Configuration

This section contains the following topics:

[About This Guide](#) (see page 23)

[Administration Task Overview](#) (see page 24)

[CA Process Automation Tabs](#) (see page 25)

[Relationships Among CA Process Automation Components](#) (see page 30)

[Cardinality of Component Associations](#) (see page 33)

[CA Process Automation Security](#) (see page 36)

About This Guide

This *Content Administrator Guide* focuses on tasks that users in the following role perform:

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

The tasks include:

- Setting up security.
- Configuring CA Process Automation to support content development and production use.

Notes:

For work flows related to setup tasks for a new content design environment or a new production environment, see the Online Help.

For details about how content designers use web services methods, see the *Web Services Reference*.

For details about how content designers create processes and other automation objects, see the *Content Designer Guide*. For details on operators, see the *Content Designer Reference*.

For details about how production users and content administrators use CA Process Automation in a production environment, see the *Production User Guide*.

Before you begin using this guide, be sure that all tasks described in the CA Process Automation *Installation Guide* have been performed.

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 358).
- 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.

CA Process Automation Tabs

You perform most configuration and administration tasks from the Configuration tab on CA Process Automation.

Availability of tabs depends on access rights granted the logged-on user. When you log in to CA Process Automation for the first time, you are presented with a tabbed view. A description of how to use each tab follows. Open online help for task flows related to each tab.

Home

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

Library

Typically, content administrators create the folders and grant access rights to the folders. Content designers create objects from their folders here and access their objects for edit. If the object is a process, the editor is the Designer tab.

- Folders - The folder structure is up to the administrator. Folders can contain subfolders and automation objects. A recommended structure is to create folders for global objects such as global datasets and global calendars at the root level. Consider creating a folder for each process at the root level and a subfolder for objects that the process uses. The folder structure created in the design environment is imported to the production environment when the process is completed and tested. This plan simplifies the export/import process.
- Recycle Bin - Purge deleted folders or restore purged folders.
- Search - Search for content objects by folder, keyword, or date.
- Object list for the folder you select or the search criteria you enter. You can open objects to work on from this display. For example, navigate to your folder and create an object, such as Resources. The object that you create appears on the grid. Click the default name to open the editor for that object. For example, click a Resources object to open the Resources Editor. Click a Process object to open that process on the Design tab.

Designer

Content designers design a planned process on the Main Editor canvas with operators they drag and drop from the Operators palette. A Dataset palette and a Properties palette is displayed for a selected operator. Designers connect operators with links. Each operator has one input port for the incoming link and two or more output ports. Designers can switch from the Main Editor to an Exception Handler tab or to a Lane Change Handler tab.

Operations

Operations include the following palettes.

Links

Specifies the following standard links:

- Process Instances - Instances of processes that have been started. Process Instances vary in their state.
- Operators - Operators within started processes and tasks from schedules. The bar chart shows operators by state, including: running, timeout, completed, failed, and aborted. Details for each operator include the instance name, state, and the touchpoint name on which it ran, among others.
- Task List - All users can view their own task list, and task lists for any group 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 currently active processes.
- Global Schedules - Schedules that you can use to start any process or selected operators. You can filter the display by date, by Orchestrator or agent touchpoint, and by current or archived.
- Start Requests - Requests to start specified processes on demand.

Process Watch

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

Start Request

Users can view a bar graph of queued, running, completed, and failed instances of start requests that have recently run. 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 data set structure for a selected dataset and its name-value pairs.

Resources

Users can select a resources object from the expanded Resources palette and manually override the displayed values for Amount and Used. Users can also change the state.

Schedules

Users can select a schedule from the expanded Schedules palette. Users can specify the run date and whether to show activity for all nodes or a selected orchestrator. Users can specify whether to display current schedules or archived schedules. For the selected schedule, displays the task name, the actual start and end times, the state, the type, calendar name if specified, exclude dates, and the scheduled time.

Configuration

The administrator responsible for configuring CA Process Automation accesses the Configuration tab. By default, Environments, Orchestrators and agents inherit settings that administrators configure at the Domain level. Operators inherit settings that are configured at the operator category level.

Configuration Browser

Two views are displayed--one for configuring logical attributes of the domain hierarchy, another for configuring properties of the Orchestrators and agents you install.

- Domain hierarchy
Configure the Domain, the Default Environment, the Orchestrator touchpoint, the agent touchpoints and proxy touchpoints, and the host groups.
- Orchestrators
Configure the Domain Orchestrator and any additional installed Orchestrators.
- Agents
Configure associations and settings for all installed Agents.

Manage User Resources

System administrators access the CA Process Automation User Resources folder to add or updates scripts used in content development.

Installations

System administrators install additional Orchestrators or cluster nodes for the Domain Orchestrator or additional Orchestrator. Administrators also install agents.

Reports

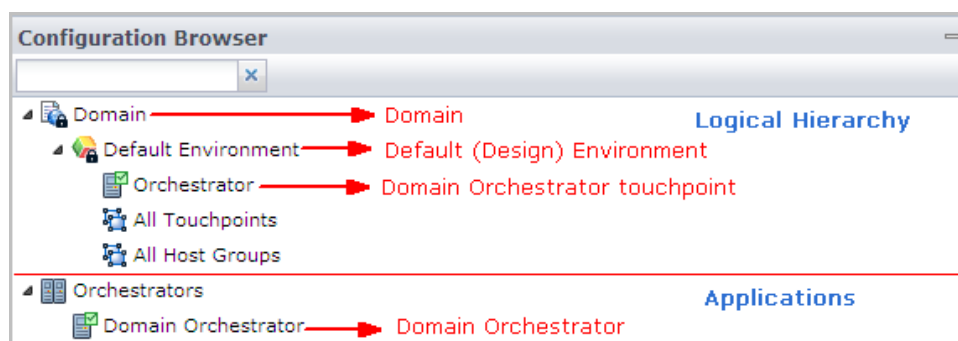
All users can access predefined reports or upload custom reports designed with the BIRT RCP Designer.

Relationships Among CA Process Automation Components

As a CA Process Automation administrator, you architect and configure the CA Process Automation Domain. Before you begin, it is helpful to understand the context for important physical and logical entities. The following example introduces the relationships among the following CA Process Automation-specific entities: Domain, environment, Orchestrator, agent, and touchpoint.

Everything in CA Process Automation that belongs to an enterprise is under one Domain. Separate Domains require separate installations of CA Process Automation.

The first CA Process Automation Orchestrator that you install is the Domain Orchestrator. The Domain Orchestrator manages all configurations and the software repository. Technically, managing the software repository means managing the versions of the automation objects. The Domain Orchestrator installed application is represented on the Configuration tab under the Orchestrators node. The touchpoint that associates the Domain Orchestrator with the Default Environment is displayed in the logical hierarchy under Default Environment as Orchestrator.

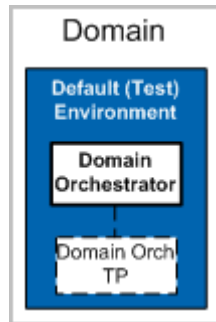


The Domain Orchestrator has a library of automation object definitions that all Orchestrators can share. The shared library is separate from its runtime database.

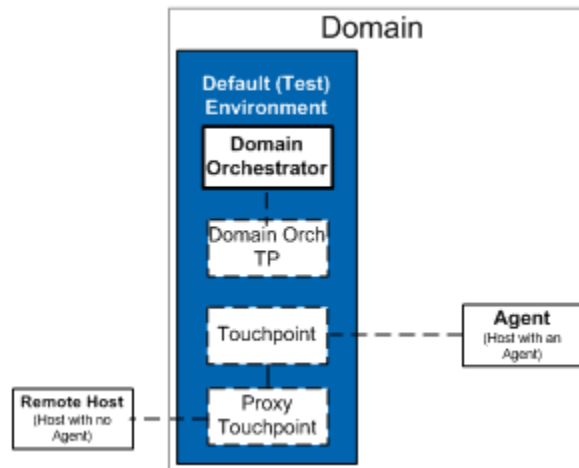
If you add an Orchestrator to an environment, that Orchestrator has its own database for storing runtime objects. The added Orchestrator can share the library of definitions belonging to the Domain Orchestrator or any selected Orchestrator.

Processes that content designers develop are run on the Orchestrator in the Default Environment. Content is typically developed and tested on Orchestrators in an environment that is kept separate from the production environment.

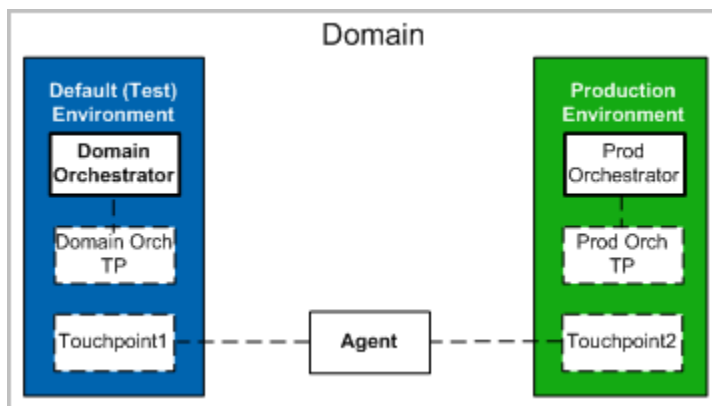
At installation, the Domain includes the Default Environment; the Default Environment includes the Domain Orchestrator. The Default Environment can be used for designing and testing processes. Content designers create processes that run on the Orchestrator. Operators in processes target the touchpoint that is associated with the Orchestrator. The following diagram depicts the touchpoint as a block with a border of dashes. The diagram depicts the association between the touchpoint and the Domain Orchestrator as a dashed line.



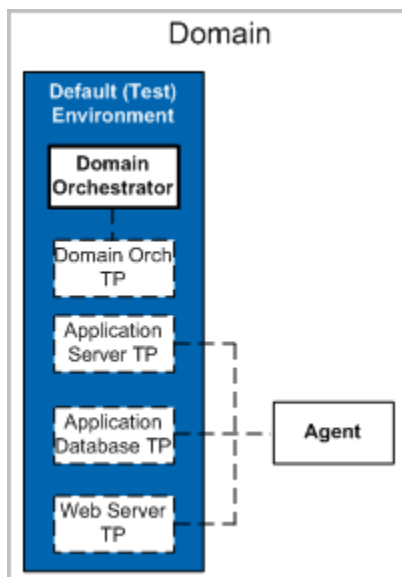
A process that runs on an Orchestrator can include operators that target hosts other than the host where the Orchestrator is installed. Such target hosts typically require installation of a CA Process Automation agent. You associate touchpoints with agents. Content designers access the agent through its touchpoint name. When it is not possible to install an agent on a target host, proxy touchpoints are used. Proxy touchpoints extend the use of touchpoints so that Orchestrators can run operators on a remote host, that is, a host with no installed agent. When a touchpoint is configured with an SSH connection to a remote host, it is a proxy touchpoint.



Agents belong to the Domain, but touchpoints belong to a specific environment. A touchpoint is a mapping of an agent to an environment. You can associate different touchpoints in different environments to the same agent. Processes that run on Orchestrators in different environments can target the same agent by specifying the environment-specific touchpoint.



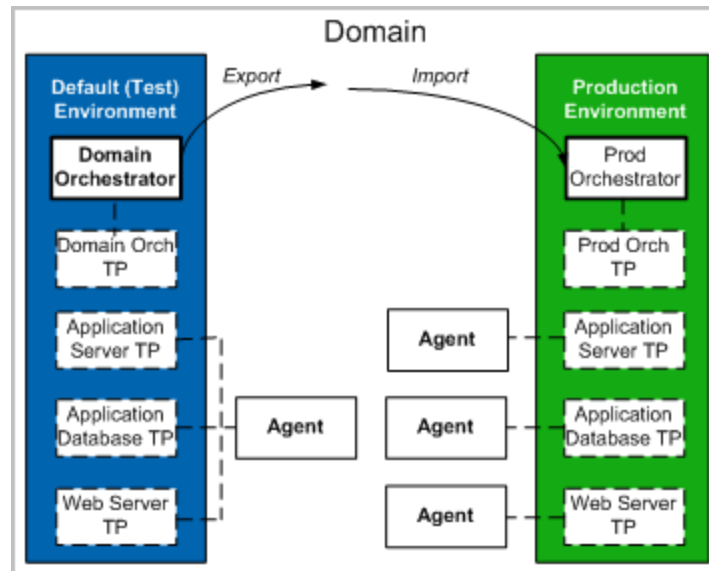
Typically, the design environment has a limited number of hosts. A production environment has many hosts. In a production environment, different software is installed on different hosts. For testing purposes, you can install multiple types of software on a single agent host. In this case, you associate multiple touchpoints to the same agent host. Separate touchpoints can simplify migration of a process to the Production Environment. Consider, for example, a requirement to automate a process that involves operations on an application server, an application database, and a web server. You prepare for process development by installing the required software on a host in the Test Environment. Install an agent on that host. Then, define one touchpoint for the application server, one for the application database, and a third for the web server. The following diagram depicts an agent with associations to three touchpoints.



You can establish multiple environments, each with its own data. The only way data is transferred from one environment to another is through export and import procedures.

Consider the plans and migration steps that precede running a tested process in the Production Environment. For this simple example, you identify the hosts on which the required application server, web server, and application database are running. You install agents on those hosts, and associate with each agent a touchpoint with the same name as the corresponding touchpoint in the Test Environment. Then, you export the designed and tested library from the Test Environment and import it into the library of an Orchestrator in the Production Environment.

No modification to a tested process is needed. Consider the following diagram which shows three agents that are associated with separate touchpoints in the Production Environment. Each agent is mapped to the same touchpoint names that were used in the Test Environment. While a Test Environment typically has one Orchestrator and few agents, the Production Environment can have multiple Orchestrators and thousands of agents.



More information:

[About the Domain Hierarchy, Orchestrators, and Agents](#) (see page 133)

Cardinality of Component Associations

CA Process Automation offers you flexibility. You can install as many Orchestrators and agents as you need. You can define as many environments, touchpoints and host groups as you need. These components and associations are represented under the Domain tree.

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. 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 and 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 testing. Then, you can create a separate environment for Production. Each environment must have at least one Orchestrator.

Note: Content designers can package their designed content. Typically, an administrator exports a package from the Default Environment and then imports it into the Production environment. Data also can be transferred across domains.

- An environment can have one or more Orchestrators. Orchestrators are installed on hosts.

Note: An Orchestrator can be a standard Orchestrator or a clustered Orchestrator. A clustered Orchestrator is composed of multiple nodes.

- The Domain can have as many agents as you need. Agents are installed on hosts. Agents are independent of environments.

Environments and Touchpoints

Both environments and touchpoints are logical entities.

- Each touchpoint belongs to one environment.
- Each environment can have many touchpoints.

Orchestrators and Touchpoints

After you install an Orchestrator, you create a touchpoint that associates the Orchestrator with a specific environment. Operators within 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 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.
- If the "Target" of an operator in a process is not specified, the operators execute on the Orchestrator touchpoint running the process.

Agents and Touchpoints

For an agent to be available as a target for an operator, associate the agent with a touchpoint, a proxy touchpoint, or a host group.

- An agent can be associated with one or more touchpoints.
 - When an agent is associated with one touchpoint, operators can run directly on a host with an installed agent by targeting its touchpoint.
 - When an agent is associated with multiple touchpoints on the same host, the touchpoints typically target different components on the host. For example, one touchpoint could be defined to access a database while another accesses a third-party product.
 - You can associate an agent with touchpoints that belong to different environments. This type of association provides the mechanism for defining processes that can be migrated across environments without changing target host information.
- A touchpoint can be associated with one or more agents. You can assign the same priority to multiple agents. You can assign a different priority to each agent.
 - When agents have different priorities, operators run on the agent with the highest priority. If the highest priority agent is unavailable, the operator runs on an available agent with a lower priority. This design helps ensure that a target host is available.
 - When multiple agents with the same priority are associated with a touchpoint, operators run on the least busy 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 the target of an operator, but where installation of an agent is not practical.

- An agent can be associated 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 an agent is associated with a proxy touchpoint, operators within a process can run on the remote host by targeting the proxy touchpoint.

Agents, Host Groups, and Remote Hosts

A host group is a group of remote hosts that are configured with a common host name pattern or with an IPv4 subnet expressed in CIDR notation.

- An agent can be associated with one or more host groups.
- A host group can be associated with one or more agents.
- When an agent is associated with a host group, you manually configure SSH connections. You 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: See [Syntax for DNS Host Names](#) (see page 358).

CA Process Automation Security

As an administrator, your concerns for security can include:

- [Securing the CA Process Automation application](#) (see page 37).
- [Securing data transfer between CA Process Automation and CA EEM](#) (see page 38).
- [Securing data transfer between Orchestrators and agents](#) (see page 39).

More information:

[Administer Basic CA EEM Security](#) (see page 41)

Securing the CA Process Automation Application

One aspect of securing the CA Process Automation application is to prevent unauthorized users from logging in. Another is to limit the use of functionality based on the role of the logged on user. Implementing security for the CA Process Automation application includes the following components:

- Authentication mechanisms.

When CA EEM is selected as the directory server (user store), CA Process Automation uses CA EEM to authenticate users at login. CA EEM compares the credentials users enter at login with user name and password combinations in its User Accounts. The user is allowed to log in only if a match is found.

You can help protect CA Process Automation from unauthorized login by having users change their password periodically and the suspending or disabling the default accounts. See the following for details:

[Change Your Own Password in CA EEM](#) (see page 44).

[Suspend or Disable a User Account](#) (see page 38).

- Authorization mechanisms and role-based security.

When CA EEM is selected as the directory server (user store), CA Process Automation uses CA EEM for user authorization. CA EEM examines policies and lets users perform tasks only on those parts of the user interface to which they are authorized. Authorization for the PAMAdmins, Designers, Production Users, and PAMUsers group is set by default. Users added to these groups inherit the authorization.

You can create role-based security such that users belonging to different groups access only parts of CA Process Automation needed for the role they perform. In addition, you can use CA EEM policies to assign individuals your trust to activities where 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 342)

Suspend or Disable 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.

You can 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.

To suspend or disable an obsolete user account

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.

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 341)

[When CA Process Automation Uses Encryption](#) (see page 341)

[How Authentication and Authorization Work](#) (see page 344)

Securing Data Transfer Between Orchestrators and Agents

To secure the data transfer between Orchestrators and agents, install CA Process Automation in secure mode. This is done by selecting Support Secure Communication when you set General Properties for the Domain Orchestrator.

Secure mode means that the data transferred between Orchestrators and agents uses the secured, encrypted HTTPS protocol.

When you install CA Process Automation in secure mode, your URL is in the following format:

```
https://<hostname|IP_address>:8443/itpam/
```


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 67) if you are creating custom roles and custom policies.

This section contains the following topics:

[Determine Process for Achieving Role-Based Access](#) (see page 42)

[Browse to CA EEM and Log In](#) (see page 43)

[Change Your Own Password in CA EEM](#) (see page 44)

[Review Permissions for Default Groups](#) (see page 45)

[Create User Accounts with Default Roles](#) (see page 54)

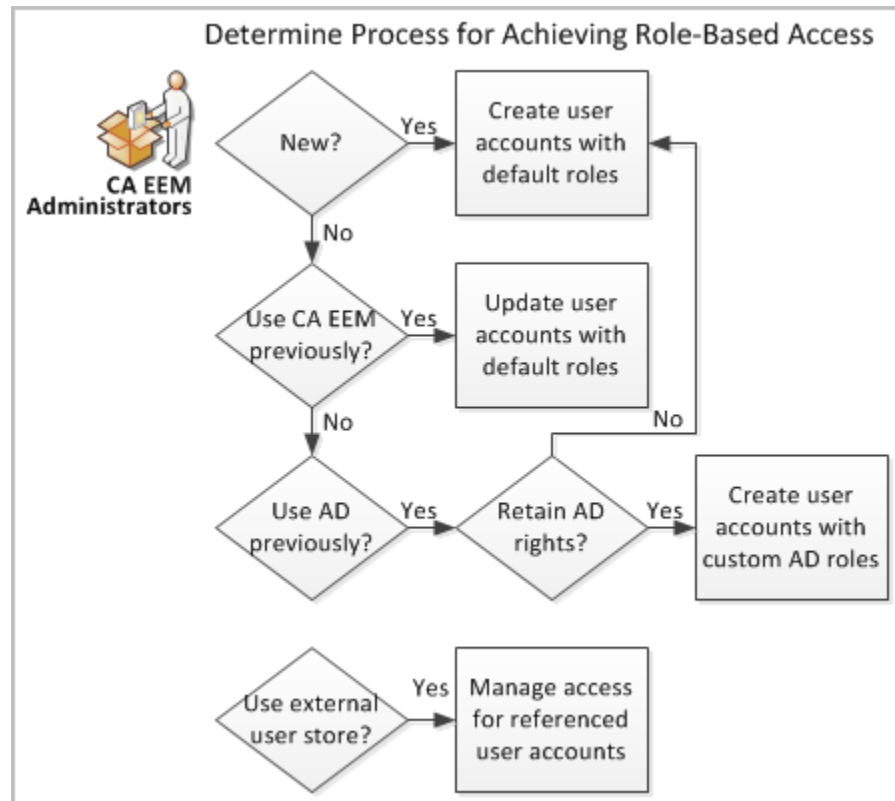
[Update User Accounts with Default Roles](#) (see page 58)

[Manage Access for Referenced User Accounts](#) (see page 59)

Determine Process for Achieving Role-Based Access

Security administration with CA EEM varies for the following scenarios:

- 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.
- 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.



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

- [Create user accounts with default roles](#) (see page 54).
- [Update user accounts with default roles](#) (see page 58).
- Create user accounts with custom AD roles.
See [How to Transition Roles Used in Active Directory to CA EEM](#) (see page 98).
- [Manage access for referenced user accounts](#) (see page 59).

Browse to CA EEM and Log In

To manage users, user groups, and access policies for CA Process Automation in CA EEM, log in to the Process Automation application in CA EEM.

Follow these steps:

1. Use the following URL to browse to the CA EEM that CA Process Automation uses.
`https://hostname:5250/spin/eiam`
The CA Embedded Entitlements Manager dialog opens.
2. Select **Process Automation** from the Application drop-down list.
If you assigned another name to the CA Process Automation application, select the name you assigned.
3. Type one of the following sets of credentials:
 - Type **EiamAdmin** and the password that was established at installation for the EiamAdmin user.
 - Type your own user name and password if you have been granted CA EEM access by the EiamAdmin user.
4. Click Log In.

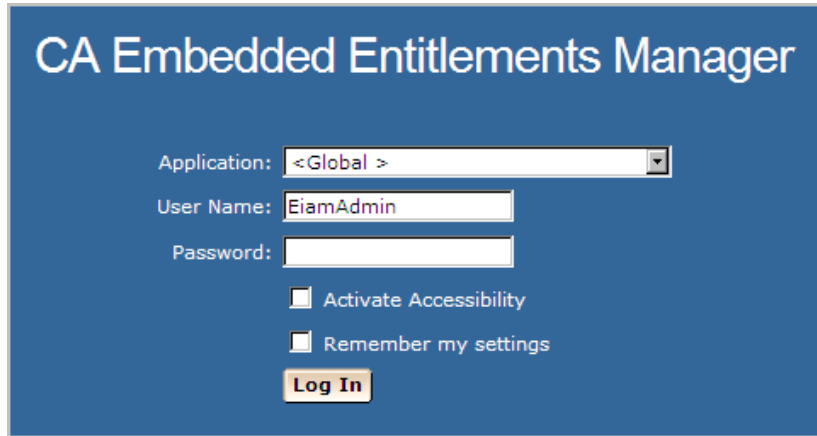
Change Your Own Password in CA EEM

CA Process Automation users can change their own passwords in CA EEM.

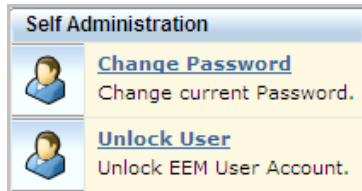
Follow these steps:

1. Open a browser and enter the URL for the CA EEM server used by CA Process Automation. For example:
`https://hostname_or_IPaddress:5250/spin/eam/`

The CA Embedded Entitlements Manager (CA EEM) Log In dialog appears.



2. For Application, select <Global>.
3. Delete EiamAdmin if this default User Name appears.
4. Enter your CA Process Automation user name and password, and then click Log In.
5. Click Change Password.



6. Enter your CA Process Automation user name and old password. Then enter your new password in both the New password and Confirm password fields and click OK.



The screenshot shows a web interface for 'Self Administration'. Underneath, there is a 'Change Password' section with four input fields: 'User Name:', 'Old password:', 'New password:', and 'Confirm password:'.

7. Browse to CA Process Automation and log in with your new credentials.

Review Permissions for Default Groups

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: pamproducer

Password: pamproducer

PAMUsers

The default PAMUsers group is granted minimal permissions. This group is designed for users who examine reports or view the state of operations.

Default user credentials

User Name: pamuser

Password: pamuser

Detailed permission descriptions follow:

- [PAMAdmins group permissions](#) (see page 47).
- [Designers group permissions](#) (see page 48).
- [Production Users group permissions](#) (see page 50).
- [PAMUsers group permissions](#) (see page 52).

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

PAMAdmins Group Permissions

Members of the PAMAdmins group are granted all permissions through CA EEM policies. A summary follows.

Home tab

- Log in to CA Process Automation and use the Home tab - PAM40 User Login Policy.

Library tab

- View the Library tab - PAM40 LibraryBrowser Policy.
- Control the library folders and their contents - Environment_Library_Admin right in the PAM40 Environment Policy.

Designer tab

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

Operations tab

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

Configuration tab

- View the Configuration Browser (all palettes) - PAM40 Configuration Policy.
- Configure at the Domain level or perform an action that requires locking the Domain - PAM40 Domain Policy.
- Configure at the Environment level or perform an action that requires locking an environment - PAM40 Environment Policy.
- Install agents or Orchestrators - PAM40 Configuration Policy.
- Manage User Resources - PAM40 Configuration Policy.

Reports tab

- View the Reports tab, generate reports, and add new reports - PAM40 Reports Policy.

Designers Group Permissions

User accounts associated with the Designers application group are granted and denied the permissions through CA EEM policies. A summary of granted and denied permissions follows:

Granted permissions

Permissions that CA EEM grants to users who are assigned the Designers group determine tab access and access within a tab.

Home tab

- Log in to CA Process Automation and use the Home tab - PAM40 User Login Policy.

Library tab

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

Designer tab

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

Operations tab

- View the Operations tab (all palettes) - PAM40 Operations Policy.
- Control the schedules displayed in the Operations tab - 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.

Configuration tab

- View the Configuration Browser (all palettes) - PAM40 Configuration Policy.

Denied permissions

Permissions that CA EEM does not grant to users who are assigned the Designers group deny the ability to perform certain actions, or access certain tabs or palettes.

Configuration tab

- Configure at the Domain level or select a menu option that requires locking the Domain - PAM40 Domain Policy.
- Configure at the Environment level or select a menu option that requires locking an environment - PAM40 Environment Policy.
- Install agents or Orchestrators - PAM40 Configuration Policy.
- Manage User Resources - PAM40 Configuration Policy.

Reports tab

- View the Reports tab, generate reports, add new reports - PAM40 Reports Policy.

Production Users Group Permissions

User accounts associated with the Production Users application group are granted and denied the permissions through CA EEM policies. A summary of granted and denied permissions follows:

Granted permissions

Permissions that CA EEM grants to users who are assigned the Production Users group determine tab access and access within a tab.

Home tab

- Log in to CA Process Automation and use the Home tab - PAM40 User Login Policy.

Library tab

- View the Library tab - PAM40 LibraryBrowser Policy.
- Read access to the Library tab - PAM40 Environment Policy (prerequisite to PAM40 Object Policy).
- Navigate the folder structure in the Library tab and view automation objects listed in each folder - PAM40 Object Policy.

Operations tab

- View the Operations tab (all palettes) - PAM40 Operations Policy.
- Control the schedules displayed in the Operations tab - PAM40 Schedule Policy.
- Inspect any dataset displayed in the Dataset palette of the Operations tab - PAM40 Dataset Policy.
- Monitor or start any process displayed in the Operations tab - PAM40 Process Policy.
- Start and dequeue the start request form displayed in the Operations tab - PAM40 Start Request Form policy.

Configuration tab

- View the Configuration Browser (all palettes) - PAM40 Configuration Policy.

Reports tab

- View the Reports tab, generate reports, add new reports - PAM40 Reports Policy.

Denied permissions

Permissions that CA EEM does not grant to users who are assigned the Production Users group deny the ability to perform certain actions, or the access to certain tabs or palettes.

Library tab

- Control the library folders and their contents - PAM40 Environment Policy.
- Create, delete, or edit folders or access automation objects in their respective editors, where the process automation object editor is the Designer tab - PAM40 Object Policy.

Designer tab

- View the Designer tab - PAM40 Designer Policy.

Operations tab

- Modify any dataset displayed in the Dataset palette of the Operations tab - PAM40 Dataset Policy.
- Control a resources instance, that is, edit the displayed amount value - PAM40 Resources Policy.
- Control (debug) any process displayed in the Operations tab - PAM40 Process Policy.

Configuration tab

- Configure at the Domain level or select a menu option that requires locking the Domain - PAM40 Domain Policy.
- Configure at the Environment level or select a menu option that requires locking an environment - PAM40 Environment Policy.
- Install agents or Orchestrators - PAM40 Configuration Policy.
- Manage User Resources - PAM40 Configuration policy.

PAMUsers Group Permissions

User accounts associated with the PAMUsers application group are granted and denied the permissions through CA EEM policies. A summary of granted and denied permissions follows:

Granted permissions

Permissions that CA EEM grants to users who are assigned the PAMUsers group determine tab access and access within a tab.

Home tab

- Log in to CA Process Automation and use the Home tab - PAM40 User Login Policy.

Library tab

- View the Library tab - PAM40 LibraryBrowser Policy.
- Read access to the Library tab - PAM40 Environment Policy.

Operations tab

- View the Operations tab (all palettes) - PAM40 Operations Policy.

Reports tab

- View the Reports tab, generate reports, add new reports - PAM40 Reports Policy.

Denied permissions

Permissions that CA EEM does not grant to users who are assigned the PAMUsers group deny the ability to perform certain actions, or access certain tabs or palettes.

Library tab

- Control the library folders and their contents - PAM40 Environment Policy.
- Create, delete, or edit folders in the Library or access automation objects in their respective editors, where the process automation object editor is the Designer tab - PAM40 Object Policy.

Designer tab

- View the Designer tab - PAM40 Designer Policy.

Operations tab

- Control schedules - PAM40 Schedule Policy.
- Inspect or modify any dataset displayed in the Dataset palette of the Operations tab - PAM40 Dataset Policy.
- Monitor or start, or debug any process displayed in the Operations tab - PAM40 Process Policy.
- Control a resources instance, that is, edit the displayed amount value - PAM40 Resources Policy.

- Start and dequeue the start request form displayed in the Operations tab - PAM40 Start Request Form policy.

Configuration tab

- View the Configuration Browser - PAM40 Configuration Policy.

