CA Process Automation

User Interface Reference

Service Pack 04.2.02

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.

Contents

Chapter 1: Library Tab

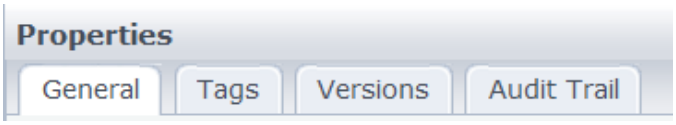
This section provides field descriptions for the Library tab and for the dialog boxes that you can access from the Library tab. The topics are sequenced alphabetically, by page name.

Mapping for Object Properties Tabs

This section defines fields listed under tabs displayed when selecting the properties for each object.

Object Properties: Calendar, Custom Icon, Custom Operator Dataset, Interaction Request Form, Process Watch, Resources

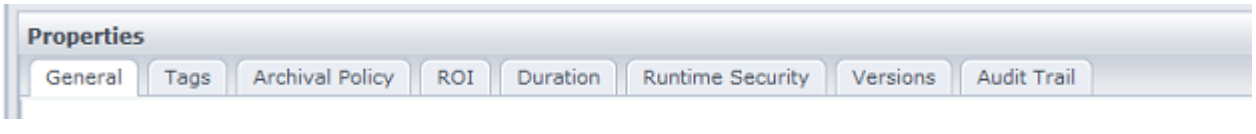
Equation 1: Properties for a selected object can include the following tabs: General, Tags, Versions, Release, and Audit Trail



- General (see page 20)
- Tags (see page 31)
- Versions (see page 32)
- Audit Trail (see page 16)

Object Properties: Process

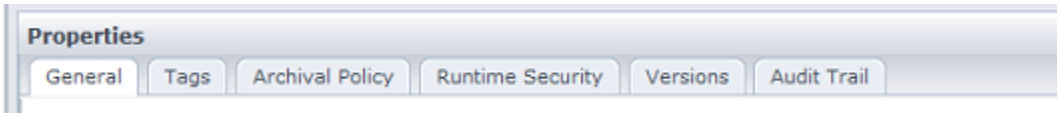
Equation 2: Properties for a selected object can include the following tabs: General, Tags, Archival Policy, ROI, Duration, Runtime Security, Versions, Release, and Audit Trail



- General (see page 20)
- Tags (see page 31)
- Archival Policy
- ROI (see page 25)
- Duration (see page 17)
- Runtime Security (see page 26)
- Versions (see page 32)
- Audit Trail (see page 16)

Object Properties: Schedule

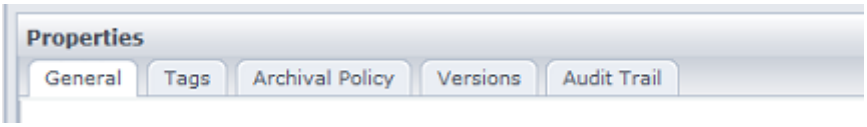
Equation 3: Properties for a selected object can include the following tabs: General, Tags, Archival Policy, Runtime Security, Versions, Release, and Audit Trail



- General (see page 20)
- Tags (see page 31)
- Archival Policy
- Runtime Security (see page 27)
- Versions (see page 32)
- Audit Trail (see page 16)

Object Properties: Start Request Form

Equation 4: Properties for a selected object can include the following tabs: General, Tags, Archival Policy, Versions, Release, and Audit Trail



- General (see page 20)
- Tags (see page 31)
- Archival Policy
- Versions (see page 32)
- Audit Trail (see page 16)

Calendar Object:: Advanced Tab

Union

Indicates that one or more of the linked conditions must be satisfied for the combined condition to be satisfied.

Place one or more branches or basic conditions under this icon.

Intersection

Indicates that the linked conditions must all be satisfied for the combined condition to be satisfied.

Place one or more branches or basic conditions under this icon.

Exclusion

Indicates a basic condition or a branch to be excluded from a rule.

All dates are excluded that are not otherwise selected. It is therefore only useful to exclude days when they are selected by another part of the rule. For example, no purpose is served by excluding Tuesdays unless they are defined as valid days by other conditions and operators in a rule. So if a condition specifies the work week (Monday through Friday) as valid days, you could use the Exclusion operator to exclude Tuesdays from this set.

Expand the Exclusion operator to show the Included and Excluded branches.

Click a branch and then add a condition or operator to define included or excluded dates.This operator has two sets of branched arguments:

Included: One or more basic conditions or branches that represent dates to be included in the rule.

Excluded: One or more basic conditions or branches representing dates to be excluded from the dates defined by the Included set.

Like

Use the Like operator to use an existing set of dates defined by another calendar object in your rule. This operator has the following parameters:

Calendar Name: The name of the referenced calendar.

Delta: Shifts the valid dates defined by the referenced Calendar by the specified number of days. Enter a negative number to move the dates earlier, or a positive number to move the dates later.

Open Days: When checked, indicates that the delta or shift only applies to open days.

For example, a new calendar rule could reference another calendar specifying backup days with a delta of 1. The resulting condition in the new calendar rule specifies the day immediately following backup days.

Dates List

Specifies individual dates (with years) that can be added, deleted, or reordered.

Date Interval

Specifies a regular daily, weekly, or monthly interval in a range of dates from beginning to end.

For example, every week from March 1, 2015 to July 1, 2016.

- **Beginning**: The starting date for the range.
- **End**: The ending date for the range.
- **Repeat Forever**: Check this box to ignore the End date and extend the interval indefinitely.
- **Step**: Indicates the quantity of units (days, weeks, or months) in each interval. For example, an interval with a unit of week and default Step of 1 occurs once in week 1, again in week 2, and a third time in week 3. When Step is set to 3, the interval occurs once in weeks 1 to 3, again in weeks 4 to 6, and a third time in weeks 7 to 9.
- **Unit**: Specifies the recurrence frequency or interval. Select Day, Week, or Month.

Date Without Year List

Specifies a list of explicit anniversary dates (without years) that can be added, deleted, or reordered.

This condition is commonly used to specify holidays that fall on the same day every year. Examples include January 1st and December 25th.

Date Without Year Interval

Specifies an anniversary interval of dates without a year.

For example, from March 21st to June 20th (for Spring).

- **Beginning**: The starting date without a year for the interval.
- **End**: The ending date without a year for the interval.

Year Interval

Specifies an interval of years.

You can specify leap years by starting an interval on a leap year and specifying a step of 4 (such as 2000 to 2024 with a step of 4).

- **Beginning**: The starting year for the interval.
- **End**: The ending year for the interval.
- **Step**: The number of years from one valid year to the next valid year.

Month Interval

Specifies one or more months in the year.

The first semester is specified with a range from 1 to 6 with a step of 1. The second semester is specified with a range from 7 to 12 with a step of 1.

- **Beginning**: The starting month for the interval.
- **End**: The ending month for the interval.
- **Step**: The number of months from one valid month to the next valid month.

Week of the Month Interval

Specifies one or more weeks in the month.

CA Process Automation implements ISO standards for partial weeks. A week which intersects with a given month is considered to be part of the month if the Thursday of that week falls in the month.

For example, if June 1st is a Friday, the First week of the month starts on June 4th. If June 1st is a Wednesday, the first week of the month starts on May 30th.

It is possible to have the “first Monday of the month” not be “Monday of the first week of the month.” To define the former, it is simpler to combine “Day of the month” and “Day of the Week” conditions.

- **Beginning**: The starting week for the interval.
- **End**: The ending week for the interval.
- **Step**: The number of weeks from one valid week to the next valid week.
- **Reverse**: Counting starts with the last week of the month and goes backwards.

Week of the Year Interval

Specifies one or more weeks in the year.

CA Process Automation implement ISO standards for partial weeks. A week which intersects with a given year is considered to be part of the year if the Thursday of that week falls in the year.

For example, if January 1st is a Friday, the First week of the year starts on January 4th. If January 1st is a Wednesday, the first week of the year starts on December 30th of the previous year.

It is therefore possible to have the “first Monday of the year” not be “Monday of the first week of the year.” To define the former, it is simpler to combine “Day of the year” and “Day of the Week” conditions.

- **Beginning**: The starting week for the interval.
- **End**: The ending week for the interval.
- **Step**: The number of weeks from one valid week to the next valid week.
- **Reverse**: Counting starts with the last week of the year and goes backwards.

Day Interval

Specifies an interval of valid days (between 1 to 31) in a month with a starting day, an ending day, and a step.

You can also specify that the iteration start from the end of the month or that only open days are counted in each step. Open days are those days not specified by a condition or rule that closes or excludes dates.

For example, the last day of the month is specified by the interval beginning and ending with 1 with Reverse selected. The last weekday of the month would be specified when the Open check box is also selected and a Weekday Interval specifying Monday through Friday is added with an And operator.

- **Beginning**: The starting day for the interval.
- **End**: The ending day for the interval.
- **Step**: The number of days from one valid day to the next valid day.
- **Reverse**: Counting in steps starts with the last day of the month and goes backwards.
- **Open Days**: Counting in steps includes only open days when days are closed by a condition or rule.

Day of the Year Interval

Specifies an interval of valid days (between 1 and 366) in a year with a starting day, an ending day, and a step. The day 366 is valid on leap years.

You can also specify that the iteration start from the end of the year or that only open days are counted in each step. Open days are those days not specified by a condition or rule that closes or excludes dates.

For example, you can specify winter as the interval from December 21st to March 20th.

Or for a slightly more complicated example, to specify every 10th day throughout the entire year, you could use a range from 1 to 365 (or 366 for a leap) with a step of 1. You could specify the last ten open days of the year with a starting day of 1, an ending day of 10, with Reverse and Open selected.

- **Beginning**: The starting day for the interval.
- **End**: The ending day for the interval.
- **Step**: The number of days from one valid day to the next valid day.
- **Reverse**: Counting in steps starts with the last day of the year and goes backwards.
- **Open**: Counting in steps includes only open days.

Day of the Week Interval

Specifies one or more days of the week (from Monday through Sunday) as an interval with a starting day, an ending day, and a step.

For example, weekends are specified by the interval beginning on Saturday and ending on Sunday with a step of 1.

- **Beginning**: The starting day for the interval
- **End**: The ending day for the interval.
- **Step**: The number of days from one valid day to the next valid day.

Weekday of the Month

Specifies a weekday in an indexed week of a particular month. The week is indexed from either the beginning or the end of the month.

- **Weekday**: Specifies the day of the week.
- **Month**: Specifies the month for which the week day is applicable.
- **Week Index**: Specifies the index of the week for which the week day would be applicable. (Value can be 1 to 5 because in any month there cannot be more than 5 weeks)
- **Reverse**: If you select this check box, the counting for the week index starts from the last week.

  For example, if you select Monday as a weekday, September as a month, and 3 as a Week Index: in September, the third Monday is included in the calendar. If you selected the reverse check box, in September, the third Monday from the last is included in the calendar.

Weekday of the Year

Specifies a weekday in an indexed week of the year. The week is indexed from either the beginning or the end of the year.

- **Weekday**: Specifies the day of the week.
- **Week Index**: Specifies the index of the week for which the week day is applicable. (Value can be 1 to 53 because in a year there cannot be more than 53 weeks)
- **Reverse**: If you select this check box, the week index counting starts from the last week.

  For example, if you select Monday as a weekday, 43 as the Week Index, the forty third Monday of the year is included in the calendar. If you selected the reverse check box then the forty third Monday from the last week is included in the calendar.

Object Properties: Archival Policy Tab (Process, Start Request Form, Schedule)

The Archival Policy tab indicates how long the server archives a completed instance of a process or schedule object and contains the following fields:

Minimum Days of Process History

Defines the minimum number of days that the system retains completed and failed instances of processes. The age of an instance is measured in hours. If an instance ends at 10:00 p.m. and you set this option to one day, the instance remains in the Library until 10:00 p.m. the following day.

Default: This input field defaults to 0.

Minimum Number of Failed Instances

Defines the minimum number of Failed instances of the Object (Process, Schedule, and SRF) that are retained. To view the retained instances of an object, select the Current filter of the respective object from the Operations dashboard.

The remaining objects are archived and to view the archived objects, select the Archived filter of the respective object from the Operations dashboard. When the Failed instances exceed the specified value in the field, the product archives the object instances with the oldest timestamp of completion.

However, the instances are archived only after they are retained for a minimum number of days as specified in the Minimum Days of Process History field.

Default: This input field defaults to 0. You can specify a positive integer value.

When 0 is specified, instances are archived but are not retained.

Minimum Number of Finished (Completed, Aborted) Instances

Defines the minimum number of Finished (completed and aborted) instances of the Object (Process, Schedule, and SRF) that are retained. To view the retained instances of an object, select the Current filter of the respective object from the Operations dashboard.

The remaining objects are archived and to view the archived objects, select the Archived filter of the respective object from the Operations dashboard. When the number of Finished (completed and aborted) instances exceed the specified value, the application archives the object instances with the oldest timestamp of completion.

However, the instances are archived only after they are retained for a minimum number of days as specified in the Minimum Days of Process History field.

Default value: 0. You can specify a positive integer value.

When 0 is specified, instances are archived but are not retained.

Inherit archival policy from Orchestrator

Enables you to inherit Archival Policy property settings for an object from the Orchestrator.

Default: Selected

Important: The above object level properties are applicable only if the Inherit archival policy from Orchestrator check box is cleared.

