Interaction Recorder Policy Editor Help

Printed help

PureConnect powered by Customer Interaction Center® (CIC)

Last updated November 13, 2018

Abstract

This document is a printable version of the Interaction Recorder Policy Editor help. Policy Editor is a single, simple, user interface for creating Interaction Recorder policies that manage recordings. Policy settings for recordings include: *What* are the interactions to be recorded; *Where* recordings are stored and archived, and how long they are retained; and *Who* can access, play, score, export, and archive recordings.

Table of Contents

Interaction Recorder Policy Editor

Introduction

Interaction Recorder Policy Editor is a single, simple user interface for creating Polices that manage recordings. Policy settings for recordings include:

- *What* are the interactions to be recorded?
- *Where* recordings are stored and archived, and how long they are retained?
- *Who* can access, play, score, export, and archive recordings?

For more information, see About Interaction Recorder Policy Editor.

About Interaction Recorder Policy Editor

Policy Editor is a single, simple, user interface for creating Interaction Recorder policies that manage recordings. Policy settings for recordings include: *What* are the interactions to be recorded; *Where* recordings are stored and archived, and how long they are retained; and *Who* can access, play, score, export, and archive recordings.

Use Policy Editor to create:

- **Initiation** policies for determining *What* interactions are recorded
- **Retention** policies for deciding *Where* recordings are stored and archived, and how long they are retained
- **Security** policies for managing *Who* can access, play, score, export, and archive recordings

For more information on creating policies, see:

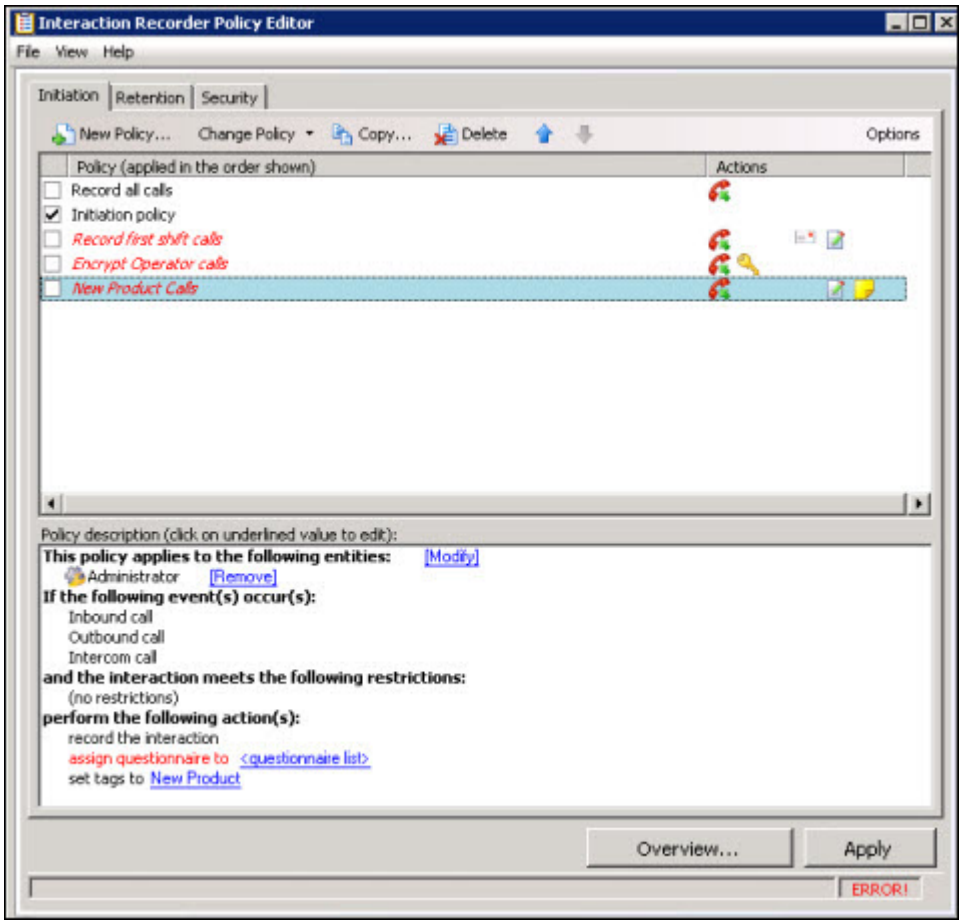
- Creating an Initiation Policy
- Creating a Retention Policy
- Creating a Security Policy

For more information on using Policy Editor, see About the Policy Editor User Interface.