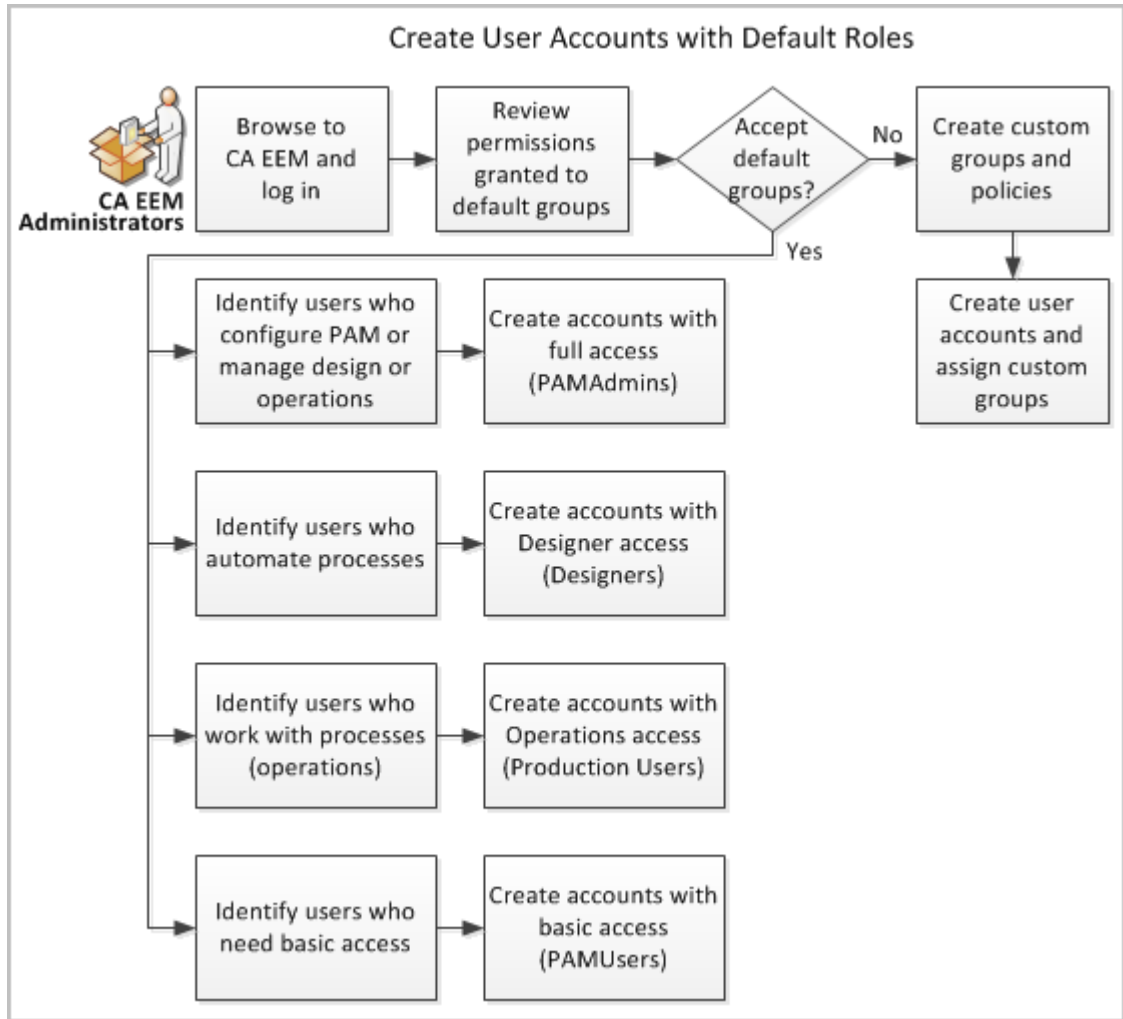
Note: When access to the tab is denied, all permissions that are related to the tab are also denied.

Create User Accounts with Default Roles

CA EEM Administrators use CA EEM to set up user accounts that are used for authentication. Administrators also use CA EEM to set up role-based views for authorization. Roles or groups for designers and production users grant permissions on folders in the Library tab, and on automation objects in the Designer tab and Operations tab.

An CA EEM administrator can set up all the user accounts and policies in CA EEM. Or, this user can [grant CA EEM access to selected administrators](#) (see page 78).

The task flow can be illustrated as follows:



1. [Browse to CA EEM and log in](#) (see page 43).
2. [Review permissions for default groups](#) (see page 45).
3. [Create user accounts for administrators](#) (see page 55).
4. [Creates user accounts for designers](#) (see page 56).
5. [Create user accounts for production users](#) (see page 57).
6. [Create user accounts with basic access](#) (see page 57).

Create User Accounts for Administrators

Administrators require full access to all CA Process Automation features. You can grant this access by associating the user accounts for administrators with the PAMAdmins group.

Follow these steps:

1. [Browse to CA EEM and log in](#) (see page 43).
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. Click Add Application User Details.
The pane refreshes to show the Application Group Membership section.
6. Select PAMAdmins from Available User Groups and click > to move it to Selected User Groups.
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) Complete the Global Group Membership field if you use CA Process Automation with another CA Technologies product that uses this CA EEM.
9. 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.
10. (Optional) Complete the remaining fields on the New User page.
11. Click Save, then click Close.
12. Click Log Out.

More information:

[Grant CA EEM Access to Selected Administrators](#) (see page 78)
[Change Your Own Password in CA EEM](#) (see page 44)

Create User Accounts for Designers

Create a user account for each designer who requires access to automation objects in CA Process Automation. Automation objects are used to automate processes.

Follow these steps:

1. [Browse to CA EEM and log in](#) (see page 43).
2. Click the Manage Identities tab.
3. Click New User.

The New User page opens.
4. Type the User ID to assign to the user account in the Name field.
5. Click Add Application User Details.
6. Select Designers from Available User Groups and click > to move it to Selected User Groups.
7. Enter the global user details.
8. Type and verify a password.

Users can change their own password in CA EEM.
9. (Optional) Complete the remaining fields on the New User page.
10. Click Save, then click Close.
11. Click Log Out.

Create User Accounts for Production Users

Create a user account for each production user who requires access to CA Process Automation to monitor and interact with automated processes.

Follow these steps:

1. [Browse to CA EEM and log in](#) (see page 43).
2. Click the Manage Identities tab.
3. Click New User.
The New User page opens.
4. Type the User ID to assign to the user account in the Name field.
5. Click Add Application User Details.
6. Select Production Users from Available User Groups and click > to move it to Selected User Groups.
7. Enter the global user details.
8. Type and verify a password.
Users can change their own password in CA EEM.
9. (Optional) Complete the remaining fields on the New User page.
10. Click Save, then click Close.
11. Click Log Out.

Create User Accounts with Basic Access

PAMUsers is a default group that you can assign to user accounts. You can assign PAMUsers to accounts you set up for users with restricted access. PAMUsers grants the use of the Home tab, the use of the Reports tab, and view-only access to the Library tab and the Operations tab. A user with only PAMUsers access can become familiar with CA Process Automation, but is not able to create or configure anything.

Follow these steps:

1. [Browse to CA EEM and log in](#) (see page 43).
2. Click the Manage Identities tab.
3. Click New User.
The New User page opens.
4. Type the User ID to assign to the user account in the Name field.
5. Click Add Application User Details and 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 own password.
8. (Optional) Complete the remaining fields on the New User page.
9. Click Save, then click Close.
10. Click Log Out.

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 43).
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: PAMAdminsThe 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 details about customizing this setting, see [Set Maximum Number of CA EEM Users or Groups](#) (see page 61).

User accounts from a referenced external user store are loaded as read-only records. If a new user needs an account, you 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 user access to CA Process Automation and its components, but the referenced user store manages authentication. Global users who are granted login access log on to CA Process Automation with the user name and password created in the referenced user store.

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

Consider the following approaches to managing access for users with accounts stored in an external user store.

- 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 those global groups.

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 and 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 allow login access to all global users in that global group. Add the group to the PAM40 Designer Policy to give access to the Designer tab.

- Create a dynamic group composed 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 allows all users in your AD to have full access to CA Process Automation without any configuration in CA EEM. While simple to implement, it lacks the security you gain from role-based access.

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

ou=Global Groups

More information:

[Assign an Application Group to a Global User](#) (see page 62)

[Create a Dynamic User Group Policy](#) (see page 64)

[Integrate Active Directory with CA EEM](#) (see page 65)

Set Maximum Number of CA EEM Users and Groups

When preparing to integrate a large referenced user store, verify that the user store does not contain more than 10,000 users and groups. The `eem.max.search.size` default value, 10000, is the threshold for the number of users and groups that CA Embedded Entitlements Manager can accept during transfer.

If you do not specify search criteria when search in CA Process Automation for available users and the following message appears, increase the threshold.

Maximum search limit exceeded.

Note: This threshold applies only when CA EEM is used as the directory server.

You can override the default threshold of 10000 in the `OasisConfig.properties` file by specifying a new value for the following parameter:

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

We recommend that you set this value to more than 2000.

To set the maximum number of CA EEM users or groups

1. Log on as an administrator to the server where the Domain Orchestrator is installed.
2. Stop the Domain Orchestrator, if it is running.
3. Navigate to the following folder, where *install_dir* refers to the path where the Domain Orchestrator is installed:

```
install_dir/server/c20/.config
```
4. Open `OasisConfig.properties` with an editor.
5. Use Find to locate the `eem.max.search.size` parameter or scroll to the end of the file.
6. Change the value from 10000 to an appropriate value.
7. Save the file and exit.
8. Restart the Domain Orchestrator.

Search for Identities Matching Specified Criteria

When you reference a large external user store, specify search criteria. Search criteria limits the returned global user account records to the one you need or a relevant subset.

To search for a global user account matching specified criteria

1. Log in to the CA Process Automation application in CA EEM.
2. Click Manage Identities.
3. Select Global Users in the Search Users pane.
4. Review the Attribute drop-down list to determine whether any listed attribute is assigned a value for the user or users you plan to search for.
 - If so, select an applicable attribute. For example, select Name.
 - If not, 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.

Assign an Application Group to a Global User

All users defined to CA EEM are global users. Global users include:

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

You can define a global user explicitly and assign an application group in the process of creating the global user account. If you reference an external user store, you can retrieve selected global user accounts individually and assign an application group to each account.

When you assign an application group to a global user, that user can perform all actions granted by policies containing that application group.

- Assigning the PAMAdmins application group to a global user gives that user full permissions in CA Process Automation.
- Assigning the Designers application group to a global user gives that user the permissions typically required for designing automated processes.
- Assigning the Production Users application group to a global user gives that user the permissions typically required for using automated process in a production environment.
- Assigning the PAMUsers application group to a global user gives that user minimal access rights in CA Process Automation.
- Assigning a custom group to a global user gives that user rights granted by the policies to which that custom group belongs.

To assign an application group to a global user from a referenced user store

1. Log in to the CA Process Automation application in CA EEM.
2. [Search for identities matching specified criteria](#) (see page 62).
3. Click the name of the target user displayed under Users.
The User account of the select user opens.
4. Click Add Application User Details to expand "Process Automation": User Details.
Application Group Membership dialog opens with Available User Groups populated and Selected User Groups blank.
5. Select the appropriate group for this global user from the Available User Group list. Click the right arrow to move that group to the Selected User Groups list.
6. (Optional) To apply CA EEM changes to CA Process Automation immediately, select the Configure tab, Session, Synchronize Cache.
7. Click Save.

The target global user can now log in to CA Process Automation with their global user name and password. At login, the user has access to the functionality granted to all members of the assigned application group.

Create a Dynamic User Group Policy

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

You can create a dynamic group composed of Users, Application Groups, Global Groups, or Dynamic Groups. For example, you can create a dynamic group of Global Groups or Application Groups based on Name, Description, or Group Membership. Or, you can create a dynamic 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.

To create a dynamic user group policy

1. Log in to the CA Process Automation application in CA EEM.
2. Click Manage Access Policies.
3. Click New Dynamic Group Policy to the left of Dynamic User Group Policies.
The New Dynamic Group Policy page appears.
4. For Name, enter a group name that indicates what this group of users has in common. Optionally, enter a description.
5. Select a policy type. The default is Access Policy.
6. Select Identities as follows:
 - a. For Type, select User, Application Group, Global Group, or Dynamic Group and click Search Identities.
 - b. For Attribute, Operator, and Value, enter the expression that sets the criteria for membership in this group and click Search. An example follows:
Select User, enter Job Title Like Manager and click Search. The result is all users who have the job title of Manager.
 - c. Select the identities who are to be members of this dynamic group. Click the Move arrow to move your selections to the Selected Identities list.
7. For Actions, select belong.
8. In the Add Resource field, enter the value you entered in the Name field and click the Add button. This action indicates that the selected identities belong to the dynamic group resource you created.
9. Optionally, add more filters.

10. Click Save.
11. Click the Dynamic User Group Policies link to view the dynamic user group you created.

Integrate Active Directory with CA EEM

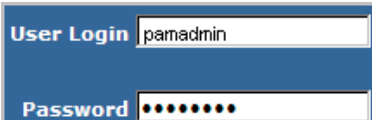
If your Active Directory users need access to CA Process Automation, point to AD as an external user store during the CA EEM installation.

You can manage user accounts that reference AD like any referenced user account. Alternatively, you can also use the following approach to accomplish the integration from within Active Directory.

To integrate CA EEM with Active Directory from Active Directory

1. Create an Organizational Unit (OU) for all CA Process Automation users and groups.
2. Create PAMAdmins as a global security group.
3. Create PAMUsers as a local security group.
4. Make PAMAdmins a member of PAMUsers.
5. Create a user with the name pamadmin.
6. Make the pamadmin user a member of both groups.

This approach provides a single login to CA Process Automation with the pamadmin/pamadmin credentials that are predefined for the default pamadmin user. This login provides full access to all CA Process Automation functionality. In the following example, pamadmin was entered as the password:



The image shows a login interface with two input fields. The first field is labeled 'User Login' and contains the text 'pamadmin'. The second field is labeled 'Password' and contains a series of ten black dots, indicating that the password is hidden.

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:

- [Permissions Reference](#) (see page 67)
- [Granting Administrators Access to CA EEM](#) (see page 76)
- [Customizing User Access with CA EEM Policies](#) (see page 79)
- [How to Transition Roles Used in Active Directory to CA EEM](#) (see page 98)
- [Touchpoint Security with CA EEM](#) (see page 103)
- [Authorizing Runtime Actions with CA EEM](#) (see page 117)

Permissions Reference

For your convenience, tables are provided listing all permissions and dependencies. Topics follow:

- [Permissions by tab](#) (see page 68).
- [Permissions dependencies](#) (see page 72).
- [Filters for permissions](#) (see page 75).

Permissions by Tab

Selected actions on predefined CA EEM policies grant permissions to tabs, palettes, folders, and automation objects. The following tables describe the permissions that each of these actions grants to groups (identities) in the corresponding policies. You can create a policy where an action is not selected for a specified group. When a user in that group logs in, the feature that is associated with the unselected action is unavailable.

If you create custom policies from these resource classes, use this table 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 permissions are ordered from the lowest to the highest permission. To view the Library tab, you must have LibraryBrowser_User permission and either Environment_Library_User or Environment_Library_Admin permission. See [Permissions Dependencies](#) (see page 72) for details.

Action Key (Localized Name)	Resource Class for Policy	Permissions
LibraryBrowser_User (Library Browser User)	LibraryBrowser (Library Browser)	View access to the Library tab.
Object_List (List)	Object	View folder or automation object in the Library Browser. Define customized views of the library.
Environment_Library_User (User)	Environment	Access to Orchestrators added to environments. View, export, search automation objects in the Library tab if the access is set. Prerequisite to many permissions on the Operations tab.
Object_Read (Read)	Object	Navigate through a folder path and open any automation object in the corresponding designer/viewer. <i>Implicit:</i> List

Action Key (Localized Name)	Resource Class for Policy	Permissions
Object_Edit (Edit)	Object	Edit a folder or an automation object in a folder. <i>Implicit:</i> Read, List
Object_Delete (Delete)	Object	Delete a folder or delete an automation object added to a folder. <i>Implicit:</i> Edit, Read, List
Object_Admin (Admin)	Object	Create a folder or any automation object. <i>Implicit:</i> Delete, Edit, Read, List.
Environment_Library_Admin (Content Administrator)	Environment	Create, Delete, Edit, Read, and List on all automation objects in the Library tab.

Design Tab

Users with access to the Design tab typically are granted access to the Library tab. Minimally, designers need the following Library tab permissions to be able to save a process they are designing: LibraryBrowser_User, Environment_Library_User, and Object_Edit (which includes Object_List, and 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 need access to the Operations tab in the design environment; production users need access to the Operations tab in the production environment. To view the Operations tab, you must have either Environment_Library_User or Environment_Library_Admin permission. See [Permissions Dependencies](#) (see page 72) for details.

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.

Action Key (Localized Name)	Resource Class for Policy	Permissions
Process_Monitor (Monitor)	Process	Open a running instance of a process in the Process Designer, monitor progress, and set breakpoints. <i>Implicit:</i> List
Process_Start (Start)	Process	Start an instance of a process. <i>Implicit:</i> Monitor, List
Process_Control (Control)	Process	Suspend, restart, resume, or abort instances of a process. <i>Implicit:</i> Start, Monitor, List
Operations_Schedules (Schedules)	Operations	Can view Active Schedules link in the Operations tab.
Agenda_Control (Control)	Agenda	Activate and deactivate a schedule on a touchpoint. <i>Implicit:</i> Read, List
Operations_Datasets (Datasets)	Operations	Open the Datasets palette in the Operations tab.
Dataset_Inspect (Inspect)	Dataset	View a dataset object and read values of variables in the dataset. <i>Implicit:</i> List
Dataset_Modify (Modify)	Dataset	Create, Edit, and Delete the dataset object. <i>Implicit:</i> Inspect, Read, List
Operations_Resources (Resources)	Operations	Open the Resources palette in the Operations tab.
Resources_Control (Control)	Resources	Lock unlock, take, return, or add a parameter to a resource. Add or remove a resource unit. <i>Implicit:</i> Read, List
Operations_User_Requests (User Requests)	Operations	Open the User Requests palette in the Operations tab.

Action Key (Localized Name)	Resource Class for Policy	Permissions
Operations_Task_List (Task List)	Operations	Use the Task List link in the Operations tab and view tasks for yourself, your group, or any group and access your own tasks from the Home tab.
StartRequestForm_Dequeue (Dequeue)	Start Request Form	Dequeue a process that was placed in the queue by a start request form. <i>Implicit:</i> Start, List
StartRequestForm_Start (Start)	Start Request Form	Start a task that a start request form defines. <i>Implicit:</i> List
Execute	TouchPoint Security	Execute scripts or programs within operators. The impacted operators are derived from specified operator categories. The impact occurs when the target is a specified touchpoint in a specified environment.

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

Administrators perform installation, configuration. Other user can have view access.

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

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

More information:

[Permissions Dependencies](#) (see page 72)

Permissions Dependencies

The following table describes the dependent resource class action (permission) for each resource class action on the predefined CA EEM policies for CA Process Automation. If you use custom groups alone rather than supplementing PAMUsers, consider the dependencies when you assign actions to custom groups in default or custom policies.

You can assign an action listed in column 1 in a custom policy for a resource class listed in column 2 to a custom group. If you create such a custom policy, assign that custom group to the dependent actions listed in column 3.

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)

Action Key (Localized Name)	Resource Class for Custom Policy	Dependent Actions Key (Localized Name)
Environment_Library_User (User)	Environment	Console_Login (User)
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 Agent Resources and 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)

Action Key (Localized Name)	Resource Class for Custom Policy	Dependent Actions Key (Localized Name)
Operations_Schedules (Schedules)	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 <i>/folder</i> Note: If object is created in the root folder, Object_List is not needed.
Dataset_Inspect (Inspect) Dataset_Modify (Modify)	Dataset	Console_Login (User) Environment_Library_User (User) Object_List (List) with resource <i>/folder</i> Note: If object is created in the root folder, Object_List is not needed.
Process_Control (Control) Process_Monitor (Monitor) Process_Start (Start)	Process	Console_Login (User) Environment_Library_User (User) Object_List (List) with resource <i>/folder</i> Note: If object is created in the root folder, Object_List is not needed.
Resources_Control (Control)	Resources	Console_Login (User) Environment_Library_User (User) Object_List (List) with resource <i>/folder</i> Note: If object is created in the root folder, Object_List is not needed.
StartRequestForm_Start (Start) StarRequestForm_Dequeue (Dequeue)	Start Request Form	Console_Login (User) Environment_Library_User (User) Object_List (List) with resource <i>/folder</i> Note: If object is created in the root folder, Object_List is not needed.

Action Key (Localized Name)	Resource Class for Custom Policy	Dependent Actions Key (Localized Name)
Execute	Touchpoint Security	Console_Login (User) Console_Client_Launch (CA Process Automation Client) Environment_Library_User (User) Object_List (List) with resource <i>/folder</i> Note: If object is created in the root folder, Object_List is not needed.

More information:

[Permissions by Tab](#) (see page 68)

Filters for Permissions

Permissions in CA EEM are defined as Resource Class actions. You can limit certain actions you grant to a group or user with filters. When you define a filter, you select a valid named attribute and enter a value.

The actions in the following table belong to policies based on the associated resource class. If you assign an Action to a custom group, you can create a filter with the corresponding named attribute and assign a value.

Action Key (Localized Name)	Resource Class for Policy	Named Attribute for Filter
Operations_Process_Watch (Process Watch)	Operations	ENVIRONMENT TOUCHPOINT
Operations_Schedules (Schedules)	Operations	ENVIRONMENT TOUCHPOINT
Operations_User_Requests (User Requests)	Operations	ENVIRONMENT TOUCHPOINT
Object_List (List)	Object	SECURITY_CONTEXT_ID
Object_Read (Read)		SECURITY_CONTEXT_GRP
Object_Edit (Edit)		ENVIRONMENT
Object_Delete (Delete)		OBJECT_TYPE
Object_Admin (Admin)		
Agenda_Control (Control)	Agenda	ENVIRONMENT

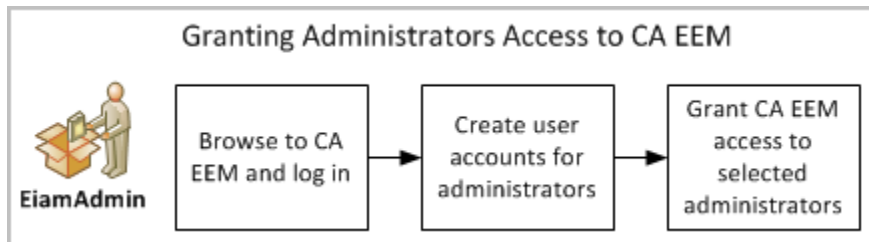
Action Key (Localized Name)	Resource Class for Policy	Named Attribute for Filter
Dataset_Inspect (Inspect) Dataset_Modify (Modify)	Dataset	ENVIRONMENT
Process_Control (Control) Process_Monitor (Monitor) Process_Start (Start)	Process	SECURITY_CONTEXT_ID SECURITY_CONTEXT_GRP ENVIRONMENT
Resources_Control (Control)	Resources	ENVIRONMENT
StartRequestForm_Start (Start) StarRequestForm_Dequeue (Dequeue)	Start Request Form	ENVIRONMENT
Execute	TouchPoint Security	ENVIRONMENT TOUCHPOINT

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 43).
2. [Create user accounts for administrators](#) (see page 55).
3. [Grant CA EEM access to selected administrators](#) (see page 78).

More information:

[Grant CA EEM Access to Selected Administrators](#) (see page 78)

Grant CA EEM Access to Selected Administrators

By default, the EiamAdmin user is the only user who can log in to CA EEM. You need CA EEM access to manage user accounts, groups, and policies. The EiamAdmin user can grant this ability to one or more additional administrators and specify the objects that those administrators can manage. The process includes defining a new group, creating a custom policy for this group, and then assigning the new group to user accounts.

Follow these steps:

1. [Browse to CA EEM and log in](#) (see page 43).
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. Add a description.
 - e. Do not select an Application Group.
 - f. Click Save.
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 such as Administer Users and Policies, then click OK.
 - e. Select [User] EiamAdmin and [User] CERT-Process Automation from the Selected Identities list, and then click Delete.
 - f. Click Search Identities for Type Group and click Search.
 - g. Select the new group, EEMAdmins and click the right arrow to move that user group (ug) to Selected Identities.
 - h. Select and delete all of the resources except ApplicationInstance, Policy, User, UserGroup, GlobalUser, GlobalUserGroup, and Folder.
 - i. Verify that the read and write actions are selected.
 - j. Click Save.

Your policy resembles the following example:

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 individual administrators.
 - a. Click Manage Identities.
 - b. Click Application User Details for Search Users. Select Group Membership as attribute, LIKE as Operator, and PAMAdmins as Value. Click Go.

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

The user account of that administrator opens. EEMAdmins is displayed as an available user group.
 - d. Move EEMAdmins to Selected User Groups.
 - e. Click Save.
 - f. Repeat for each administrator to whom you want to grant CA EEM privileges.

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.

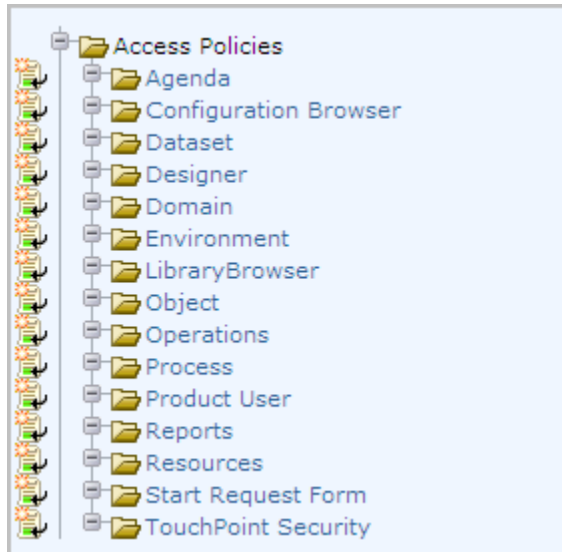
You can restrict user access to specified folders. For example, you can create a folder for each designer and restrict designers access to their own folder and folders designed for common use.

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.

Default Resource Classes and Custom Policies

CA Process Automation Resource Classes are listed under Access Policies in CA EEM. You can create a custom policy for any resource class. You can create custom policies from scratch or based on a predefined policy.



Predefined policies exist for the CA EEM resource classes.

You can save the predefined Access Policies under a new name, using Save As, and customize as needed. Creating custom policies based on the predefined policies helps you achieve changes such as the following:

- Provide the assigned group additional access not granted by the predefined policy. For example, your custom policy can grant the Designers group access to the Installation palette on the Configuration tab so that they can install agents.
- Remove access granted to an assigned group by the predefined policy. For example, your custom policy can remove permission for members of the PAMUsers group to access the Reports tab.
- Replace a default group, such as PAMAdmins, with groups that better reflect the CA Process Automation roles defined at your site. For example, you may want to reserve PAMAdmins for your Domain administrator and create separate environment administrator group for each environment. See [Create User Accounts with Custom AD Roles](#) (see page 98) for details on how to create separate access rights for Content Administrators and Configuration Administrators.
- Add filters to create 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 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 Start or Control rights, 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 invokes the "Execute Start Request Form" method has Start or Dequeue permissions, the method runs successfully. If the user who invokes the method does not have execute rights on the target object, the method fails. Method failure is reported with a message in the SOAP operator dataset.

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

Typical objectives include:

- Limit access to a specified environment with the Agenda, Dataset, System, Process, Resources, Start Request Form, 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 name of the Environment:

Left type/value	Operator	Right type/value
named attribute	STRING	value
Environment	EQUAL ==	Test

- Limit access to a specified Folder or specified 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.

Resources	Actions
Add resource: <input type="text"/>	Object_List (List) Object_Read (Read) Object_Edit (Edit) Object_Delete (Delete) Object_Admin (Admin) [All Actions]
<input type="text" value="/folder_name"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>

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 example, the Object Type is set to Package.

Left type/value	Operator	Right type/value
named attribute	STRING	value
Object Type	EQUAL ==	Package

You can specify any of the following for Object Type values:

- The resource classes:
 - Agenda, the resource class for Schedule.
 - Dataset
 - Process
 - Resources
 - Start Request Form
- Calendar
- Custom Icon
- Custom Operator
- Folder
- Interaction Request Form
- Package
- 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 45).
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 on Tabs and Palettes](#) (see page 68).
 - If the permission is on an automation object, see [Permissions on Automation Objects](#).
4. [Create a policy based on an existing policy](#) (see page 84), where the existing policy is a predefined, default policy.
5. [Grant or revoke an action for a default group](#) (see page 84).

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 43).
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 85).

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. If you want users who belong to the Designers group to be able to install agents on their hosts, you can add that ability. Check Configuration_Installations (Installations) for Designers on the PAM40 Configuration Policy.

General			
Folder:			
Name: PAM40 Configuration Policy			
Selected Identities			
Identities		Actions	
		Client_Configuration_User (View Configuration Browser)	
		Configuration_Installations (Installations)	
		Configuration_User_Resources (User Resources)	
[Default]		<input type="checkbox"/>	<input type="checkbox"/>
PAMAdmins		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Designers		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Production Users		<input checked="" type="checkbox"/>	<input type="checkbox"/>

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	<pre> WHERE ((ug:Name == val:Designers AND req:action {} val:Control AND name:Environment == val:Default Environment) OR (ug:Name == val:Production Users AND req:action {} val:Control AND name:Environment == val:Production Environment)) </pre>

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 98).

Create a Custom Group

You can create a custom application user group in CA EEM. You grant that group rights by adding the group to policies and selecting appropriate actions. Then you assign that group to individual user accounts.

Note: The policies to which a custom group must be added depend on whether the group supplements the PAMUsers group.

Follow these steps:

1. [Browse to CA EEM and log in](#) (see page 43).
2. Click the Manage Identities tab.
3. Click Groups.

The Groups panel opens.

4. Click the icon next to Application Groups to create a New Application Group.
5. Enter a name for the group and optionally a description.
6. Skip the Application Group Membership selection.
7. Click Save.

The new group appears for selection as an application user group when you define new users.

8. (Optional). Select Show application groups under Search Groups and click Go.
Your new group displays with other existing groups including the default groups.
9. 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 43).
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 43).
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 what a specified CA Process Automation user can see and do. You can create CA EEM rules such that a user can only see or use one automation object instance or one automation object. For example, you can create rules such that a user has access to one dataset or can access only datasets. This assumes you create a folder structure based on object types, either from the root folder or within a folder subordinate to the root folder.

Follow these steps:

1. [Set up the folder structure with different object types in separate folders](#) (see page 92).
2. [Create a user account with no group assignment](#) (see page 93).
3. [Add the user to required default policies](#) (see page 94).
4. Add the user to the default Operations policy.
5. [Create a custom Object policy with path permissions](#) (see page 96).
6. [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 what you expect.

Set up Designer-Specific Folders

You can design the folder structure at your discretion. If you plan fine-grained access, design your folder structure such that you can specify a path to objects of a given type in the policy for that automation object. For example, if you want to restrict an individual (or group) to specified object types or to specified object types within specified projects, you can set up a folder structure that makes this type of restriction possible.

Example paths follow, where object1 represents any type of automation object, such as process or dataset.

- /designer1/object1 - each designer has a separate folder. Within each designer folder is a set of folder, one per type of automation object that developer works on. A folder for dataset can include datasets for multiple projects developed by a single designer.
- /project1/designer1/object1 - each project has its own folder, with a subfolder for each designer on the project. Each designer folder within the project includes a subfolder for each automation object type that designer develops for this project.

You can create a three-tiered folder structure.

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 select Folder. Enter a short name or code for one of your planned projects. Repeat this step for each of your planned projects.
4. Select the folder for the first project, click New and select Folder. Enter the user ID of a designer assigned to this project. Repeat this step for each designer.
5. Repeat the preceding step for each project.
6. Select the folder for the first designer on the first project, click New and select Folder. Enter the name of an automation object that this designer develops for this project. Repeat this step for each automation object that this designer develops for this project.
7. Repeat the preceding step for each designer on this project.
8. Repeat the preceding two steps for each project.

Note: Consider the following folder structures if you do not want to limit access for an individual:

- /object1 - each folder under root represents a different type of automation object. All developers in all project who develop objects of this type work in this folder.
- /designer1 - each folder under root represents a different designer. Each designer develops all objects for all projects within their own folder

- /project1 - each folder under root represents a different project. All designers working on a given project work in the folder for that project and develop all automation objects required by that project in the project folder.

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 43).
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:

[Grant CA EEM Access to Selected Administrators](#) (see page 78)
[Change Your Own Password in CA EEM](#) (see page 44)

Add the User to Required Default Policies

When you create a user account with no group assignment, you must give the user basic access to CA Process Automation. For this scenario, basic access is provided by adding the user account name to the following policies and actions.

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

After giving the user navigation access to folders on the Library tab, grant access to the Operations tab. Select the object for which the restriction applies. Datasets and Resources are examples. The action you select depends on the object to which the user is restricted.

Follow these steps:

1. [Browse to CA EEM and log in](#) (see page 43).
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. Click Search Identities with Type set to User.
 - d. Click Search. Select the user identifier from the displayed list and click the down arrow.
 - e. Select Console-Login (User) for the user you added.
 - f. Click Save. 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. Click Search Identities with Type set to User.
 - d. Click Search. Select the user identifier from the displayed list and click the down arrow.
 - e. Select Environment_Library_User (User) for the user you added.
 - f. Click Save. 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. Click Search Identities with Type set to User.

- d. Click Search. Select the user identifier from the displayed list and click the right arrow.
 - e. Select LibraryBrowser_User (Library Browser User) for the user you added.
 - f. Click Save. Click Close.
6. Add the user to the PAM40 Operations Policy.
- a. Click the link for Operations under Access policies.
 - b. Click the PAM40 Operations Policy link in the Policy Table.
 - c. Click Search Identities with Type set to User.
 - d. Click Search. Select the user identifier from the displayed list and click the down arrow.
 - e. Select Operations_Datasets (Datasets) for the user you added.
 - f. Select Operations_Resources (Resources) for the user you added.
 - g. Click Save. 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 43).
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 67) section.

Follow these steps:

1. [Browse to CA EEM and log in](#) (see page 43).
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.

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 Granted to Default Groups](#) (see page 45).
- Point to AD as an external user store.
Note: See [Manage Access for Referenced User Accounts](#) (see page 59). See [Integrate Active Directory with CA EEM](#) (see page 65).
- 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.