Important! If an object is deleted, then the archival policy for the object defaults to server level settings defined in the Configuration browser.

Note: In previous releases, you could not retrieve the archived instances to the current filter. In this release, if you increase the number to retained instances of Archival Policy (from 3 to 4 here), the instances that are archived in previous Archival Run are retained to the Current Filter.

Consider the following Archival Policy Settings at the Configuration Browser level:

- *Minimum Number of Days of Process History= 3*

  Result after Archival Thread is executed. (after 12 minutes).

  All the instances that are younger than three days are retained and the instances beyond three days are archived.

Now, change Policy at the Configuration Browser as follows:

- *Minimum Number of Days of Process History= 4*

  Result after Archival Thread is executed (after 12 minutes). All the instances that are younger than four days are retained.

  Instances that were earlier archived beyond three days (fourth day), are also now retrieved to the current filter.

The behavior of retrieving the archived instances to the current filter is applicable to the following Archival Parameter fields:

- *Minimum Days of Process History*
- *Minimum Number of Failed Instances*
- *Minimum Number of Finished (Completed, Aborted) Instances*

Object Properties: Audit Trail Tab

The Audit Trail tab contains the following fields:

Last Updated

Indicates the date and time that the action occurred.

Username

Identifies the User ID of the user that invoked the action.

Action Type

Indicates the type of action. For example, Locked or Unlocked.

Version

Specifies the versions of the selected automation object.

itpam--Object Properties: Basic Tab (Calendar) (v4.2)

Calendar Rule

Specifies the recurrence interval or that the rule is based on manual selection. The manual selection includes specification of the start date and end date during which the rule is applicable. Alternatively, specifies Repeat Forever.

Repeat Daily

As an alternative to a calendar rule to Repeat Daily or Repeat Weekly, for example, you can specify a different repeat interval. For example, repeat every 3 days, or every 15 days or every 60 days.

Summary

Summarizes the calendar rule or repeat interval, including dates to exclude.

Object Properties: Custom Icon Tab

The Custom Icon tab is specific to the Custom Icon automation object. The tab lets you select a base icon graphical element from a list and add an icon modifier to the base icon. As you make a selection, the result is displayed in the Custom Icon Preview area.

Object Properties: Dataset Tab (Custom Operator)

The Dataset tab lets content designers define and group operator dataset variables that contain information that a custom operator returns. The configurations and settings in the Dataset palette of a custom operator are the same as for any other dataset. For each output parameter name/value pair on the left, you can configure whether to hide the parameter value from output.

Hide from output

Specifies whether to include the parameter with the output.

- **Selected:** Indicates to hide the parameter; the output parameter is not displayed in the dataset.
- **Cleared:** Indicates that the parameter is to be included in output parameters; the dataset includes the output parameter.

Object Properties: Duration Tab (Process)

The Duration tab contains the following fields:

Enabled

Specifies whether you can define the run interval for a process.

Values: This check box has one of the following values:

- **Selected** - The Expected Duration and Warning Threshold fields are enabled.
- **Cleared** - The Expected Duration and Warning Threshold fields are not enabled.

Default: Cleared

Expected Duration

Defines the expected duration for a process (in days, hours, and minutes).

Warning Threshold

Defines how far in advance the user is warned when the process run exceeds its expected duration.

Object Properties: Form Tab (Custom Operator)

The Form tab for a custom operator contains the following fields:

Left pane

Form Elements folder

Contains all of the available types of elements to include on a form.

All of the form elements are explained in the *Content Designer Guide*.

Custom Operator folder

Displays the structure of your form. Drag and drop form elements to the pages of your form from here.

Page Layout level

A custom operator may require additional parameters as input into the function of the operator. You can add property pages to group these additional parameters. When you add pages to the custom operator to this section, they appear as expandable sections in the Properties palette of the Process Designer.

After creating property pages, you can add customizable parameters (fields) to them, nested beneath the page layout level.

Middle pane

Custom parameters

Each custom operator can have one or more pages of parameters that are based on its ancestor or base operator. You can modify and configure these parameters. All operator parameters are described in the *Content Designer Reference*.

Right pane

Property Pane

Use this pane to view or edit the variables in the form elements. For example, set the Invisible property to true, change the Label that identifies a field, or specify a function for an event.

Object Properties: Form Tab (Interaction Request Form)

The Form tab for an interaction request form contains the following fields:

Left pane

Form Elements folder

Contains all of the available types of elements to include on a form.

All of the form elements are explained in the *Content Designer Guide*.

Interaction Request form folder

Contains the Page Layout folder, which includes the Page element for your form. The Page element is the canvas that you can build your form on. You can drag and drop form elements to the pages of your form here.

Middle pane

Form Pages

The layout for the pages of your form appears here. Click a control to edit its properties. For forms with multiple pages, click Back and Next to view other pages. Users can also click Next and Back to view the form pages.

You can drag and drop form elements from the left pane to the page to design the forms.

Right pane

Property Pane

Use this pane to view or edit the variables in the form elements. For example, set the Invisible property to true, change the Label that identifies a field, or specify a function for an event.

Object Properties: Form Tab (Start Request Form)

The Form tab for a start request form contains the following fields:

Left pane

Form Elements folder

Contains all of the available types of elements to include on a form.

All of the form elements are explained in the *Content Designer Guide*.

Start Request form folder

Contains the Page Layout folder, which includes the Page element for your form. The Page element is the canvas that you can build your form on. You can drag and drop form elements to the pages of your form here.

Middle pane

Form Pages

The layout for the pages of your form appears here. Click a control to edit its properties. For forms with multiple pages, click Back and Next to view other pages. Users can also click Next and Back to view the form pages.

You can drag and drop form elements from the left pane to the page to design the forms.

Right pane

Property Pane

Use this pane to view or edit the variables in the form elements. For example, set the Invisible property to true, change the Label that identifies a field, or specify a function for an event.

Object Properties: General Tab

The General properties of every library object contain the following fields:

Note: All properties are read-only *except* Description.

Name

Specifies the object name.

Current Version

Specifies the version of the object.

Type

Specifies the object type for this automation object.

Owner

Specifies the user ID of the user who created this object.

Checked Out By

Specifies the user ID of the user who modified this object last.

Date Created

Specifies when the object was created.

Date Modified

Specifies when the object was modified.

Path

Specifies the folder path for the object.

Orchestrator

Specifies the name of the Orchestrator on which this object runs.

Description

Specifies the object description.

Use deprecated locking mechanism (Dataset objects)

This check box specifies whether an operator accessing a named dataset from the Library takes a global, cluster-wide lock.

Values: This check box has one of the following values:

- **Selected** - An operator accessing a named data set—for read, write, or both—takes a global, cluster-wide lock for access by multiple processes. This locking is the legacy method that is used in previous versions of PAM and is provided for backwards compatibility. This method requires that other operators that are accessing any other named data set to wait while it completes its operation. This method represents a reduction in the speed of process execution in an otherwise high-performance system. This method is recommended, when multiple processes or operators simultaneously updates the same dataset variable. For example, Counter.
- **Cleared** - The named data set accessed by the operator takes a lock for itself only. This method is much faster than the legacy cluster-wide lock method. When reading from the dataset, no lock is taken. When writing to the dataset, the lock is taken and released only at the end of the operator and is relatively short.

Default: Cleared for new dataset objects. Imported dataset objects from previous versions have their check box selected by default.

Object Properties: Group Configuration

Object Properties: Preview Tab (Calendar)

The Preview tab lets you view the calendar dates you defined on the Basic tab or the on the Advanced tab.

Included Dates

Displays all the dates included in your calendar rule settings.

Preview Exclusion Calendar

Displays exceptions to rules.

- Included Dates: The calendar preview displays dates included in your calendar with bold dark blue numbers.
- Excluded Dates: The calendar preview displays dates that are manually or automatically omitted from the calendar rules with light blue numbers.
- Conflicting Dates: The calendar preview displays dates that overlap or conflict with the dates defined by an optional exclusion calendar with bold red numbers.

Delta

Specifies the number of days an eligible date is shifted when it falls on an omitted or excluded date. A negative Delta value shifts forward (earlier), and a positive value shifts backward (later). When this value is zero (the default), the eligible date, normally included in the calendar rule, is marked in bold red and omitted.

Max Shift

Defines the maximum number of shifts or adjustments to allow if repeated shifts fall on closed days.

Object Properties: Version Tab

The Version tab contains the following field:

Release Version

Identifies the specific version of a folder or content package that was imported, or that you want to export, then import, to a production environment. This field is locked in the following circumstances:

- The object was exported with its release version in nonmodifiable mode.
- The release version was in nonmodifiable mode before the export.

Note: The Version tab is visible only for a folder or content package.

Object Properties: Resources Tab

Name

Defines the name of the resource object.

State

In the Operations dashboard, specifies whether the resources object is locked or unlocked. The resources operator controls this field. You can manually override the displayed state.

Values

Locked: A running process cannot update the Used value of this resource.

Unlocked: A running process can update the Used value of this resource.

Default: Unlocked

Amount

Lists the total number of units assigned to a resource. The number of units serves as a quota in a process. Quotas for operators in processes are drawn from this number. This arbitrary value that does not necessarily quantify the number of units of any actual computer or system resource (such as CPU, memory, or bandwidth). There are no rules about the quantity of a resource. You can specify an amount of *1*, so only one instance of a CPU-intensive operator can be run by any process at any given time.

Used

In the Operations dashboard, defines the number of this resource that is in use. A new resource typically starts with this value set to 0. The maximum Used value is the value that is displayed for Amount. Dataset variables can set resource usage. Usage can be fine-tuned on a touchpoint without opening and configuring processes that consume a resource. For example, if you set the amount to *100*, you could change a usage variable from *10*, to *20*, to *50*, or even to *100* to accommodate demands on a touchpoint. More commonly, a Resource operator changes these settings programmatically in a process or schedule.

Note: The Manage Resources operator in a running process increases the number as units of this resource are consumed. The number decreases as units are freed.

Default: 0

% Usage

Position your mouse over this visual indicator to view the usage percentage, that is the Used value divided by the Amount value.

Description

Describes the new system resource or your resource management goal. This field accepts multiple-line descriptions.

Object Properties: ROI Tab (Process)

The ROI tab contains the following fields:

Enable ROI

Enables the ROI fields.

Values: This check box has one of the following values:

- **Selected** - The Manual Labor Time, Manual Process Elapsed Time, Criticality, and App/System Group Name fields are enabled.
- **Cleared** - The Manual Labor Time, Manual Process Elapsed Time, Criticality, and App/System Group Name fields are not enabled.

Default: Cleared

Manual Labor Time (hh:mm)

Specifies the cumulative number of staff hours and minutes it takes to trigger manually multiple operations within the process. As an example, you have a process that contains three steps, one of which backs up files into a folder that you must first create. The time that you spend creating, placing, and naming the folder is added to the overall manual labor time. This value does not include the time that it takes to back up the files.

Manual Process Elapsed Time (hh:mm)

Specifies the cumulative number of staff hours and minutes it takes to execute the entire process manually, start-to-finish. Using the previous example, this sum includes the following time frames:

- The time that it takes to create and name the folder receiving your backup files (manual labor time).
- The time that it takes to back up the files (manual execution time).

Criticality

Specifies the criticality for this process.

Values: High, Medium, or Low.

Note: The ROI report displays the criticality of the process.

App/System Group Name

Optionally, as you build processes, tag each process through this field with a common group name under which they are sorted in the ROI Report.

Note: You can group processes by group name in the ROI report. Click the Reports tab and run the Return on Investment Report for an application or system group.

Object Properties: Runtime Security Tab (Process objects)

The Runtime Security controls ensure that users without proper permissions cannot start a process.

Runtime Security

Specifies whether to enable or disable the runtime security explicitly or through an inheritance option.

Note: When you explicitly enable or disable the run-time security, changes to inherited settings have no impact.

Values:

- **Inherit from Orchestrator:** The process object inherits security settings from the Orchestrator.
- **Enable:** The product verifies user permissions before accessing automation objects from the database. After you enable the run-time security, the product uses enforcement when a process starts.
- **Disable:** The product ensures backward compatibility for existing processes during, for example, system upgrades. The processes run as they did before this release.

Default: Inherit from Orchestrator

Run as Owner

Specifies whether to run processes with the permissions of either the process owner or the user who started the process instance. This check box is active only when you set the Runtime Security property to Enabled or Inherit from Orchestrator. Only Environment Content Administrators or the process owner can select this check box.

Values:

- **Selected**: The current identity is the process owner. The product enforces an access control list for the process owner, regardless of who started the process. The product loads private copies of the process and the owner-created objects.
- **Cleared:** The current identity is the user who started the process. The product verifies the user permissions.

Default: Cleared

Enable Operator Recovery

Specifies whether to automate the operator recovery. This option applies to process objects only. Recovery applies to specific 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.

Values:

- **Selected:** Recovery starts running the affected processes. The operators that target the proxy touchpoint run.
- **Cleared:** Operator recovery is disabled.

Default: Selected

Object Properties: Runtime Security Tab (Schedule)

The Runtime Security controls ensure that users without proper permissions cannot start a process. The runtime security can be enabled or disabled either explicitly or through an inheritance option. When set explicitly, changes to inherited settings have no impact. The Runtime Security tab contains the following fields:

Inherit from Orchestrator

This default value sets security settings as inherited from the Orchestrator.

Enable

Enabling runtime security allows CA Process Automation to verify permissions of a user before accessing automation objects from the database. Once enabled, runtime security enforcement is used when a process starts.

Disable

Disabling runtime security ensures backward compatibility for existing processes during, for example, system upgrades. Processes continue to run as they have before this release.

Object Properties: Settings Tab (Custom Operator)

Target

Specifies where the custom operator is to run.

- Click the Search icon to open the Object Browser. Navigate to the target environment and select an Orchestrator touchpoint, an agent touchpoint, a proxy touchpoint, or a touchpoint group. Alternatively, enter the IP address or host name that matches a pattern specified in a Host Group in this environment.
- Specify a dataset that points to a valid target.

Target is a calculated expression.

Specifies that the Target entry is a calculated expression. Calculated expressions specify a target dynamically at runtime. Consider the following examples:

- Use a string dataset variable containing the name of the touchpoint.
- Use an Object Reference dataset variable that points to the touchpoint.

Important! When a process is destined for an import as a content package, specify the IP address or FQDN in a dataset. A dataset can be modified in the import environment, but the Target field cannot.

Match target in Host Groups only?

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

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

Values: The drop-down list has the following values:

- **Inherit** - Use the inherited value, either Enabled or Disabled.
- **Enabled** - The scope of the search depends on whether the "Lookup DNS when matching target in Host Groups" field is enabled or disabled.
  - If a DNS lookup is disabled, searches: Host group reference to a remote host (exact)
  - If a DNS lookup is enabled, searches: Host group reference to a remote host (exact or DNS lookup result)
- **Disabled** - Search the Domain components in the following order:
  a. Touchpoint (exact or a DNS lookup result)
  b. Orchestrator (exact or a DNS lookup result)
  c. Agent (exact or a DNS lookup result)
  d. Proxy touchpoint mapping to a remote host (exact or DNS lookup result)
  e. Host group reference to a remote host (exact or DNS lookup result)

Default: Inherit

Lookup DNS when matching target in Host Groups?

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

Values: This drop-down list has the following values:

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

Default: Inherit from Environment.

Target is Read-Only

Indicates the target is read-only and cannot be changed.

Run as Caller User

Indicates the operator runs as if it were the calling entity.

'Run as Caller User' is Read-Only

Indicates the operator runs as if it were the calling entity, but as read-only so that it cannot be changed.

Group

Specifies a group name for your custom operator. This setting is used as the title of the group or folder in the Operators palette. You can use the same group name for related custom operators so that they all appear under the same folder in the Operators palette. The Custom Operator Group configuration defines common parameters and values for custom operators in the group.

Display Name

Indicates the name that is shown in the Operators palette with the icon for your custom operator. The name should be short and based on the function of your operator. Display Name is also used to provide the initial value for the Name field on the Information page of the Operator Properties. You can use any combination of letters, digits, spaces, and underscore characters.

Custom Operator Pre-execution

Specifies any code that must be performed before the custom operator runs.

Custom Operator Post-execution

Specifies any code that must be performed after the custom operator runs.

Object Properties: Tags Tab

The Tags tab contains the following field:

Tags

Identifies a comma-separated value list with no spaces, for example:

```
value1,value2,value3
```

Object Properties: Versions Tab

The Versions tab contains the following fields:

Version

Specifies the versions of the selected automation object.

Release Version

Identifies the specific version of an object that was imported, or that you want to export, then import, to a production environment. You can set this identifier on any individual object.

The product locks this field in the following circumstances:

- The object was imported as part of a content package.
- The object was imported from a package (in release 4.1.00) with its release version in nonmodifiable mode.

Current

Specifies whether this version is the current version.

- Enabled indicates that this version is not designated as the current version.
- Disabled indicates that this version is designated as the current version. This version is used when the process runs and is launched by default when the object is opened from the Library.

Baseline

Specifies whether this object was saved as a baseline. A baseline object can be used but cannot be edited. For example, you can save a package as a baseline before you export it.

- Enabled indicates that this object was not saved as a baseline.
- Disabled indicates that this object was saved as a baseline.

Last Modified On

Specifies when the object was last modified.

Modified By

Specifies the User ID of the last user who modified this object.

Created On

Specifies when the object was created.

Created By

Specifies the user ID of the user who created this object.

Chapter 2: Designer Tab

This section provides field descriptions for the Designer tab and for the dialog boxes that you can access from the Designer tab. The topics are sequenced alphabetically, by page name.

Note: For information about operators, see the *Content Designer Reference*.

Process Designer

When you open a process from the Library Browser, the Designer tab appears. Each open process appears in its own tab.

View Menu

Hides the Operators, Dataset, Properties, and Navigation palettes. You can dock the properties and datasets palettes to the right or bottom.

Operators Palette

Drag and drop operators from this palette to your process layout. You can enter search criteria (for example, "Get") to filter out nonmatching operators.

Dataset Palette

Use this palette to view, edit, and add variables in process or operator datasets.

Properties Palette

Use this palette and its additional buttons and windows to manage the properties of the currently selected operator.

Navigation Palette

Use this palette to navigate to specific regions inside large processes with multiple lanes. As a convenience, you can pan in any direction within this palette instead of scrolling the main designer layout up or down.

Process Designer

The actual process design appears in this work area, canvas, or layout. The Process Designer includes the background grid and one or more lanes.

Handler Editors

In addition to the Main Editor, the designer also includes two other tabs along the bottom for editing exception and lane change handlers.

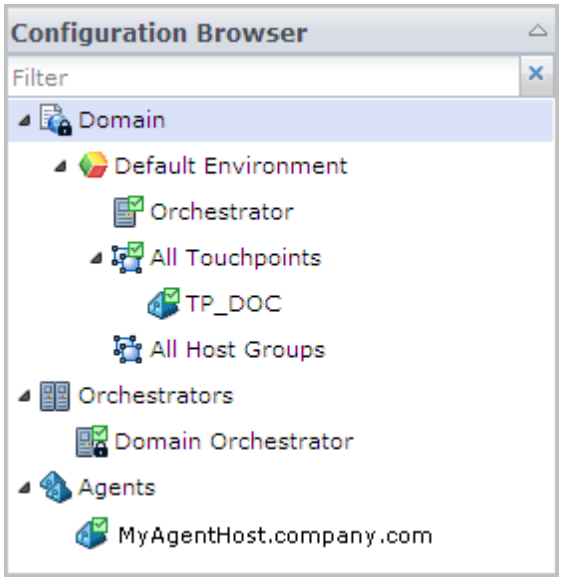
See the *Content Designer Guide* for more information.

Chapter 3: Configuration Tab

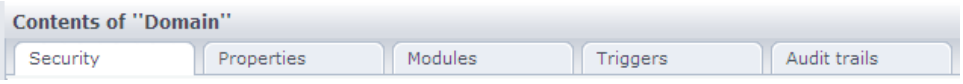
This section provides field descriptions for the Configuration tab and for the tabs that you can access from the Configuration tab. The topics are sequenced alphabetically, by tab name.

Mapping for Configuration Browser Tabs

The tabs the Configuration Browser displays depend on the node you select in the Domain hierarchy, an Orchestrator host, or an agent host. This chapter defines the fields on the various tabs.

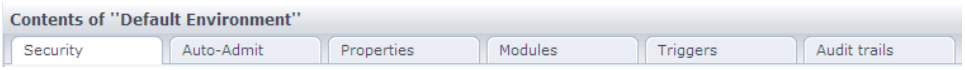


Domain Hierarchy: Domain



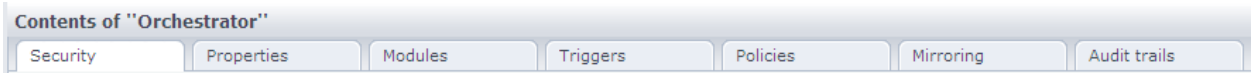
- Security (see page 96)
- Properties: Domain (see page 80)
- Modules (see page 42)
- Triggers (see page 99)
- Audit trails (see page 39)

Domain Hierarchy: Environment



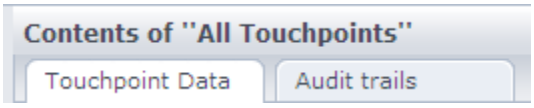
- Security (see page 96)
- Auto-Admit (see page 40)
- Properties: Environment (see page 86)
- Modules (see page 42)
- Triggers (see page 99)
- Audit trails (see page 39)

Domain Hierarchy: Orchestrator Touchpoint



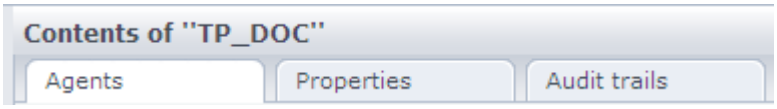
- Security (see page 96)
- Properties: Orchestrator Touchpoint (see page 93)
- Modules (see page 42)
- Triggers (see page 99)
- Policies (see page 74)
- Mirroring (see page 41)
- Audit trails (see page 39)

Domain Hierarchy: All Touchpoints



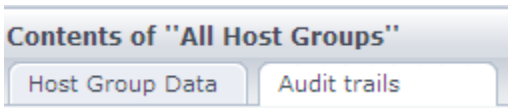
- Touchpoint Data (see page 98)
- Audit trails (see page 39)

Domain Hierarchy: Agent Touchpoint



- Agents (see page 38)
- Properties: Agent Touchpoint (see page 78)
- Audit trails (see page 39)

Domain Hierarchy: All Host Groups

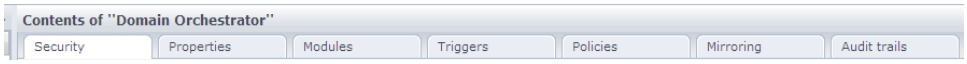


- Host Group Data (see page 41)
- Audit trails (see page 39)

Domain Hierarchy: Agent Hosting Host Group

- Agents (see page 38)
- Properties: Host Group (see page 88)
- Audit trails (see page 39)

Orchestrators: Orchestrator Host



- Security (see page 96)
- Properties: Orchestrator Host (see page 91)
- Modules (see page 42)
- Triggers (see page 99)
- Policies (see page 74)
- Mirroring (see page 41)
- Audit trails (see page 39)

Agents: Agent Host

- Properties: Agent Host (see page 77)
- Modules (see page 42)
- Associated Touchpoints (see page 40)
- Audit trails (see page 39)

Add Agent Touchpoint

The Add Agent Touchpoint dialog opens when you initiate a touchpoint creation by selecting an agent from the Agents Palette. After you create a touchpoint with one agent, you can associate other agents with this same touchpoint.

Touchpoint Name

Adds a name that operators can target to run the operator on one agent that is associated with the touchpoint. the agent selection is based on the configured agent priority and availability.

Agents

The Agents tab displays the following read-only properties when you select an agent touchpoint on the Domain hierarchy:

Name

Identifies each agent that is associated with the selected touchpoint.

Status

Displays whether the agent touchpoint is active or inactive. Operators can run on an agent only when the agent is active.

Priority

Indicates the priority that is set for the corresponding agent host.

- If the touchpoint is associated with only one agent host, the priority is **1**.
- If the agent is associated with two hosts and one host is selected as preferred, the preferred agent is priority **1.** The other agent is priority **2**.
- If multiple agent hosts have the same priority, the product uses load balancing for the selection.

Agent Host

Identifies the FQDN of each agent host that is associated with the selected touchpoint.

Audit Trail

The audit trails on the Configuration tab display audited actions for the selected node in the Domain hierarchy. Audit trails are sorted by user ID and time and are available for the following nodes:

- Domain
- environment
- Orchestrator
- agent
- touchpoint, touchpoint group, and host group

The following descriptions are for read-only columns:

Object Name

Displays the name of the selected node (for example, Domain, environment, Orchestrator, or agent).

Last Updated

Displays the date and time at which the node was last updated.

Username

Displays the user ID of the user that started the action.

Action Type

Displays the type of action (for example, Added, Changed, Deleted, Moved, Enabled, Locked, or Renamed).

Description

Displays a description of the action, including the new values of changed properties.

Auto-Admit

To automate the creation of touchpoints, configure auto-admit patterns. An *auto-admit pattern* is either a host name pattern or an IP address subnet. An auto-admit pattern enables the bulk assignment of touchpoints to agent hosts. The bulk assignment applies to hosts that have host names or IP addresses that match specified patterns. The product associates the touchpoints with the selected environment. The name of each automatically generated touchpoint is the same as the display name of the associated agent.

IP Address Patterns

Defines one or more IPv4 subnets that include hosts where agents reside. The auto-admit process creates a touchpoint for each agent host with an IP address in a specified subnet.

Example:

The CIDR pattern 155.32.45.0/24 matches IP addresses in the range 155.32.45.0 through 155.32.45.255.

Host Name Patterns

Defines one or more regular expressions for patterns that name hosts on which agents are installed. The auto-admit process creates a touchpoint for each agent host that has a host name that matches the regular expression.

Example:

The host name pattern ca\.com$ adds a touchpoint to all agents and Orchestrators that have host names that end with ca.com.

Associated Touchpoints or Host Groups

The Associated Touchpoints or Host Groups tab shows the following associations to the selected agent host:

- Agent and specific touchpoints.
- Agent and specific proxy touchpoints.
- Agent and specific host groups.
- Agent and touchpoint groups.