Security settings of Domain	
Domain Administrator	ITPAMAdmins
CA Process Automation User	ITPAMUsers
Environment Configuration Administrator	ConfigAdmin
Environment Content Administrator	ContentAdmin
Environment User	EnvironmentUser

Use the following process to manually migrate role-based access from Active Directory to CA EEM:

1. Migrate role-based access for users in the Domain Administrator role.
See [Create User Accounts for Administrators](#) (see page 55).
2. Migrate role-based access for users in the CA Process Automation User role.
See [Create User Accounts with Basic Access](#) (see page 57).
3. Migrate role-based access for users in the Environment Configuration Administrator role as follows:
 - a. [Create the custom ConfigAdmin group](#) (see page 99).
 - b. [Grant permissions to the custom ConfigAdmin group](#) (see page 100).
 - c. [Create user accounts for Environment Configuration Administrators](#) (see page 101).
4. Migrate role-based access for users in the Environment Content Administrator role as follows:
 - a. [Create the custom ContentAdmin group](#) (see page 101).
 - b. [Grant permissions to the custom ContentAdmin group](#) (see page 102).
 - c. [Create user accounts for Environment Content Administrators](#) (see page 102).
5. Migrate role-based access for users in the Environment User role.
See [Create User Accounts for Production Users](#) (see page 57).

Create the Custom ConfigAdmin Group

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

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. Create the Environment Configuration Administrators group:
 - a. Click New Application Group.
 - b. Enter ConfigAdmin as the name of the group and optionally a description
 - c. Do not add an application group membership.
 - d. Click Save.
5. 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. Log in to the CA Process Automation application in CA EEM.
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 43)
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:

[Approach to Configuring Touchpoint Security](#) (see page 131)

[Configure Touchpoint Properties](#) (see page 201)

[Configure Orchestrator Touchpoint Properties](#) (see page 153)

[Configure Environment Properties](#) (see page 142)

[Configure Domain Properties](#) (see page 129)

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.

Access Control List Configuration			
Resources	Actions	Filters	
Add resource: ApplicationInstance	read write		
<input type="checkbox"/> ApplicationInstance	<input checked="" type="checkbox"/> <input type="checkbox"/>	value	STRING value EQUAL ==
<input type="checkbox"/> Policy	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	named attribute ResourceClassName	STRING value EQUAL == TouchPointSecurity

- 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.

Access Control List Configuration			
Resources	Actions	Filters	
Add resource:			
ApplicationInstance	read write		
<input type="checkbox"/> ApplicationInstance	<input checked="" type="checkbox"/> read <input type="checkbox"/> write		
<input type="checkbox"/> Policy	<input checked="" type="checkbox"/> read <input checked="" type="checkbox"/> write	named attribute: ResourceClassName == value: TouchPoint Security	
<input type="checkbox"/> User	<input checked="" type="checkbox"/> read <input type="checkbox"/> write		
<input type="checkbox"/> GlobalUser	<input checked="" type="checkbox"/> read <input type="checkbox"/> write		
<input type="checkbox"/> UserGroup	<input checked="" type="checkbox"/> read <input type="checkbox"/> write		
<input type="checkbox"/> GlobalUserGroup	<input checked="" type="checkbox"/> read <input type="checkbox"/> write		
<input type="checkbox"/> Treat resource names as regular expressions			

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.

Scoping Policies			
Name/Description	Actions	Resources	Filters
Users Defining Touchpoint Security Policies Enables specified users to create custom policies only with the TouchPoint Security resource class.	read write	ApplicationInstance Policy GlobalUser User UserGroup GlobalUserGroup	WHERE (req:resource == val:ApplicationInstance ApplicationInsta AND req:action { } val:read) ApplicationInsta OR (req:resource == val:Policy Policy AND req:action { } val:read,write Policy AND name:ResourceClassName == val:TouchPoint Security) Policy OR (req:resource == val:GlobalUser GlobalUser AND req:action { } val:read) GlobalUser OR (req:resource == val:User User AND req:action { } val:read) User OR (req:resource == val:UserGroup UserGroup AND req:action { } val:read) UserGroup OR (req:resource == val:GlobalUserGroup GlobalUserGrou AND req:action { } val:read) GlobalUserGrou

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]	<input checked="" type="checkbox"/> 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 111).

A process with an operator target protected by a Touchpoint Security policy can finish successfully only if 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.

More information:

[Grant Users CA EEM Access to Define Touchpoint Security Policies](#) (see page 103)

[Create a Touchpoint Security Policy](#) (see page 112)

Use Cases: When Touchpoint Security is Needed

Touchpoint security is needed in cases such as the following:

- 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:

- The host with an agent associated with a touchpoint.
- The host with an agent associated with a proxy touchpoint with an SSH connection to a remote host.
- The host with an agent associated with a host group that references and has a connection to remote hosts.

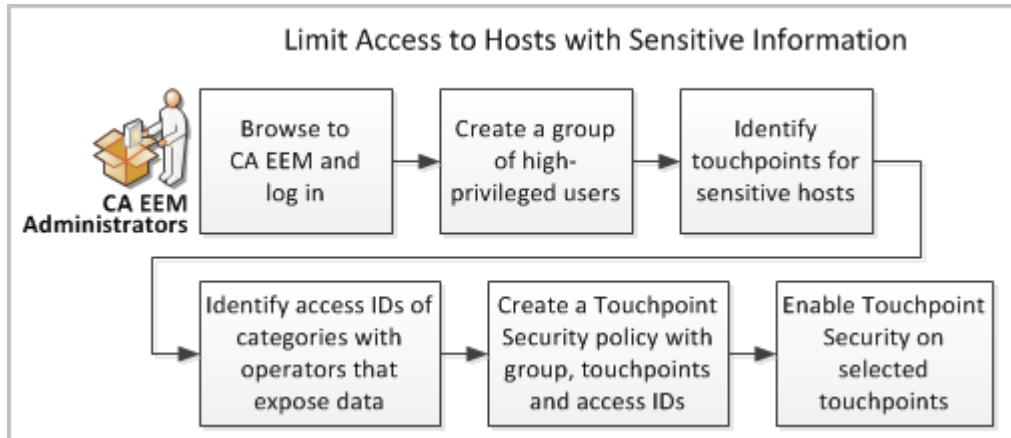
- Consider the case where you are running an agent on a host as root (Unix) or administrator (Windows) or some user with certain rights. Suppose you have a reason to run all scripts and programs on that agent under the same identity as the agent itself. That is, you do not want to switch to another user that requires credentials. You want to prevent a security risk by disallowing low-privileged users from running any script under the same identity as the agent, such as root.
- Consider the case where you are leveraging host groups which define default operating system credentials for executing Command Execution operators on entire subnets. Suppose 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 execute a process can select operator targets at runtime for operators designed with a variable in the target field. An operator target is typically a touchpoint, although it can be a proxy touchpoint or an FQDN or IP address referenced by a host group. This flexible design allows any user who is authorized to execute the process to select a target at runtime.

A security problem occurs when an available touchpoint requires limitations placed on 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 Service Desk designed for general access while the other touchpoint is designed for administrators only. Touchpoint Security helps ensure that only administrators can run this example operator on the touchpoint 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 executing operators on their local hosts. Touchpoint Security can provide this protection. When Touchpoint Security is configured to be active, authorization to execute each operator on the selected target is verified at runtime. Policy enforcement helps ensure that users who run a process can execute 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 diagram suggests an approach to accomplish this security goal.



Example Sequence

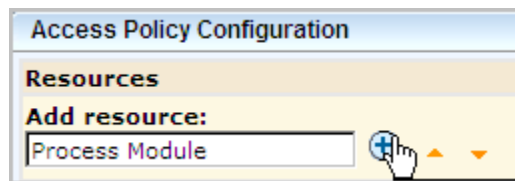
1. [Browse to CA EEM and log in](#) (see page 43).
2. Create a group of high-privileged users.
See [Create the Custom ContentAdmin Group](#) (see page 101).
3. Identify touchpoints associated with sensitive hosts.
See [View the Touchpoints and Host Groups for a Selected Agent](#) (see page 188).
4. Identify categories with operators that can make changes. Then, identify the Access Control IDs associated with these categories.
 - See [Example: Secure Critical Touchpoint](#) (see page 114)s for Access Control IDs to consider.
 - Find descriptions of each category in the section [Operator Category Support by Orchestrators and Agents](#) (see page 298).
 - See the *Content Designers Reference* for operator descriptions.
5. Create a Touchpoint Security policy with this group, operator categories, and touchpoints.
See [Create a Touchpoint Security Policy](#) (see page 112).
6. Enable Touchpoint Security on selected touchpoints.
 - See [Configure Touchpoint Properties](#) (see page 201).
 - See [Configure Proxy Touchpoint Properties](#) (see page 218).
 - See [Configure Host Group Properties](#) (see page 229).

More information:

[Approach to Configuring Touchpoint Security](#) (see page 131)

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. Rather, you identify the categories to which those operators belong. You identify the categories, not by name, but rather by their Access Control IDs.



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.
2. Click the Configuration tab.
3. Select an agent from the Agents node and then select the Modules tab.
4. Take note of 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. Use this list as a reference when you enter selected module names in the Resources field in a Touchpoint Security policy.

Create a Touchpoint Security Policy

Running a process executes specific operators on specified targets in a specified sequence. A custom Touchpoint Security policy grants permission to specified users or groups to execute specified operators on specified targets.

To create a Touchpoint Security policy

1. [Browse to CA EEM and log in](#) (see page 43).
2. Click the Manage Access Policies tab.
3. Click the New Access Policy button for Touchpoint Security under Access policies.
The new access policy form for the Touchpoint Security resource class appears.
4. 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 access is being granted as follows:
 - 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 PAMUsers.
6. Click Search Identities.
The list of identities matching your search criteria appear.
7. Select the identities to which this policy applies and 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 associated with the Source Operator Category that includes the operators to which this policy applies. Then, click Add. For example:

Access Control ID	Source Operator Category
Process Module	Command Execution
File Module	File Management
File Transfer Module	File Transfer
Network Utilities Module	Network Utilities

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

10. Add a filter to specify the environment containing the targets to which this policy applies.
 - Named attribute is Environment.
 - STRING operator is EQUAL.
 - Value is *environment_name*.
11. Add other filters to specify the targets by touchpoint name, that is, Touchpoint EQUAL *touchpoint name*.
12. Save the policy.

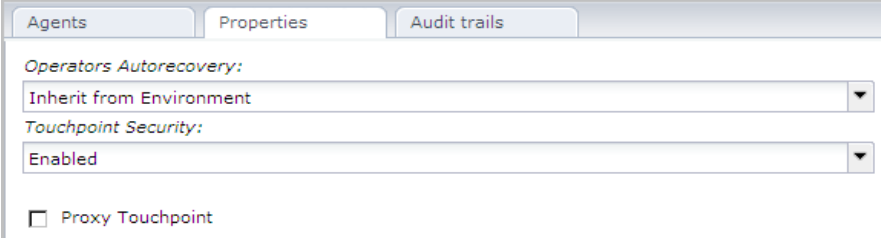
If policies on Touchpoint Security are configured for enforcement, the policy is evaluated and enforced.

Example: Secure Critical Touchpoints

Touchpoint security helps ensure that execution of 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, each attempt to execute an operator on this touchpoint is evaluated against Touchpoint Security policies.



The screenshot shows a configuration window with three tabs: Agents, Properties, and Audit trails. The Properties tab is active. It contains the following settings:

- Operators Autorecovery:** A dropdown menu set to "Inherit from Environment".
- Touchpoint Security:** A dropdown menu set to "Enabled".
- Proxy Touchpoint

Example: Touchpoint Security Policy for Critical Touchpoints

To help ensure that only high-privileged users execute 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 filters for touchpoints that reference sensitive hosts. Consider the following example Global Touchpoint Security Policy. The example policy grants the High-Privileged Users group authorization to execute 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

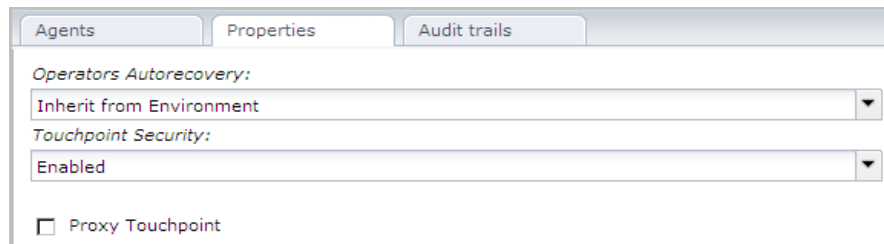
Example: Secure the Touchpoint for My Host

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 Dependencies](#) (see page 72)

[Filters for Permissions](#) (see page 75)

Change Ownership for Automation Objects

The owner has full control of an automation object or folder. You must be logged in to CA Process Automation as the owner or the Environment Content Administrator to change ownership of an automation object. The user who creates an automation object is, by default, its owner. If you set ownership of a folder to a user who is not an administrator, that user is the only non-administrator who can access that folder.

Ownership of a process is used when Runtime Security is enabled. If you enable Runtime Security, then only the owner you set for a given process can start that process.

Follow these steps:

1. Click the Library tab.
2. Select one or more objects including folders.
3. In the toolbar, click Set Owner.
The Set Owner dialog opens.
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 and Unlock the Domain](#) (see page 119)

[Configure the Contents of the Domain](#) (see page 119)

[Maintain the Domain Hierarchy](#) (see page 132)

Lock and Unlock the Domain

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

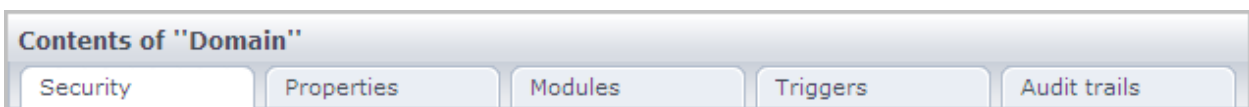
Follow these steps:

1. [Browse to CA Process Automation and log in](#) (see page 18).
2. Click the Configuration tab.
3. Expand the Configuration Browser palette.
4. Select the Domain and click Lock.

As soon as you complete configuration changes, unlock the Domain. Select the 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 122).
- Properties
See [Configure Domain Properties](#) (see page 129).
- Modules
See [Configuring Operator Categories](#) (see page 244). 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 300). This topic is followed by configuration details for each trigger type.
- Audit Trails
See [View the Audit Trail for the Domain](#) (see page 329).

More information:

[Maintaining the Domain](#) (see page 347)

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

CA Process Automation uses CA EEM for user authentication and authorization.

Before you install CA Process Automation, you install CA Embedded Entitlements Manager (CA EEM). When you install CA Process Automation, the CA Process Automation application registers with CA EEM. Registration populates CA EEM with predefined policies and predefined groups. Each predefined group has a predefined CA Process Automation user. A certificate file helps ensure successful connectivity between CA Process Automation and CA EEM.

Important! To put into effect any security setting changes you make at the Domain level, restart *each* affected Orchestrator in the Domain. Orchestrators for which Domain level security settings have been overridden at the environment or Orchestrator levels are unaffected.

The CA EEM security settings appear on the Security tab for the Domain. Typically, the only setting you modify is the setting controlling the frequency of updating CA Process Automation with CA EEM changes.

Follow these steps:

1. Click the Configuration tab.
2. Select the Domain node and click Lock.
3. Click the Security tab.

The Security tab displays the security settings of the Domain in fields that you can edit.

4. Examine the security settings.

FIPS-compliant certificate

Specifies whether the algorithms used to encrypt data that is transferred between CA EEM and CA Process Automation are 140-2 compliant.

Selected - Indicates that 140-2 compliant algorithms are used. CA EEM is configured to operate in FIPS mode.

Cleared - Indicates that MD5 algorithms are used.

CA EEM Backend Server

The name of the computer hosting the CA EEM server.

CA EEM Application Name

When you register the CA Process Automation application with CA EEM, specify a parameter named Application Name. The application is registered with CA EEM using this name.

Default: Process Automation

CA EEM Certificate Name

The name of the CA EEM certificate is required for CA Process Automation to connect to CA EEM. During installation, one of the following certificates is uploaded.

- PAM.p12 if you cleared the FIPS-compliant certificate setting.
- PAM.pem if you selected the FIPS-compliant certificate setting.

CA EEM Certificate Password

During registration, a password is provided if FIPS mode is not selected. This password is required to connect to the CA EEM server.

CA EEM Certificate Key

During registration, a certificate key is provided if CA EEM FIPS mode is selected.

CA EEM Cache Update Interval (in seconds)

Specifies the frequency in seconds that CA EEM updates CA Process Automation with CA EEM changes to CA Process Automation user accounts, groups, and policies. CA Process Automation uses the information stored in the cache between updates.

Note: Reducing the update interval when you are testing and refining custom policies makes this task go more quickly.

Default: 1800 seconds

Minimum value: 60 seconds

5. Make the required changes to the security settings.
6. Click Save.
7. Right-click the Domain, and select Unlock.
8. Take the following actions if you make certificate changes:
 - a. Verify that the password of the certificate of new application matches the old CA EEM Certificate Password value.
 - b. Put the new certificate under the public/certification folder.
`install_dir\server\c2o\.c2orepository\public\certification`
9. If you changed the configuration, restart each affected Orchestrator in the Domain.
 - [Stop the Orchestrator](#) (see page 172).
 - [Start the Orchestrator](#) (see page 173).

Note: Changing the FIPS-compliant certificate setting requires a manual procedure. For details about this procedure, see [Change the CA EEM FIPS Mode Security Setting](#) (see page 124).

More information:

[Control Frequency of Updating CA Process Automation with CA EEM Changes](#) (see page 20)

[Manage Certificates](#) (see page 350)

[Start the Orchestrator](#) (see page 173)

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 used to encrypt data 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.

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 also impacts 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.

To change the FIPS-compliant certificate security setting

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), do the following: Replace PAM.cer and PAM.key with PAM.p12 and a password.

Note: For details, see [Use the iGateway Certificate Utility \(igwCertUtil\)](#) (see page 127).
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 172).
 - [Start the Orchestrator](#) (see page 173).

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 that level (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.

Use the iGateway Certificate Utility (igwCertUtil)

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 124).

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. For example, you can edit 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 network traffic. The setting you specify at the domain level can be inherited or overridden at the agent level.

Content administrators who belong to the PAMAdmins group have permissions to lock the Domain and edit Domain properties. The Domain_Admin permissions in the CA EEM Domain policy grants authorization.

Follow these steps:

1. Click the Configuration tab.
2. [Lock the domain](#) (see page 119).
3. Edit the Domain properties as needed. You can edit any field except Host Name, Orchestrator Name, and Status. Field descriptions follow:

Domain URL

Identifies the URL of the Domain Orchestrator. The correct format depends on whether you selected Support Secure Communication on the General Properties page when installing the Domain Orchestrator. When installed in secure mode, the OasisConfig.properties setting for oasis.transport.secure is set to true. You can enter either the hostname or the IP address of the Domain Orchestrator. The ports are configurable.

- For secure communication, use the following syntax:

```
https://hostname_or_IPaddress:8443/itpam
```

- For nonsecure communication, use the following syntax:

```
http://hostname_or_IPaddress:8080/itpam
```

Host Name

Identifies the host where the Domain Orchestrator is installed. For example, server1.mycompany.com

Orchestrator Name

Identifies the name of the Domain Orchestrator. The name is Domain Orchestrator, by default.

Status

Identifies that status of the Domain. For example, Active or Locked by *user ID*.

Periodic Heartbeat Frequency (In Minutes)

Specifies the frequency in minutes with which agents send a heartbeat back to the Domain Orchestrator. Agents inherit this value unless it is overridden at the agent level.

Default: 2

Touchpoint Security

Indicates whether to verify and enforce user rights on the targets within a given process. User rights are configured in a custom CA EEM policy that uses the Touchpoint Security resource class. Execute rights can be granted a user or group for a given environment or touchpoint.

Note: See [Approach to Configuring Touchpoint Security](#) (see page 131).

Values:

- Enabled: Enforce user rights when an operator attempts to run on a target specified in a Touchpoint Security policy.
- Disabled: Allow an operator to run on the specified targets without validating or enforcing user rights.

Default:

Disabled - supports backward compatibility.

4. Click Save.
5. [Unlock the Domain](#) (see page 119).

More information:

- [Lock and Unlock the Domain](#) (see page 119)
- [Approach to Configuring Touchpoint Security](#) (see page 131)

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:

[Create a Touchpoint Security Policy](#) (see page 112)

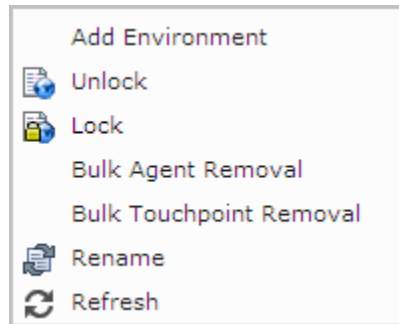
[Configure Domain Properties](#) (see page 129)

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 119).

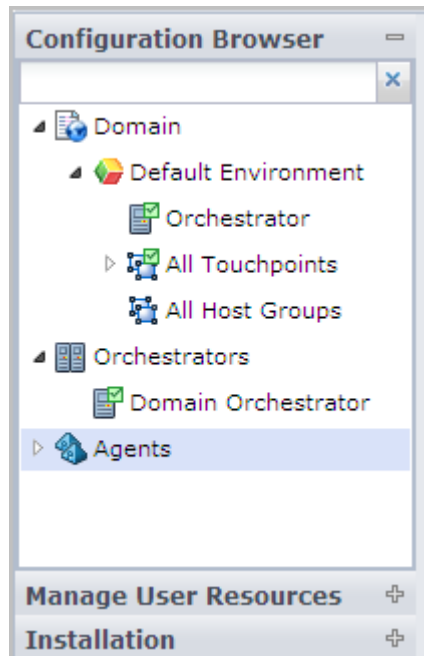
These tasks change the Domain Hierarchy by renaming a node or by adding or removing nodes.



- Add Environment - See [Add an Environment to the Domain](#) (see page 136).
- Remove Environment - See [Remove an Environment from a Domain](#) (see page 137).
- Bulk Agent Removal - See [Remove Selected Agents in Bulk](#) (see page 192).
- Bulk Touchpoint Removal - See [Remove Unused Empty Touchpoints in Bulk](#) (see page 205).
- Rename the Domain - See [Rename the Domain](#) (see page 138).

About the Domain Hierarchy, Orchestrators, and Agents

On the Configuration Browser palette on the Configuration tab, there is one root object. At installation, the root object is named Domain. The Domain is the parent element for all configurable elements in CA Process Automation.



The Configuration Browser displays both physical and logical entities.

Physical

Physical components are installed components. You can install Orchestrators and agents.

Orchestrators

- Domain Orchestrator: At installation, the single physical component is the Domain Orchestrator.
- Other Orchestrators: Administrators can install other Orchestrators from the Installation palette.

Agents

Administrators can install Agents from the Installation palette.

Logical

Logical entities make up the Domain hierarchy, which is made up of one or more environments. Each environment has one or more Orchestrator touchpoints. Each environment can have touchpoints and host groups that are associated with agents.

Domain

The Domain is the root node of the Domain hierarchy. CA Process Automation has one Domain.

Default Environment

The Default Environment is the environment that is created at installation.

Orchestrator (touchpoint)

The Orchestrator that is displayed under Default Environment at installation is the Orchestrator touchpoint that associates the Domain Orchestrator with the Default Environment. You add a separate touchpoint for each Orchestrator you install.

Note: The touchpoint for a clustered Orchestrator associates its environment with the load balancer for that cluster. When such a touchpoint is used as a target for an operator, the load balancer chooses the target node.

All Touchpoints

At installation, this node is empty. For each agent you install, you associate it with one or more environments with touchpoints. The All Touchpoints node under Default Environment contains only touchpoints that are associated with the Default Environment.

All Host Groups

At installation, this node is empty. You can add host groups to this node. First, create SSH connections from an agent to a group of remote hosts. Then, create a host group that refers to these remote hosts. Associate the host group with the Default Environment.

Another Environment

You can add a separate environment for production use. Each environment needs at least one Orchestrator touchpoint.

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

You can install additional Orchestrators. You associate each new Orchestrator with an environment through the touchpoint for that Orchestrator. You associate each agent that you install with an environment through a touchpoint named in All Touchpoints. If you create Host Groups, those entities are displayed in the All Host Groups for the new environment.

Most operators in most processes run on an Orchestrator. That is, the operators composing the process target the Orchestrator touchpoint. All operators can run on Orchestrators.

After you install agents, you can create agent touchpoints. Optionally, you can create touchpoint groups that are composed of selected touchpoints. An agent runs on a host computer separate from the Orchestrator. Not all categories of operators can run on agent touchpoints.

Each environment has its own set of touchpoints; these touchpoints are listed in the "All Touchpoints" node for that environment. Each touchpoint maps to an Orchestrator or agent. Only one touchpoint can map to an Orchestrator. Multiple touchpoints can map to an agent. A single touchpoint can map to multiple agents.

Each environment can have its own set of host groups. An agent hosts each host group. Host groups are composed of remote hosts. The "All Host Groups" group in an environment lists all the host groups in that environment.

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.

The Configuration Browser palette is open.

2. Select the Domain node and click Lock.

The Domain icon is displayed with a padlock to indicate that it is locked.

3. Right-click the Domain and select Add Environment.

4. Enter a name for the environment, and click OK.

The new environment name appears under the Domain with nodes for adding All Touchpoints and All Host Groups. Initially, the new environment is missing an Orchestrator.

5. Click Save.

6. Click Unlock.

Remove an Environment from the Domain

If you have Domain Administrator rights, you can delete an environment from the Domain. If the environment is populated, you can package and export what you want to move and then import it into another environment before deleting the environment.

To delete an environment

1. Before you delete an environment with content to save, create an export of the contents of its Orchestrators as follows:

- a. Click the Library tab.
- b. Select the Orchestrator drop-down list and select the Orchestrator in the environment to be deleted.
- c. Right-click the root folder and select Export, Relative Paths.

If on Windows, the File Download dialog appears asking whether to open or save <foldername>.xml.

- d. Click Save, navigate to a local folder that is shared, and click Save.
2. To import the saved content into the Library of a different Orchestrator:

- a. Select a different Orchestrator on the Orchestrator drop-down list of the Library tab.
- b. Right-click the import folder and select Import.
- c. Click Browse in the Import dialog.

On a Windows host, the Choose File to Upload opens at the folder where you exported the file.

- d. Select the xml file to import and click Open.
- e. Select the action to perform if an imported object has the same name as an existing object.
- f. Complete the following fields:

Set imported version as current

Specifies whether all of the objects being imported should have their version set as current.

- Checked - Save as current.
- Cleared - Retain their designation from before the import.

Make imported Custom Operators available

Specifies whether any custom operators that are imported are to be made available in this new environment.

- Checked - Make custom operators available.
- Cleared - Do not make custom operators available.

- g. Click Submit.

The Object imported successfully message appears.

- h. Click OK.

3. Click the Configuration tab.

The Configuration Browser palette is open.

4. Right-click the Domain, and click Lock.

The Domain icon displayed with a padlock to indicate that it is locked.

5. For each Orchestrator in the environment to be removed, do the following:

- a. [Quarantine the Orchestrator](#) (see page 170).

- b. [Remove the Orchestrator from the environment](#) (see page 150).

6. Right-click the environment, and click Delete.

A confirmation message appears.

7. Click Yes.

8. Click Save.

9. Right-click the Domain, and click Unlock.

Rename the Domain

Throughout the documentation and help, we use the name Domain to refer to 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.

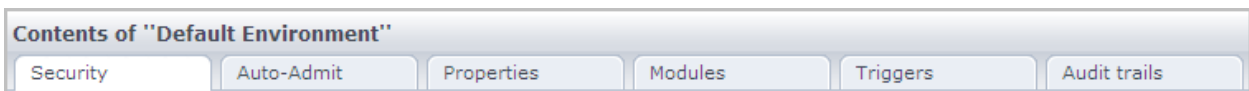
This section contains the following topics:

[Configure the Contents of an Environment](#) (see page 139)

[Update an Environment Hierarchy](#) (see page 146)

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 140).
- Auto-Admit
See [Add Touchpoints for Agents in Bulk](#) (see page 198).
- Properties
See [Configure Environment Properties](#) (see page 142).
- Modules
See [Enable an Operator Category and Override Inherited Settings](#) (see page 144).
- Triggers
See [Specify Trigger Settings for an Environment](#) (see page 145).
- Audit trails
See [View the Audit Trail for an Environment](#) (see page 331).

View or Reset Security Settings for a Selected Environment

One CA EEM handles security for the entire Domain, including all environments added to a Domain and all additional Orchestrators added after the Domain Orchestrator. (The Domain Orchestrator is the Orchestrator installed first.)

When Inherit is selected, the environment inherits all the security settings from the Domain. You may want to change the EEM Cache Update Interval while you are working in CA EEM. With a short update interval, any changes you make in CA EEM are reflected in CA Process Automation at the set update interval.

To change the security settings of a selected environment

1. Click the Configuration tab.
2. In the Configuration Browser palette, right-click the target environment, and select Lock.

The Security settings of the selected environment appear.
3. Clear the Inherit check box.

4. Examine the following settings and modify where appropriate.

FIPS compliant certificate

This read-only field specifies whether the algorithms used to encrypt data transferred between CA EEM and CA Process Automation are 140-2 compliant.

Selected - Indicates that 140-2 compliant algorithms are used. CA EEM is configured to operate in FIPS mode.

Cleared - Indicates that MD5 algorithms are used.

EEM Backend Server

The name of the computer hosting the CA EEM server.

EEM Application Name

When you register the CA Process Automation application with CA EEM, specify a parameter named Application Name. The application is registered with CA EEM using this name.

Default: Process Automation

EEM Certificate Name

The name of the certificate is required to connect to CA EEM. CA EEM provides the certificate during CA Process Automation registration. The certificate name is obtained from PAM_eem.xml and must be present in this folder:

```
<install_dir>/server/c2o/.c2orepository/public/certification
```

During installation, CA Process Automation asks for this certificate and automatically uploads it to the specified folder.

Default:

PAM.p12 if FIPS compliant certificate is cleared

PAM.pem if FIPS compliant certificate is selected.

One of the following:

EEM Certificate Password

During registration, a password is provided if FIPS compliant certificate is cleared. This password is required to connect to the CA EEM server.

EEM Certificate Key

During registration, a certificate key is provided if CA EEM FIPS compliant certificate is selected.

EEM Cache Update Interval (sec)

The frequency with which CA Process Automation is updated with CA EEM changes to CA Process Automation user accounts, groups, and policies. CA Process Automation uses the information stored in cache between updates.

5. Click Apply.

6. Click Save.
7. Right-click the environment, and select Unlock.
8. If you make certificate changes, be sure that the password of the certificate of new application is same as the old one. Put the new certificate under public/certification folder.
9. If you changed the configuration, restart each affected Orchestrators in the environment.
 - [Stop the Orchestrator](#) (see page 172).
 - [Start the Orchestrator](#) (see page 173).

Note: Changing the FIPS compliant certificate setting requires a manual procedure. For details, see [Change the CA EEM FIPS Mode Security Setting](#) (see page 124).

More information:

[Configure CA EEM Security Settings for the Domain](#) (see page 122)

[Control Frequency of Updating CA Process Automation with CA EEM Changes](#) (see page 20)

Configure Environment Properties

You configure properties for a selected environment in the Configuration tab. You must have Environment Configuration Administrator rights to configure environment properties or override the settings at a level that can inherit from the environment.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain and select the name of the environment to configure.
3. Right-click the environment and select Lock.
4. Select the Properties tab of the locked environment.
5. View or change displayed properties as needed.

Name

Indicates the name of the environment. This field is a read-only field.

To rename the environment, lock the Domain, right-click the environment name in the Configuration Browser palette, and select Rename.

Status

Indicates the status of the selected environment.

Operators Auto Recovery

Specifies whether to automate recovery. Recovery applies to certain operators that fail with a SYSTEM_ERROR. Operators subject to recovery must be part of 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 their targets. Operator targets can be Orchestrators, touchpoints, hosts that are connected to proxy touchpoints, or hosts in a host group.

Values:

- (Default) Selected - Automates recovery.
- Cleared - Prevents automated recovery.

Touchpoint Security

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

Values:

- (Default) Inherit from Domain
- Enabled - Enforce 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.

6. Click Apply.
7. Click Save.
8. Right-click the environment and select Unlock.

Updated environment properties are in effect.

More information:

[Approach to Configuring Touchpoint Security](#) (see page 131)

[Customize Agent Settings for Operator Categories](#) (see page 186)

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 244) for field-level details.

7. Click Save.
8. Click Close.
9. Right-click the environment and select Unlock.

More information:

[Configure File Management](#) (see page 275)

[Configure Command Execution](#) (see page 251)

[Configure Network Utilities](#) (see page 280)

[Configure Web Services](#) (see page 287)

[Configure Process Control](#) (see page 282)

Specify Trigger Settings for an Environment

Trigger settings are disabled at the environment level by default. If trigger settings 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.