Name

Identifies a touchpoint, proxy touchpoint, host group, or touchpoint group that is associated with the selected agent host.

Associated Touchpoints and Host Groups

Identifies the path to each touchpoint, proxy touchpoint, and host group that is associated with the selected agent in the Domain hierarchy.

Host Group Data

The Host Group Data tab displays the following properties when you select the All Host Groups node of the Domain hierarchy:

Name

Identifies each host group in an environment of the Domain hierarchy.

Status

Indicates the status of each host group, either Enabled or Disabled.

Display Name of Agent/Orchestrator

Identifies the display name of the agent host where the named host group resides.

Mirroring: Orchestrator

Orchestrators mirror data and configuration information that is stored on the Domain Orchestrator. The mirroring setting defines how often an Orchestrator queries the Domain Orchestrator for changes. When the Orchestrator detects changes to the Domain Orchestrator, the mirroring process copies the relevant changes to the selected Orchestrator at the next mirroring interval.

Mirroring Interval (Minutes)

Defines the frequency (in minutes) with which the selected Orchestrator queries the Domain Orchestrator for changes.

Note: You can update this property only for nondomain Orchestrators that are listed under the Orchestrators node. This property is read-only for Orchestrator touchpoints.

Default: 60

Note: See Properties: Agent Host (see page 77) for information about the Mirroring Interval (Minutes) setting for agents.

Modules

The fields on the Modules tab depend on the node you select in the Configuration Browser.

- The Modules tab displays the following fields when you select the Domain node:
  - Name
  - Access Control ID
  - Description
- The Modules tab displays the following fields when you select the environment, Orchestrator touchpoints, or Orchestrator hosts node:
  - Name
  - Access Control ID
  - Enable/Disable

Note: For information about configuring default properties for operator categories, see the *Content Administrator Guide*.

Name

Identifies the CA Process Automation operator categories (modules).

Access Control ID

Defines a value for each operator category. Use this value rather than the operator category name when you add resources to a Touchpoint Security policy in CA EEM.

Note: For information about using access control IDs in Touchpoint Security policies, see the *Content Administrator Guide*.

Description

Displays a brief description of the corresponding operator category.

Enable/Disable

Defines the status of each operator category at the selected node. This field is read-only for Orchestrator touchpoints.

Values: This field can have one of the following values:

- **Enabled** - At the environment level, this setting enables the right-click Edit option that lets you override inherited values for this operator category.
- **Disabled** - This setting Indicates that this operator category is not ready for use.
- **Inherit from Domain** (environment nodes) - This setting indicates that the environment inherits the values that are set at the Domain level.
- **Inherit from Environment** (Orchestrators nodes) - This setting indicates that the Orchestrator inherits the values that are set on the parent environment.

Default: Disabled

Catalyst

The Catalyst operator category configuration sets default property values for Catalyst operators.

Note: See the *Content Administrator Guide* for information about configuring default Catalyst property settings. See the *Content Designer Reference* for operator-level information about Catalyst.

Default Catalyst Properties

Sets default values for Catalyst properties.

UCF Broker URL

Defines the default UCF broker URL. The associated operator inherits this setting.

The following example shows a URL for basic communications:

`http://hostname:7000/ucf/BrokerService`

The following example shows a URL for secure communications:

`Secure: https://hostname:7443/ucf/BrokerService`

In both examples, *hostname* represents the host on which the UCF broker resides.

Product property configuration file name

Defines the name of the UCF Product property configuration file, which customizes the properties in the generic Create operator.

Default Catalyst Security

Defines default values for the Catalyst security credentials.

Default Username

Defines the default Catalyst user ID.

Default Password

Defines the password that the product associates with the specified default user name.

The product encrypts the password value.

Default Catalyst Claims

Defines default Catalyst named claims.

Claim Name

Defines the names of one or more claims.

Claim Value

Defines the value for a named claim.

Default Catalyst Password Claims

Defines default Catalyst password claims.

Claim Name

Defines the names of one or more claims.

Claim Value

Defines the value for a named claim.

Command Execution

The Command Execution operator category configuration sets default property values for Command Execution operators.

Note: See the *Content Designer Reference* for operator-level information.

Default Telnet Properties

Sets default values for the Telnet properties.

Pseudo Terminal Type

Defines the default pseudo terminal type for a Telnet connection.

Values: This property can have one of the following values:

- VT100 - Used for hosts with a Linux operating system.
- VT400 - Used for hosts with a Windows operating system.

Default: VT100

Port

Defines the default port with which to connect to the remote host.

Note: Port 23 is the system TCP/UDP port for Telnet.

Default: 23

Connection Timeout (sec)

Defines the interval (in seconds) that the connection waits to time out.

Values: You can set this value to any positive integer.

Login Scheme

Specifies the default login scheme.

Values: This property can have one of the following values:

- User name and password
- Password only
- Log in without user name and password

User Login Text Prompt

Defines the default value for the text prompt that accepts a user name.

User name

Defines the user name with which to log in to the remote host.

Password Text Prompt

Defines the default value for the text prompt that indicates that the remote host requires a password for the specified user name.

Password

Defines the default password the product associates with the specified user name.

User Command Prompt

Defines the command prompt that indicates that the remote host is ready for commands.

The following command prompts are typical:

- >
- ?
- #

The following entry matches any input (including new lines) followed by a $ (dollar sign), > (greater than), ? (question mark), : (colon), or # (hash).

.*[$>?:#]

Note: Enclose $ in square brackets (that is, [$]) within a regular expression. A dollar sign without brackets has a specific meaning in regular expressions.

Time to Wait for Prompts (sec)

Defines the interval (in seconds) that the product waits for a command prompt before timing out.

Run Commands as Another User?

Specifies whether to run the script or the specified commands as a different user.

Values: This property can have one of the following values:

- **Selected** - Switch the user after login.
- **Cleared** - Do not switch the user after login.

Default: Cleared

Switch User Command

Defines the operating system-specific command that switches the user on the remote host. The command "su -root" switches users to the root user.

Examples:

`su - username`

`sudo su - username`

Switch User Password Text Prompt

(Optional) If the remote host requires a password to switch users, this property defines a regular expression for the default text prompt.

The text prompt is typically "Password: " or "password: ". Replace "P" or "p" with ".*" in the regular expression to match any input (including new lines) and the uppercase or lowercase "p" in “password: “.

Switch User Password

(Optional) If the remote host requires a password to switch users, this property defines the default password to enter at the password text prompt.

Switch User Command Prompt

Defines the command prompt that indicates that the remote host is ready for commands from the switched user.

The following command prompts are typical:

- $
- >
- #

The following entry matches any input (including new lines) followed by a $ (dollar sign), > (greater than), ? (question mark), : (colon), or # (hash).

`.*[$>?:#]`

Note: Enclose $ square brackets (that is, [$]) when you use a regular expression. A dollar sign without brackets has a specific meaning in regular expressions.

Default SSH Properties

Sets default values for Secure Shell (SSH) properties.

Pseudo Terminal Type

Defines the default pseudo terminal type for requests for an SSH connection.

Values: This property can have one of the following values:

- VT100 - Used for hosts with a Linux operating system.
- VT400 - Used for hosts with a Windows operating system.

Default: VT100

Port

Defines the default port with which to connect to the remote host.

Note: Port 22 is the system port for the SSH protocol.

Default: 22

User name

Defines the user name with which to log in to the remote host.

Use Default Private Key for Login?

Specifies whether to log in with a private key. The alternative is to use the password information.

Values: This property can have one of the following values:

- **Selected** - Use the Private Key Inline Content or the Default Private Key Path value to log in.
- **Cleared** - Use a password to log in.

Default: Cleared

Password

Defines the default password the product associates with the specified user name.

Private Key Inline Content

Defines the content of a default private key with which to log in to the remote host.

Default Private Key Path

Defines the path to a default private key with which to log in to the remote host.

Passphrase for Key

Defines the passphrase with which to unlock the content of the default private key.

Note: The passphrase is required only if the default private key was created with a passphrase.

Run Commands as Another User?

Specifies whether to run the script or the specified commands as a different user.

Values: This property can have one of the following values:

- **Selected** - Switch the user after login.
- **Cleared** - Do not switch the user after login.

Default: Cleared

Switch User Command

Defines the operating system-specific command that switches the user on the remote host. The command "su -root" switches to the root user.

Examples:

`su - username`

`sudo su - username`

Switch User Password Text Prompt

(Optional) If the remote host requires a password to switch users, this property defines a regular expression for the default text prompt.

The text prompt is typically "Password: " or "password: ". Replace "P" or "p" with ".*" in the regular expression to match any input (including new lines) and the uppercase or lowercase "p" in “password: “.

Switch User Password

(Optional) If the remote host requires a password to switch users, this property defines the default password to enter at the password text prompt.

Switch User Command Prompt

Defines the command prompt that indicates that the remote host is ready for commands from the switched user.

The following command prompts are typical:

- #
- >
- $

The following entry matches any input (including new lines) followed by a $ (dollar sign), > (greater than), ? (question mark), : (colon), or # (hash).

.*[$>?:#]

Note: Enclose $ in square brackets (that is, [$]) when you use a regular expression. A dollar sign without brackets has a specific meaning in regular expressions.

Default Windows Command Execution Properties

Sets default values for the Windows command execution properties.

Shell

Defines the command interpreter for the profile and for shell commands.

Example: cmd.exe

Profile

Defines a shell script that the command execution operator interprets before it starts a user process for which no profile is specified. The command execution operator uses the command interpreter that the Shell program specifies to interpret the profile. The profile can contain any noninteractive command that the shell interpreter understands.

Require user credentials

Specifies the default command execution operator behavior when user credentials are required but not specified.

Values: This property can have one of the following values:

- Defaults To User Under Which Touchpoint is Run - The process operators use the user credentials under which the agent or Orchestrator process is running.
- Defaults To User Specified Below - Command execution operators use the user credentials that are configured in the User and Password fields.
- No Default - Command execution operators use the credentials that are supplied at run time for the account under which to run.

Default: Defaults To User Under Which Touchpoint is Run

User

Defines the shell account that starts any user process that lacks a user name and a password.

- Enter a user ID with only necessary permissions so users cannot define and start processes to which they otherwise have no access.
- Leave the user ID and password blank to force users to provide credentials when they start processes through the product.

Password

Defines the password the product associates with the specified user.

Note: Passwords in the Command Execution configurations are protected and cannot be modified through a program, passed to external methods, or referenced.

Confirm Password

Verifies the value that you specified in the Password property.

Load OS User Profile

Specifies whether to load the user profile that the product associates with the specified User and Password values.

Values: This property can have one of the following values:

- **Selected -** Load the user profile.
- **Cleared -** Do not load the user profile.

Default: Cleared

Default UNIX Command Execution Properties

Sets default values for the UNIX command execution properties.

Shell

Defines the command interpreter for the profile and for shell commands.

Examples:

- /bin/bash
- /bin/csh
- /bin/ksh

Profile

Defines a shell script that the command execution operator interprets before it starts a user process for which no profile is specified. The command execution operator uses the command interpreter that the Shell program specifies to interpret the profile. The profile can contain any noninteractive command that the shell interpreter understands.

Require user credentials

Specifies the default command execution operator behavior when user credentials are required but not specified.

Values: This property can have one of the following values:

- Defaults To User Under Which Touchpoint is Run - The process operators use the user credentials under which the agent or Orchestrator process is running.
- Defaults To User Specified Below - Command execution operators use the user credentials that are configured in the User and Password fields.
- No Default - Command execution operators use the credentials that are supplied at run time for the account under which to run.

Default: Defaults To User Under Which Touchpoint is Run

User

Defines the shell account that starts any user process that lacks a user name and a password.

- Enter a user ID with only necessary permissions so users cannot define and start processes to which they otherwise have no access.
- Leave the user ID and password blank to force users to provide credentials when they start processes through the product.

Password

Defines the password the product associates with the specified shell user.

Note: Passwords in the Command Execution configurations are protected and cannot be modified through a program, passed to external methods, or referenced.

Confirm Password

Verifies the value that you specified in the Password property.

Load OS User Profile

Specifies whether to load the user profile that the product associates with the specified User and Password values.

Values: This property can have one of the following values:

- **Selected -** Load the user profile.
- **Cleared -** Do not load the user profile.

Default: Cleared

Disable Password Check

Specifies whether to disable the password verification.

Values: This property can have one of the following values:

- **Selected** - The product does not verify the specified password. In this case, user credentials are not required.
- **Cleared** - The product verifies the specified password.

Default: Cleared

Databases

The Databases operator category configuration specifies default property settings for Databases operators of the following database types:

- Oracle
- MSSQL (Microsoft SQL Server)
- MySQL
- Sybase.

Note: For details about configuring default property settings, see "Configure Databases" in the *Content Administrator Guide*. For operator-level details, see the *Content Designer Reference*.

Default Oracle Properties

Specifies the database properties when an instance of an Oracle database server hosts one or more CA Process Automation databases.

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: This property can have 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: thin

Driver

Specifies the value oracle.jdbc.OracleDriver as the default driver.

Server Host

Specifies the host where the Oracle database is running.

Server Port

Specifies the default port for the Oracle database.

UserName

Specifies the default user name for the Oracle database user.