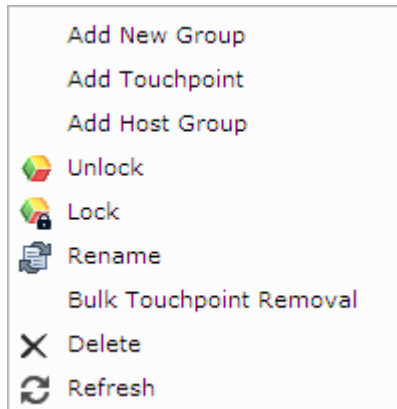
7. If you select Enabled, then right-click the trigger and select Edit. Edit the settings using the following as a guide:
 - [Configure File Trigger Properties at the Domain Level](#) (see page 308).
 - [Configure Mail Trigger Properties at the Domain Level](#) (see page 311).
 - [Configure SNMP Trigger Properties at the Domain Level](#) (see page 315).
 - [Configure Catalyst Trigger Properties at the Domain Level](#) (see page 302).
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 207)
- Add Touchpoint
See [Add a Touchpoint and Create an Association](#) (see page 197) and other details in the "Administer Touchpoints" and the "Administer Proxy Touchpoints" chapters.
See also [Add an Orchestrator to an Environment](#) (see page 149).
- Add Host Group
See [Create a Host Group](#) (see page 227) and other details in the Administer Host Groups chapter.
- Rename
See [Rename an environment](#) (see page 148).
- Bulk Touchpoint Removal
See [Remove Unused Empty Touchpoints in Bulk](#) (see page 205).
- 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 150).
 - Any agent touchpoint.
 - Any touchpoint group.
 - Any host group.

Rename an Environment

You can rename an existing environment in a Domain. Administrators with Environment Administrators rights can rename an environment.

To rename an environment

1. Click the Configuration tab.
The Configuration Browser palette is open.
2. Right-click the Domain, and click Lock.
The Domain icon displayed with a padlock to indicate that it is locked.
3. Right-click the environment, and click Lock.
The Environment icon displays with a padlock to indicate that it is locked.
4. Right-click the environment, and select Rename.
5. Enter a new name for the environment, and click Enter.
6. Click Save on the toolbar.
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. Typically, 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 that 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 156)

Delete an Orchestrator Touchpoint

An Orchestrator touchpoint is a logical entity that associates a selected Orchestrator, or its load balancer, with a specific environment. You can delete that touchpoint. 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. That is the touchpoint that associated an installed Orchestrator with an environment is removed. You can add this Orchestrator to another environment.

More information:

[Quarantine an Orchestrator](#) (see page 170)

[Disable an Orchestrator Touchpoint](#) (see page 158)

Chapter 7: Administer Orchestrators

Orchestrators are the engines that manage and execute automation objects, and direct agents to perform required actions as part of the execution. Orchestrators can be standalone or clustered for high availability and scalability. Each standalone Orchestrator or cluster of Orchestrators maintains its own library, containing its automation objects.

The Domain Orchestrator is a special Orchestrator that defines a Domain and maintains the configuration and status of all components in that Domain. As part of maintaining status, the Domain Orchestrator is periodically sent status updates by all other components in the Domain.

Each Orchestrator can only participate in one CA Process Automation environment. You configure host-specific settings for the Orchestrator in the Orchestrators node. You configure touchpoint-specific setting for the same Orchestrator in the Environment node.

This section contains the following topics:

[About Orchestrators](#) (see page 151)

[Configure the Contents of an Orchestrator Touchpoint](#) (see page 152)

[Update the Hierarchy of an Orchestrator Touchpoint](#) (see page 155)

[Configure the Contents of an Orchestrator Host](#) (see page 159)

[Maintain the Orchestrator Host](#) (see page 169)

About Orchestrators

After the Domain Orchestrator is up and running, you can install other Orchestrators from the Installation palette on the Configuration tab. Installation of an additional Orchestrator means installing a different engine on a different host. Each Orchestrator has its own database with its own suite of libraries. If you create something in the Domain Orchestrator, it is not seen in the new Orchestrators.

Each Orchestrator must be associated with a touchpoint. When you add an Orchestrator to an environment, you are associating the Orchestrator with a touchpoint in an environment.

To meet requirements for additional power, you can add a cluster node to any Orchestrator. In this architecture, the Orchestrators in the cluster node share the same reporting database.

When we say that Orchestrators are the "engines" of CA Process Automation, we mean that Orchestrators process the content designed with CA Process Automation. All processes run on Orchestrators. You can run a process on one Orchestrator that runs a subprocess on a separate Orchestrator, where each Orchestrator has its own libraries. An agent can perform steps in a process, such as running a script. Orchestrators and agents communicate using a pair of ports. The default for Orchestrators is port 7001; the default for agents is port 7003.

When the Orchestrator has an agent complete a step, the agent returns the results of the step to the Orchestrator. In a cluster setup, an Orchestrator node sends a request to an agent on port 7003. The agent sends the result to any node of the requesting Orchestrator on port 7001. One of the cluster nodes picks up the agent result from a shared queue.

You can view information about an Orchestrator under its environment or under the Orchestrators node.

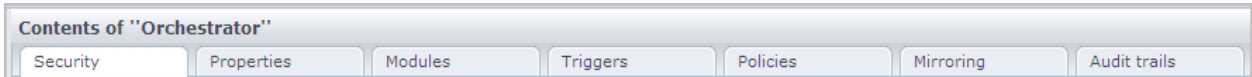
Configure the Contents of an Orchestrator Touchpoint

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 159).

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 153).
- 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.
The Configuration Browser palette opens.
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 following setting.

Touchpoint Security

Specifies whether to inherit the value for Secure configured in Environment properties, or set the value to true or false at the Orchestrator level.

Values:

- (Default) Inherit from Environment.
- Enabled - Enforce each Touchpoint Security policy that specifies users that are allowed to execute operators on the current target.
- Disabled - Do not verify whether the user running the process has execute rights on the current target.

- a. Click Apply
- b. Click Save.
- c. Right-click the Orchestrator, and select Unlock.

6. View the following informational properties.

Note: For details see, [Configure the Contents of a Selected Orchestrator Host](#) (see page 159).

Operators Autorecovery

Specifies whether to automate recovery.

Status

Specifies the status of the Orchestrator. Statuses include active, locked (and the name of the user who locked it), and quarantine.

Orchestrator Name

Specifies the name of the Orchestrator

Host Name

Specifies the name of the host computer that is associated with the Orchestrator.

Domain Orchestrator

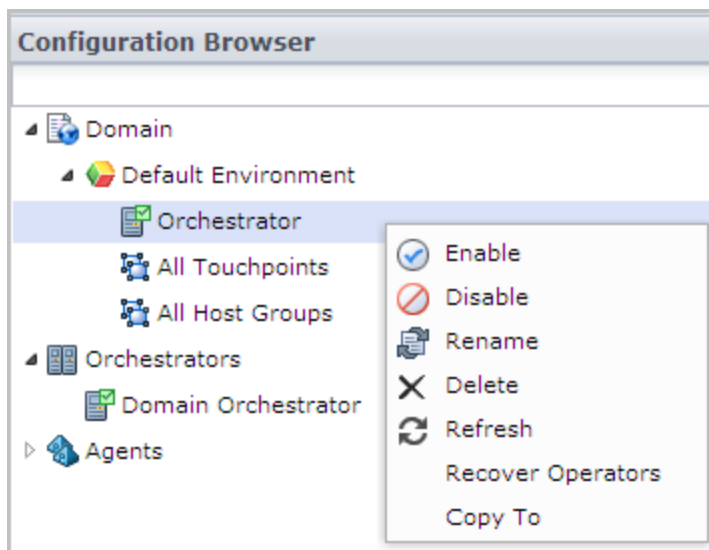
A true or false property that specifies whether the Orchestrator is the Domain Orchestrator.

Display Name

Specifies the display name of the Orchestrator.

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 158).
- Rename - Specify a new name for the Orchestrator touchpoint.
- Delete - Right-click an Orchestrator touchpoint and select Delete. Only the touchpoint is deleted.
- Recover Operators
See [Recover Operators on the Target Orchestrator](#) (see page 157).
- Copy To
See [Create a Touchpoint Group with Selected Touchpoints](#) (see page 209)

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.

If you installed a load balancer for node 1 of this Orchestrator, add a touchpoint to the environment and map it to the load balancer for that Orchestrator. When you add nodes to the clustered Orchestrator, the previously defined touchpoint is used. The load balancer determines which node handles a request that targets the touchpoint.

To add a touchpoint for an Orchestrator

1. Click the Configuration tab.
2. Right-click the environment where you want to add a touchpoint and select Lock.
3. Expand the Orchestrators palette.
4. Right-click the target Orchestrator, select Configure Touchpoint At, and then click the name of the environment you locked.
5. In the Add Orchestrator Touchpoint dialog, enter a name for the new touchpoint, and then click OK.
6. Expand the Browser palette.
7. Right-click the environment where you added the touchpoint and select Unlock.
The Unsaved Data dialog prompts you to save changes.
8. Click Yes.

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

A new Orchestrator touchpoint is added to the selected environment.

More information:

[Add an Orchestrator to an Environment](#) (see page 149)

Recover Operators on the Target Orchestrator

Manual recovery is always enabled. That is, you can invoke Recover Operators whether the target level Operator Auto Recovery is set to True, False, or Inherit from Environment. Operator recovery is called for 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 Processes

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.

Note: You cannot run Operators recovery on a target that is disabled.

Follow these steps:

1. Open the Configuration tab.
2. In the Configuration Browser, expand the Domain and then the Environment in which any 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.

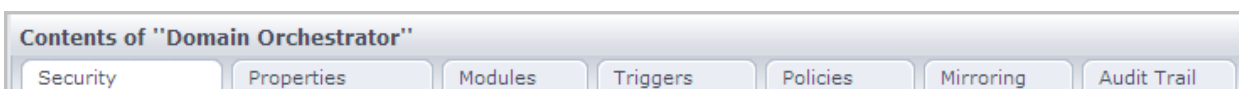
More information:

[Quarantine an Orchestrator](#) (see page 170)

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 159).
- Properties
See [Configure Orchestrator Touchpoint Properties](#) (see page 153).
- Modules
See [Override Operator Category Settings Inherited from Environment](#) (see page 164).
- Triggers
See [Activate Triggers for an Orchestrator](#) (see page 165).
- Policies
See [Configure Orchestrator Policies](#) (see page 166).
- Mirroring
See [Configure Orchestrator Mirroring](#) (see page 168).
- Audit Trails
See [View the Audit Trail for an Orchestrator](#) (see page 332).

View Orchestrator Security Settings

CA EEM is used for user authentication and user authorization for all Domain users. That is, users are allowed to log in to CA Process Automation only if they enter credentials found in a CA EEM user account. Users are authorized to take various actions based on policies that reference the user account or its application group. When Inherit is selected, the Orchestrator inherits all the security settings from its environment. These settings affect the entire Domain.

We recommend you accept the Inherit setting for the Security tab.

Follow these steps:

1. Click the Configuration tab.
2. In the Configuration Browser palette, expand Orchestrators.
3. Right-click the Orchestrator you want to configure, and click Lock.
4. Click the Security tab.
5. Clear the Inherit check box.
6. Examine the following settings and modify where appropriate.

FIPS-compliant certificate

This read-only field specifies whether the algorithms used to encrypt data transferred between CA EEM and CA Process Automation are 140-2 compliant.

Selected - Indicates that 140-2 compliant algorithms are used. CA EEM is configured to operate in FIPS mode.

Cleared - Indicates that MD5 algorithms are used.

CA EEM Backend Server

The name of the computer hosting the CA EEM server.

CA EEM Application Name

When you register the CA Process Automation application with CA EEM, specify a parameter named Application Name. The application is registered with CA EEM using this name.

Default: Process Automation

CA EEM Certificate Name

The name of the certificate is required to connect to CA EEM. CA EEM provides the certificate during CA Process Automation registration. The certificate name is obtained from PAM_eem.xml and must be present in this folder:

```
<install_dir>/server/c2o/.c2orepository/public/certification
```

During installation, CA Process Automation asks for this certificate and automatically uploads it to the specified folder.

Default:

PAM.p12 if FIPS compliant certificate is cleared

PAM.pem if FIPS compliant certificate is selected.

One of the following:

CA EEM Certificate Password

During registration, a password is provided if FIPS mode is not selected. This password is required to connect to the CA EEM server.

CA EEM Certificate Key

During registration, a certificate key is provided if CA EEM FIPS mode is selected.

CA EEM Cache Update Interval (in seconds)

The frequency with which CA Process Automation is updated with CA EEM changes to CA Process Automation user accounts, groups, and policies. CA Process Automation uses the information stored in cache between updates.

Default:

1800 seconds (30 minutes)

7. Click Save
8. Click Unlock.
9. If you make certificate changes, be sure that the password of the certificate of new application is same as the old one. Put the new certificate under public/certification folder.
10. If you changed the configuration, restart the Orchestrator.
 - [Stop the Orchestrator](#) (see page 172).
 - [Start the Orchestrator](#) (see page 173).

Note: Changing the FIPS compliant certificate setting requires a manual procedure. For details, see [Change the CA EEM FIPS Mode Security Setting](#) (see page 124).

More information:

[Configure CA EEM Security Settings for the Domain](#) (see page 122)

[View or Reset Security Settings for a Selected Environment](#) (see page 140)

Configure Orchestrator Host Properties

The Orchestrator Properties pane provides information about the status and configuration of the Orchestrator. The only field you can update is Touchpoint Security. After you have defined a Touchpoint Security policy for processes that run on this Orchestrator, enable this setting.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Orchestrators node.
3. Select the Orchestrator you want to configure, and click Lock.
4. Click the Properties tab to view Orchestrator properties settings.
5. View the setting for Operators Autorecovery.

Operators Autorecovery

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

Values:

- (Default) Inherit from Environment - same setting as for Environment.
 - True - Automates recovery.
 - False - Prevents automated recovery.
6. Examine the Touchpoint Security setting in light of whether you have a Touchpoint Security policy in place. If you added a Touchpoint Security policy, this setting should be set to True either explicitly or through inheritance.

Touchpoint Security

Specifies whether to inherit the value configured or inherited in Environment properties, or set the value to true or false at the Orchestrator level.

Values:

- (Default) Inherit from Environment
- Enabled - Enforce applicable policy that specifies users allowed to execute operators on the current target.
- Disabled - Do not verify whether the user running the process has execute rights on the current target.

7. View the following informational properties.

Status

Specifies the status of the Orchestrator. Statuses include active, locked (and the name of the user who locked it), and quarantine.

Orchestrator Name

Specifies the name of the Orchestrator

Host Name

Specifies the name of the host computer associated with the Orchestrator

Is Domain

A true or false property that specifies whether the Orchestrator is the Domain Orchestrator.

Display Name

Specifies the display name of the Orchestrator

8. Click Save.
9. 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 244) 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 File Management](#) (see page 275)

[Configure Command Execution](#) (see page 251)

[Configure Network Utilities](#) (see page 280)

[Configure Web Services](#) (see page 287)

[Configure Process Control](#) (see page 282)

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 299).
 - 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.

More information:

[Administer Triggers](#) (see page 299)

[Configure File Trigger Properties at the Domain Level](#) (see page 308)

[Configure Mail Trigger Properties at the Domain Level](#) (see page 311)

[Configure SNMP Trigger Properties at the Domain Level](#) (see page 315)

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. Expand the Orchestrators palette.
3. Select the Orchestrator to configure, and click Lock.
4. Click the Policies tab and examine the settings in light of the following field descriptions.

Automation Object Versioning

Specifies the policy for retaining old versions during check-in of an edited automation object, where options include:

- Allow user to overwrite existing version on check-in.
- Always create a version on check-in.

Default Process Handlers

Specifies the complete path to the process to use as the default process for the selected Orchestrator. Default process handlers can provide default lane change rules and exception handling. This ability takes affect when these rules are not specified in the process itself. Click the button at the end of the field to open the Object Browser, select an process from the CA Process Automation library, and click OK. The Open button opens the default process.

Minimum Number of Days of Process History

Defines the number of days to save process instances that ran on a touchpoint or remote host. Keeping this value small avoids excessive growth of the library and consequent increase to the system response time.

For example, if you configure one day and a process ends at a certain time, the process remains in the library until that same time on the following day.

Minimum Number of Failed Instances

Defines the minimum number of failed instances of any process to retain in the history. Excess failed process instances are deleted beginning with the oldest only if the history exceeds the configured Minimum Days of Process History.

Minimum Number of Completed Instances

Defines the minimum number of completed instances of the process object to retain in the history. Excess completed process instances are deleted in order of age (oldest first) only if in history longer than the configured Minimum Days of Process History.

Minimum Number of Audit Messages

Specifies the minimum number of audit messages retained in the audit history.

Minimum Number of Days of Audit History

Specifies the minimum number of days of audit history retained.

Maximum Number of Log Messages

Specifies the maximum number of log messages that can be retained and displayed when the process instance is opened from a process watch.

Secure Attachments

Specifies whether to require authentication when a user attempts to access attachments outside of CA Process Automation.

Values:

- Selected - Attachments are secured. The user must supply a valid user ID and password to access attachments.
- Cleared - Attachments are not secured. The user can access attachments without supplying valid credentials.

Minimum Number of Days of Attachments History

Specifies the minimum number of days to store an attachment in the CA Process Automation database before deleting it.

Users can trigger processes using web services. 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 inside that process. A user can forward an attachment to the outgoing web services call using the SOAP operator.

Enable Runtime Security

Specifies whether to enforce runtime security. If selected, enforcement impacts processes where Runtime Security is enabled. Runtime Security is enabled for processes that are set to Enable. Runtime Security is enabled for processes that inherit an enabled setting.

Values:

- Selected - Enforce runtime security on all processes where it is configured.
- Cleared - Do not enforce runtime security on any process.

5. Edit as needed.
6. Click Save.

Your changes are put into effect.

7. Click Unlock.

Note: If you select the option to enforce runtime security, use Set Owner to establish ownership of each affected process object. See online help or the *Content Designer Guide* for details.

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.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Orchestrators node.
3. Select the Orchestrator to configure and click Lock.
4. Click the Mirroring tab.
5. Complete the following field:

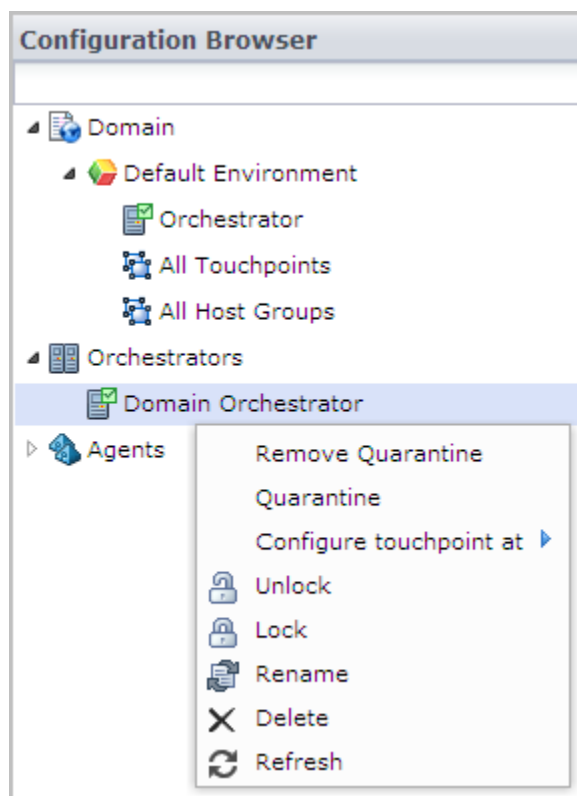
Mirroring Interval (Minutes)

Specifies the number of minutes between checks for changes. The selected Orchestrator contacts the Domain Orchestrator. If changes exist, these changes are mirrored to the selected Orchestrator.

6. Click Save.
7. 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 171).
- Quarantine
See [Quarantine an Orchestrator](#) (see page 170).
- Configure touchpoint at
See [Configure Orchestrator Touchpoint Properties](#) (see page 153).
- 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 171)

[Delete an Orchestrator Touchpoint](#) (see page 150)

[Disable an Orchestrator Touchpoint](#) (see page 158)

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.

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. Do one of the following:
 - 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, where XX is either 32 or 64, depending on the system.

```
install_dir\\server\c2o\bin\wrapper_XX\stopc2osvc.bat
```

3. If you logged in to a UNIX or Linux host, do the following:
 - 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. That is, run:

`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 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. Do one of the following:
 - Select Programs, CA, CA Process Automation 4.0, 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, where XX is either 32 or 64, depending on the system.

`install_dir\server\c2o\bin\wrapper_XX\startc2osvc.bat`
3. If you logged in to a UNIX or Linux host, do the following:
 - 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:

[Administer Triggers](#) (see page 299)

[Configure File Trigger Properties at the Domain Level](#) (see page 308)

[Configure Mail Trigger Properties at the Domain Level](#) (see page 311)

[Configure SNMP Trigger Properties at the Domain Level](#) (see page 315)

Chapter 8: Administer Agents

The first CA Process Automation you install contains the Domain Orchestrator. The Domain Orchestrator and other Orchestrators you add run the processes and schedules created by content designers. Orchestrators can direct agents to run steps in a process and return the results. Agents can participate in any number of environments within a Domain.

An agent is a CA Process Automation component you install on a host. You associate touchpoints with the agent and an environment. You target the touchpoints to execute operators on the agent host.

You can associate an agent with proxy touchpoints or host groups to execute operators on remote hosts that have no agent. Operators can execute on a remote host with no agent when an SSH connection is configured from the agent host to the target remote host. To execute on a remote host, operators target the proxy touchpoint.

See "Administer Touchpoints" for details about how to configure failover or load balancing among agents associated with the same touchpoint.

See "Administer Proxy Touchpoints" and "Administer Host Groups" for details about establishing SSH connections.

For information about installing the agent software on a host computer, see "Install CA Process Automation Components" in the *Installation Guide*.

This section contains the following topics:

[Configure Agents to Support Operator Targets](#) (see page 176)

[Install an Agent Interactively](#) (see page 180)

[Add an Agent Touchpoint](#) (see page 182)

[Add an Agent Host Group](#) (see page 183)

[Configure the Contents of a Selected Agent](#) (see page 183)

[Quarantine an Agent](#) (see page 189)

[Remove Quarantine from an Agent](#) (see page 189)

[Rename an Agent](#) (see page 190)

[Manage the Decommissioning of a Host with an Agent](#) (see page 190)

[How to Start or Stop an Agent](#) (see page 193)

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.

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.
4. At the File Download prompt, click Run to start the installer. 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.
The default JRE folder for Windows follows, where *jre* has a release-specific name:
C:\Program Files\Java\jre
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) Suppress short-cut creation entirely
12. Examine the Domain URL and the URL of the Domain Orchestrator from which you launched the agent installation. Click Next.

13. Complete the General Properties page as follows:

- a. Accept the Agent Host name entry. This name identifies the host from which you started the installation.
- b. Change or accept the default Display Name, the host name.
- c. Accept 7003 as the Agent Port unless this port is used. Alternatively, enter another port number such as 57003.
- d. If you launched the agent installation from a Windows host, select Install as Windows Service.
- e. (Optional) Select Start Agent After Installation.

Starting the agent lets you view the active agent and continue with agent configuration.

14. 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.

15. Read the displayed explanation and complete the setting in one of the following ways.
 - If you use Windows PowerShell, select the check box to set the execution policy of PowerShell to Remote Signed and browse to the PowerShell location of the host. Click Next.

This setting enables you to run Windows PowerShell scripts through this agent.

- If you do not use Windows PowerShell, click Next.

Agent installation begins.

16. Click Finish.

17. (Windows only) Start the agent service. Click Start, Programs, CA, *agent-name*, Start agent service.
18. Click the Configuration Browser palette on the Configuration tab.
19. Click Refresh.
20. Expand Agents and verify that your agent name is listed.

Add an Agent Touchpoint

If an operator must target a given host, install an agent on that host. Then, select that agent and configure its touchpoint.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Agents node.
3. Select the agent and click Lock.
4. Right-click the agent and select Configure touchpoint at, then select the environment.
A prompt to lock the selected environment appears.
5. Click Yes to lock the selected environment.
The Add Agent Touchpoint dialog appears.
6. Enter a name for the new touchpoint that is different from the hostname, and click OK.
The new touchpoint appears under the All Touchpoints node for the associated environment.
7. Click Save and click OK to confirm.
8. Select the agent and select Unlock.
9. Select the locked environment and select Unlock.

More information:

[Administer Touchpoints](#) (see page 195)

[Administer Proxy Touchpoints](#) (see page 215)

Add an Agent Host Group

If an operator must target a remote host within a given subnet or with a hostname beginning with a certain pattern, install an agent on the host for the host group. Then establish an SSH trust relationship from that agent host to each remote host in the subnet. Finally, select that agent and configure its host group.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Agents node.
3. Select the agent and click Lock.

A prompt to lock the selected environment appears.
5. Click Yes to lock the selected environment.

The Add Agent Host Group dialog appears.
6. Enter a name for the new host group that is different from the hostname, and click OK.

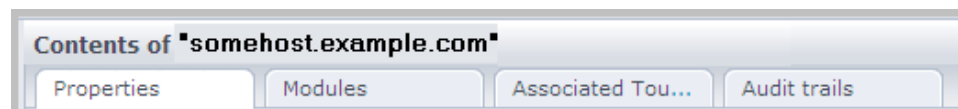
The new host group appears in the Associated Touchpoints/Host Groups tab.
7. Click Save.
8. Select the agent and select Unlock.
9. Select the locked environment and select Unlock.

More information:

[Administer Host Groups](#) (see page 223)

Configure the Contents of a Selected Agent

Many Properties settings are retrieved during 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 on the Agent touchpoint.



The four tabs for the Agent menu follow:

- Properties
See [Configure Agent Properties](#) (see page 184).
- Modules
See [Customize Agent Settings for Operator Categories](#) (see page 186).
- Associated Touchpoints and Host Groups
See [View the Touchpoints and Host Groups for a Selected Agent](#) (see page 188).
- Audit Trails
See [View the Audit Trail for an Agent](#) (see page 334).

Configure Agent Properties

You can set agent properties for the frequency with which the agent sends the Domain Orchestrator a heartbeat and the frequency with which the agent checks with the Domain Orchestrator for updates. The agent sends the Domain Orchestrator a heartbeat at startup and on the configured schedule as long as it is active. The Domain Orchestrator sends an acknowledgment to the agent in response to the heartbeat or domain updates, if available. The Domain Orchestrator sends mirrored updates to the agent on the schedule set as the mirroring interval.

You can set agent properties in the Configuration Browser.

Follow these steps:

1. Click the Configuration tab and expand Agents.
2. Right-click the agent to configure, and select Lock.
3. Select the Properties tab for the selected agent.

- (Optional) Review view-only properties.

Status

Specifies agent status, that is, whether the agent is active, locked (and the name of the user who locked it), or in quarantine.

Agent Name

Specifies the name of the agent. For information about renaming an agent, see “Rename an Agent.”

Host Name

Specifies the fully qualified domain name (FQDN) of the host computer on which the agent is installed. A hostname is an FQDN when all the labels up to and including the top-level domain name are specified.

Note: See [Syntax for DNS Host Names](#) (see page 358).

Host Address

Specifies the IP address of the host computer on which the agent is installed.

- (Optional) Update the values of the following properties.

Mirroring Interval (Minutes)

Specifies the mirroring interval in minutes for the agent. Agents mirror data and configuration information stored on the Domain Orchestrator. This setting specifies how often an agent checks for changes on the Domain Orchestrator to update mirrored information stored locally.

Default: 60

Periodic Heartbeat Frequency (Minutes)

Specifies the frequency with which the selected agent sends a heartbeat to the Domain Orchestrator. The default value at the Domain level is every two minutes, that is 2.

Valid values: A numeric value, Never, or Inherit from Domain.

Default: Inherit from Domain

Note: The agents always send a heartbeat at agent startup.

- Right-click the agent, and select Unlock.

The Unsaved Data dialog prompts you to save changes.

- Click Yes.

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

Customize Agent Settings for Operator Categories

Settings that you configured on the Modules tab for the Domain are inherited by all environments, all Orchestrators, and all agents. Administrators can edit the configuration at lower levels of the Domain hierarchy. Administrators can enable categories of operators on any agent and can edit the configurations as needed.

Follow these steps:

1. Click the Configuration tab.
2. Expand agents and right-click the selected agent and 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 and select Edit.
6. Change the property settings of the selected category for the selected agent. Use the following field descriptions of Domain level setting for reference:
 - [Configure Catalyst](#) (see page 246).
 - [Configure Command Execution](#) (see page 251).
 - [Configure Databases: Oracle properties](#) (see page 261).
 - [Configure Databases: MSSQL Server properties](#) (see page 263).
 - [Configure Databases: MySQL properties](#) (see page 264).
 - [Configure Databases: Sybase properties](#) (see page 266).
 - [Configure Directory Services](#) (see page 268).
 - [Configure Email](#) (see page 273).
 - [Configure File Management](#) (see page 275).
 - [Configure File Transfer](#) (see page 278).
 - [Configure Network Utilities](#) (see page 280).
 - [Configure Process Control](#) (see page 282).
 - [Configure Utilities](#) (see page 284).
 - [Configure Web Services](#) (see page 287).
7. Click Save. Click OK to the verification message.
8. Right-click the locked agent and 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 the Agents palette.
2. Select the agent you want to configure and click Lock.
3. Select 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. Select Unlock.

The selected operator category is disabled on the selected agent.

More information:

[Operator Categories and Where Operators Run](#) (see page 298)

[Configure File Management](#) (see page 275)

[Configure Command Execution](#) (see page 251)

[Configure Network Utilities](#) (see page 280)

[Configure Web Services](#) (see page 287)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Enable or Disable an Operator Category](#) (see page 295)

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 195).
- [Administer Proxy Touchpoints](#) (see page 215).
- [Administer Host Groups](#) (see page 223).

View the Touchpoints and Host Groups for a Selected Agent

From the Associated Touchpoint tab for a selected agent, you can view the touchpoints and host groups for that agent.

Follow these steps:

1. Click the Configuration tab and expand the Agents palette.
2. Select the agent for which you want to view touchpoints and host groups.
3. Select the Associated Touchpoint tab.

Name

Displays the name of the touchpoint or host group for the selected agent.

Associated Touchpoints and Host Groups

Displays the hierarchy, where the root node is Domain, that is:

- *Domain/environment/touchpoint*
- *Domain/environment/touchpoint*

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 computer name during agent installation. You can rename the agent. For example, you could replace the FQDN for the host with Agent-<hostname>.

Follow these steps:

1. Click the Configuration tab and expand the Agents node.
2. Select the agent to rename and click Lock.
3. Right-click the agent and select Rename.
The agent name can be changed.
4. Enter the new name.
5. Click Save.
6. Select the agent and click Unlock.

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:

[Associate a Touchpoint with a Different Agent](#) (see page 204)

[Remove Selected Agents in Bulk](#) (see page 192)

[Remove Unused Empty Touchpoints in Bulk](#) (see page 205)

Remove an Agent

When you no longer want an agent that you have installed, uninstall that agent from the host and then delete that agent from the Agent palette.

To remove an agent from the Agents palette

1. Click the Configuration tab.
2. Right-click Domain and select Lock.
3. Select the Agents palette.
4. Verify that the target agent is unlocked and not quarantined.
5. Right-click the target agent and select Delete.

A confirmation dialog appears.

6. Click OK.
7. Select the Browser palette and click Save.
8. Right-click Domain and select 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.

To remove selected agents in bulk

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 Unock.

More information:

[Lock and Unlock the Domain](#) (see page 119)

[Manage the Decommissioning of a Host with an Agent](#) (see page 190)

[Remove Unused Empty Touchpoints in Bulk](#) (see page 205)

How to Start or Stop an Agent

How to start and stop an agent depends on the operating system used on the host where the agent is installed.

- Microsoft Windows - Windows Service
- Unix or Linux - command line

For Windows, access the Services console from Administrative Tools in the Control Panel. From there, you can start or stop the agent service. Or, use the Start menu option. For example:

Programs > CA > CA Process Automation Agent > Start Agent Service

Programs > CA > CA Process Automation Agent > Stop Agent Service

For details on a UNIX or Linux operating system, see the following:

- [Start a CA Process Automation Agent on a UNIX or Linux Host](#) (see page 194)
- [Stop a CA Process Automation Agent on a Unix or Linux Host](#) (see page 194)

Start CA Process Automation Agent on a UNIX or Linux Host

You can start a CA Process Automation Agent on UNIX or Linux host when you see that it displays as inactive on the Agents palette.

To start a CA Process Automation Agent on a UNIX or Linux host

1. Change directories to the AGENT_HOME/pamagent.

Note: The default location is AGENT_HOME=usr/local/CA/PAMAgent.

2. Run the following command:

```
./c2oagtd.sh start
```

The agent starts running.

Stop CA Process Automation Agent on a UNIX or Linux Host

You can stop a CA Process Automation agent running on a UNIX or Linux host.