Password

Specifies the password that is associated with the specified Default UserName.

ServiceID

Specifies the Oracle Service ID.

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.

Maximum Rows

Specifies the default maximum rows to retrieve.

Values: This value can be one of the following:

10 to 512

Default: 10

Client Encryption

Specifies one of the data encryption methods that Oracle supports, where RCA_128 and RCA_256 are for domestic editions only.

Values: This property can have one of the following values:

- RC4_40
- RC4_56
- RC4_128
- RC4_256
- DES40C
- DES56C
- 3DES112
- 3DES168
- SSL
- AES128
- AES256
- AES192

Client Checksum

Specifies checksums that Oracle supports. See your Oracle documentation.

Default: MD5

Default MSSQL Server Properties

Specifies the database properties when an instance of Microsoft SQL Server hosts one or more CA Process Automation databases.

Driver

Specifies com.microsoft.sqlserver.jdbc.SQLServerDriver as the default driver for MSSQL Server.

Server Host

Specifies the host where the MSSQL Server is running.

Server Port

Specifies the default MSSQL Server port, typically 1433.

UserName

Specifies the default user name for the MSSQL Server database user.

Password

Specifies the password that is associated with the specified Default UserName.

Maximum Rows

Specifies the default maximum rows to retrieve.

Values: This property can have one of the following values:

10 to 512

Default: 10

Database Name

Specifies the MSSQL database name.

Instance Name

Specifies the MSSQL instance name.

Default MySQL Properties

Specifies the database properties when an instance of a MySQL database server hosts one or more CA Process Automation databases.

Driver

Specifies com.mysql.jdbc.Driver as the default driver for MySQL.

Server Host

Specifies the host where the MySQL database is running.

Server Port

Specifies the default MySQL database port.

UserName

Specifies the default user name for the MySQL database user.

Password

Specifies the password that is associated with the specified Default UserName.

Maximum Rows

Specifies the default maximum rows to retrieve.

Values: This property can have one of the following values:

10 to 512

Default: 10

Database Name

Specifies the MySQL database name.

Default Sybase Properties

Specifies the database properties when an instance of a Sybase database server hosts one or more CA Process Automation databases.

Server Type

Specifies the default Sybase relational database system.

Values: This property can have one of the following values:

- Adaptive Sever Anywhere (ASA)
- Adaptive Server Enterprise (ASE)

Connection Protocol

Specifies the default connection protocol.

Default: TDS

Driver

Specifies the default driver.

Default: com.sybase.jdbc2.jdbc.SybDriver

Server Host

Specifies the host where the Sybase database is running.

Server Port

Specifies the default port for the Sybase database.

UserName

Specifies the default user name for the Sybase database user.

Password

Specifies the password that is associated with the specified Default UserName.

Maximum Rows

Specifies the default maximum rows to retrieve.

Values: This property can have one of the following values:

10 to 512

Default: 10

Cache Buffer Size

Specifies the amount of memory that the driver uses to cache insensitive result set data.

Values: This property can have one of the following 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: -1

Batch Performance Workaround

Specifies the default batch performance work-around.

Values: This property can have one of the following values:

- **Selected** - The JDBC v3.0 compliant mechanism
- **Cleared -** The native batch mechanism.

Directory Services

The Directory Services operator category configuration specifies default property settings for Directory Services operators.

Note: For information about configuring default property settings for directory services, see the *Content Administrator Guide*. For operator-level details, see the *Content Designer Reference*.

Default Directory Services Configuration

Sets the default values for the Directory Services properties on an interface that supports Microsoft Active Directory and other LDAP directory services.

Batch Size

Defines the default batch size for returning the operation results so the server can optimize performance and resources.

Values: This property can have one of the following values:

- **0 -** The server specifies the batch size.
- A whole number in the range 1 through 10000.

Default: 10

Max Number of Search Results

Defines the maximum number of objects the product returns when you run one of the following Directory Services operators:

- Get Object
- Get User

Values: This value can be a whole number in the range 1 through 1000.

Default: 100

Factory Initial

Defines the fully qualified class name of the factory class that creates an initial context.

Default: com.sun.jndi.ldap.LdapCtxFactory

Factory State

Defines 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

Defines 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

Defines a colon-separated list of language tags (the tags are defined in RFC 1766). Leave this field blank to let the LDAP server determine the language preference.

Referral

Specifies how the LDAP server handles referrals.

Values: This property can have one of the following values:

- **Ignore** - The LDAP server ignores referrals.
- **Follow** - The LDAP server follows referrals.
- **Throw** - The LDAP server returns the first encountered referral and then stops the search.

Default: Ignore

Security Authentication

Defines the authentication mechanisms for the LDAP server.

Values: This property can have one of the following values:

- **Blank -** The LDAP server uses no authentication (anonymous). Verify that the LDAP server supports anonymous connections.

  Note: This setting limits the LDAP operator. CA Process Automation creates an anonymous connection with the LDAP server. User login credentials are ignored.

- **Simple** - The LDAP server uses weak authentication (a clear-text password). Select this option when you set the Security Protocol to SSL.
- **A space-separated SASL mechanism list -** The LDAP server supports any type of authentication agreed on by the LDAP client and server. Enter a space-separated Simple Authentication and Security Layer (SASL) mechanism list (RFC 2222).

Security Protocol

Specifies whether to use a secure connection.

Values: This property can have one of the following values:

- **SSL** - The connection is secure. The SSL protocol permits LDAP server connections through a secure socket.

Important! If you are connecting to Active Directory (AD), type **ssl** in lower case. AD rejects the value SSL.

- **Blank -** The connection is basic (that is, it is not secure).

Connection Timeout

Defines the connection timeout value, in seconds.

Values: This property can have one of the following values:

- **0** - No timeout.
- A whole number in the range 1 through 600.

Default: 60

LDAP Server

Defines the default LDAP server URL or IP address.

LDAP Server Port

Defines the default LDAP server port.

Values: This property can have one of the following values:

- **389** - The Lightweight Directory Access Protocol (LDAP) port.
- **636** - The port for the LDAP protocol over TLS/SSL.
- Another valid port.
- *Blank* - The LDAP server port must be specified at the operator level.

Default: *Blank*

LDAP User

Defines the name for the default LDAP user. Operators can use this default or can override it.

Password for LDAP User

Defines the password that is associated with the specified default LDAP user. Operators can use this default or can override it.

Base DN

Defines the default Base Distinguished Name (DN) at which the LDAP user is located. Operators can use this default or can override it.

User Prefix

Specifies the default user prefix. Use the value that reflects how your LDAP server stores user names. For example, uid=*user-name*,ou=people,o=mycompany or cn=*distinguished-name*,ou=people,o=mycompany

Values: This property can have one of the following values:

- **uid -** The LDAP server uses unique user identifiers.
- **cn -** The LDAP server uses a common name for all users. If duplicate names exist, selecting this value could cause issues.

Default: uid

Email

The Email operator category configuration specifies default property settings for Email operators.

Note: For more information about configuring default Email property settings, see the *Content Administrator Guide*. For operator-level details, see the *Content Designer Reference*.

Default Email Properties

Sets the default values for Email operator properties.

SMTP Server for Outgoing e-mail

Defines the default SMTP server for outgoing Java email alerts.

From Address for Outgoing e-mail

Defines the default email address that the product displays in the sender field of outgoing Java email alerts. Fully configure this account. For example:

username@*company-name*.com

Protocol for Connection

Specifies the default protocol with which the product receives emails from a remote server or from a remote web server.

Values: This property can have one of the following values:

- IMAP
- POP3
- IMAP-SSL
- POP3-SSL

Mail Server

Defines the default mail server from which the product retrieves email.

Mail Server Port

Defines the default port for inbound email.

Values: This property can have one of the following values:

- **143** - 143 is the default IMAP port for an unsecured connection.
- **110** - 110 is the default POP3 port for an unsecured connection.
- **993** - 993 is the default IMAP-SSL port for a secured connection.
- **995** - 995 is the default POP3-SSL port for a secured connection.
- Another valid port.
- *Blank* - No default port is set for a secured or an unsecured connection.

Username

Leave this property blank if the value is always defined at the operator level.

Password

Defines the password of the mail server user.

Leave this property blank if the Username value is always defined at the operator level.

File Management

Configuration of the File Management operator category (module) includes property settings for the following operating systems:

- Microsoft Windows
- UNIX or Linux

Default Windows File Management Properties

Sets the default values that the File Management operators that run in a Microsoft Windows environment use.

Require user credentials

Specifies how to determine the user name and the password that the File Management operators require.

Values: This property can have one of the following values:

- Default to User Specified Below
- Default to User Under Which Touchpoint is Run

User

Defines the default user name for authentication. This value is required only if you set Require User Credentials to Default to User Specified Below.

Password

Defines the password that the product associates with the specified default user. This value is required only if you set the User property.

Confirm Password

Verifies the value that you specified in the Password property.

Compression Utility

Defines the command that compresses a file or directory.

```
WZZIP -P -r {0} {1}
```

- {0} defines the output compressed file name.
- {1} defines the name of the source file to compress.

Uncompress Utility

Defines the command that extracts a compressed file or directory.

```
WZUNZIP -d -o -yO {0}
```

{0} defines the name of the compressed file to extract.

Default UNIX File Management Properties

Sets the default values that the File Management operators that run in a UNIX environment use.

Require user credentials

Specifies how to determine the user name and the password that the File Management operators require.

Values: This property can have one of the following values:

- No Default
- Default to User Specified Below
- Default to User Under Which Touchpoint is Run. If you select this value, run a touchpoint or server as a service.

User

Defines the default user name for authentication. This value is required only if you set Require User Credentials to Default to User Specified Below.

Shell

Defines the default operating system shell, for example: /bin/bash, /bin/csh/, or /bin/ksh.

Password

Specifies the password for the default user.

Defines the password that the product associates with the specified default user. The operator uses the password to start user processes that do not specify a password.

Confirm Password

Verifies the value that you specified in the Password property.

Disable Password Check

Specifies whether the product verifies the password when it switches users to run a process or a script on a UNIX host.

Values: This property can have one of the following values:

- **Selected** - The product does not verify the password.
- **Cleared** - The product verifies the specified password.

Compression Utility

Defines the command that compresses a file or directory.

```
gzip -qrf {0}
```

{0} defines the name of the source file to compress.

Uncompress Utility

Defines the command that extracts a compressed file or directory.

```
gunzip -qrf {0}
```

{0} defines the name of the compressed file to extract.

File Transfer

The File Transfer operator category (module) configuration sets only the default UDP port for trivial FTP (TFTP).

Default File Transfer Properties

Sets the default values for File Transfer operator properties.

Default UDP Port for Trivial FTP

Defines the default UDP port for TFTP. Operators can use this value or can override it.

Note: Port 69 is the system port for TFTP.

Values: Any valid port number.

Default: 69

Network Utilities

Default Network Utilities SNMP Properties

Sets the default values for Network Utilities operator properties.

Poll Frequency (secs)

Defines the frequency (in seconds) with which to evaluate conditions on an SNMP variable. The poll frequency determines how often a Network Utilities operator synchronously obtains the object identifier (SNMP OID) for a device.

Process Control

Default Process Control Properties

Sets the default values for Process Control operator properties.

Time to keep completed user interaction (in minutes)

Defines the maximum interval (in minutes) that a task remains displayed in the Tasks List after a user finishes the task. When a Start Request Form with an Interaction Request Form starts a process, the process creates a task on the Operations tab Tasks link. The Operations tab also displays the task Completion Date when a user finishes the task.

Note: The process that runs when the task completes remains accessible for a configurable interval.

Default: 2

Utilities

The Utilities module configuration has one tab. The Default Invoke Java Operator Properties tab sets the default property values for the Invoke Java operators.

Use Strict Java Mode?

Specifies whether to enforce typed variable declarations, method arguments, and return types in the main method of the Invoke Java operator at runtime.

Values: This property can have one of the following values:

- **Selected:** Enforces typed variable declarations, method arguments, and return types in the main method at runtime.
- **Cleared:** Does not enforce typed variable declarations, method arguments, and return types in the main method at runtime.

Default: Selected.

CA Process Automation executes the main method code of the operator in a BeanShell interpreter, which supports BeanShell scripting syntax and Java syntax. When you select this field, the BeanShell interpreter runs under the Strict Java Mode, which:

- Enforces typed variable declarations, method arguments, and return types.
- Modifies the scoping of variables to look for the variable declaration first in the parent namespace. For example, a Java method inside a Java class.

Note: Many BeanShell commands do not work in Strict Java Mode.

External Jar Paths

Defines the paths to the external jars that the product loads by default when an Invoke Java operator runs on an agent.

Important: To load the JAR files, define a separate path for each file that ends with that JAR file name. To load .class files, define the path to the appropriate directory. The .class files can be in the directory. The location depends on whether this package is a named package or an unnamed package.

Paths have the following syntax rules:

- With one of the following formats, enter the full path to the JAR file that resides on the agent host:
  - Start the path with '**/**'.
  - Start the path with '****'.
  - With the form: '**^.:.***' (caret, period, colon, period, asterisk)

    Use this form for a regular expression that starts with one character followed by a colon - : - and then the rest of the string.

    A regular expression in the form x:*string*, where *x* is a single character.
- With one of the following formats, enter the full path to a JAR file that you can download over HTTP (basic) or HTTPS (secure):
  - Start the path with 'http://'.
  - Start the path with 'https://'.