To stop CA Process Automation Agent on a UNIX or Linux host

1. Change directories to the AGENT_HOME/pamagent.

Note: The default location is AGENT_HOME=usr/local/CA/PAMAgent

2. Run the following command:

```
./c2oagtd.sh stop
```

The agent stops running.

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](#) (see page 196)

[Add a Touchpoint to a Selected Environment](#) (see page 197)

[Add an Agent to an Existing Touchpoint](#) (see page 198)

[Add Touchpoints for Agents in Bulk](#) (see page 198)

[Configure How Operators Select the Target Agent](#) (see page 200)

[Configure Touchpoint Properties](#) (see page 201)

[Rename a Touchpoint](#) (see page 203)

[Associate a Touchpoint with a Different Agent](#) (see page 204)

[Remove Unused Empty Touchpoints in Bulk](#) (see page 205)

[Manage Touchpoint Groups](#) (see page 207)

Touchpoint Implementation Strategy

You can create touchpoints as you need them. That is, create touchpoints for process targets in the design environment before the design process starts. Then, create touchpoints for targets in the production environment during process transitioning. During transition, you do not change any target reference in operators. Rather, you create the same touchpoint names or proxy touchpoint names that you used in the design environment, but you associate these touchpoints to the production environment.

Consider this process:

1. Obtain 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 targeted external system.
4. Designers run and test the process, where operators in the process target that touchpoint for testing.
5. During the transitioning of a process to the production environment, take the following steps for each target that is an agent touchpoint:
 - a. Identify the host that is running the application, database, or system to target.
 - b. Install an agent on the identified host.
 - c. Create a touchpoint that associates this agent with the production environment and name that touchpoint with the same name that was used in the design environment.
6. During the transitioning of a process, take the following steps for each target that is a proxy touchpoint.
 - a. Identify 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 that was used for the proxy touchpoint in the design environment.

Add a Touchpoint to a Selected Environment

You can add touchpoints one at a time or you can add them in bulk.

Use the following procedure to add a touchpoint to a selected environment and then select the agent to associate it with.

Follow these steps:

1. Click the Configuration tab.
2. Click the Configuration Browser palette.
3. Expand Domain.
The configured environments are displayed.
4. Right-click the environment to configure, and click Lock.
5. Right-click the environment, and click Add Touchpoint.
The Add Touchpoint dialog opens.
6. For Touchpoint Name, enter a name for the new agent touchpoint.
7. Select Agent, if not selected by default.
8. From the list of available agents, select the agent that you want to associate with the touchpoint.
9. Click Add.
A new agent touchpoint is added to All Touchpoints in the environment.
10. Click Save in the menu bar and then click OK to the confirmation prompt.
11. Right-click the environment, and click Unlock.
The touchpoint that you added appears under All Touchpoints in its environment.

More information:

[Configure Touchpoint Properties](#) (see page 201)

[Configure Proxy Touchpoint Properties](#) (see page 218)

Add an Agent to an Existing Touchpoint

You can add an agent to an existing Touchpoint from the target agent.

Follow these steps:

1. Click the Configuration tab.
2. Right-click the environment to configure, and click Lock.
3. Click the Agents palette.
4. Right-click the agent to add to an existing touchpoint, point to Configure Touchpoint At, and select an environment.

The Add Agent Touchpoint dialog appears.

5. Enter the name of an existing touchpoint and click OK.
6. Click the Configuration Browser palette, right-click the locked Environment, and click Unlock.

The Unsaved Data dialog prompts you to save changes.

7. Click Yes.

More information:

[Configure How Operators Select the Target Agent](#) (see page 200)

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. Automatically added touchpoints are named with the display name of the agents that match the specified patterns.

An *auto-admit pattern* is a hostname pattern expressed as a regular expression or an IP address subnet expressed in CIDR notation. Auto-admit patterns configured for an environment enable automatic assignment of touchpoints to agent hosts with host names or IP addresses that match the patterns.

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.

To add touchpoints to agents using auto-admit patterns

1. Click the Configuration tab.
2. Expand the Browser palette.

3. Right-click the environment you want to configure, and click Lock.
4. Click the Auto-Admit tab.
5. Click Add (the button with the green + sign) above the IP Address Patterns.

An entry field appears.

6. 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.

7. Click Add above the IP Address Patterns.

An entry field appears.

8. 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.

9. Right-click the environment, and click Unlock.

10. 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:
 - host1.mycompany.com 155.32.45.5 with display name of host1
 - host2.mycompany.com 155.32.45.50 with display name of host2

The following touchpoints are automatically added based on the auto-admit patterns:

- touchpoint name: Host1 in Environment1
- touchpoint name: Host2 in Environment1
- touchpoint name: Host2 in Environment2

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 Touchpoint Properties

You can configure properties for a touchpoint or a proxy touchpoint.

Follow these steps:

1. Click the Configuration tab.
2. Expand the environment with the touchpoints to configure, and expand All Touchpoints.
3. Right-click the environment and select Lock.
4. Select the touchpoint to configure and click the Properties tab.
5. Set the Operators Auto Recovery property.

Operators Auto Recovery

Specifies whether to automate recovery. Recovery applies to operators that fail with a `SYSTEM_ERROR` and whose recoverable processes are in `BLOCKED`, `RUNNING`, or `WAITING` state when the recovery is triggered. When automatic recovery is configured and the previously inactive touchpoint becomes active, affected operators are reset. The reset operators begin running on the touchpoint and their processes continue execution.

Values:

- (Default) Inherit from Environment - same setting as for Environment.
- True - Automates recovery.
- False - Prevents automated recovery.

6. Set the Touchpoint Security property. Enabled is meaningful only if you have defined Touchpoint Security policies in CA EEM.

Touchpoint Security

Specifies whether to inherit the value for Touchpoint Security configured in Environment properties, or set the value at the Touchpoint level.

Values:

- (Default) Inherit from Environment - same setting as for Environment.
 - Enabled - Enforce the applicable policy that specifies users allowed to execute operators on the current target, if it exists.
 - Disabled - Do not verify whether the user running the process has execute rights on the current target.
7. If this touchpoint is a proxy touchpoint, configure the following properties, otherwise, skip this step.

Proxy Touchpoint

Indicates whether this touchpoint is a proxy touchpoint. A proxy touchpoint is mapped to a host on which no agent is installed. A touchpoint that is not a proxy touchpoint is mapped to a host with an installed agent. Select to enable fields for configuring the remote host and values for SSH authentication.

SSH Keys Path

(Optional) The path on the agent host in which the private key file is stored. This field applies only if you generate a key pair for SSH public key authentication. Enter either the absolute path or a relative path.

Note: 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. The <user_name>.pub must be copied to the .ssh directory in the home directory of <user_name> on the remote host. Its contents must be appended to the authorized_keys file.

Remote Host

Specifies the fully qualified domain name (FQDN) or IP address of the target computer.

Note: See [Syntax for DNS Host Names](#) (see page 358).

Remote User Name

Specifies the user name with which a connection is made to the SSH Daemon on the target host. The SSH user account must have sufficient permissions to perform administrative tasks on the target computer.

Note: The <user_name> for the SSH user account on the remote host must match this value. The <user_name> specified when generating a key pair with ssh-keygen must match this value.

Remote Password

The password for the user account associated with the remote user name. This value is also used as the passphrase if connectivity is established through SSH public key authentication.

Maximum number of active processes

Specifies the maximum number of concurrent connections that the proxy touchpoint can open on the target remote host. Any process that is initiated after this threshold is reached is retained in queue until a running processes finishes.

Operating system

Specifies the operating system of the target remote host.

- (Default) Windows Variant - Manages categories of operators for Microsoft Windows operating systems such as Windows Server 2008.
- UNIX Variant - Manages categories of operators for operating systems such as Solaris and Linux.

8. Click Apply.
9. Click Save.
10. Right-click the environment and select Unlock.

Rename a Touchpoint

Renaming a touchpoint has no prerequisites unless the Run Program operator or Run Script operator run on this touchpoint.

Important! The Run Program operator and the Run Script operator in the Command Execution category reference touchpoints directly by name. For that reason, renaming a touchpoint requires you to update references to the touchpoint in the Run Program operator and the Run Script operator before renaming.

You can rename a touchpoint.

Follow these steps:

1. Click the Configuration tab.
2. Right-click the environment you want to configure, and click Lock.
3. Right-click the touchpoint in the environment that you want to rename, and click Rename.
4. Enter the new name of the agent touchpoint, and click OK.
5. Right-click the environment, and click Unlock.
The Unsaved Data dialog prompts you to save changes.
6. Click Yes.

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 referenced in the process is associated with only one agent and that agent is installed on a host scheduled for decommission. If the touchpoint was associated with multiple agents, no action would be 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 in CA Process Automation 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.

To replace the agent association for a given touchpoint

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.
A Warning message appears that requests confirmation before deleting the agent touchpoint.
4. Click OK.
The agent 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 190)

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.

Important! Only remove touchpoints that are not referenced in processes that are still needed.

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.

To remove empty touchpoints in bulk

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 192)

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:

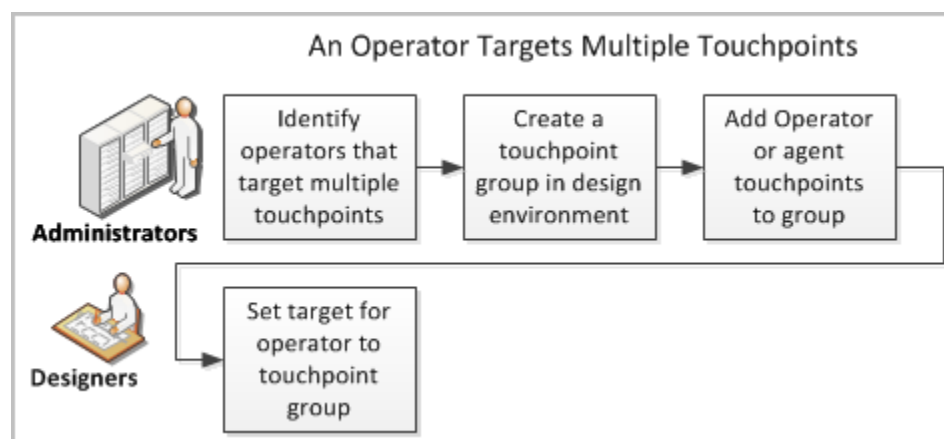
- The Reload command that is executed on a touchpoint group updates the touchpoint list for all touchpoints within the group.
- The Refresh command that is executed on a touchpoint group updates property settings for all touchpoints in the group.
- An operator that is configured to execute on a group 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

Create a touchpoint group that can serve as an operator target when a given operator must target multiple touchpoints at once. The process automation plan can include the identification of operators that must run on multiple hosts at the same time. The scenario is illustrated as follows:



The Copy to menu option for Operator touchpoints and agent touchpoints is used as part of this scenario. If you need to execute an operator on multiple Operator touchpoints at once, do the following:

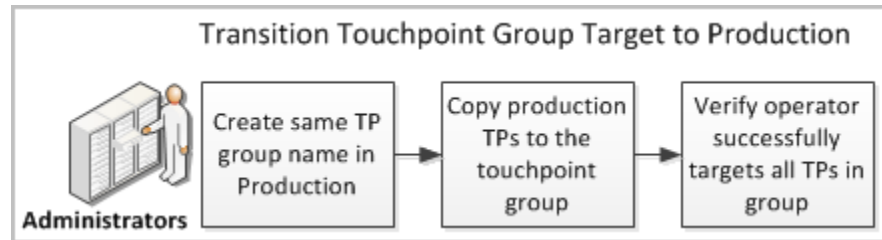
1. Create a touchpoint group.
2. Copy the Operator touchpoints to this group
3. Specify the touchpoint group name as the target for the operator.

If you need to execute an operator on multiple agent touchpoints at once, do the following:

1. Create a touchpoint group.
2. Copy the agent touchpoints to this group.
3. Specify the touchpoint group name as the target for the operator.

You also can include Operator and agent touchpoints in the same touchpoint group.

When administrators transition a touchpoint group target to the production environment, they retain the touchpoint group name. They associate the production Orchestrators or agents 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 or agent represented by a touchpoint in that group.



Create a Touchpoint Group with Selected Touchpoints

You add a Touchpoint Group at the environment level. You select each touchpoint for the group from the Domain hierarchy. You can select an Orchestrator touchpoint or an agent touchpoint. You use the Copy to option to copy a selected touchpoint to a touchpoint group.

Follow these steps:

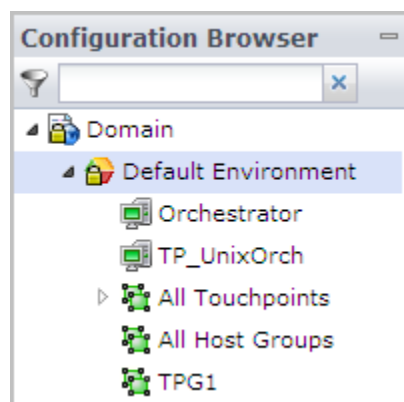
1. Click the Configuration tab.
2. Expand the Domain hierarchy to display the Orchestrators in a given environment.
3. Create a touchpoint group:

- a. Right-click an environment and select Add New Group.

The Add Touchpoint Group dialog opens.

- b. 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.

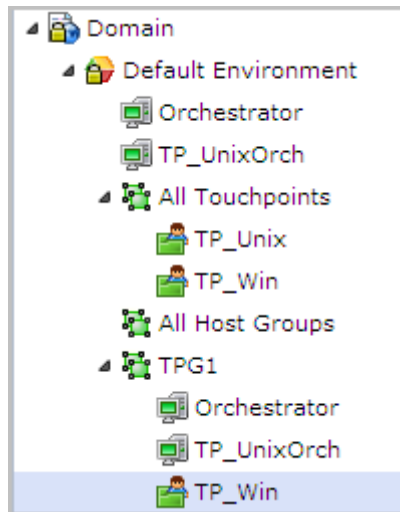


- c. Click Save.

Note: You cannot successfully add an Orchestrator to an unsaved touchpoint group.

- 4. Copy Orchestrator touchpoints and agent touchpoints to the touchpoint group. An example follows:
 - a. Right-click an Orchestrator and 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 and select the same <group name>.
 - d. Click Save.
 - e. Expand All Touchpoints, right-click an agent touchpoint, select Copy to and select the same <group name>.

The TPG1 touchpoint group displays contents of two Orchestrator touchpoints and one agent touchpoint in the following example:



More information:

[Manage Touchpoint Groups](#) (see page 207)

Create a Touchpoint Group

You can create your own named groups to group touchpoints functionally or logically.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain, select the environment to configure, and click Lock.
3. Right-click the environment, and click Add New Group.
4. In the Add touchpoint Group dialog, enter a name for the new touchpoint group.
5. Click OK.
6. Select the environment, and select Unlock.
The Unsaved Data dialog prompts you to save changes.
7. Click Yes.

Rename a Touchpoint Group

Content administrators can rename a touchpoint 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 rename, and click Rename.
4. Enter a new name for the group, and click Enter.
5. Select the environment and select Unlock.
The Unsaved Data dialog prompts you to save changes.
6. Click Yes.

Add a Touchpoint to a Touchpoint Group

You can add a touchpoint to any existing group using the Copy To functionality.

To add a touchpoint to a group

1. Click the Configuration tab.
2. Expand the Domain, select the environment to configure, and click Lock.
3. Right-click a touchpoint that you want to add to a group, point to Copy To, and click the group name.

The specified group now contains a shortcut for the touchpoint.

4. Repeat the previous step to add more touchpoints to the group.
5. Select the environment and click Unlock.

The Unsaved Data dialog prompts you to save changes.

6. Click Yes.

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](#) (see page 215)

[Configure Proxy Touchpoint Properties](#) (see page 218)

[Use a Proxy Touchpoint](#) (see page 221)

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 5.0 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 216)
- [Create the SSH User Account on the Remote Host of the Proxy Touchpoint](#) (see page 217)
- [Create an SSH Trust Relationship to the Remote Host](#) (see page 217)
- [Configure Proxy Touchpoint Properties](#) (see page 218)

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 216)

Configure Proxy Touchpoint Properties

You can create a proxy touchpoint by reconfiguring an existing agent touchpoint to target the 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, click the agent touchpoint to make a proxy touchpoint.

- Click the Properties tab. Either set the following properties or use the default values.

Operators Auto Recovery

Specifies whether to automate recovery. Recovery applies to certain operators that fail with a `SYSTEM_ERROR`. Operators subject to recovery must be part of processes that are in a `BLOCKED`, `RUNNING`, or `WAITING` state. Select `True` to begin recovery when this proxy touchpoint becomes active. Each Orchestrator within the environment automatically initiates the recovery. Recovery starts running the affected processes. The operators that target the proxy touchpoint run.

Values:

- (Default) Inherit from Environment - same setting as for Environment.
- `True` - Automate recovery.
- `False` - Do not automate recovery.

Touchpoint Security

Specifies whether to inherit the value for `Secure` configured in Environment properties, or set the value to `Enabled` or `Disabled` at the touchpoint level.

Values:

- (Default) Inherit from Environment - same setting as for Environment.
- `Enabled` - Enforce each applicable policy that identifies the users that are allowed to execute operators on the current target.
- `Disabled` - Do not verify whether the user running the process has execute rights on the current target.

- Select the Proxy Touchpoint check box.

Proxy Touchpoint

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. Selection enables fields for configuring the remote host and values for SSH authentication.

- Configure the following properties:

SSH Keys Path

If you generated a key pair for SSH public key authentication, specifies the path on the agent host for storing the private key file, `user_name`. Enter either the absolute path or a relative path.

Note: 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.

Remote Host

Specifies the fully qualified domain name (FQDN) or IP address of the target computer.

Note: See [Syntax for DNS Host Names](#) (see page 358).

Remote User Name

Specifies the user name with which to connect to the SSH Daemon on the target host. The SSH user account must have sufficient permissions to perform administrative tasks on the target computer.

Remote Password

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.

Maximum number of active processes

Specifies the maximum number of concurrent SSH connections that the proxy touchpoint can open on the target remote host. 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.

Operating system

Specifies the operating system of the target remote host.

- (Default) Windows Variant - Manages operator categories for Microsoft Windows operating systems such as Windows Server 2008.
- UNIX Variant - Manages operator categories for operating systems such as Solaris and Linux.

7. Click Save.
8. Right-click the environment and select Unlock.

More information:

[Add a Touchpoint to a Selected Environment](#) (see page 197)

[Configure Touchpoint Properties](#) (see page 201)

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 207)

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 358).

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:

[How a Target Host Can Be Specified in an Operator](#) (see page 223)

[About Host Groups](#) (see page 224)

[How Host Groups Compare to Proxy Touchpoints](#) (see page 225)

[Host Group Implementation Process](#) (see page 226)

[View Details about All Host Groups](#) (see page 238)

How a Target Host Can Be Specified in an Operator

Content designers can create operators that execute on target hosts that have a touchpoint associated with either an active agent or an Orchestrator. Content designers reference such a host by its touchpoint name.

Content designers can create operators that execute on target hosts that have no active agent. Such a remote host is an eligible target if it has a proxy touchpoint or a host group reference. Content designers reference a host mapped to a proxy touchpoint by its proxy touchpoint name.

Content designers can create an operator that executes on the same target host each time the operator executes by specifying the target with its *AgentID*. The content designer must copy this System variable from the dataset generated by a previous execution of this same operator and paste it into the Target field of the operator.

To support the ability to specify a target host with its IP address or FQDN, administrators configure a host group that includes a reference to target hosts. Because a host group is defined as a subnet or a host name pattern, a host group can include hosts that have associated touchpoints or proxy touchpoints.

When a given target can be referenced in multiple ways, content designers with an interest in efficient processing use the first applicable reference from the following list.

1. Touchpoint, if the Orchestrator or an agent is running on the target.
2. Proxy touchpoint, if the target is a remote host for which a proxy touchpoint is defined.
3. IP address or FQDN, if the target is a remote host and the designated name or IP address matches a pattern configured in a host group.
4. IP address or FQDN, if you cannot identify the Orchestrator or touchpoint running on the IP/FQDN at runtime.
5. Agent ID of the agent or Orchestrator, if the operator must run on a specific agent or Orchestrator.

Note: For details, see the *Content Administrator Guide* appendix, "How Targets of an Operator Are Processed."

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, hostname 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.

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.

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.

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 227).
2. [Configure the Host Group Properties](#) (see page 229). 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 232).
 - (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 5.0 or later 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 234). 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 235).
- [Create a trust relationship to a remote host referenced by a host group](#) (see page 236).

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 216)

Create a Host Group

You can create a host group in either of the following ways:

- Add a host group to a selected environment and then select the agent.
- Configure a host group on an agent and then select the environment.

Within an environment, the agent name to host group name combination must be unique. That is, you cannot use the same name for two host groups with different configurations.

To create a host group through an environment and then select the agent

1. Click the Configuration tab.
2. Select the environment you want to configure and click Lock.
3. Right-click the locked environment, and select Add Host Group.

The Add Host Group: *environment* appears.

4. Enter the host group name.
5. Select a displayed agent and click Add.

The dialog closes. The host group name appears under All Host Groups for the selected environment.

To create a host group on an agent and then select the environment

1. Click the Configuration tab.
2. Expand the Agents node.
3. Right-click the desired agent, select Configure Host Group at, and select the desired environment.

If the environment is not locked, the following message appears: "Environment "<selected environment>" must be locked before configuring a new touchpoint. Do you want to lock it first?"

Click Yes.

The Add Agent Host Group dialog appears.

4. 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. The new host group s displayed under All Host Groups for the selected environment.
 - Click the Agents palette 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 226)

Configure Host Group Properties

Configuring host group properties includes:

- Specifying whether the computers referenced by the host group have an operating system that is a Windows variant or a UNIX variant.
- Specifying values the agent host uses to gain SSH access to each remote host referenced by the associated host group.
- Specifying how operators auto recovery is handled.
- Specifying how remote hosts in this host group are secured from unauthorized execution of operators.
- Specifying the maximum number of active processes. This threshold controls the number of SSH connections to the target remote host. Most SSHD servers 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, per destination. If you set the value to 20 and run 40 scripts at the same time on the same target host, only 20 run concurrently. New ones start as others finish. With host groups, where the same agent acts a proxy for multiple remote hosts, each remote host has its own 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. Certain operating systems support a high number of current TCP connections.

You can configure a host group.

Follow these steps:

1. Click the Configuration tab.
2. Expand the Domain.
3. Expand the environment with the host group to configure.
4. Expand All Host Groups.
5. Select the host group to configure and click the Properties tab.

6. Set the properties of the selected host group.

Operators Autorecovery

Specifies whether to automate recovery. Recovery applies to operators that fail with a `SYSTEM_ERROR` and whose recoverable processes are in `BLOCKED`, `RUNNING`, or `WAITING` state when the recovery is triggered. When automatic recovery is configured and the previously inactive host group becomes active, recovery processing is done. Affected operators begin running on the specified remote host referenced by this host group and their processes continue execution.

Values:

- (Default) Inherit from Environment - same setting as for Environment.
- True - Automates recovery.
- False - Prevents automated recovery.

Touchpoint Security

Specifies whether to inherit the value for Touchpoint Security configured in Environment properties, or set the value to true or false at the touchpoint level.

Values:

- (Default) Inherit from Environment - same setting as for Environment.
- Enabled - Enforce applicable policy that specifies users allowed to execute operators on the current target.
- Disabled - Do not verify whether the user running the process has execute rights on the current target.

SSH Keys Path

(Optional) Indicates the location on the agent host where the private key file is stored. CA Process Automation accesses this location for the private key required when connecting to a remote host through SSH public key authentication. For example:

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.

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*.

Note: See [Syntax for DNS Host Names](#) (see page 358).

Remote User Name

Specifies the user name to assign to the user account on *each* remote host referenced by the host group. This name is used to connect to the SSH Daemon on the target remote host.

If you configure public key authentication, this value must be specified as the *user-name* in the command to generate key files.

Remote Password

The password associated with the Remote User Name. This same password must be defined in the user account defined on each host referenced by a given host group.

If using public key authentication with a passphrase, specify this value as the passphrase when creating the keys.

Maximum Number of Active Processes

Specify the maximum number of concurrent connections that can be open simultaneously on any remote host.

Note: When that number is reached, further tasks wait for the next available connection.

Operating system

Indicate the operating systems of the remote hosts. Select from the following:

- (Default) Windows Variant - Manages categories of operators for Microsoft Windows operating systems such as Windows Server 2008.
- UNIX Variant - Manages categories of operators for operating systems such as Solaris and Linux.

7. Click Save to save the changes.
8. Right-click the locked environment and select Unlock.

More information:

[Host Group Implementation Process](#) (see page 226)

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.
\.	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.comaaaaaa)

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>/c2otmp
```

More information:

[Host Group Implementation Process](#) (see page 226)

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

You can create a trust relationship between a host with a host group configured on its agent and a target remote host referenced in the host group. Creating such a trust relationship is optional. When you create a user account on the target host *and* a trust relationship to that host, the trust relationship serves as a backup mechanism for creating SSH connectivity. If user/password authentication fails, CA Process Automation uses private/public key-based authentication.

To make SSH key-based authentication available, first use the SSH-keygen program to generate a private/public key pair and save the private key to the path configured as SSH Keys Path. Next, copy the public key file to each remote host referenced by the host group. On each remote host, place 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 referenced by a host group.

Follow these steps:

1. Log on to the host with the agent on which the host group is defined.
2. Open a command prompt and change directories to a path from which you want to generate the key pair.

For example, if you downloaded OpenSSH on a Windows system, change directories to `C:\Program Files\OpenSSH\bin` for the directory containing the `ssh-keygen` executable file.

3. Generate a key pair with the following command, where `user_name` must be the value you configured as Remote User Name in the Host Group:

```
ssh-keygen -t dsa -b 1024 -f user_name
```

The following message and prompt appear:

```
Generating the public/private dsa key pair.
```

```
Enter passphrase <empty for no passphrase>:
```

4. Enter the value you configured as Remote Password in the Host Group. This value is required.

The following prompt appears:

Enter same passphrase again:

5. Enter the Remote Password value again.

The following messages appear:

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 private key file named *user_name* and the public key file named *user_name.pub* are created. The passphrase for the key file is the same as the password on the user account used for SSH access.

6. Move the private key file named *user_name* in the location 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 referenced by the host group and place it where the SSH Daemon can find it.

Different SSH Daemons follow different conventions. Examine the `ssh-keygen` options for formatting requirements for the public key file.

8. For OpenSsh, the public key contained in *user_name.pub* must be appended to the file which contains all authorized keys used by that host. The OpenSSH SSH daemon, `sshd`, searches the `authorized_keys` file. The `authorized_keys` file is expected to be present in the `.ssh` directory in the home directory path.

- a. Run the following `cat` command on each host referenced by the host group:

```
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 from the agent host.

```
ssh user_name@remote_host
```

More information:

[CA Process Automation-Specific Requirements for SSH Connectivity](#) (see page 216)
[Host Group Implementation Process](#) (see page 226)

View Details about All Host Groups

You can view the names of each host group in the selected environment, with its status and the display name of the agent to which it is associated.

To view details about all host groups in a selected environment

1. Click the Configuration tab.
2. Click the All Host Groups node under a selected environment.
3. Examine the list in the HostGroupData tab.

Chapter 12: Administer Operators By Category

This chapter describes how to configure common default settings for operators at the category level and relevant concepts.

This section contains the following topics:

[Operator Categories and Operator Folders](#) (see page 240)

[Example: Category Settings Used by Operator](#) (see page 242)

[Configuring Operator Categories](#) (see page 244)

[Category Configuration and Operator Inheritance](#) (see page 294)

[Enable or Disable an Operator Category](#) (see page 295)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Operator Categories and Where Operators Run](#) (see page 298)

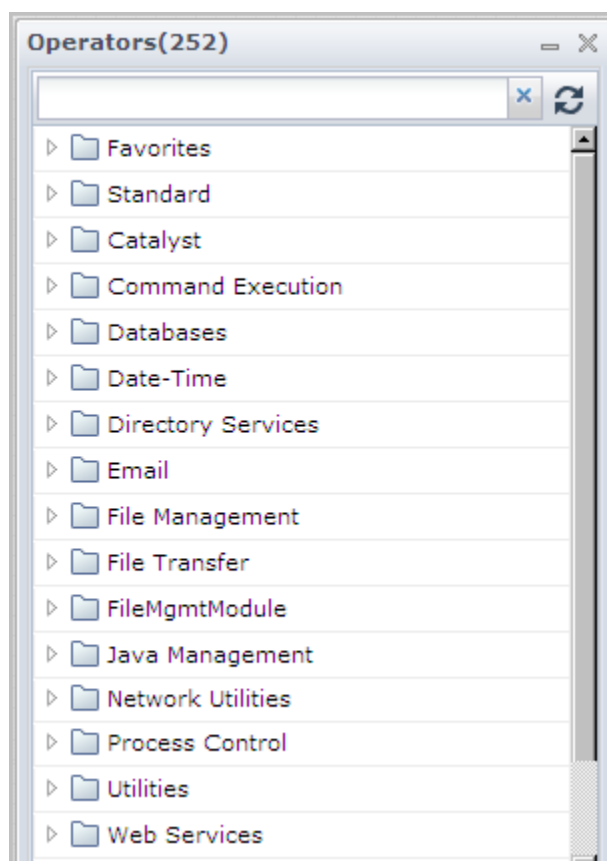
Operator Categories and Operator Folders

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. Operator folders are displayed in the Operators palette in the Design tab.

When you click the Configuration tab, select Domain, and click the Modules tab, the operator categories are listed under Name.

Contents of "Domain"				
Security	Properties	Modules	Triggers	Audit trails
Name ^	Description			
Catalyst	Provides access to Catalyst connectors			
Command Execution	Runs programs and scripts on host operating environments.			
Databases	This is the Databases Module to talk to various database servers			
Date-Time	Executes time and calendar constraints in CA Process Automation processes.			
Directory Services	Provides an interface to support LDAP/AD.			
Email	This is the mail service which read mails from the server through IMAP/POP3 protocols.			
File Management	This module monitors directory, files, and their contents			
File Transfer	Provides file transfer operations (FTP/SFTP).			
Java Management	Provides a management interface to external system that support JMX.			
Network Utilities	Provides various utilities and operations to network services.			
Process Control	Runs, monitors and controls CA Process Automation Processes.			
Utilities	This module consists of utility operators which are used in PAM processes			
Web Services	Provides an interface to external services exposed through SOAP.			

When you click the Design tab, click View and select Operators, the displayed folder names reflect the same operator grouping as the operator categories you configure.



Content designers create automated processes with operators they select from the Operators palette. Each operator performs a distinct operation. To help designers quickly locate the operator they need, operators are grouped by 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 operator category values at the Domain level. The values are inherited at the environment level, and then at the Orchestrator or Agent touchpoint level. Inherited values can be overridden at any level. Operator category default values are then inherited by the operators. Content designers can accept or override these values.

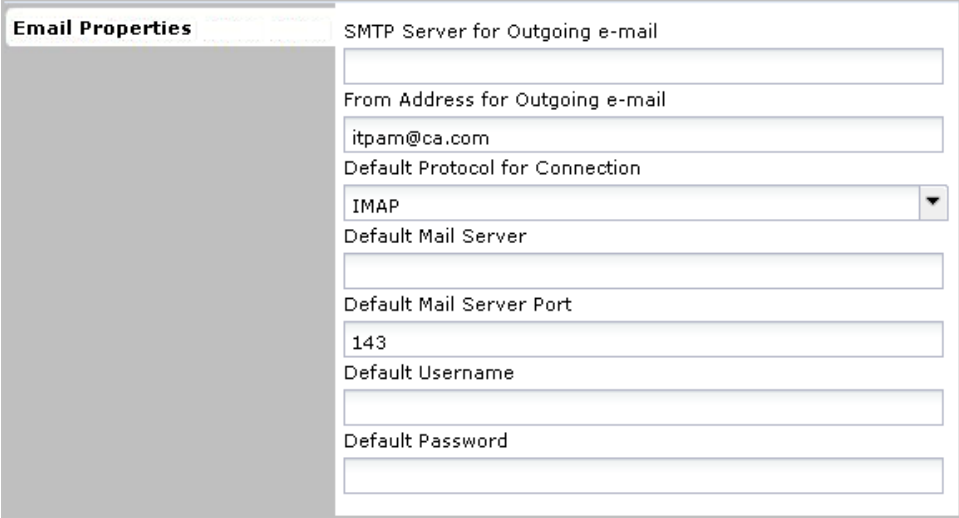
More information:

[Category Configuration and Operator Inheritance](#) (see page 294)

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.