  Note: Verify that the specified path does not require an authentication and does not go through an HTTP proxy.
- Enter the relative path to a JAR file that you uploaded using the User Resources folder in the Manage User Resources palette. The product appends the JAR file path to the User Resources directory path of the agent that runs the Invoke Java operator.

  Note: The product addresses any path that does not start with / or \\, is not of the form **^.:.***, or that does not start with http or https as a relative path.

Use Default Logger?

Specifies whether to use an instance of a logger object to log data to the log file.

Values: This property can have one of the following values:

- **Selected:** Log data to the log file. The logger opens and closes the file. The logger is available in the context of the main method code of the Invoke Java operator. The logger can be used as 'logger.debug()', 'logger.info', and so on.
- **Cleared:** Do not log data to the log file.

Default: Cleared

Log File Path

Defines the path to the log file that the logger uses. This path points to a file that resides on a CA Process Automation agent host.

Log Level

Specifies the level at which to log data. Each log level prints messages for that level and all levels above it. For example, WARN prints WARN, ERROR, and FATAL messages.

Values: This property can have one of the following values:

- **0:** DEBUG
- **1:** INFO
- **2:** WARN
- **3:** ERROR
- **4:** FATAL

Default: 0: DEBUG

Append to Default Log File?

Specifies whether to append new log messages to the default log file or to overwrite old logs with the new logs.

Values: This property can have one of the following values:

- **Selected:** Append new log messages to the default log file.
- **Cleared:** Delete the contents of the existing default log file before writing the new log messages.

Default: Cleared

Default Log Data Without Logging Info?

Specifies whether the logger writes log messages with or without the following prefix:

```
Day Month Year Hours:Minutes:Secs Logo_level [UUID of the
Invoke_Java operator]:
```

Values: This property can have one of the following values:

- **Selected:** Exclude the prefix from all log messages.
- **Cleared:** Include the prefix with each log message.

Default: Cleared

Web Services

Default Web Services Properties.

Sets the default values for Web Services operator properties.

Maximum result length (bytes)

Defines the maximum size (in bytes) of the XML value that datasets can store. The SOAP operators include the Invoke SOAP Method and Invoke SOAP Method Async. Both SOAP operators store the entire response as long as it does not exceed the configured Maximum result length. If the result exceeds the configured length, the result is truncated.

Default: 1048576

URL Part for Async SOAP Servlet

Defines the servlet location for incoming HTTP calls and SOAP calls. The specified servlet location is appended to the base server URL. Accept the default unless you create custom SOAP handlers.

Default: /itpam/soap

Async SOAP Servlet Method

Defines the servlet method that handles incoming responses for asynchronous SOAP calls from the product.

Default: AsynSoapResponse

Default Web Services HTTP Properties

Sets default values for Web Services operator HTTP properties.

Validate SSL Certificate?

Specifies whether to validate the SSL certificate. This setting is relevant when querying an HTTPS URL.

Values: This property can have the following values:

- **Selected** - Make an HTTP call *only* if the SSL certificate is valid. If the SSL certificate is invalid, the HTTP call fails.
- **Cleared** - Make an HTTP call without considering the validity of the SSL certificate.

Default: Cleared

HTTP Authentication?

Specifies whether the HTTP server at the URL specified in the operator requires HTTP authentication.

Values: This property can have the following values:

- **Selected** - The HTTP server at the specified URL requires authentication.
- **Cleared** - The HTTP server at the specified URL does not require an authentication.

Default: Cleared

NTLM Authentication?

Specifies whether the HTTP server at the URL specified in the operator requires NTLM authentication.

Values: This property can have the following values:

- **Selected** - The HTTP server at the specified URL requires authentication.
- **Cleared** - The HTTP server at the specified URL does not require an authentication. In this case, the product uses basic HTTP authentication.

Default: Cleared

HTTP Preemptive Authentication

Specifies whether the CA Process Automation HTTP operator should be configured to use HTTP Preemptive Authentication (instead of HTTP Authentication), which prompts the operator to send Basic HTTP Authentication to the Web service without negotiation.

User name

Defines the user name with which to access the URL specified in the operator. This user name can be authenticated.

Password

Defines the password that the product associates with the specified user name.

Domain name

Defines the name of the domain for authenticating with the URL specified in the operator.

Values: This property can have the following values:

- *A valid domain name*

  NTLM authentication requires a domain name.

- *Blank*

  NTLM authentication does not require a domain name.

Note: For an NTLM authentication, the product uses the domain name exactly as you define it. For a non-NTLM authentication, the product appends the domain name to the user name as in the following example if the domain name is required:

```
User name=user name@domain name
```

Use Proxy?

Specifies whether the HTTP call goes through a proxy server.

Values: This property can have the following values:

- **Selected** - The HTTP call goes through a proxy server.
- **Cleared** - The HTTP call does not go through a proxy server.

Default: Cleared

Proxy Host

Specifies one of the following methods to define the default proxy host:

- Use HTTP or HTTPS to define the default URL to the proxy host.
- Use the proxy server FQDN.

  Note: If you enter the FQDN, the product uses the HTTP protocol to contact the proxy host. For more information, see Syntax for DNS Host Names.

Proxy Port

Defines the default port of the proxy server.

Values: This value can be any valid port number.

For example:

- 80 (HTTP)
- 8080 (alternate HTTP)
- 443 (HTTPS)

Proxy Authentication?

Specifies whether the proxy requires authentication.

Values: This property can have the following values:

- **Selected** - The proxy host requires authentication.
- **Cleared** - The proxy host does not require an authentication.

Default: Cleared

Proxy NTLM Authentication?

Specifies whether the proxy host at the specified proxy URL requires NTLM authentication.

Values: This property can have the following values:

- **Selected** - The proxy host requires NTLM authentication.
- **Cleared** - The proxy host does not require an NTLM authentication. In this case, the product uses basic HTTP authentication.

Default: Cleared

Proxy Preemptive Authentication

Specifies whether the CA Process Automation HTTP operator should be configured to use Proxy Preemptive Authentication (instead of Proxy Authentication), which prompts the operator to send Proxy Authentication to the Web service without negotiation.

Proxy User name

Defines the user name with which to access the proxy host. This name can by authenticated by the proxy host.

Proxy Password

Defines the password that the product associates with the specified proxy user name.

Proxy Domain name

Defines the name of the domain for authenticating with the proxy host.

Values: This property can have the following values:

- *A valid domain name*

  NTLM authentication requires a domain name.

- *Blank*

  NTLM authentication does not require a domain name.

Note: For an NTLM authentication, the product uses the domain name exactly as you define it. For a non-NTLM authentication, the product appends the domain name to the user name as in the following example if the domain name is required:

```
user name=user name@domain name
```

HTTP Version

Defines the default HTTP protocol version.

Values: This property can have one of the following values:

- 1.0
- 1.1

Default: 1.1

Connection Timeout (sec)

Defines the maximum interval (in seconds) to wait for an HTTP connection before the operator times out.

Values: Any positive integer that indicates the number of seconds, where 0 (zero) sets no timeout.

Default: 0

Socket Timeout (sec)

Defines the maximum interval (in seconds) to wait between consecutive HTTP response data packets.

Values: Any positive integer that indicates the number of seconds, where 0 (zero) sets no timeout.

Default: 0

Handle Redirects?

Specifies whether redirects are handled automatically.

Values: This property can have the following values:

- **Selected** - The product handles redirects automatically.
- **Cleared** - The product does not handle redirects automatically.

Default: Cleared

Maximum Number of Redirects

Defines the maximum number of redirects to process. If the number of redirects after a request exceeds the configured value, an error is raised.

Default: 100

Policies

The Orchestrator Policies settings specify history settings for processes that run on the Orchestrator touchpoint. They also specify the default schedule and the default process in the library. You can configure separate policies for separate Orchestrators. The Delete Archive Instances button appears only on the Orchestrator host.

Automation Object Versioning

Specifies the policy for retaining old versions when you check in an edited automation object, where options include:

- Allow User to Overwrite Existing Version on Check in
- Always Create a New Version on Check in

Default Process Handlers

Defines the complete path to 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 a 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.

If you configure one day, the process remains in the library for a minimum of 24 hours. After this time elapses, the process instances are archived.

Minimum Number of Failed Instances

Defines the minimum number of Failed instances of each object for every object type (process, schedule, and SRF) that are retained. To view the retained instances of an object, select the Current filter of the respective object from the Operations dashboard. The remaining objects are archived and to view the archived objects, select the Archived filter of the respective object from the Operations dashboard.

When the Failed instances exceed the specified value, the application archives the instances of each object for every object type, with the oldest timestamp of completion. However, the instances are archived only after they are retained for a minimum number of days as specified in the Minimum Days of Process History field.

For example:

If there are 3 objects (Process,Schedule, SRF) and assume each object has 3 object instances, then there are 9 object instances for the 3 objects. If you specify 1, then 1 object instance for each object type is retained and the remaining is archived.

Default value: 0. You can specify a positive integer value.

When 0 is specified, instances are archived but are not retained.

Minimum Number of Finished (Completed, Aborted) Instances

Defines the minimum number of Finished (completed and aborted) instances of each object for every object type (process, schedule, and SRF) that are retained. To view the retained instances of an object, select the Current filter of the respective object from the Operations dashboard.

The remaining objects are archived and to view the archived objects, select the Archived filter of the respective object from the Operations dashboard.

When the Finished (completed and aborted) instances exceed the specified value, the application archives the instances of each object for every object type, with the oldest timestamp of completion.

However, the instances are archived only after they are retained for a minimum number of days as specified in the Minimum Days of Process History field.

For example:

If there are 3 objects (Process,Schedule, SRF) and assume each object has 3 object instances, then there are 9 object instances for the 3 objects. If you specify 1, then 1 object instance for each object type is retained and the remaining is archived.

Default value: 0. You can specify a positive integer value.

When 0 is specified, instances are archived but are not retained.

Maximum Number of Log Messages

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

Minimum Number of Days of Attachments History

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

Users can use web services to trigger processes. A user can directly start a process or schedule a Start Request Form. Users can send files as attachments in the web services calls. When a web service call triggers a process, users can access the files in that process. A user can use the SOAP operator to forward an attachment to the outgoing web services call.

Option to Purge Archived Data

Defines the policy for purging archived data. Options include:

Values: The drop-down list includes the following values:

- **Do Not Purge Archived Data -** Archived process instances are retained until manually purged.
- **Purge Archived Data Daily** - Purge archived process instances as a scheduled task according to the settings of the following two fields.
- **Purge Data Without Archiving** - The process instances are retained as active for a configured interval. When that interval elapses, the data is purged. No process instances are archived.

Start Time to Purge Archived Data Daily

Defines the time of day at which to purge the archived instances that have been retained for the configured number of days. The time is specified in hh:mm format, where the range is 00.00 (12:00 AM) to 23.59 (11:59 PM).

Default: 00:01 (1 minute after midnight)

Number of Days to Keep Archived Data

Defines the number of days to retain archived process instances. After an archived instance is kept for the configured number of days, it is purged at the specified time.

Default: 10

Secure Attachments

Specifies whether to authenticate users who attempt 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 credentials.

Enable Runtime Security

Specifies whether to permit processes to use runtime security.

Values:

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

Note: If you select the Enable Runtime Security option here, you can select Run as Owner as the Runtime Security option for a process. In this case, use Set Owner to establish your ownership of each affected process object. For more information, see the online help or the *Content Designer Guide*.

Delete Archived Instance

The button lets you purge currently archived instances on demand. (This button appears on a selected Orchestrator host, not on a selected Orchestrator touchpoint.)

Properties: Agent Host

The following fields are displayed in the Properties tab when you select a host from the Agents node in the Configuration Browser.

Status

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

Agent Name

Specifies the name of the agent. By default, the agent name is the same as the host name.

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.

Host Address

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

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

Heartbeat Interval (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: The following values are valid:

- A numeric value
- Never
- Inherit from Domain.

Default: Inherit from Domain

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

Properties: Agent Touchpoint

Properties for agent touchpoints are configured when you add agents. When you create connectivity from an agent to a remote host for the purpose of targeting the remote host, you select proxy touchpoint and configure connection parameters.

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 in 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.

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.

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.

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 SSH Connections

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.

Default: 20

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.

Properties: Domain

The details that the Configuration Properties tab displays depend on the selected node. Environments inherit many properties that are set at the Domain level. The following descriptions are for fields that appear on the Properties tab when the Domain is selected.

Domain URL

Identifies the URL of the Domain Orchestrator that is set during the installation. The 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.

- The following syntax indicates secure communication:

  `https://`*`hostname_or_IPaddress`*`:8443/`

- The following syntax indicates basic communication:

  `http://`*`hostname_or_IPaddress`*`:8080/`

  hostname_or_IPaddress

If a load balancer was set up, the URL connects to the load balancer. If no load balancer was set up, the URL connects to the Domain Orchestrator.

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.

Default: Domain Orchestrator

Status

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

Heartbeat Interval (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

Agent Configuration Update Interval (minutes)

The field lets you define the frequency at which the Domain orchestrator checks and, if appropriate, sends configuration updates to agents.

Touchpoint Security

Indicates whether to enforce user rights on the targets. All user rights are configured in a custom CA EEM policy that uses the Touchpoint Security resource class. The execute rights can be granted a user or group for a given environment or touchpoint.

Note: See Approach to Configuring Touchpoint Security.

Values: The drop-down list has the following values:

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

Default: Disabled - supports backward compatibility.

Match Target in Host Groups only

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

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

Values: The drop-down list has the following values:

- **Enabled** - The scope of the search depends on whether the "Lookup DNS when matching target in Host Groups" field is enabled or disabled.
  - If a DNS lookup is disabled, searches:

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

    Host group reference to a remote host (exact or DNS lookup result)
- **Disabled** - Search the Domain components in the following order:
  a. Touchpoint (exact or a DNS lookup result)
  b. Orchestrator (exact or a DNS lookup result)
  c. Agent (exact or a DNS lookup result)
  d. Proxy touchpoint mapping to a remote host (exact or DNS lookup result)
  e. Host group reference to a remote host (exact or DNS lookup result)

Default: Disabled

Lookup DNS when matching target in Host Groups

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

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

Values: This drop-down list has the following values:

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

Default: Disabled

Option to Purge Reporting Data

Specifies whether to purge reporting data daily.

This field is applicable if either the Enable Process Reporting checkbox or the Enable Operator Reporting checkbox is selected.

Note: Exempted from purging is data related to configuration changes (add or update Orchestrators, agents, touchpoints) and data related to checking in or importing library objects.

Values:

- Do Not Purge Reporting Data
- Purge Reporting Data Daily

Start Time to Purge Reporting Data Daily

Specifies the time of day at which to delete reporting data. For example, to start the purge at 6:30 PM, specify the military time equivalent, 18:30.

This field is applicable if the Option to Purge Reporting Data is set to Purge Reporting Data Daily.

Values:

00:00 through 23:59

This range, in HH:mm format, means 12:00 AM (start of the day) through 11:59 PM (end of the day) for your local time zone.

Number of Days to Keep Reporting Data

Specifies the number of days to retain reporting data before it is purged.

For example, an entry of 14 specifies to purge all reporting data that is more than two weeks old. The age of reporting data for process instances and operator instances is calculated from when the instance started running.

This field is applicable if the Option to Purge Reporting Data is set to Purge Reporting Data Daily.

Values:

An integer in the range 1 through 3650, inclusive.

Enable Process Logs

Indicates whether to enable the Logs option in the Designer tab View menu. This setting determines whether to display or to hide logs for runtime process instances.

Values: This check box has one of the following values:

- **Selected** - Display process logs.
- **Cleared** - Do not display process logs.

Default: Selected

Enable Operator Recovery

Indicates how to handle any operator recovery when the following sequence of events occurs:

1. A touchpoint becomes inactive while the Process Execution is in progress.
2. A user activates this touchpoint.

Consider the following example: The Delay operator starts a process on TP1. The process goes into waiting state. If TP1 becomes inactive, the process stays in waiting state. While the process is in waiting state, a user activates the inactive touchpoint.

Values: This check box has one of the following values:

- **Selected** - Recover all operators in the process when the inactive touchpoint is activated.
- **Cleared** - Do not recover operators.

Default: Selected

Note: This setting has major impact on the Assign User Task operator, the Invoke SOAP Method Async operator, and the Start Process operator.

- While one or more operators run on the Orchestrator touchpoint, entries are not created in the Runtime Database C2O Recovery State table.
- While one or more operators run on an agent touchpoint, entries are not created in the following Runtime database folder:

agent_install_dir\\PAMAgent\.recovery*UUID*\.nodes*TP1*\.svcops

Enable Process Reporting

Indicates whether reporting data is generated for processes. Both predefined reports and custom reports use this data. Search for reports containing the word *process* in the Reports tab to view titles of process reports.

Values: This check box has the following settings:

- **Selected** - Generate reporting data for processes.
- **Cleared** - Do not generate reporting data for processes.

Default: Selected

Enable Operator Reporting

Indicates whether reporting data is generated for operators. This setting applies to operator-related reporting data used by custom reports and predefined reports.

Values: This check box has one of the following values:

- **Selected** - Generate reporting data for operators.
- **Cleared** - Do not generate reporting data for operators.

Default: Selected

Delete Reporting Data

Specifies the date range for the reporting data to delete. All reporting data that is generated within the date range you specify is deleted immediately, on demand. The date range of reporting data for process instances and operator instances is calculated from when the instance started running. This button opens a dialog with the following two fields that let you select dates from calendars.

- From Date
- To Date

Properties: Environment

The details on the Configuration Properties tab depend on the selected node in the Configuration Browser. The following descriptions are for fields that appear on the Properties tab when an environment is selected.

Name

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

Status

Indicates the status of the selected environment as Active or Locked by <username>.

Operators Autorecovery

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: This value can be one of the following:

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

Default: Selected

Touchpoint Security

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

Values: This value can be one of the following:

- **Inherit from Domain** - Use the value configured for this field in Domain properties.
- **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.

Default: Inherit from Domain.

Match target in Host Groups only?

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

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

Values: The drop-down list has the following values:

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

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

    Host group reference to a remote host (exact or DNS lookup result)
- **Disabled** - Search the Domain components in the following order:
  a. Touchpoint (exact or a DNS lookup result)
  b. Orchestrator (exact or a DNS lookup result)
  c. Agent (exact or a DNS lookup result)
  d. Proxy touchpoint mapping to a remote host (exact or DNS lookup result)
  e. Host group reference to a remote host (exact or DNS lookup result)

Default: Inherit from Domain

Lookup DNS when matching target in Host Groups?

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

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

Values: This drop-down list has the following values:

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

Default: Inherit from Domain.

Properties: Host Group

Properties for a selected Host Groups are defined with the following fields.

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 in 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:

- **Inherit from Environmen**t - same setting as for Environment.
- **True** - Automates recovery.
- **False** - Prevents automated recovery.

Default: Inherit from Environment

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:

- **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.

Default: Inherit from Environment

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*.

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 SSH Connections

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.

Properties: Orchestrator Host

The following fields appear on the Properties tab for the selected Orchestrator host. The following fields are read-only: Is Domain, Host Name, Orchestrator Name, and Status.

Note: For information about configuration, see the "Configure Orchestrator Host Properties" in the *Content Administrator Guide*.

Is Domain

Specifies whether the selected Orchestrator host is the Domain Orchestrator, where selected indicates True.

Host Name

Specifies the name of the host computer on which the selected Orchestrator is installed.

Orchestrator Name

Specifies the name of the physical Orchestrator host.

Status

Specifies the status of the selected Orchestrator host. Statuses include Active, Inactive, Active/Locked (and the name of the user who locked it), and Quarantine.

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: This value can be one of the following:

- **Inherit from Environment** - same setting as for Environment.
- **True** - Automates recovery.
- **False** - Prevents automated recovery.

Default: Inherit from Environment

Match target in Host Groups only?

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

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

Values: The drop-down list has the following values:

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

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

    Host group reference to a remote host (exact or DNS lookup result)
- **Disabled** - Search the Domain components in the following order:
  a. Touchpoint (exact or a DNS lookup result)
  b. Orchestrator (exact or a DNS lookup result)
  c. Agent (exact or a DNS lookup result)
  d. Proxy touchpoint mapping to a remote host (exact or DNS lookup result)
  e. Host group reference to a remote host (exact or DNS lookup result)

Default: Inherit from Environment

Lookup DNS when matching target in Host Groups?

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

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

Values: This drop-down list has the following values:

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

Default: Inherit from Environment.

Properties: Orchestrator Touchpoint

The following fields appear on the Properties tab for the selected Orchestrator touchpoint. All fields are read-only. The read-only fields reflect the values for the associated Orchestrator.

Is Domain

Specifies whether the selected Orchestrator touchpoint is associated with the Domain Orchestrator. Default value is Domain name.

Host Name

Specifies the name of the host computer on which the associated Orchestrator is installed.

Orchestrator Name

Specifies the name of the corresponding physical Orchestrator host, which is displayed under the Orchestrators node.

Display Name

Specifies the name displayed in the Configuration Browser for the selected Orchestrator touchpoint. The name can be the default name or the value specified by selecting Rename for the selected Orchestrator touchpoint.

For example, you name the original Orchestrator in the Domain hierarchy to Domain Orchestrator Touchpoint to differentiate it from the Domain Orchestrator (physical) displayed under the Orchestrators node.

Status

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

Operators Autorecovery

Specifies the setting configured for the associated Orchestrator.

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: This value can be one of the following:

- **Inherit from Environment**
- **True** - Enforce Touchpoint Security policies for this target and allow access only if the user has been granted this permission.
- **False** - Do not verify whether the user running the process has execute rights on the current target.

Default: Inherit from Environment

Match target in Host Groups only?

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

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

Values: The drop-down list has the following values:

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

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

    Host group reference to a remote host (exact or DNS lookup result)
- **Disabled** - Search the Domain components in the following order:
  a. Touchpoint (exact or a DNS lookup result)
  b. Orchestrator (exact or a DNS lookup result)
  c. Agent (exact or a DNS lookup result)
  d. Proxy touchpoint mapping to a remote host (exact or DNS lookup result)
  e. Host group reference to a remote host (exact or DNS lookup result)

Default: Inherit from Environment

Lookup DNS when matching target in Host Groups?

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

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

Values: This drop-down list has the following values:

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

Default: Inherit from Environment.

Security

The following fields appear on the Security tab for the selected node in the Domain hierarchy or for the selected node under Orchestrators.

Note: For the configuration procedure, see the *Content Administrator Guide*.

Inherit (Not applicable to the Domain level)

Specifies whether the selected node on the hierarchy inherits the values that are configured at the parent level for that node.

Values: The setting can be one of the following values:

Selected - Inherit the values

Cleared - Do not inherit the values.

Default: Selected

Note: Typically, the only value you configure at the environment level is the CA EEM Cache Update Interval. The other values are CA EEM related and are set at the installation of the Domain Orchestrator. One CA EEM serves the entire Domain.

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

CA EEM Cache Update Interval (in seconds)

Specifies the interval in seconds between the CA EEM updates to its internal cache. The cache contains current settings of CA Process Automation user accounts, groups, and policies. When CA EEM updates its cache, CA EEM sends CA Process Automation the contents of the refreshed cache.

Note: Reducing the update interval when you are testing and refining custom policies makes this task go more quickly, but at the sacrifice of performance.

Default: 1800 seconds

Minimum value: 60 seconds

CA Process Automation cache of user permissions: The CA Process Automation security function gets user permissions from a secondary cache. Permissions in this cache are valid for 30 seconds. If the cache age is greater than 30 seconds, the security function requests user permissions from CA EEM. The security function then updates the secondary cache with the query results and resets the cache age. This maximum cache age is handled internally, but can be altered by adding the eem.cache.timeout parameter to the OasisConfig.properties file and setting a new value.

Default: Domain Name

Touchpoint Data

The following descriptions are for read-only fields on the Touchpoint Data tab for the All Touchpoints node in the Domain hierarchy.

Name

Identifies the name of each touchpoint under a given environment in the Domain hierarchy..

Status

Indicates the status of each touchpoint, whether Enabled or Disabled.

Display Name of Agent/Orchestrator

Specifies the name of the agent host associated with the named touchpoint.

Triggers

One or more of the following fields appear on the Triggers tab for the selected node.

- Name and Description appear for Domain.
- Name and Enable/Disable appear for environment, Orchestrator touchpoints, and Orchestrators. The Enable/Disable setting can be made active by locking the selected environment or Orchestrator host node.

Note: For information about configuring triggers, see "How to Configure and Use Triggers" in the *Content Administrator Guide*.

Name

Lists the names of the four CA Process Automation triggers, with right-click options to Edit or View the selected trigger.

- Catalyst Trigger - See Catalyst Trigger Fields (see page 100).
- File Trigger - See File Trigger Fields (see page 103).
- Mail Trigger - See Mail Trigger Fields (see page 105).
- SNMP Trigger - See SNMP Trigger Fields (see page 107).

Description

Displays a short description of the corresponding trigger.

Enable/Disable

Specifies the status of each trigger at the selected node. This field is read-only for Orchestrator touchpoints.

Values: This value can be one of the following:

- **Enabled** - At the environment level, enables the right-click Edit option that allows you to override inherited values for this trigger.
- **Disabled** - Indicates that this trigger is not ready for use.
- **Inherit from Domain** (environment nodes) - Inherits values set at the Domain level.
- **Inherit from Environment** (Orchestrator hosts) - Inherits values set at the parent environment.

Default: Disabled

Catalyst Trigger

General Properties displays an Add parameter icon, which opens the Catalyst Subscriptions dialog. A Catalyst trigger supports the specification of default values for properties that enable processes to be triggered upon the receipt of a Catalyst event. The following descriptions are for fields on each of the Catalyst Subscription tabs.

Subscription

Each subscription references a Catalyst Connector with a filter.

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.

MDR

Specifies settings for the connecting product.

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.

Filter

Specifies the events to process.

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.

Catalyst Security

Specifies authorization information.

Username

Specifies the default user name.

Password

Specifies the password associated with the default user name.

Claims: Claim Name

Specifies the username for UCF Subscription.

Claims: Claim Value

Specifies the password associated with the Username.

Password Claims: Claim Name

Specifies the username for UCF Subscription.

Password Claims: Claim Value

Specifies the password associated with the Username.