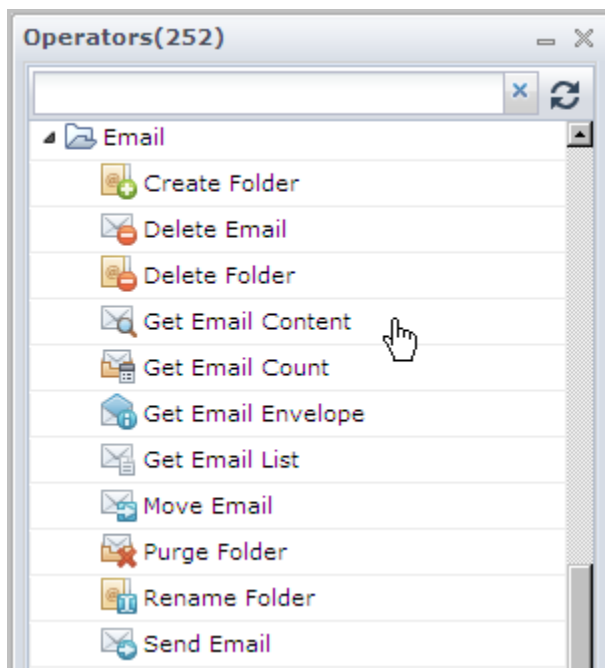
Consider the configuration in Email Properties, where the Default Protocol for Connection is set to IMAP and the Default Mail Server Port is set to 143. You configure the default mail server, default user name, and default password.



The screenshot shows a configuration window titled "Email Properties". On the left is a grey sidebar with the title "Email Properties". The main area contains several settings:

- SMTP Server for Outgoing e-mail: [Empty text box]
- From Address for Outgoing e-mail: itpam@ca.com
- Default Protocol for Connection: IMAP (dropdown menu)
- Default Mail Server: [Empty text box]
- Default Mail Server Port: 143
- Default Username: [Empty text box]
- Default Password: [Empty text box]

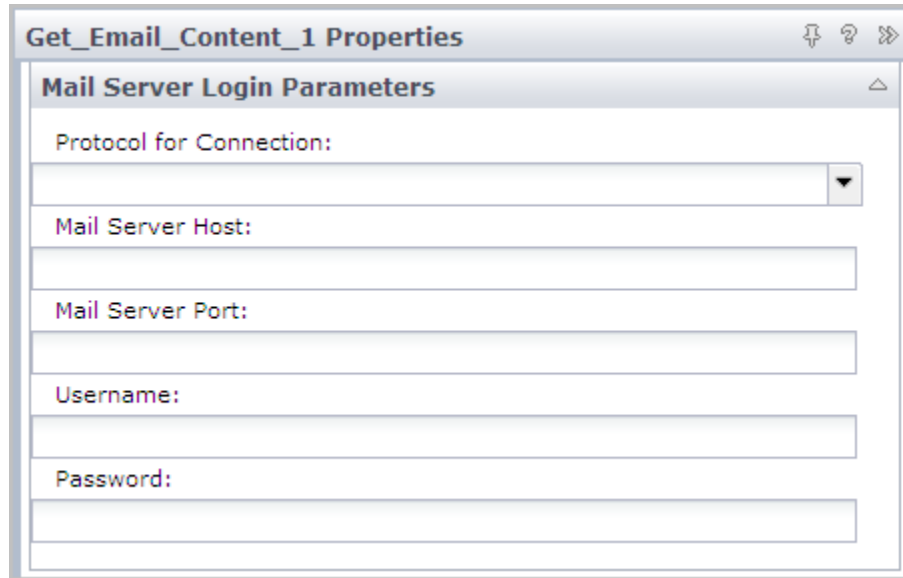
When a content designer automates a process for email, one of the operators available for use is Get Email Content.



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 Design 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 with Domain Administrator rights can 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 296).

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.

You can override any configured setting at the operator level.

Note: For details on operator level overrides, see the *Content Designer Reference*.

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.

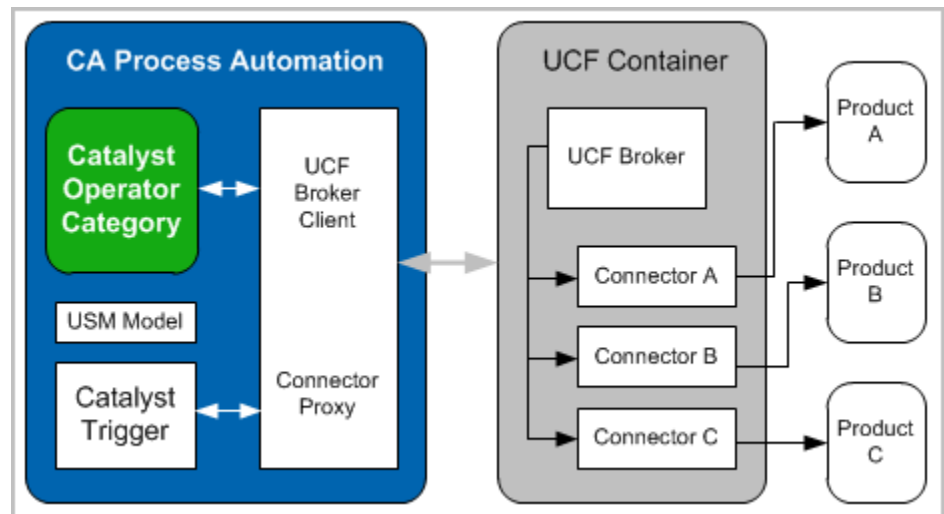
The CA Process Automation Catalyst allows Unified Connector Framework (UCF) connectors to be used in automated processes. The Catalyst operators support the UCF create, read, update, delete (CRUD), and event subscription interfaces. The operators expose Unified Service Model (USM) object types and properties.

Using the common USM Model and standard UCF interfaces allows Catalyst to be compatible 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, using the UCF Broker and Connector proxy interfaces, as illustrated:



Configure Catalyst

You can configure Catalyst by completing four tabs. The password values are encrypted

Follow these steps:

1. Click the Configuration tab.

The Configuration Browser opens with Domain selected by default.

2. Click the Modules tab.
3. Right-click Domain and select Lock.
4. Right-click Catalyst and select Edit.

The Catalyst Property tab opens.

5. Complete the following settings:

UCF Broker URL

Specifies the default UCF Broker URL. The associated Operator inherits this setting.

Product property configuration file name

Specifies the name of the Product property configuration file. This file is used to customize the properties shown in the generic Create operator.

6. Click Save.
7. Click the Catalyst Security tab.
8. Enter your values using the following descriptions as needed.

Default Username

Specifies the Catalyst user ID.

Default Password

Specifies the Catalyst password that is associated with the Default Username.
The password values are encrypted.

9. Click the Catalyst Claims tab and complete the configuration.

Default Claims

Click Add and enter the first claim name with its value.

Repeat this step for each default claim.

Use the up and down arrows to sequence the claims as needed.

Claim Name

Specifies the name of the claim.

Claim Value

Specifies the value for the named claim.

10. Click the Catalyst Password Claims tab and complete the configuration.

Default password claims

Click Add and enter the first claim name with its value.

Repeat this step for each default password claim.

Use the up and down arrows to sequence the claims as needed.

Claim Name

Specifies the name of the claim.

Claim Value

Specifies the value for the named claim.

11. Click Save and Close.

The values configured in the open dialog are saved.

12. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

13. With Domain still selected, click Unlock.

14. If you are finished configuring the operator categories on the Modules tab, right-click Domain and select Unlock.

More information:

[About Catalyst](#) (see page 245)

[Category Configuration and Operator Inheritance](#) (see page 294)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Configuring Operator Categories](#) (see page 244)

Load Catalyst Descriptors

A Catalyst connector descriptor specifies the capabilities of the connector, including the operations that it supports. Each operation further specifies its parameters. Descriptors that you load into CA Process Automation display in the Execute operator (in the Catalyst operator category). The descriptors are displayed at various levels: Operation Categories (drop down), Operation (drop down), and Parameters (editor values).

You can load a Catalyst descriptor from your local host into the remote Domain Orchestrator as a user resource. All resources are replicated to each new Orchestrator.

Follow these steps:

1. Click the Configuration tab.
2. Expand Manage User Resources in the left pane.

3. Expand the root folder and select the ucf subdirectory.
An entry for the CA Process Automation embedded connector displays.

4. Click New resource.

5. Enter the following fields:

Resource Name

The name of the descriptor.

Resource Path

Leave this field blank; the ucf subfolder path was defined in step 3.

The jar must be loaded into the ucf directory.

Resource File

Browse to and select the descriptor JAR file.

Module Name

If you want to group descriptors by module (operator category), enter the name.

Resource Description

Enter any information about the descriptor.

6. Click Save.

The descriptor displays in the list of user resources.

Note: The descriptor is available in the Execute operator once you restart the Orchestrator. See the *Content Designer Reference* for more information about the Execute operator in the Catalyst category.

More information:

[Manage User Resources](#) (see page 319)

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](#) (see page 251)

Configure Command Execution

Administrators who can lock the Domain can configure Command Execution settings at the Domain level. Values for all fields can be overridden at the operator level. The values you enter for this 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 *Reference Guide* for the operator configuration of these same fields.

Command Execution configuration is entered in the following tabs:

- Telnet Properties
You configure connectivity and specify the login scheme and related details. You also indicate whether to switch users after logging in to the remote host, and specify the switching details.
- SSH Properties
You configure specifications of the terminal type, the authentication details for logging on to a remote host, and optionally, options for switching users after login.
- Windows Command Execution Properties
- UNIX Command Execution Properties

Follow these steps:

1. Click the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab, right-click Command Execution, and select Edit.
4. Select the Telnet Properties tab.

Default Pseudo Terminal Type

Specifies the default pseudo terminal to request on the Telnet connection.

Default:

VT100

Default Port

Specifies the default port to use to connect to the remote host.

Note: Port 23 is the system TCP/UDP port for Telnet.

Default:

23

Default Connection Timeout (sec)

Specifies the number of seconds the connection waits to time out.

Values:

Any positive integer.

Default Login Scheme

Specifies the default login scheme.

Values:

This value can be one of the following:

- User name and password
- Password only
- Log in without user name and password.

Default User Login Text Prompt

Specifies a regular expression for Login or something similar. The default text prompt value that accepts a login id.

This prompt is typically "Login: " or "login: ". Specifying ".*ogin: " matches any input (including new lines), a lowercase "l" or an uppercase "L" followed by "ogin: ".

Example Value:

.*ogin.*:

Default User name

Specifies the user name to use to log in to the remote host.

Default Password Text Prompt

Specifies a regular expression for the default text prompt that indicates that the remote host requires a password for the user logging in.

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" followed by anything or nothing followed by a colon.

Example value:

.*assword.*:

Default Password

Specifies the default password to use for logging in to the remote host.

Default User Command Prompt

Specifies a regular expression for the command prompt that indicates that the remote host is ready for commands.

Typical command prompts are "#", ">", "\$". The entry, ".*[\$>?:#]", matches any input (including new lines) followed by \$ (dollar sign), > (greater than), ? (question mark), : (colon), or # (pound sign).

Example value:

```
.*[$>?:#]
```

Note: When you use a regular expression, enclose the dollar sign in square brackets, that is, [\$]. A dollar sign without brackets has a special meaning in regular expressions.

Default Time to Wait for Prompts (sec)

Specifies the number of seconds to wait for a command prompt before giving up on the prompt to send the commands.

Default Run Commands as Another User?

Specifies whether to run the script or the specified commands as a different user.

Values:

This value can be one of the following:

- Selected - Indicates to switch users after login.
- Cleared - Indicates not to switch users after login.

Default:

Cleared.

Default Switch User Command

Specifies the operating system-specific command to switch user on the remote host. The command "su -root" switches users to the root user.

Example commands:

```
su - <username>
```

```
sudo su - <username>
```

Default Switch User Password Text Prompt

(Optional) If the remote host requires a password for switching the logged on user to another user, specifies the default text prompt as a regular expression.

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: ".

Example value:

```
.*assword.*:
```

Default Switch User Password

(Optional) If the remote host requires a password for switching the logged on user to another user, specifies this default password to enter at the password text prompt.

Default Switch User Command Prompt

Specifies the command prompt, as a regular expression, for the prompt that indicates that the remote host is ready for commands as the switched user.

Typical command prompts are "#", ">", "\$". The entry, ".*[\$>?:#]", matches any input (including new lines) followed by \$ (dollar sign), > (greater than), ? (question mark), : (colon), or # (pounds sign).

Example values:

```
.*[$]
```

```
.*[$>?:#]
```

Note: When you use a regular expression, enclose the dollar sign in square brackets, that is, [\$]. A dollar sign without brackets has a special meaning in regular expressions.

5. Select the SSH Properties tab.

Default Pseudo Terminal Type

Specifies the pseudo terminal type to request on the SSH connection. (VT100 typically works with Linux hosts; VT400 typically works with Windows hosts.)

Default:

```
VT100
```

Default Port

Specifies the default port to use to connect to the remote host.

Note: Port 22 is the well-known TCP/UDP port for the Secure Shell (SSH) Protocol

Values:

- 22
- Another valid port number. The range of valid port numbers ends at 65535.

Default:

22

Default User name

Specifies the user name to use when logging in to the remote host.

Use Default Private Key for Login?

Specifies whether to use a private key for logging in. (The alternative is to use password information.)

Values:

This value can be one of the following:

- Selected - Indicates to use a private key for logging in.
Note: The operator setting determines whether the operator uses the specified Default Private Key Inline Content or the specified Default Private Key Path.
- Cleared - Indicates not to use a private key; rather, use a password, where the default is your entry for Default Password.

Default:

Cleared

Default Password

Specifies the default password to use for logging in to the remote host.

Default Private Key Inline Content

Specifies the content of a default private key for logging in to the remote host. (Click Browse (...) and retrieve the key content.)

Default Private Key Path

Specifies the path to a default private key for logging in to the remote host.

Default Passphrase for Key

Specifies the passphrase to unlock the content of the default private key.

Note: The passphrase is required if the default private key was created with a passphrase.

Default Run Commands as Another User?

Specifies whether to run the script or the specified commands as a different user.

Values:

This value can be one of the following:

- Selected - Indicates to switch users after login.
- Cleared - Indicates not to switch users after login.

Default:

Cleared

Default Switch User Command

Specifies the operating system-specific command to switch user on the remote host. The command "su -root" switches users to the root user.

Example commands:

```
su - <username>
sudo su - <username>
```

Default Switch User Password Text Prompt

(Optional) If the remote host requires a password for switching users, specifies a regular expression for the default text prompt.

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: ".

Example value:

```
.*assword.*:
```

Default Switch User Password

(Optional) If the remote host requires a password for switching users, specifies the password to enter at the password text prompt.

Default Switch User Command Prompt

Specifies 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 "#", ">", "?". The entry, ".*[\$>?:#]", matches any input (including new lines) followed by \$ (dollar sign), > (greater than sign), ? (question mark), : (colon), or # (pound sign).

Example values:

```
.*[$]
```

```
.*[$>?:#]
```

Note: When you use a dollar sign in a regular expression, enclose it within a pair of square brackets. A dollar sign without brackets has a special meaning in regular expressions.

6. Select Windows Command Execution Properties

Default shell

Shell command interpreter to use for the profile and for shell commands.

Example: cmd.exe. (Do not use Command.exe.)

Default profile

Defines a shell script file that is interpreted before starting a user process for which no profile is indicated. The profile file is interpreted using the command interpreter specified by Shell program. The profile can contain any noninteractive command understood by the shell interpreter.

Require user credentials

Select one of the following from the drop-down menu to specify that Process operators use the selected option when user credentials are not specified.

- (Default) Defaults to the user under which touchpoint is run.
Process operators use the user credentials under which the agent or Orchestrator process is running.
- Defaults to the specified Default user.
Process operators use the user credentials configured as Default user and Default password.
- No default.
Process operators use the user credentials supplied at runtime.

Default user

The shell account to use when starting user processes that lack a user name and a password.

- Specify a user ID with only necessary permissions to prevent users from defining and launching processes through CA Process Automation to which they otherwise have no access.
- Leave the user ID and password blank to force users to enter a user name and password when they start processes through CA Process Automation.

Default password

The password for the Shell user account.

Note: Passwords that are part of Command Execution configurations are protected and cannot be modified through a program, referenced, or passed to external methods.

Confirm Password

Reenter the Default password for confirmation.

Load OS User Profile

Specifies whether to load the user profile associated with the specified default user and default password.

Selected

Loads the user profile.

Cleared

Does not load the user profile.

7. Select UNIX Command Execution Properties.

Default shell

Shell command interpreter to use for the profile and for shell commands.

Examples - One of the following:

/bin/bash

/bin/csh

/bin/ksh

Default profile

Defines a shell script file that is interpreted before starting a user process for which no profile is indicated. The profile file is interpreted using the command interpreter specified by Shell program. The profile can contain any noninteractive command understood by the shell interpreter.

Require user credentials

Select one of the following from the drop-down menu to specify that Process operators use the selected option when user credentials are not specified.

- (Default) Defaults to the user under which touchpoint is run.
Process operators use the user credentials under which the agent or Orchestrator process is running.
- Defaults to the specified Default user.
Process operators use the user credentials configured as Default user and Default password.
- No default.
Process operators use the user credentials supplied at runtime.

Default user

The shell account to use when starting user processes that lack a user name and a password.

- Specify a user ID with only necessary permissions to prevent users from defining and launching processes through CA Process Automation to which they otherwise have no access.
- Leave the user ID and password blank to force users to enter a user name and password when they start processes through CA Process Automation.

Default password

The password for the Shell user account.

Note: Passwords that are part of this configuration are protected and cannot be modified through a program, referenced, or passed to external methods.

Confirm Password

Reenter the Default password for confirmation.

Load OS User Profile

Specifies whether to load the user profile associated with the specified default user and default password.

Selected

Loads the user profile.

Cleared

Does not load the user profile.

Disable Password Check

One of the following settings:

Selected - Disables password checking.

Cleared - Verifies the specified password.

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. With Domain selected, click Unlock.

More information:

[About Command Execution](#) (see page 249)

[Category Configuration and Operator Inheritance](#) (see page 294)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Configuring Operator Categories](#) (see page 244)

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.

Configure Databases: Oracle Properties

You can configure the Databases category of operators for Oracle.

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab, select Databases, and click Edit.
4. Click the Oracle Properties tab.
5. Complete the following settings:

Default Driver Type

Specifies the default type of Oracle JDBC driver.

Note: Use a JDBC version that matches the version of the Java Development Kit.

Values:

Select one of the following values:

- thin

The Thin Driver type is for use 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 for use on the client-side with Oracle installed. OCI drivers use the Oracle Call Interface (OCI) for interactions with the Oracle database.

- kprb

The KPRB driver is used for writing Java database stored procedures and triggers.

Default Driver

Specifies the value `oracle.jdbc.OracleDriver` as the default driver.

Default Server Host

Specifies the host where the Oracle database is running.

Default Server Port

Specifies the default port for the Oracle database.

Default UserName

Specifies the default user name for the Oracle database user.

Default Password

Specifies the password that is associated with the specified Default UserName.

Default ServiceID

Specifies the Oracle Service ID.

Default TNS Name

Specifies 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 connectivity to the database. This information includes information such as the IP address, the port, and the database Service ID.

Default Maximum Rows

Specifies the default maximum rows to retrieve.

Valid values:

10 to 512

Default:

10

Default Client Encryption

Specifies one of the data encryption methods that Oracle supports, where RCA_128 and RCA_256 are for domestic editions only.

Values:

- RC4_40
- RC4_56
- RC4_128
- RC4_256
- DES40C
- DES56C
- 3DES112
- 3DES168
- SSL
- AES128
- AES256
- AES192

Default Client Checksum

Specifies checksums that Oracle supports. See your Oracle documentation.

Default:

MD5

6. Click Save and Close.

The values configured in the open dialog are saved.

7. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

8. With Domain selected, click Unlock.

More information:

[Configuring Operator Categories](#) (see page 244)

[Category Configuration and Operator Inheritance](#) (see page 294)

[About Databases](#) (see page 260)

Configure Databases: MSSQL Server Properties

You can configure the Databases category of operators for MSSQL Server.

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab, select Databases, and click Edit.
4. Click the MSSQL Server Properties tab.
5. Complete the following settings:

Default Driver

Specifies com.microsoft.sqlserver.jdbc.SQLServerDriver as the default driver for MSSQL Server.

Default Server Host

Specifies the host where the MSSQL Server is running.

Default Server Port

Specifies the default MSSQL Server port, typically 1433.

Default UserName

Specifies the default user name for the MSSQL Server database user.

Default Password

Specifies the password that is associated with the specified Default UserName.

Default Maximum Rows

Specifies the default maximum rows to retrieve.

Valid values:

10 to 512

Default:

10

Default Database Name

Specifies the MSSQL database name.

Default Instance Name

Specifies the MSSQL instance name.

6. Click Save and Close.

The values configured in the open dialog are saved.

7. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

8. With Domain selected, click Unlock.

More information:

[About Databases](#) (see page 260)

[Category Configuration and Operator Inheritance](#) (see page 294)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Configuring Operator Categories](#) (see page 244)

Configure Databases: MySQL Properties

You can configure the Databases category of operators for the MySQL Server.

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab, select Databases, and click Edit.
4. Click the MySQL Server Properties tab.

5. Complete the following settings:

Default Driver

Specifies com.mysql.jdbc.Driver as the default driver for MySQL.

Default Server Host

Specifies the host where the MySQL database is running.

Default Server Port

Specifies the default MySQL database port.

Default UserName

Specifies the default user name for the MySQL database user.

Default Password

Specifies the password that is associated with the specified Default UserName.

Default Maximum Rows

Specifies the default maximum rows to retrieve.

Valid values:

10 to 512

Default:

10

Default Database Name

Specifies the MySQL database name.

6. Click Save and Close.

The values configured in the open dialog are saved.

7. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

8. With Domain selected, click Unlock.

More information:

[About Databases](#) (see page 260)

[Category Configuration and Operator Inheritance](#) (see page 294)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Configuring Operator Categories](#) (see page 244)

Configure Databases: Sybase Properties

You can configure the Databases category of operators for Sybase.

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab, select Databases, and click Edit.
4. Click the Sybase Properties tab.
5. Complete the following settings:

Default Server Type

Specifies the default Sybase relational database system.

Values:

Select one of the following values:

- Adaptive Sever Anywhere (ASA)
- Adaptive Server Enterprise (ASE)

Default Connection Protocol

Specifies the default connection protocol.

Default:

TDS

Default Driver

Specifies the default driver.

Default:

com.sybase.jdbc2.jdbc.SybDriver

Default Server Host

Specifies the host where the Sybase database is running.

Default Server Port

Specifies the default port for the Sybase database.

Default UserName

Specifies the default user name for the Sybase database user.

Default Password

Specifies the password that is associated with the specified Default UserName.

Default Maximum Rows

Specifies the default maximum rows to retrieve.

Valid values:

10 to 512

Default:

10

Default Cache Buffer Size

Specifies the amount of memory that the driver uses to cache insensitive result set data.

Values:

- -1

All data is cached.

- 0

Up to 2 GB of data is cached.

- X

Specifies 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.

Default Batch Performance Workaround

Specifies the default batch performance work-around.

Values:

- True

The JDBC v3.0 compliant mechanism

- False

The native batch mechanism.

6. Click Save and Close.

The values configured in the open dialog are saved.

7. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

8. With Domain selected, click Unlock.

More information:

[About Databases](#) (see page 260)

[Category Configuration and Operator Inheritance](#) (see page 294)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Configuring Operator Categories](#) (see page 244)

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

You can configure Directory Services. The Directory Services operator category provides an interface to support LDAP/AD.

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab.
4. Select Directory Services and click Edit.

5. Complete the following settings:

Batch Size

Specifies the batch size to return operation results, so the server can optimize performance and usage of resources. For example, 10.

Values:

- 0
The server specifies the batch size.
- See Limits.

Limits:

This value must be a whole number in the range from 1 through 10000.

Max Number of Search Results

Specifies the maximum number of objects to return when executing one of the following Directory Services operators:

- Get Object
- Get User

Limits:

This value must be a whole number in the range from 1 through 1000.

Factory Initial

Specifies the fully qualified class name of the factory class that creates an initial context.

Default:

`com.sun.jndi.ldap.LdapCtxFactory`

Factory State

Specifies 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.

Factory Object

Specifies 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.

Language

Specifies 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.

Referral

Specifies how the LDAP server is to handle referrals.

Values:

- ignore
Ignores referrals.
- follow
Follows referrals.
- throw
Returns the first encountered referral and stops and search.

Security Authentication

Specifies authentication mechanisms for the LDAP server to use.

Values:

- None
Specifies to use no authentication (anonymous). Verify that the LDAP server supports anonymous connections.

Notes:

This setting limits the LDAP operator.

CA Process Automation creates an anonymous connection with the LDAP server. User login credentials are ignored.

- Simple
Indicates the use of weak authentication (clear-text password). Select this option when you set Security Protocol to SSL.
- Space-separated SASL mechanism list
Enter a space-separated SASL mechanism list, where SASL is the Simple Authentication and Security Layer (RFC 2222). This specification lets LDAP support any type of authentication agreed upon by the LDAP client and server.

Security Protocol

Specifies whether connectivity is secure.

Values:

- ssl

Important! If connecting to Active Directory (AD), type **ssl** in *lowercase*. AD rejects the value **SSL**.

Indicates the protocol that permits LDAP server connections through a secure socket.

- Blank

Indicates nonsecure connections.

Connection Timeout

Specifies the connection timeout value in seconds.

Values:

- 0

No timeout.

- See Limits

Limits:

This value must be a whole number in the range from 1 through 600.

Default LDAP Server

Specifies the default LDAP Server URL or IP address.

Default LDAP Port

Specifies the default port for the LDAP Server.

Values:

- 389

The ldap port for Lightweight Directory Access Protocol (LDAP).

- 636

The ldaps port for the ldap protocol over TLS/SSL.

Default LDAP User

Specifies the default LDAP User. Operators can use this default or can override it.

Default Password for LDAP User

Default Password for LDAP User. Operators can use this default or can override it.

Default Base DN

Specifies the default Base Distinguished Name (DN) where the LDAP user is located. Operators can use this default or can override it.

Default User Prefix

Specifies the Default User Prefix to use.

Values:

- uid
- cn

6. Click Save and Close.

The values configured in the open dialog are saved.

7. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

8. With Domain selected, click Unlock.

More information:

[About Directory Services](#) (see page 268)

[Category Configuration and Operator Inheritance](#) (see page 294)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Configuring Operator Categories](#) (see page 244)

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 Email

You can configure default settings for Email operators.

Follow these steps:

1. Click the Configuration tab.
2. Select Domain and click Lock.
3. Click the Modules tab.
4. Right-click Email and select Edit.
5. Complete the following settings:

SMTP Server for Outgoing e-mail

Specifies the SMTP server for Java e-mail alerts.

From Address for Outgoing e-mail

Specifies the email address to appear in the sender field of outgoing Java e-mail alerts. Fully configure this account. For example:

username@company-name.com

Default Protocol for Connection

Specifies the default protocol to use to receive emails from a remote server or remote web server.

Values:

- IMAP
- IMAP-SSL
- POP3
- POP3-SSL

Default Mail Server

Identifies the mail server from which email is retrieved.

Default Mail Server Port

Specifies the port for inbound emails.

Values:

- 110
POP3 port for unsecured connection.
- 995
POP3-SSL port for secured connection.
- 143
IMAP port for unsecured connection.
- 993
IMAP-SSL port for secured connection.

Default Username

Leave blank if this value is always specified at the operator level.

Default Password

Leave blank if this value is always specified at the operator level.

6. Click Save and Close.
The values configured in the open dialog are saved.
7. Click the Save toolbar button.
The saved changes are applied to the CA Process Automation configuration.
8. With Domain selected, click Unlock.

More information:

[About Email](#) (see page 272)

[Category Configuration and Operator Inheritance](#) (see page 294)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Configuring Operator Categories](#) (see page 244)

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 275)

Configure File Management

You can configure default settings for the File Management category of operators for Windows or for UNIX. Use the tab for the target operating system to configure File Management. To expand a field for an entry that is longer than the space provided, right-click the field and select Expand.

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.

3. Click the Modules tab.
4. Select File Management and click Edit.
5. Click Windows File Management Properties and complete the following fields::

Require user credentials

Select a value from the drop-down list.

Valid values:

- Default to user specified below (see Step 6).
- Default to User under which touchpoint is run.
- No default.

Compression Utility

Specifies the utility or command for compressing a file or directory.

Uncompress Utility

Specifies the utility or command for uncompressing or extracting a file or directory.

6. If you require user credentials (selected Default to user specified below), complete the following fields.

Default User

The default user login.

Default Password

Specifies the password for the default user.

Confirm Password

Retype the password for confirmation.

7. Click UNIX File Management Properties and complete the following fields, where conditional fields are documented in the next step:

Require user credentials

Select a value from the drop-down list.

Valid values:

- Default to user specified below (see Step 8).
- Default to User under which touchpoint is run.
- No default.

Shell

Specifies the default shell of the operating system, for example: /bin/bash, /bin/csh/ or /bin/ksh.

Disable Password Check (UNIX)

Specifies whether to check the password when switching users to run a process or script on a UNIX host.

Selected - Disables password checking.

Cleared - Verifies the specified password.

Compression Utility

Specifies the utility or command for compressing a file or directory.

Uncompress Utility

Specifies the utility or command for uncompressing a file or directory.

8. If you require user credentials (selected Default to user specified below), complete the following fields.

User

The default user login.

Password

Specifies the password for the default user. The password is used when starting user processes that do not specify a password.

Confirm Password

Retype the password for confirmation.

9. Click Save and Close.

The values configured in the open dialog are saved.

10. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

11. With Domain selected, click Unlock.

More information:

[Configuring Operator Categories](#) (see page 244)

[About File Management](#) (see page 275)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

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

Administrators 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 details, see [Category Configuration and Operator Inheritance](#) (see page 294).

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab.
4. Right-click File Transfer and select Edit.

5. Complete the following field:

Default UDP Port for Trivial FTP

Specifies the default UDP port for TFTP. This value can be overridden at the operator level.

Note: Port 69 is the well-known UDP port for Trivial File Transfer.

Value

Any valid port number.

Default

69

6. Click Save and Close.

The values configured in the open dialog are saved.

7. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

8. With Domain selected, click Unlock.

More information:

[Override Settings Inherited by a Category of Operators](#) (see page 296)

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 280)

Configure Network Utilities

You can configure the Network Utilities category of operators. The one configurable property has no default value.

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab.
4. Right-click Network Utilities and select Edit.

5. Configure the following field:

Poll Frequency (secs)

Specifies the frequency with which to evaluate conditions on an SNMP variable. Frequency is expressed in seconds. This search frequency determines how often a Network Utilities operator synchronously obtains the object identifier (SNMP OID) on a device.

6. Click Save and Close.

The values configured in the open dialog are saved.

7. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

8. With Domain selected, click Unlock.

More information:

[About Network Utilities](#) (see page 280)

[Category Configuration and Operator Inheritance](#) (see page 294)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Configuring Operator Categories](#) (see page 244)

About Process Control

Operators in the Process Control category can run only on Orchestrator touchpoints. Operators contained in Process Control:

- Start and interpret CA Process Automation processes.
- Invoke other categories to execute operators in an instance of a process object.
- Enforce dependencies.
- Monitor category invocations and use their outcomes to execute succeeding branches of a process.

When a process is started, a copy (named an instance) is made and changes to that copy do not affect other copies or the original process. You can start a process by any of the following methods:

- With the Form Designer.
- By a schedule.
- By another process.
- By an external application that uses a CA Process Automation trigger.
- By an external application that uses SOAP calls. See the *Web Services Reference*.

If you are using a highly decentralized architecture, consider defining logical groups of operator categories in an environment and configure Process Control on a selected touchpoint in each group. Processes are then started on the touchpoint running the Process Control operators for a group. You configure a touchpoint specifically for running multigroup processes. A decentralized architecture for running processes reduces the load on individual computers, the impact of potential incidents, and the amount of data that remote hosts exchange.

More information:

[Configure Process Control](#) (see page 282)

Configure Process Control

You can configure the default setting for operators in the Process Control category.

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab.
4. Right-click Process Control, and select Edit.

5. Configure the following setting.

Time to keep completed user interaction (in minutes)

When a process is started with a Start Request Form that includes a Interaction Request Form, a task is created. That task is displayed on the Tasks link in the Operations tab. When a user finishes the task, the task Completion Date is also displayed. This parameter determines the maximum number of minutes that a task remains displayed after a user finishes the task. After the specified delay, the task is removed from the Tasks list.

Note: The process that runs when the task completes remains accessible for a configurable period of time.

6. Click Save and Close.

The values configured in the open dialog are saved.

7. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

8. With Domain selected, click Unlock.

More information:

[About Process Control](#) (see page 282)

[Category Configuration and Operator Inheritance](#) (see page 294)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Configuring Operator Categories](#) (see page 244)

About Utilities

The Utilities category in the Modules tab 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 operators in the Utilities category.

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab.
4. Right-click Utilities and click Edit.
5. Click Add and specify external JAR files as follows.

Default External Jars

Specifies the paths to the external jars to load by default in the Invoke Java operator.

List the path to each external JAR file that the Invoke Java operator uses when it runs on this Orchestrator or an agent.