File Trigger

File triggers support the start of operators or processes that access highly volatile data and designed to be rerun frequently, for example, every 60 seconds. The following descriptions are for fields on the General Properties tab for File Trigger.

General Properties

File trigger properties tell the Orchestrator where and how often to look for new files with names that match the configured pattern. When found, CA Process Automation parses the content and triggers the process specified in the content.

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>/standalone 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>/standalone 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>/standalone 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

Interval (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".

```
.*.prg
```

Mail Trigger

The configuration of the mail trigger supports automatic replies to incoming emails that meet configured criteria. The following descriptions are for fields on the General Properties tab of the Mail Trigger dialog.

General Properties

Specifies default properties for Mail triggers.

Default Trigger Process (Orchestrator only)

Specifies how to handle emails that have invalid XML content in the message body or attachment.

Values:

- Blank - Ignore emails with no valid XML trigger content.
- The full path of the process that the Domain Orchestrator is to start. (One default process can be defined for each Orchestrator.)

IMAP Mail Server

Specifies the hostname or IP address of the mail server that receives incoming emails. The Inbox folder for the configured email account is searched for new emails. This server must have the IMAP protocol enabled. The Mail Trigger does not support POP3.

IMAP Server Port

If the default TCP port for an IMAP server is used, enter 143. If a nondefault port is used or secure communication is set up on a different port, obtain the correct port to enter from an administrator.

User Name

Specifies the user name 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.

Mail Processing Interval (seconds)

Frequency is seconds with which CA Process Automation searches the IMAP server for new incoming emails into the specified account. The user name and password specify the account.

Default:

2

Save mail attachments to database

Specifies whether to save attachments of mails that trigger CA Process Automation processes in the database.

- Selected: CA Process Automation saves attachments of mails to the CA Process Automation database and populates the data set of the process being started with relevant information of the attachments.
- Cleared: CA Process Automation does not save email attachments.

Outgoing SMTP Mail Server

Specifies the server name for the outgoing SMTP mail server. When a triggering email with valid XML content is received in the configured account of the IMAP mail server, an acknowledgment email is returned. The acknowledgment email is returned to the sender through the outgoing SMTP server.

SMTP Server Port

Specifies the port of the outgoing mail server.

Default:

25

Use secure SMTP connection

Specifies whether to process over a secure connection to the SMTP mail server.

- Selected - Enables a secure connection to the SMTP mail server.
- Cleared - The mail server does not allow a secure connection.

Default:

Cleared

SNMP Trigger

The SNMP trigger configuration specifies the process to run upon the receipt of an SNMP trap meeting the specified filter criteria. The following descriptions are for fields to configure on the General Properties tab of the SNMP Trigger dialog.

General Properties

Specifies SNMP trigger properties that enable processes to be triggered upon the receipt of an SNMP trap.

Description

Describes the SNMP trap filter.

Source IP address

Specifies the IPv4 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.

Values:

- Regular expression matching the SNMP trap OID.
- Blank - Accepts SNMP traps with any OID.
- .* (dot asterisk) - Accepts SNMP traps with any OID, 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. For example, testpayload.

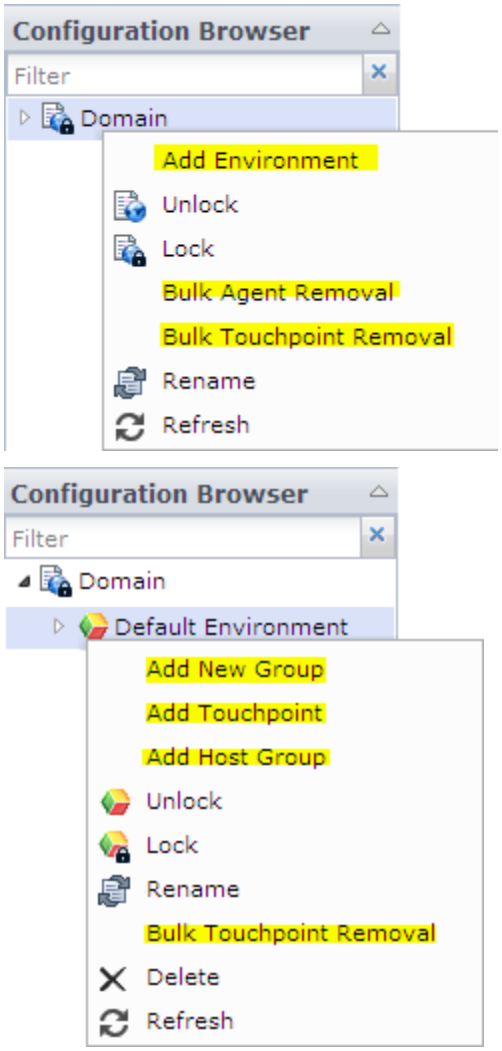
Process Path

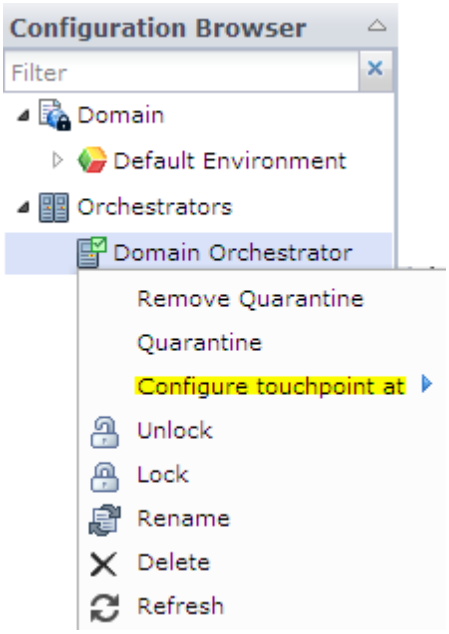
Specifies the full path of the Process to run when receiving an SNMP trap that matches the filter criteria. The checked-in version of the Process Path is used during execution.

Note: Click search to load the Object Browser, from which you can select the process path.

Mapping for Configuration Browser Dialogs

This chapter defines fields displaye when you right-click a node in the Configuration Browser and select an action.





Add Host Group

The Add Host Group menu option is available from the right-click menu when you lock an environment. The Add Host Group option opens the Add Host Group: *environment* dialog. A host group allows an operator target to be expressed as a host name or IP address that is included in the Host Group pattern.

The Add Host Group: *environment* dialog contains one field and a Filter drop-down list. The field description follows:

Host Group Name

Defines the name for a host group.

Add New Environment

The Domain must be locked to add an environment to the Domain.

Enter an environment name

Defines the name of the environment to add. For example, Production Environment.

Add New Group

The Add New Group menu option is available from the right-click menu when you lock an environment. The Add New Group option opens the Add Touchpoint Group dialog. An operator can target a touchpoint group. The operator runs simultaneously on each agent that is associated with each touchpoint in the touchpoint group.

Touchpoint group name

Defines the name of a new group to which you can add individual touchpoints.

Add Touchpoint

The Add Touchpoint menu option is available from the right-click menu when you lock an environment. The Add Touchpoint option opens the Add Touchpoint: *environment* dialog. This dialog lets you associate the touchpoint with one or more agents or with an Orchestrator. When an operator targets a touchpoint, the operator typically runs on an agent (based on its priority or load balancing) associated with the touchpoint. If the touchpoint is associated with an Orchestrator, the operator runs on that Orchestrator.

The Add Touchpoint: *environment* dialog contains one field, a drop-down list from which you can select Agent, Orchestrator, or All, and a Filter drop-down list. The field description follows:

Touchpoint Name

Defines the name for the touchpoint.

Bulk Agent Removal

The Bulk Agent Removal dialog appears when you lock the Domain, right-click the Domain and select Bulk Agent Removal. Administrators specify search criteria that includes the agents that are candidates for removal. From the search results, administrators indicate the agents to remove and then click the Delete button.

Note: Removing the agent reference does not uninstall the agent from the host. You can delete the agents that are active or inactive from the domain.

Search Request

Contains controls for defining the search request. Select one of the radio buttons and optionally enter a search expression.

Search by IP address pattern (radio button)

Indicates that the specified Search expression is an IP address pattern. For example, 10.131.91.0/24.

Search by host name pattern (radio button)

Indicates that the specified Search expression is a host name pattern.

Search Expression

Defines an expression that includes all agents that you want to remove. Leave the field blank to return all agents

Agent Results

Lists all agents that match the search criteria.

Select the agents to delete.

Lists the search results by Agent Name, Agent Host Name, IP Address and Status, where each row is preceded by a check box.

Selected - Remove this agent reference from the CA Process Automation Domain.

Cleared - Do not include this agent in the bulk agent removal.

Bulk Touchpoint Removal

You can remove touchpoints in bulk at either the Domain level or for a specific environment.

An administrator uses the Bulk Touchpoint Removal dialog to search for touchpoints that are not mapped to agents and then delete them all at once.

Search Request

The Search Request area includes a field and a Search button.

Search Expression

Defines a pattern that includes the touchpoint names that are candidates for removal.

Empty Touchpoint

Lists all touchpoints that are not mapped to agents but that match the search criteria.

Select the touchpoints to delete.

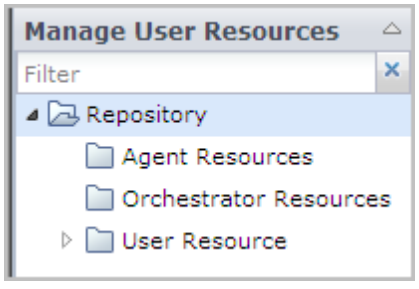
Lists the search results by Name, Status, and (conditionally) Environment where a check box precedes each row.

Selected - Remove this touchpoint reference from the selected environment or from the Domain, depending on where the bulk touchpoint removal was invoked.

Cleared - Do not include this touchpoint in the bulk touchpoint removal.

Mapping for Manage User Resources Pages

The Manage User Resources palette on the Configuration tab contains three folders. Users can upload resources to each of these folders. Users select a folder and click New to display the page with fields.



Following is the folder to topic mapping for the Manage User Resources repository:

- Agent Resources (see page 113)
- Orchestrator Resources (see page 113)
- User Resources (see page 114)

Agent Resources

Agent Resources is a folder on the Domain Orchestrator. You can upload a resource such as a jar file to the Agent Resources folder. Restarted agents can use the uploaded agent resources.

The Add New Resource: "Untitled" page contains the following fields:

Resource Name

Specifies the name of the resource.

Example Values: Oracle Driver, MySQL Driver, or Sybase Driver.

Resource File

Specifies the file with its current path.

Module Name

(Optional) Specifies a user-defined module name.

Resource Description

(Optional) Specifies a meaningful description.

Orchestrator Resources

Orchestrator Resources is a folder on the Domain Orchestrator. You can upload a JAR file to the Orchestrator Resources folder. Restarted Orchestrators can use the uploaded Orchestrator resources.

The Add New Resource: "Untitled" page for Orchestrator Resources contains the following fields:

Resource Name

Specifies the name of the resource.

Example Values: Oracle Driver, MySQL Driver, or Sybase Driver.

Resource File

Specifies the file with its current path.

Module Name

(Optional) Specifies a user-defined module name.

Resource Description

(Optional) Specifies a meaningful description.

User Resource

You can add scripts to the User Resources folder in the global Repository. Orchestrators and agents can invoke user resources by reference.

The following fields appear on the Add New Resource: "Untitled" page for User Resource:

Resource Name

Specifies how the resource is labeled, where the label can be a file name such as buildscript.js

Resource Subfolders Path

Specifies the path to the resource from the current folder, for example, /Windows Scripts.

Resource File

Specifies the file with its path.

Module Name

Specifies the name of the module.

Resource Description

Specifies a description that is visible to users.

Chapter 4: Operations Tab

This section provides field descriptions for the Operations tab and for the dialog boxes that you can access from the Operations tab. The topics are sequenced alphabetically, by page name.

Datasets Palette

The Dataset palette lets you view, edit, and add variables in process or operator datasets. See the *Production User Guide* for instructions.

Each dataset has an expandable list of defined parameters in the right-hand pane that displays the parameters name and value.

Value

When you double-click the Value field of a parameter, you can edit and save the parameter.

View Expression

When you right-click a dataset row, you can select View Expression to get an expression for that variable to use in process definitions.

Add Indexed value

When you right-click a parameter and select Add Indexed value, a new indexed field value is added to the array.

Delete Indexed value

When you right-click a parameter, you can select Delete Indexed Value and confirm the deletion.

Process Watch

The Process Watch palette lets you define and monitor the selected automation objects in CA Process Automation.

Start

When you right-click the a process in the Process Watch palette and select Start Process, the process instance that you started appears in the right pane.

Start Suspended

You can start an instance of a process in a suspended state to achieve any of the following objectives:

- Insert breakpoints.
- Set parameters.
- Make other changes before the process runs.
- Monitor or control the execution of a process.
- Debug the sequence of steps in the process.

Resources Palette

The Resource palette lets a content administrator edit resource properties to handle load balancing in CA Process Automation.

Amount

Lists the total number of units that are assigned to a resource.

Used

Indicates the number of assigned units.

Description

Provides a description of the resource.

Start Request Palette

The Start Request palette lets a production user or content administrator start a start request form.

Start

When you right-click a start request in the Start Requests palette and select Start, you can view both the form instance and the process instance in the right pane.

Index

S

T

U

V

W