Important: To load each JAR file, specify a separate path that ends with that JAR file. To load .class files, specify the path to their directory. The .class files can be in the directory. The location depends on whether this package is a named package or an unnamed package.

For each external JAR file:

- Enter the full path to the JAR file that resides on the host with the Orchestrator or agent. Specify the full path in one of the following ways:
 - Start with '/'
 - Start with '\\'
 - With the form: '^.:.*'

A regular expression in the form *one character:string*.

- Enter the full path to a JAR file that can be downloaded over HTTP. Specify the path as follows:
 - Start with 'http://'
 - Start with 'https://'

Note: Verify that this path does not require authentication and does not go through an HTTP proxy.

- Enter the relative path to a JAR file that was uploaded in User Resources of Manage Versions. CA Process Automation appends the JAR file path to the path of the User Resources directory of the Orchestrator or agent that is running the Invoke Java operator.

Note: Any path that does not start with / or \\, is not of the form '^.:.*', or does not start with http/https is treated as a relative path.

6. Use the up and down arrows to sequence the list. Click Delete to remove a selected line.
7. Complete the fields. Mouse over the fields for tips. Descriptions follow:

Use Default Logger?

Specifies whether to log data to a log file.

Selected

Log data to a log file and enable configuration fields.

Cleared

Do not create logs.

Default Log File Path

Specifies the path to the log file to make available to code specified in operator configuration.

Default Log Level

Specifies the level at which to log.

Append to Default Log File?

Specifies whether to append current logs to the default log file.

Default Log Data Without Logging Info?

Specifies whether to log data without the info type logs.

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. With Domain selected, click Unlock.

More information:

[Configuring Operator Categories](#) (see page 244)

[Category Configuration and Operator Inheritance](#) (see page 294)

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 287)

Configure Web Services

You can configure default settings for operators in the Web Services category.

Follow these steps:

1. Open the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Modules tab.
4. Right-click Web Services and select Edit.

5. Click Web Services Properties. View the default settings and modify as needed.

Maximum result length (bytes)

The maximum result length determines the maximum size (in bytes) of the XML value that is received and stored in CA Process Automation datasets. Both operators allow for the storage of the whole answer (the response); therefore, any piece that is stored must have a maximum size to avoid storing a large amount of data. If the result exceeds the configured length, the result is truncated.

URL Part for Async SOAP Servlet

Specifies the servlet location that is appended to the base server URL for handling incoming HTTP/SOAP calls. Accept the default location, /itpam/soap, unless you create custom SOAP handlers.

Async SOAP Servlet Method

Specifies the servlet method that handles incoming responses for Asynchronous SOAP calls made from CA Process Automation. The default method "AsynSoapResponse" is recommended in most cases.

6. Click the Web Services HTTP Properties. Complete as follows:

Default Validate SSL Certificate?

Specifies the operator action based on whether the SSL certificate is valid. This setting is relevant when querying an HTTPS URL.

Values:

This value can be one of the following:

- Selected - Specifies to to make the HTTP call only if the SSL certificate is valid. CA Process Automation fails the HTTP operator if the SSL certificate used by the URL is invalid.
- Cleared - Specifies to make the HTTP call even if the SSL certificate used by the URL is invalid.

Default:

Cleared

Default HTTP Authentication?

Specifies whether the HTTP server, at the URL specified in the operator, requires HTTP authentication.

Values:

This value can be one of the following:

- Selected - Indicates that HTTP authentication is required.
- Cleared - Indicates that HTTP authentication is not required.

Default:

Cleared

Default NTLM Authentication?

Specifies whether the HTTP server at the URL specified in the operator requires NTLM authentication.

Values:

This value can be one of the following:

- Selected - Indicates that NTLM authentication is required.
- Cleared - Indicates that NTLM authentication is not required. In this case, basic HTTP authentication is used.

Default:

Cleared

Default User name

Specifies the username to use when authenticating against the URL specified in the operator.

Default Password

Specifies the password to use when authenticating against the URL specified in the operator.

Default Domain name

Specifies the name of the domain to use when authenticating against the URL specified in the operator.

Values:

The value can be one of the following:

- A valid domain name. NTLM authentication requires a domain name.
- Blank.

Note: For NTLM authentication, the domain name is used as is. For non-NTLM authentication, if the domain name is required, it is appended to the user name. For example:

User name=user name@domain name

Default Use Proxy?

Specifies whether the HTTP call goes through a proxy server.

Values:

This value can be one of the following:

- Selected - Indicates that the HTTP call goes through a proxy server.
- Cleared - Indicates that the HTTP call does not go through a proxy server.

Default:

Cleared

Default Proxy Host

Identifies the default proxy host in one of the following ways:

- The default URL to the proxy host, using HTTP or HTTPS.
- The FQDN of the proxy server.

Note: If you enter the FQDN, the HTTP protocol is used to contact the proxy host. See [Syntax for DNS Host Names](#) (see page 358).

Default Proxy Port

Specifies the default port of the proxy server.

Value

This value can be any valid port number, for example:

- 80 (HTTP)
- 8080 (alternate HTTP)
- 443 (HTTPS)

Default Proxy Authentication?

Specifies whether the proxy requires authentication.

Value

This default value can be one of the following:

- Selected - Indicates that authentication is required for the proxy host.
- Cleared - Indicates that authentication is not required for the proxy host.

Default:

Cleared

Default Proxy NTLM Authentication?

Specifies whether the proxy host at the specified proxy URL requires NTLM authentication.

Values:

This value can be one of the following:

- Selected - Indicates that NTLM authentication is required for the proxy.
- Cleared - Indicates that NTLM authentication is not required. In this case, basic HTTP authentication is used.

Default:

Cleared

Default Proxy User name

Specifies the username to use when authenticating with the proxy host.

Default Proxy Password

Specifies the password associated with the specified Default Proxy User name.

Default Proxy Domain name

Specifies the name of the domain to use when authenticating with the proxy host.

Values:

This value can be one of the following:

- A valid domain name. A domain name is required for NTLM authentication.
- Blank

Note: For NTLM authentication, the domain name you enter is used as is. For non-NTLM authentication, if the domain name is required, it is appended to the user name. For example:

user name=user name@domain name

Default HTTP Version

Specifies the default HTTP protocol version.

Values:

- 1.0
- 1.1

Default:

1.1

Default Connection Timeout (sec)

Specifies the maximum number of seconds to wait for the establishment of an HTTP connection before the operator times out.

Values:

The value can be one of the following:

- Any positive integer indicating the number of seconds
- 0 (zero) for no timeout

Default:

0

Default Socket Timeout (sec)

Specifies the maximum number of seconds to wait between two consecutive HTTP response data packets.

Values:

Any positive integer indicating the number of seconds, where 0 (zero) means no timeout.

Default:

0

Default Handle Redirects?

Specifies whether redirects are handled automatically.

Values:

This value can be one of the following:

- Selected - Indicates that redirects are handled automatically
- Cleared - Indicates that redirects are not handled automatically.

Default:

Cleared

Default Maximum Number of Redirects

Specifies the maximum number of redirects to follow.

Default:

100

7. Click Save and Close.

The values configured in the open dialog are saved.

8. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

9. With Domain selected, click Unlock.

More information:

[About Web Services](#) (see page 287)

[Operator Categories and Where Operators Run](#) (see page 298)

[Override Settings Inherited by a Category of Operators](#) (see page 296)

[Configuring Operator Categories](#) (see page 244)

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.

More information:

[Operator Categories and Operator Folders](#) (see page 240)

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.

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.

More information:

[Configure File Management](#) (see page 275)

[Configure Command Execution](#) (see page 251)

[Configure Network Utilities](#) (see page 280)

[Configure Web Services](#) (see page 287)

[Configure Process Control](#) (see page 282)

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:

[Enable or Disable an Operator Category](#) (see page 295)

[Use a Proxy Touchpoint](#) (see page 221)

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](#) (see page 300)

[Configure Catalyst Trigger Properties at the Domain Level](#) (see page 302)

[Configure File Trigger Properties at the Domain Level](#) (see page 308)

[Configure Mail Trigger Properties at the Domain Level](#) (see page 311)

[Configure SNMP Trigger Properties at the Domain Level](#) (see page 315)

[Change the SNMP Traps Listener Port](#) (see page 318)

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.

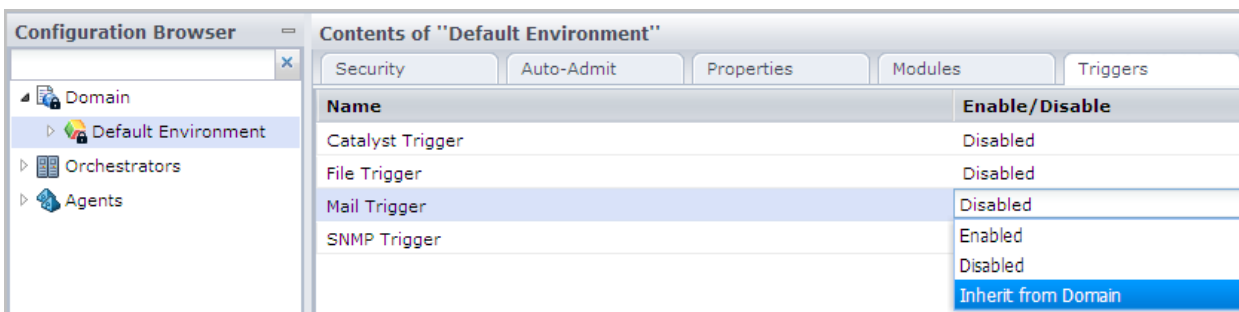
After you configure an SNMP trap trigger in CA Process Automation, external applications can send SNMP traps to CA Process Automation. When CA Process Automation receives an SNMP trap that matches object IDs (OIDs) and the payload values filter, the configured process starts. The dataset of the triggered 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.

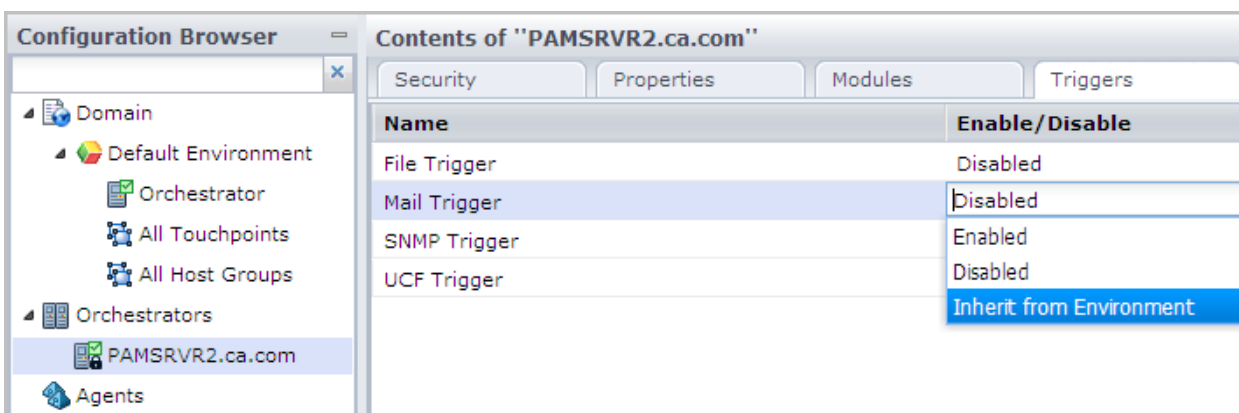
Unlike settings that the environment inherits from the Domain by default, triggers are disabled at both the environment level and Orchestrator levels by default. To enable CA Process Automation triggers that are set at Domain level, set inheritance from the Domain at the environment level. Then, set 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.

More information:

[Configure File Trigger Properties at the Domain Level](#) (see page 308)
[Configure Mail Trigger Properties at the Domain Level](#) (see page 311)
[Configure SNMP Trigger Properties at the Domain Level](#) (see page 315)
[Configure Catalyst Trigger Properties at the Domain Level](#) (see page 302)
[Activate Triggers for an Orchestrator](#) (see page 165)

Configure Catalyst Trigger Properties at the Domain Level

An administrator with Domain Administrator rights can configure Catalyst Trigger properties at the Domain level. When inherited, the Catalyst Trigger properties enable processes to be triggered upon the receipt of a Catalyst event.

The Catalyst Trigger supports a list of subscriptions, each referencing a Catalyst Connector with a filter. When a matching event is received from the Catalyst Connector, the specified CA Process Automation process is started.

The examples show how to set a Catalyst trigger that starts a process whenever an Alert object is created or updated in the Microsoft System Center Operations Manager. The properties of the Alert object are available as process variables.

You can configure Catalyst Trigger properties at the Domain level

Follow these steps:

1. Click the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Triggers tab, select Catalyst Trigger, and click Edit.
4. On the General Properties tab click the Add button to add a subscription.

The UCF Subscriptions dialog opens. This dialog includes configurable fields on the following tabs:

- Subscription
- MDR
- Filter
- UCF Security

5. Click the MDR tab first. Examine the following field descriptions and then configure the settings.

UCFBrokerURL

Defines the UCF Broker URL.

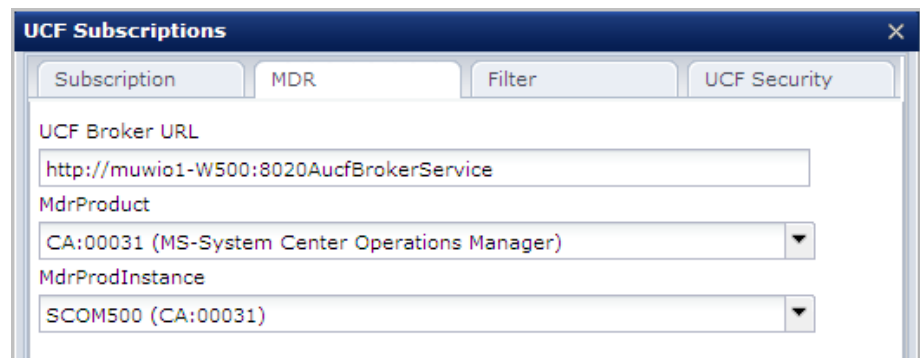
MdrProduct

Specifies a unique identifier of the connecting product. Valid entries appear in the drop-down list.

MdrProdInstance

Specifies a unique identifier of the instance of the connecting product as registered in the UCF Broker. Valid entries appear in the drop-down list.

6. Verify that your entries resemble the following example and click Apply:



- Click the Subscription tab. Examine the following field descriptions and configure the settings.

SubscriptionName

Specifies the name of the subscription. This name appears in the Subscription List when you complete the configuration.

SubscriptionID

Specifies the Subscription ID associated with the named subscription.

ProcessPath

Specifies the path to the process to execute when a matching event is received.

Enabled

Specifies whether this subscription is enabled.

Values:

One of the following:

- Selected - Enable this subscription.
- Cleared - Disable this subscription.

- Verify that your entries resemble the following example and then click Apply:

The screenshot shows a window titled "UCF Subscriptions" with a close button in the top right corner. Below the title bar are four tabs: "Subscription" (which is selected), "MDR", "Filter", and "UCF Security". The main content area contains the following fields and controls:

- SubscriptionName:** A text input field containing the text "SCOMTest".
- SubscriptionID:** An empty text input field.
- ProcessPath:** A text input field containing the text "Test/TriggerProcess".
- Enabled:** A checkbox that is checked, with the label "Enabled" next to it.

9. Click the Filter tab. Examine the following field descriptions and then configure the settings.

Create

Specifies whether to process create events.

Values:

One of the following:

- Selected - Process create events.
- Cleared - Do not process create events.

Update

Specifies whether to process update events.

Values:

One of the following:

- Selected - Process update events.
- Cleared - Do not process update events.

Delete

Specifies whether to process delete events.

Values:

One of the following:

- Selected - Process delete events.
- Cleared - Do not process delete events.

entitytype

Specifies the type of the entity.

Values:

- Alert
- Item
- Relationship

itemtype

Specifies the type of item. If not specified, then all types displayed in the drop-down list are included.

recursive

Specifies whether the connector recursively includes the item and its constituent children and relationships.

Values:

One of the following:

- Selected - Recursively includes the item and its constituent children and relationships.
- Cleared - Do not recursively includes the item and its constituent children and relationships.

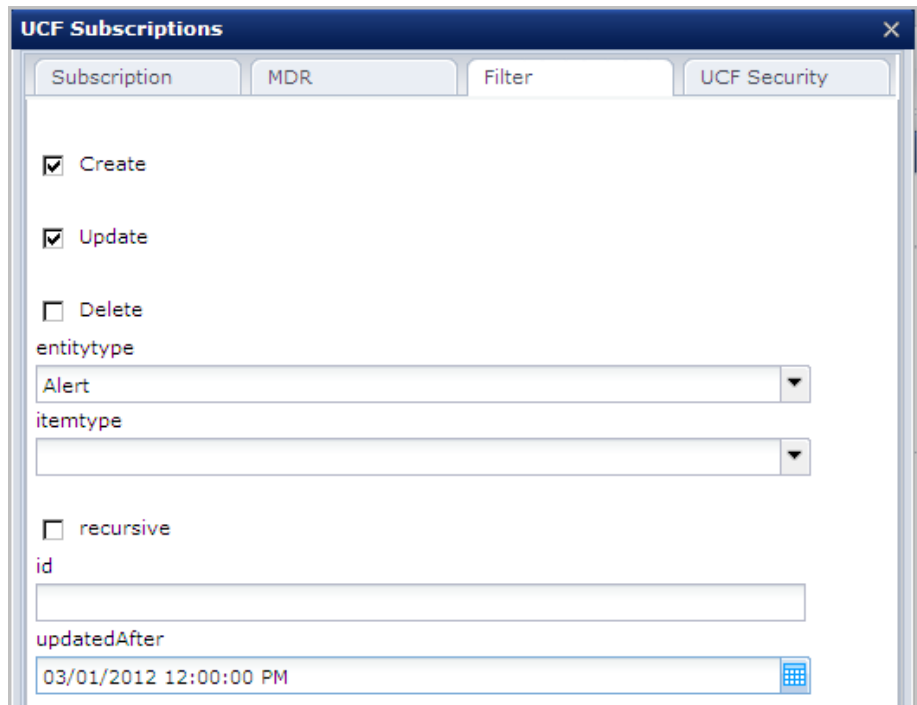
id

Specifies a specific object identifier (same as the MdrElementID).

updatedAfter

Specifies the date and time after which to begin updating objects. Click the ellipses and select the date from the calendar application. Then, click OK.

10. Verify that your entries resemble the following example and click Apply:



11. Click OK.

The subscription you defined is added to the Subscription list. To edit your definition, highlight this entry and click Edit.

12. Click the UCF Security tab.

- a. For Claims, click Add to create an entry field for each claim. Enter the claim name and the claim value.

Claim Name

Specifies the username for UCF Subscription.

Claim Value

Specifies the password associated with the Username.

- b. For Password Claims, click Add to create an entry field for each claim. Enter the claim name and the claim value

Claim Name

Specifies the username for UCF Subscription.

Claim Value

Specifies the password associated with the Username.

13. Click Save and Close.

The values configured in the open dialog are saved.

14. Click the Save toolbar button.

The saved changes are applied to the CA Process Automation configuration.

15. With Domain still selected, click Unlock.

16. Right-click Domain and select Unlock.

Configure File Trigger Properties at the Domain Level

An administrator with Domain Administrator rights can configure File Trigger properties at the Domain level. Inheritance is *not* the default. Therefore, configuration at the Domain level is used only in the following case:

- Inherit from the Domain is configured at the environment level.
- Inherit from the Environment is configured at the Orchestrator level.

CA Process Automation processes can be started using File Triggers. When operational, the Orchestrator looks for new files in the configured input directory at the configured frequency. When a new file matches the configured input file name pattern, CA Process Automation parses the content and triggers the process specified in the content. When the process starts, the triggering file is moved to the configured Processed directory. If the process cannot be started, the triggering file is moved to the configured Error directory with a file ending in ".err". The file with the .err extension describes why the trigger failed.

Note: If you create new files with the same names as existing files, the new files replace the older files.

Before configuration, create an Input directory with write permissions required for accepting trigger files pushed into this folder. Consider tying it to an FTP folder to allow remote triggering. Also create directories for receiving output that is successfully processed (Processed directory) and output that cannot be processed (Error directory). If you do not create the directories at configuration time, CA Process Automation creates them when they are first needed.

To configure File Trigger properties at the Domain level

1. Click the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Triggers tab, select File Trigger, and click Edit.

The File Trigger Properties tab opens.

4. Examine the following field descriptions and then configure settings for the File Trigger.

Input directory

Specifies the target directory for files that trigger processes. This folder receives trigger files from sources with write permissions.

- Enter the full path to the target directory. For example:

C:\Program Files\CA\PAM\R30MSSQLDomain\server\c20\triggers

- Enter a relative path that is relative to the <install_dir>/server/c2o directory.

To specify a relative path, start with a dot (.). In the following example, triggering files are added to the <install_dir>/server/c2o/triggers folder.

./triggers

Processed directory

Specifies the directory into which CA Process Automation moves all files that successfully trigger processes. If a file being added has the same name as an existing file, the older file is overwritten.

- Enter the full path to the Processed directory. CA Process Automation creates this directory if not present. You can create the directory anywhere.
- Enter a relative path that is relative to the <install_dir>/server/c2o directory, where <install_dir> is the installation directory, \$installationDir.

To specify a relative path, start with a dot (.). In the following example, successful trigger files are added to the <install_dir>/server/c2o/triggeroutput/processed folder.

./triggeroutput/processed

Error directory

Specifies the directory into which CA Process Automation moves all files that fail to trigger processes.

- Enter the full path to the Error directory. CA Process Automation creates this directory if not present.
- Enter a relative path that is relative to the <install_dir>/server/c2o directory, where <install_dir> is the installation directory, \$installationDir.

To specify a relative path, start with a dot (.). In the following example, failed trigger files are added to the <install_dir>/server/c2o/triggeroutput/error folder.

./triggeroutput/error

Stability timer (seconds)

The minimum elapsed time, in seconds, from the last modification for a file to become eligible to trigger a process. Consider, for example, a trigger file with a stability timer set to 60 seconds. Such a trigger file is bypassed if the file is modified 30 seconds before searching for new files.

Default: 2

Frequency (in seconds)

The interval in seconds with which CA Process Automation searches the Input directory for new files.

Default: 30

Input file name pattern

Specifies the file name pattern or file extension for files in the Input directory that can trigger processes. Files that do not match this pattern are never processed. The following example pattern indicates that CA Process Automation is to process only files with an extension of ".trigger".

`.*.trigger`

5. Verify that your entries are valid. The following example contains valid entries.

Input directory:	<input type="text" value="./triggers"/>
Processed directory:	<input type="text" value="./triggeroutput/processed"/>
Error directory:	<input type="text" value="./triggeroutput/error"/>
Stability timer (seconds):	<input type="text" value="2"/>
Frequency (in seconds)	<input type="text" value="30"/>
Input file name pattern:	<input type="text" value=".*.prg"/>

6. Click Save and Close.
The values configured in the open dialog are saved.
7. Click the Save toolbar button.
The saved changes are applied to the CA Process Automation configuration.
8. With Domain still selected, click Unlock.

Configure Mail Trigger Properties at the Domain Level

An administrator with Domain Administrator rights can configure Mail Trigger properties at the Domain level. Mail Trigger properties enable the triggering of processes only when inherited or configured at lower levels. Inheritance is achieved when Inherit from Domain is configured at the environment level and Inherit from the Environment is configured at the Orchestrator level.

When active, the Mail trigger searches the email account, configured as User Name and Password, for emails. CA Process Automation processes the XML content if valid content exists in the body of the email or in an attachment. The set of parameters that are created in the instance of the triggered process depends on whether the email contains valid XML content.

Before you configure Mail Trigger properties, do the following:

- Create an email account dedicated to receiving emails that trigger CA Process Automation processes.
- Verify that the IMAP service is enabled on the mail server you identify as Incoming mail server (IMAP). If enabling the IMAP service on your corporate mail server is restricted, create a “proxy” mail server with IMAP enabled. Then, specify this 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 this proxy mail server.
- (Optional) Create a default process for the Domain Orchestrator and save it to the path you configure as the Default Process handler. The default process is used 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, senderTime, and MailBody. These variables provide the email address of the sender, the email server time when the email was sent, and the complete content of the email. The default process determines any further action.

You can configure Mail Trigger properties at the Domain level.

Follow these steps:

1. Click the Configuration tab.
2. Right-click Domain and select Lock.
3. Click the Triggers tab, select Mail Trigger, and click Edit.

The Mail Trigger Properties tab opens.

4. Examine the following field descriptions and then configure settings for the Mail Trigger.

Default Trigger Process (Orchestrator only)

Do one of the following:

- Make no entry to ignore emails with no valid XML trigger content.
- Type the full path of the process to start when the triggering email does not contain valid XML content in its message body or attachment. The path to the process file configured here is for the Domain Orchestrator. (One default process can be defined for each Orchestrator.)

Note: The Browse button is disabled because this setting is Orchestrator-specific.

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 to use 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 associated with the specified user name.

Frequency of processing mails (in 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.

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

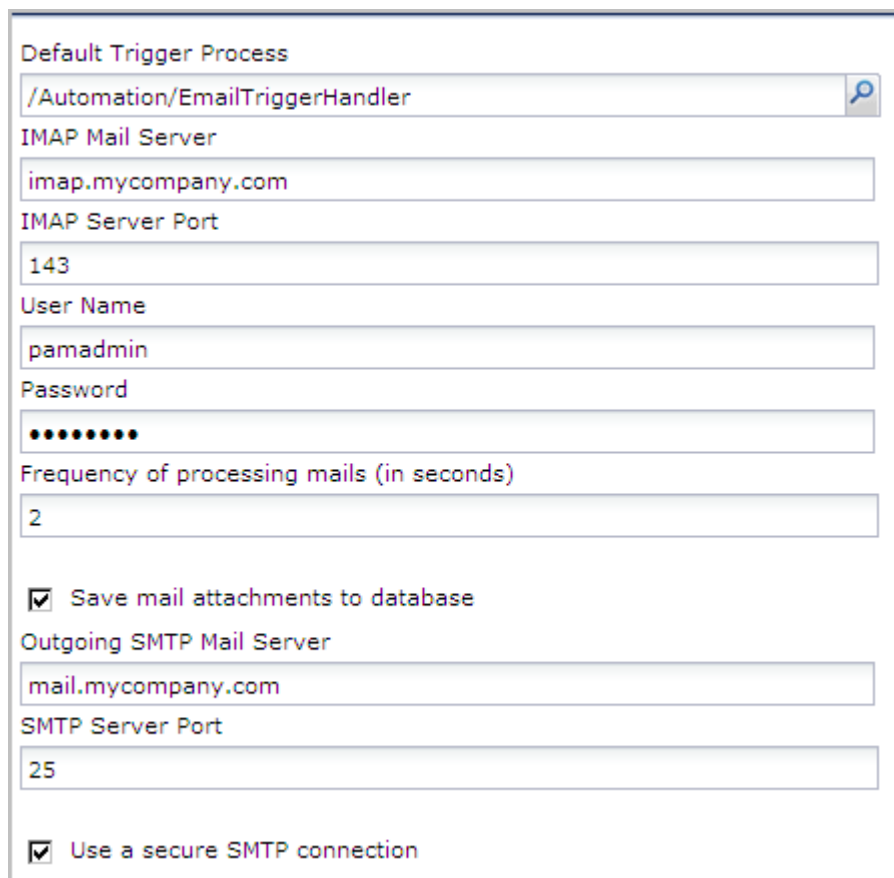
Specifies the port of the outgoing mail server. The default SMTP port is 25.

Use secure SMTP connection

Do one of the following:

- Accept the default, selected, to enable a secure connection to the SMTP mail server.
- Clear the check box if your mail server does not allow a secure connection.

5. Verify that your entries are valid. The following example shows valid entries, where mycompany represents an actual company name.



The screenshot shows a configuration dialog box with the following fields and options:

- Default Trigger Process:** /Automation/EmailTriggerHandler
- IMAP Mail Server:** imap.mycompany.com
- IMAP Server Port:** 143
- User Name:** pamadmin
- Password:** (masked with 8 dots)
- Frequency of processing mails (in seconds):** 2
- Save mail attachments to database
- Outgoing SMTP Mail Server:** mail.mycompany.com
- SMTP Server Port:** 25
- Use a secure SMTP connection


6. Click Save and Close.
The values configured in the open dialog are saved.
7. Click the Save toolbar button.
The saved changes are applied to the CA Process Automation configuration.
8. Right-click Domain and select 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 SNMP Trigger properties, verify that port 162 is accessible to CA Process Automation. If you use an alternative port for SNMP traps, modify the CA Process Automation properties file to change the port on which to listen for SNMP traps.

To configure SNMP Trigger properties at the Domain level

1. Click the Configuration tab.
The Configuration Browser palette opens with Domain selected.
2. Click Lock.
The Domain is locked.
3. Click the Triggers tab
4. Right-click SNMP Trigger, and select Edit.
The General Properties tab opens.
5. Click Add Parameter  to add a line for defining a filter.
The SNMP dialog appears.
6. Examine the following field descriptions, then configure settings for the SNMP trap filter:

Description

Describes the filter.

Source IP address

Specifies the Pv4 subnet in CIDR format against which the source IP address is matched. For example: 172.24.36.0/24 matches any source IP address in the range from 172.24.36.1 to 172.24.36.254, not counting the network address and the broadcast address, which are not assigned to hosts. To accept traps from all source IP addresses, enter 0.0.0.0/0.

Trap OID

Specifies a regular expression matching the SNMP trap object identifier (OID). An OID is a unique numeric identifier for a data object that is paired with a value in an SNMP trap message. Leave blank to accept SNMP traps with any OID. Enter the following to accept any trap, where dot (.) means any value and asterisk (*) indicates any number of times.

.*

Payload Match

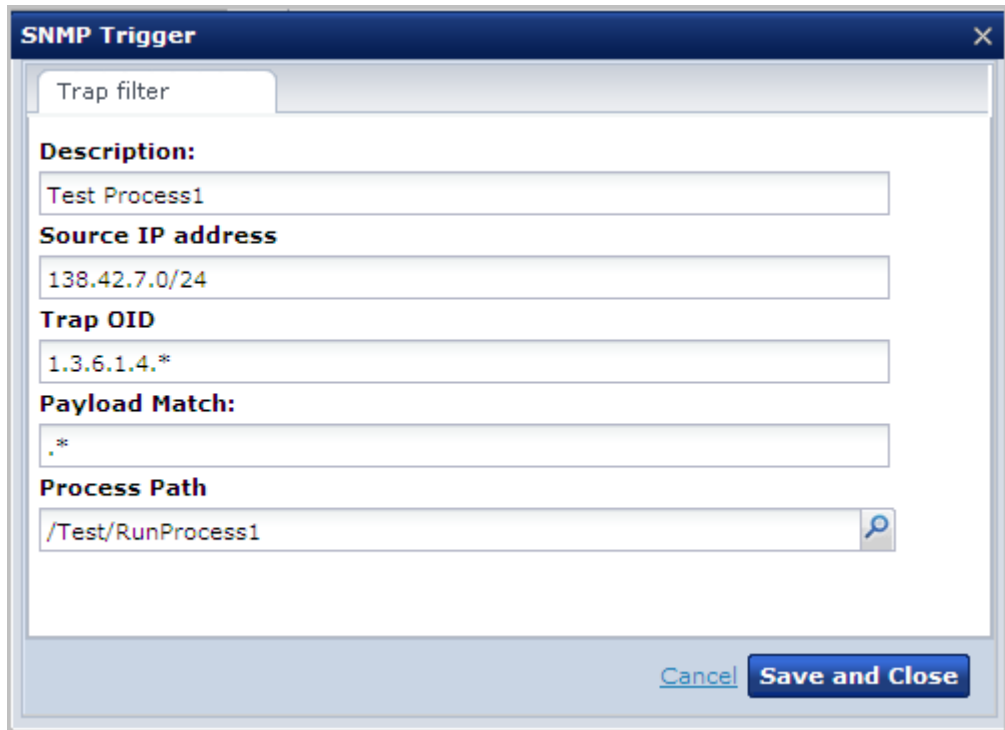
Specifies a regular expression matching any of the payload values of the trap. Leave blank (or type .*) to accept SNMP traps with any payload content.

Process Path

Specifies the full path of the Process to run when receiving an SNMP trap that matches the filter criteria. The checked-in version of the Process Path is used during execution.

Click search to load the Object Browser, from which you can select the process path.

7. Verify that your entries are valid, and then click Save and Close. The following example filter accepts SNMP traps received from any host with an IP address between 138.42.7.1 and 138.42.7.254 with an OID beginning with 1.3.6.1.4.1.[x.x.x.x.x] and at least one payload value that matches the literal string "Test Payload for trigger." Receipt of an SNMP trap matching these criteria triggers the process, RunProcess1 in the path, /Test.



- Use the Up and Down arrows to list the filters in order of precedence, where each filter has precedence over filters listed below it in the list.



- Click the Save toolbar button.
The saved changes are applied to the CA Process Automation configuration.
- With Domain still selected, click Unlock.

More information:

[Change the SNMP Traps Listener Port](#) (see page 318)

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 172).
 - b. [Start the Orchestrator](#) (see page 173).

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.

Chapter 14: Manage User Resources

You can manage user resources, Orchestrator resources, and agent resources 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.

The Manage User Resources palette can be accessed by any user who is granted the Configuration_User_Resources permissions of the Configuration Browser policy in CA EEM. However, only users who are also granted the Domain_Administrator permissions of the Domain policy can access 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](#) (see page 320)

[How to Deploy JDBC Drivers for Database Operators](#) (see page 321)

[Upload User Resources](#) (see page 321)

[Upload Orchestrator Resources](#) (see page 324)

[Upload Agent Resources](#) (see page 326)

About User Resources Management

Content administrators 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.

Users with Domain 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 re-add 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 follow:

User Resources

- Resources uploaded to the User Resources are not included in the agent or Orchestrator classpath after a restart.
- You can create subfolders within the User Resources folder.
- You do not need Domain_Admin (Administrator) rights.

Agent Resources and Orchestrator Resources

- Resources uploaded to the Agent Resources and Orchestrator Resources are included in the agent or orchestrator classpath after a restart.
- You cannot create subfolders within the Agent Resources and Orchestrator Resources folders.
- You do 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 and designers begin working with the Database operators.

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. In addition, you can add other jar files that you copied to a local directory.

After installation, you can upload jar files containing 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 details:

- [Upload Orchestrator Resources](#) (see page 324).
- [Upload Agent Resources](#) (see page 326).

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 322).
- [Delete a resource from User Resources](#) (see page 323).
- [Modify a resource in User Resources](#) (see page 323).

Note: To modify the resource path, delete the resource and add it again under a different path.

Add a Resource to User Resources

Content administrators can make shared code available to all Orchestrators and agents by uploading scripts or jar files that can be invoked with a reference. Content administrators or other users with administrative-level permissions can add scripts to the User Resources folder in the global Repository. The uploaded user resources are mirrored at the configured mirroring interval to other Orchestrators and agents in the domain.

An example follows.

Follow these steps:

1. Click the Configuration tab.
2. Click the Manage User Resources palette.
3. Expand Repository folder. Expand the User Resources folder.
4. Select the User Resources folder or one of its subfolders and click New.

The Add New Resource: "Untitled" page appears.

5. Complete the following fields using the descriptions as a guide:

Resource Name

Specifies how the resource is labeled. You can enter the file name or another meaningful label, for example:

`buildscript.js`

Resource Subfolders Path

Specifies the path to the resource from the current folder. If the folders specified in the path do not exist, they are created. For example:

`/Windows Scripts`

Resource File

Click Browse. The File Upload dialog appears. Navigate to the file to upload and click Open.

The file and its path populate the Resource File field.

Module Name

Specifies the name of the module.

Resource Description

A brief description visible to your users.

6. Verify your entries, and then click Save.

The name of the uploaded file, with its type, path, and description appear in the index of files list.

CA Process Automation copies the uploaded user resources to the following path, where *install_dir* is the directory on the server where the Domain Orchestrator was installed.

```
install_dir/server/c2o/.c2orepository/.c2ouserresources/...
```

CA Process Automation creates subfolders in this path to maintain the directory structure to the resource from the User Resources folder.

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 upload an edited resource, such as a script or jar file, that you previously added to User Resources. You can change text for Module Name and Resource Description. Before saving changes, you indicate that you want to replace the file only if you browsed to an edited Resource File.

Follow these steps:

1. Click the Configuration tab.
2. Click the Manage User Resources palette.
3. Expand Repository folder. Expand the User Resources folder.

4. Click the folder where the resource resides.
5. Right-click the row displaying the name of the resource to modify and select Edit.
The Resource page appears.

6. Evaluate the following field:

Replace File

Indicates whether to replace the existing file with the edited version of the file.

Selected - Replace the existing file with the edited file.

Cleared - Do not replace the existing file. Only save the edits to fields on the Resource page.

7. Modify the resource information, if needed. Fields you can edit include:
 - Module Name
 - Resource Description
8. If the Resource File has been updated, click Browse, navigate to the updated file and click Open. The updated file is uploaded to User Resources.
9. Leave Replace File selected if you uploaded an edited file.
10. Clear Replace File if your only updates were to fields on the Resource page.
11. Verify your entries, and then click Save.

Upload Orchestrator Resources

After installation, the Orchestrator Resources folder displays only the JDBC jar files that are added during installation. After the Orchestrator Resources folder is updated using the Manage User Resources palette, the Orchestrator Resources folder also displays the uploaded jar files.

You can upload a jar file to Orchestrator Resources on the Domain Orchestrator. When you restart the Domain Orchestrator, CA Process Automation deploys the file to the Domain Orchestrator. Mirroring occurs at the configured mirroring interval. After mirroring occurs, you restart the other Orchestrators. When the Orchestrators restart, the mirrored file becomes available for their use.

Follow these steps:

1. Browse to CA Process Automation and log in.
2. Click the Configuration tab.
3. Click the Manage User Resources palette and expand the Repository folder.
4. Select the Orchestrator Resources folder.

- Click New.

The Add New Resource: "Untitled" pane opens

- Provide upload details, using the following field descriptions as needed.

Resource Name

Specifies the name of the resource.

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.

Resource File

Specifies the file with its current path.

Click Browse, navigate to the location where you saved the jar file, and select the target file.

Module Name

Specifies a user-defined module name.

Resource Description

Specifies a meaningful description.

- Verify your entry. Then, click Save.

A line with your entry displays.

<input checked="" type="checkbox"/>	Name	File Type	File Path	Module
<input checked="" type="checkbox"/>	Sybase Driver	jar	/orchestrator resources/jconn2.jar	Sybase Driver

CA Process Automation copies the uploaded resources, for example, a JDBC driver, to the following paths, where *install_dir* is the directory on the server where the Domain Orchestrator was installed.

install_dir/server/c2o/ext-lib

install_dir/server/c2o/.c2orepository/.c2oserverresources/lib

- [Stop the Domain Orchestrator](#). (see page 172) [Start the Domain Orchestrator](#) (see page 173).

When the Domain Orchestrator restarts, all jars that you uploaded are deployed to the Domain Orchestrator Resources. That is, the jars are put in the classpath of the Domain Orchestrator.

- After mirroring occurs, restart all other Orchestrators.

All uploaded jars are deployed to all Orchestrators. That is, the jars are put in the classpath of the Orchestrators.

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. When agents are restarted, the file becomes available for their use.

Follow these steps:

1. Browse to CA Process Automation and log in.
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.

Resource Name

Specifies the name of the resource.

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.

Resource File

Specifies the file with its current path.

Click Browse, navigate to the location where you saved the jar file, and select the target file.

Module Name

Specifies a user-defined module name.

Resource Description

Specifies a meaningful description.

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.

See [How to Start or Stop an Agent](#) (see page 193) for details on restarting agents.

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](#) (see page 329)

[View the Audit Trail for an Environment](#) (see page 331)

[View the Audit Trail for an Orchestrator](#) (see page 332)

[View the Audit Trail for an Agent](#) (see page 334)

[View the Audit Trail for a Touchpoint, Touchpoint Group, or Host Group](#) (see page 335)

[View the Audit Trail for a Library Folder](#) (see page 336)

[View the Audit Trail for an Open Automation Object](#) (see page 338)

View the Audit Trail for the Domain

The audit trail for the Domain can display 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.

Administrators can view the audit trail for the Domain.

Follow these steps:

1. Select the Configuration tab.

The Configuration Browser opens, and displays the Domain contents on the right pane.

2. Click the Audit Trails tab.

All records are displayed by default. Column descriptions follow:

Object Name

Identifier of the Domain object, for example, Domain, Environment name, agent name.

Last Updated

The date and time that the action occurred.

Username

Name of the user that invoked the action.

Action Type

The type of action. For example, Changed, Deleted, Enabled, Locked, and Renamed are actions that apply to different objects.

Description

Describes the action including new values for changed properties.

3. (Optional) To customize the display, take one or more of the following actions:
 - a. To audit a single user, select Sort Ascending or Sort Descending in the Username column and then page to the block of records for that user.
 - b. To audit records that are produced during a limited time period, click the Last Updated column and select Sort Ascending or Sort Descending. Then scroll to the records within the time period of interest.
 - c. To change the number of rows that are displayed at a time, replace the Rows On Each Page.
4. Examine the records in the audit trail. If there are multiple pages of audit records, use the navigation buttons on the toolbar to display the first page, previous page, next page, or last page.

Each page displays the configured rows per page.

View the Audit Trail for an Environment

Administrators with Configuration Administrator access rights can view the audit trail for an Environment. Examples of actions on objects displayed on the audit trail for the selected Environment follow:

- Environment locked or unlocked.
- Environment property changed.
- Environment created or deleted.
- Environment or object in the Environment renamed.
- Touchpoint added, deleted, or renamed.
- Touchpoint Group added or deleted.
- Host Group added or deleted.

To view the audit trail for an Environment

1. Click the Configuration tab.

The Configuration Browser palette opens.

2. Expand the Domain node and select the Environment to audit, for example, the Default Environment.

This selection specifies the level at which the audit trail data is fetched.

3. Click the Audit trails tab.

The following columns of data display.

Object Name

Identifier for Environment object. For example, Environment name, Touchpoint name, Host Group name, or Touchpoint Group name.

Last Updated

The date and time that the action occurred.

Username

Name of user that invoked the action.

Action Type

The type of action. For example, Changed, Deleted, Enabled, Locked, and Renamed are actions that apply to different objects.

Description

Describes the action, including new values for changed properties.

4. (Optional) Customize the display. See the following examples:
 - a. To audit a single user, select a sort option on the Username drop-down list. Then browse to the block of records for that user.
 - b. To audit records produced during a limited time period, sort the rows by the Last Updated column and browse to the block of records in the time period of interest.
 - c. To change the number of rows displayed at a time, replace the Rows On Each Page value.
5. Examine the records in the audit trail.

View the Audit Trail for an Orchestrator

Users with read permissions on a configuration object can view the associated audit trail. Required access rights for viewing the audit trail for configuration objects include Environment User and View Configuration Browser.

Examples of actions on objects that are displayed on the audit trail for an Orchestrator are as follow:

- Orchestrator locked or unlocked
- Orchestrator property changed
- Orchestrator quarantined or unquarantined
- Orchestrator mapped to a Touchpoint or unmapped from a Touchpoint
- Orchestrator renamed

Follow these steps:

1. Click the Configuration tab from the CA Process Automation web interface.
The Configuration Browser pane opens.
2. Expand the Orchestrators node and select the target Orchestrator host.

3. Click the Audit Trail tab.

All records are displayed by default. Column descriptions follow:

Object Name

Identifier for the Orchestrator object.

Last Updated

The date and time that the action occurred.

Username

User that invoked the action.

Action Type

The type of action.

Description

Describes the action, including new values for changed properties.

4. (Optional) To customize the display, filter by the fields.
5. Examine the records in the audit trail. If there are multiple pages of audit records, use the navigation buttons on the toolbar to display the first page, previous page, next page, or last page.

Each page displays the configured rows per page.

View the Audit Trail for an Agent

Users with read permissions on a configuration object can view the associated audit trail. Required access rights for viewing the audit trail for configuration objects include Environment User and View Configuration Browser.

Examples of actions on objects that are displayed on the audit trail for an agent are as follow:

- Enabling an operator category on the Modules tab and changing a configured value.
- Agent quarantined or unquarantined
- Agent locked or unlocked.

For example, the following audit trail was recorded for associating a new agent with a touchpoint.

Contents of "Domain"									
Security		Properties		Modules		Triggers		Audit trails	
	Object Name	Last Updated	Username	Action Type	Description				
	FQDN of host	Feb 20, 2012 4:23:56 PM	pamadmin	Unlocked	The agent was unlocked successfully.				
	Default Environment	Feb 20, 2012 4:23:34 PM	pamadmin	Unlocked	The environment was unlocked successfully.				
	Default Environment	Feb 20, 2012 4:21:56 PM	pamadmin	Locked	The environment was locked successfully.				
	FQDN of host	Feb 20, 2012 4:21:30 PM	pamadmin	Locked	The agent was locked successfully.				

Follow these steps:

1. Click the Configuration tab.
2. Expand Agents.
3. Select the agent with the audit trail to examine.
4. Click the Audit Trails tab.

All records are displayed by default. Column descriptions follow:

Object Name

Specifies the name of the object to which the action pertains.

Last Updated

The date and time that the action occurred.

Username

User ID of the user that invoked the action.

Action Type

The type of action. For example, Locked or Unlocked.

Description

Describes the action that occurred at the specified time.

5. (Optional) To customize the display, filter by the fields.
6. Examine the records in the audit trail. If there are multiple pages of audit records, use the navigation buttons on the toolbar to display the first page, previous page, next page, or last page.

Each page displays the configured rows per page.

View the Audit Trail for a Touchpoint, Touchpoint Group, or Host Group

Users with read permissions on a configuration object can view the associated audit trail. Required access rights for viewing the audit trail for configuration objects include Environment User and View Configuration Browser.

Examples of actions on objects that are displayed on the audit trail for a Touchpoint, Touchpoint Group, or Host Group follow:

- Touchpoint was created
- Agent assigned to Touchpoint
- Touchpoint group was created
- Touchpoint added to group
- Touchpoint group renamed
- Host Group was created
- Agent assigned to Host Group

Follow these steps:

1. Click the Configuration tab.
The Configuration Browser panes opens.
2. Select one of the following objects:
 - A Touchpoint.
 - A Host Group.
 - A Touchpoint Group.

This selection specifies the level at which the audit trail data is fetched.

3. Click the Audit Trail tab.

All records are displayed by default. Column descriptions follow:

Object Name

Identifier of the selected object. For example, Touchpoint name, Host Group name, or Touchpoint Group name.

Last Updated

The date and time that the action occurred.

Username

User that invoked the action.

Action Type

The type of action.

Description

Describes the action including new values for changed properties.

4. (Optional) To customize the display, filter by the fields.
5. Examine the records in the audit trail. If there are multiple pages of audit records, use the navigation buttons on the toolbar to display the first page, previous page, next page, or last page.

Each page displays the configured rows per page.

View the Audit Trail for a Library Folder

Administrators can view the audit trail for any selected folder in the Library. The following actions are logged for folders in a Library:

- Create folder.
- Rename folder.
- Delete folder.
- Create or delete automation object.
- Retrieve automation object or folder from Recycle Bin.
- Change permissions on folder including links to old and new ACL.

To view the audit trail for a selected Library folder

1. Click the Library tab and select an Orchestrator from the Orchestrator drop-down list.
2. Select the folder on which you want to audit user actions and click Properties. Properties are displayed at the bottom of the main area.

3. Click the Audit Trail tab.

All records are displayed by default. Column descriptions follow:

Last Updated

The date and time that the action occurred.

Username

Name of user that invoked the action.

Action Type

The type of action, for example, Created or Renamed.

Version

The version number of the automation object on which the action occurred.

Description

Describes the action and, where appropriate, a link to a referenced object, version, or ACL.

4. (Optional) To customize the display, take one of the following actions:
 - Sort by a selected column and browse to the block of records of interest.
 - Hide rows you do not need. Select the drop-down option, Columns, for any column, and clear the checkboxes of columns to hide.
5. Examine the records in the audit trail.

View the Audit Trail for an Open Automation Object

Content administrators can open an automation object and view the audit trail for that object. The following action types are logged for automation objects:

- Create.
- Delete.
- Check-in and check-out.
- Rename.
- Export and Import.
- Change permissions on an automation object including links to old and new ACL.
- Retrieve from Recycle Bin.
- Change version designated as the current version.
- Update an automation object (for example, schedule) without a check-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. Select the folder containing the automation object instance you want to audit, then right-click that object instance and select Properties.

The Properties pane for the selected automation object opens.

3. If the Audit Trail tab is not displayed, click Audi Trail.

All records are displayed by default. Column descriptions follow:

Last Updated

The date and time that the action occurred.

Username

Name of user that invoked the action.

Action Type

The type of action, for example, Created or Renamed.

Version

The version number of the automation object on which the action occurred.

Description

Describes the action and, where appropriate, a link to a referenced object, version, or ACL.

4. (Optional) To customize the display, take one of the following actions:
 - Sort by a selected column and browse to the block of records of interest.
 - Hide rows you do not need. Select the drop-down option, Columns, for any column, and clear the checkboxes of columns to hide.
5. Examine the records in the audit trail.

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](#) (see page 341)

[Cryptographic Module Validated to FIPS 140-2](#) (see page 342)

[User Authentication and Authorization in FIPS Mode](#) (see page 342)

[How Authentication and Authorization Work](#) (see page 344)

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.

User Authentication and Authorization in FIPS Mode

Before you install CA Process Automation, you can set up CA EEM to authenticate users in a way supported by FIPS. In summary:

- Set FIPSMODE to on in the iGateway configuration file (...\\CA\\SharedComponents\\iTechnology\\igateway.conf).
- Select FIPS mode in the CA EEM configuration page of the installation wizard for the Domain Orchestrator.
- Create pem certification files when FIPS mode is set to on.

Note: See the *Installation Guide* for details.

Whether FIPS mode is set to on or off, the transferred data is encrypted. The difference is in the algorithms used for encryption.

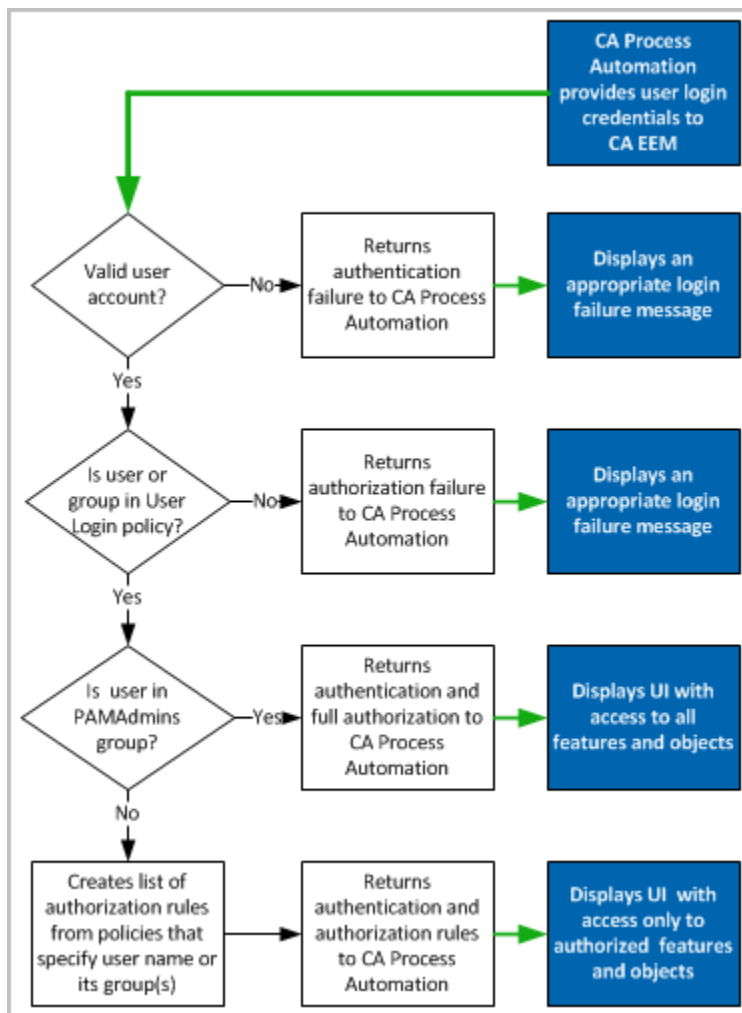
When users log in, CA Process Automation transfers the user name and password to CA EEM. CA EEM returns authentication data and authorization data to CA Process Automation.

- 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.

How Authentication and Authorization Work

In the following conceptual diagram of the authentication and authorization process,

- The shaded blocks represent actions by CA Process Automation.
- The white blocks and decisions represent actions by CA EEM.
- The thick (green) arrows represent data transfer. CA Process Automation encrypts the user name and password data it transfers to CA EEM. In response, CA EEM encrypts the authentication and authorization data it returns to CA Process Automation.



When a user attempts to log in to CA Process Automation, the following processing occurs:

1. CA Process Automation sends CA EEM the login credentials. (See the top arrow on the diagram.)
2. CA EEM determines whether the login credentials represent a valid user account.
 - a. If so, continues with Step 3.
 - b. If not, CA EEM returns an authentication failure indicator to CA Process Automation. CA Process Automation displays an appropriate login failure message.
3. CA EEM determines whether the user account or any of its association groups are Identities in the User Login policy.
 - a. If so, continues with Step 4.
 - b. If not, CA EEM returns authorization failure indicator to CA Process Automation. CA Process Automation displays an appropriate login failure message.
4. CA EEM determines whether the user account is associated with the PAMAdmins application group.
 - a. If not, continues with Step 5.
 - b. If so, CA EEM returns an indicator of successful authentication with an indicator of authorization to perform all actions. CA Process Automation allows the user to log in and displays the user interface (UI) with all features enabled so the user has full access.
5. CA EEM determines the access; CA Process Automation sets up the UI and allows the user to log in as follows:
 - a. CA EEM identifies the application groups associated with the user account.
 - b. CA EEM determines granted permissions by evaluating all other policies for that group and user name.
 - c. CA EEM returns an indicator of authentication success and a list of authorization rules for this user. Authorization rules are policy actions selected for the user or group that includes the user.
 - d. CA Process Automation sets up a session with unauthorized features disabled.
 - e. CA Process Automation allows the user to log in to this session with access only to features or objects for which they are authorized.

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](#) (see page 347)

[Back up the Domain](#) (see page 348)

[Restore the Domain from Backups](#) (see page 349)

[Manage Certificates](#) (see page 350)

[Maintain IP Addresses](#) (see page 357)

[Maintain the DNS Host Name](#) (see page 358)

[Syntax for DNS Host Names](#) (see page 358)

[Deploy the Catalyst Process Automation Connector](#) (see page 359)

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 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.

Manage Certificates

Managing certificates involve the following procedures:

- [Install the predefined CA Process Automation certificate](#) (see page 351).
- [Create and implement your own certificates for CA Process Automation](#) (see page 352).
- [Implement your third-party trusted SSL certificate for CA Process Automation](#) (see page 355).

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.

Create and Implement Your Own Certificate for CA Process Automation

You can create your own self-signed certificate to 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
 - Note:** The default was previously c2o-j.

To create and implement your own self-signed certificate

1. Using administrator credentials, log on to host where the target Orchestrator is installed.
2. Stop the Orchestrator.
 - In Windows, you can stop the Orchestrator service from the Services window. Or, run the following script, where XX is either 32 or 64, depending on the system. The default installation path, represented here as <install_dir> is C:\Program Files\CA\PAM.

```
<install_dir>\server\c2o\bin\wrapper_XX\stopc2osvc.bat
```
 - In Linux, run the c2osvrd.sh script with the - stop option. That is, run:

```
c2osvrd.sh.stop
```
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_name>.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.
 - In Windows, you can start the Orchestrator service from the Services window. Or, run the following script, where XX is either 32 or 64, depending on the system.

```
<install_dir>\server\c2o\bin\wrapper_XX\startc2osvc.bat
```
 - In Linux, run the c2osvrd.sh script with the - start option. That is, run:

```
c2osvrd.sh.start
```

Implement Your Third-Party Trusted SSL Certificate for CA Process Automation

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 for fresh installations of CA Process Automation r2.2 SP1 or later, or "c2o-j" for CA Process Automation r2.2 or earlier.

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.

To use a certificate issued by a third-party Certification Authority

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 Certification 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. Shut down the CA Process Automation Orchestrator.
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.xml` 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. Restart the CA Process Automation Orchestrator.
10. Repeat this procedure for each Orchestrator that is to use the new certificate.

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. An example install folder is C:\Program Files\CA\PAM\server\c2o.

install_folder\config\OasisConfig.properties

install_folder\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 address that change, reconfigure the agent by Updating the following file:

install_folder\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=<x.x.x.x>

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 172).
 - b. [Start the Orchestrator](#) (see page 173).

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.

Deploy the Catalyst Process Automation Connector

The Catalyst Process Automation Connector is disabled by default. You can enable it by changing a property value in the OasisConfig.properties file. When you restart the Domain Orchestrator, the Catalyst Process Automation Connector deploys and starts.

Follow these steps:

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

```
install_dir/server/c2o/.config
```
3. Open the OasisConfig.properties file.
4. Scroll to the UCF embedded connector in `jboss-service.xml` section.
5. Change the value for the property `ucr.connector.enabled` from `false` to `true`. That is:

```
ucr.connector.enabled=true
```
6. Save the file and exit.
7. Restart the Orchestrator service.
 - a. [Stop the Orchestrator](#) (see page 172).
 - b. [Start the Orchestrator](#) (see page 173).

Index

A

- Access Control ID
 - identifying for Touchpoint Security policy • 111
- access policies in CA EEM
 - ConfigAdmin • 100
 - ContentAdmin • 102
 - grant administrators access to CA EEM • 76
 - resource classes • 80
 - to define Touchpoint Security policies • 103
- administrator
 - documentation for, • 23
 - tasks performed by, • 24
- agent
 - associating with a Host Group • 227
 - configuration options • 176
 - configuring properties • 184
 - decommissioning a host with, • 190
 - installing interactively • 180
 - managing Modules on, • 187
 - quarantining • 189
 - removing • 192
 - removing a quarantine from, • 189
 - removing in bulk • 192
 - renaming • 190
 - starting on a UNIX or Linux host • 194
 - stopping on a UNIX or Linux host • 194
- application user group (CA EEM)
 - assigning to global user • 62
- archival policy
 - configuring for Orchestrator • 166
- asterisk usage
 - in Host Name patterns • 232
- audit trail
 - viewing, for Agent • 334
 - viewing, for Automation Object instance • 338
 - viewing, for Domain • 329
 - viewing, for Environment • 331
 - viewing, for Host Group • 335
 - viewing, for Library folder • 336
 - viewing, for Orchestrator • 332
 - viewing, for Touchpoint or Touchpoint Group • 335
- auto-admit patterns
 - configuring • 198

- using to add Touchpoints in bulk • 198

- automation object
 - dependencies • 72
 - ownership • 118

C

- CA EEM
 - changing refresh frequency • 20
 - FIPS mode • 342
 - granting access to an Administrator • 78
 - granting access to Touchpoint Security Policy • 103
 - resource classes • 80
 - security settings for Domain • 122
 - suspending or disabling a user account • 38
- Catalyst module
 - configuring • 246
 - defined • 245
- certificate for CA Process Automation
 - options • 351
 - predefined • 351
 - self-signed • 352
 - trusted SSL • 355

D

- Databases module
 - configuring for MSSQL Server • 263
 - configuring for MySQL • 264
 - configuring for Oracle • 261
 - configuring for Sybase • 266
- Date-Time module
 - defined • 268
- direct machine access • See host group
- Directory Services module
 - configuring • 268
 - defined • 268
- Domain
 - cardinality • 33
 - configuring CA EEM security • 122
 - configuring properties • 129
 - hierarchy • 133
 - locking and unlocking • 119
 - relationships to Environment and Touchpoint • 30
 - restoring from backups • 349

Domain Orchestrator

- starting • 173
- stopping • 172

E

Email module

- defined • 272

environment

- adding to a Domain • 136
- cardinality of associations • 33
- configuring properties for, • 142
- configuring security for, • 140
- relationships with other entities • 30
- removing from a Domain • 137
- renaming • 148

F

File module

- configuring • 275
- defined • 275

File Transfer module

- defined • 278

File trigger

- activating for Orchestrator • 165
- configuring for Domain • 308

files

- authorized_keys • 236
- itpam_eem.xml • 122

FIPS 140-2 support

- as one aspect of security • 37
- changing setting related to CA EEM FIPS mode • 124
- defined • 341
- validated modules used by CA Process Automation • 341

G

group for CA IT PAM users (CA EEM)

- adding to a policy • 89
- creating • 87
- dynamic • 64

H

host group • 223

- cardinality of associations • 33
- compared with Proxy Touchpoint • 225
- creating • 227
- defined • 224

how referenced in a request • 223

prerequisites to use • 226

relationships with other entities • 30

viewing a list of, • 238

I

inheritance

- configuration • 121
- module properties • 294

IP addresses

- maintaining • 357

ITPAM User Policy (CA EEM)

- dependencies on • 72

J

Java Management

- defined • 279

JDBC driver

- deploying for Database operators • 321
- deploying for the JDBC Connector • 324

L

locking

- domain • 119

logging on

- <Global> in CA EEM • 44
- after browsing to CA Process Automation • 18

M

Mail trigger

- activating for Orchestrator • 165
- configuring for Domain • 311

Management Console Policy (CA EEM)

- dependencies on • 72

mirroring

- Agent • 184
- Orchestrator • 168

module

- disabling • 295
- enabling • 295
- inheritance of properties • 294
- managing , on agent • 187
- overriding settings • 296
- relationship to Operators and Processes • 240
- support by Orchestrators and Agents • 298

N

Network Utilities module
configuring for TFTP • 278

O

Operator recovery
configuring for Environment • 142
configuring for Host Groups • 227
configuring for Orchestrator • 153
configuring for Touchpoint • 201
from Configuration Browser • 157

Orchestrator
activating triggers • 165
adding • 149
cardinality of associations • 33
configuring • 153
quarantining • 170
relationships to other entities • 30
removing from Environment • 150
removing quarantine • 171
setting mirroring • 168
setting policies • 166
setting properties • 153
starting • 173
stopping • 172
viewing security settings • 159

P

password
changing in CA EEM • 44
permissions
permissions, policies (CA EEM) • 68
policy
Orchestrator • 166
process
recovery of waiting, • 157
Process Control module
configuring • 282
defined • 282
Process module
configuring • 251
defined • 249
properties
Agent • 184
Domain • 129
Environment • 142
Host Group • 227

Orchestrator • 153
Touchpoint • 201
proxy touchpoint
configuring properties • 218
creating a trust relationship to the target
computer • 217
creating an SSH User Account on Remote Host •
217
how referenced in a request • 223
prerequisites • 215
SSH connectivity for • 216
using • 221

Q

quarantine
removing from agent • 189
removing from Orchestrator • 171
setting for agent • 189
setting for Orchestrator • 170

R

referenced user store
configuring AD for integration • 65
managing global users from • 59
preparing for integration • 61
regular expressions
use in configuring SNMP triggers • 315
use in defining Host Name patterns • 232
use when adding Host Groups • 229
use when adding Touchpoints in Bulk • 198
resources
a CA EEM resource class • 80
Runtime Security
enable • 166

S

scenarios
implementing Touchpoint Security • 110
security, application
defined • 37
password protection • 350
setting for Automation Objects • 118
SNMP Module
configuring • 280
defined • 280
SNMP trigger
activating for Orchestrator • 165
changing the listening port • 318

-
- configuring for Domain • 315
 - implementing • 300
 - SOAP module
 - configuring • 287
 - defined • 287
 - SSH connectivity
 - based on public key authentication • 236
 - based on user account credentials • 234
 - CA Process Automation-specific requirements • 216

T

- target of Operator
 - criteria for selecting • 223
- touchpoint
 - adding, to an Environment • 197
 - cardinality of associations • 33
 - configuring properties • 201
 - creating in bulk from auto-admit patterns • 198
 - managing a group of, • 207
 - mapping to a different Agent • 204
 - mapping to multiple Agents • 198
 - relationships to other entities • 30
 - removing in bulk • 205
 - renaming • 203
- touchpoint group
 - creating • 207
- Touchpoint Security
 - configuring for Domain • 129
 - configuring for Environments • 142
 - configuring for Host Group • 229
 - configuring for Orchestrator • 153
 - configuring for Touchpoint • 201
 - creating a policy for • 112
 - defined • 107
- Touchpoint Security policy
 - creating • 112
 - example protecting critical hosts • 114
 - example with all Modules • 115
 - granting users right to create • 103
 - identifying Module names for • 111
 - policy dependencies • 72
 - policy filters • 75
 - resource class • 80
- trigger
 - activating for an Orchestrator • 165
 - File Trigger • 308
 - implementation process • 300
 - Mail Trigger • 311
 - SNMP Trigger • 315
 - UCF Trigger • 302

U

- UCF trigger
 - configuring • 302
 - relationship to UCF-USM Module • 245
- user account for CA EEM administrator
 - creating • 78
- user account for CA Process Automation users
 - authentication and authorization • 342
 - suspend or disable in CA EEM • 38
- user account for SSH access
 - create on host referenced by a Proxy Touchpoint • 217
 - create on host referenced by Host Group • 234
- User Login Policy (CA EEM)
 - dependencies on • 72
- user resources
 - adding a script to, • 322
 - deleting a script from, • 323
- user settings
 - configuring • 19
- utilities
 - iGateway Certificate Utility (igwCertUtil) • 127
 - itpamDbScript • 19
 - ssh-keygen • 226