About the Policy Editor User Interface

Interaction Recorder Policy Editor provides a simple, straightforward, user interface to configure and update Interaction Recorder Policies. The interface includes menus, pages, toolbars, and panes for that make it easy for you to navigate when creating Policies.

To learn more about the Policy Editor user interface features, pause the mouse pointer over the menu bar, toolbar, or panes on the graphic below, and **click** to display more information.



Related Topics

About Interaction Recorder Policy Editor

Initiation Policy

About Initiation Policy

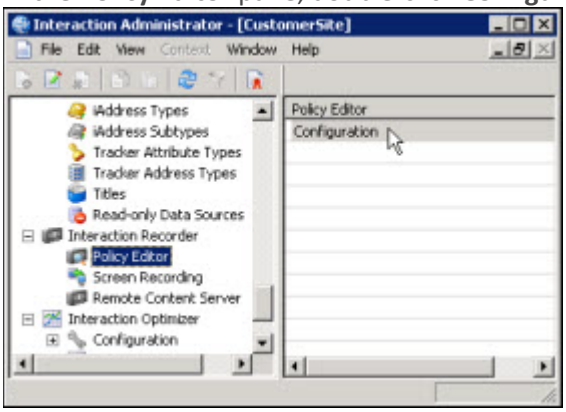
An Initiation Policy tells Interaction Recorder *What* interactions to record. Initiation policies are created in the Interaction Recorder Policy Editor on the **Initiation** page. To learn more about Initiation polices, see Creating an Initiation Policy.

Creating an Initiation Policy

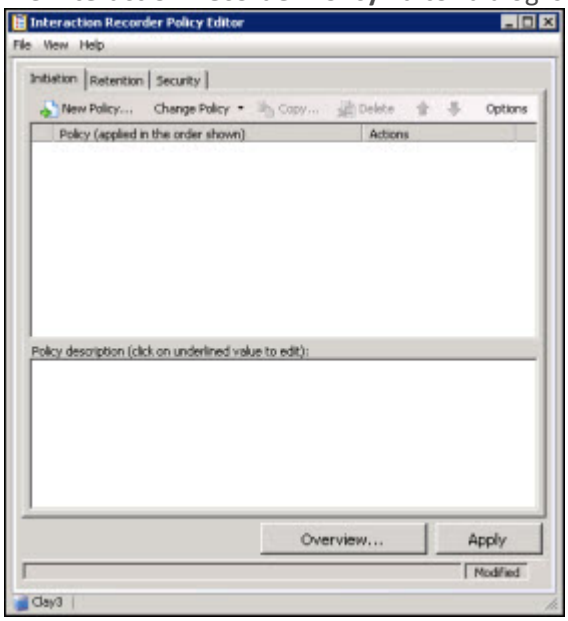
Create an Initiation Policy to tell Interaction Recorder *What* interactions to record. Initiation policies are created in Interaction Administrator under Interaction Recorder on the Policy Editor Configuration dialog, on the **Initiation** page. Here's how to create an Initiation Policy.

Start Policy Editor

1. From **Interaction Administrator** under **Interaction Recorder**, click **Policy Editor**.
2. In the **Policy Editor** pane, double-click **Configuration**.



3. The **Interaction Recorder Policy Editor** dialog is displayed.



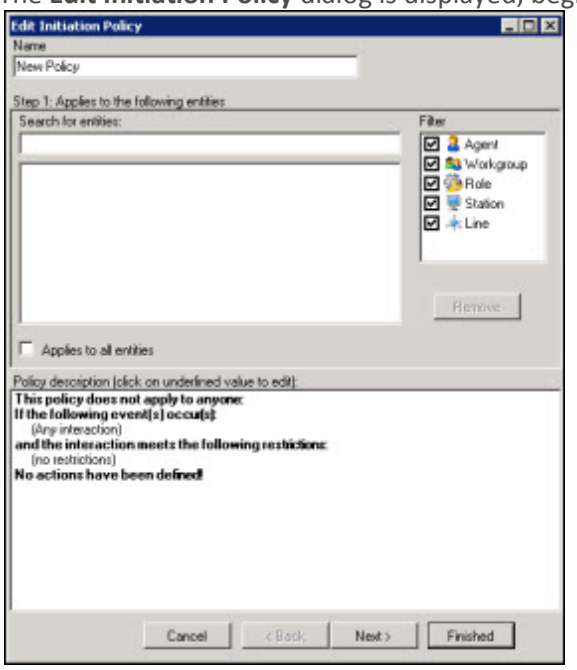
4. Click the **Initiation** tab to display the page.

Create a New Initiation Policy

To create a new Initiation Policy, on the **Initiation** page toolbar, click **New Policy** 

.

The **Edit Initiation Policy** dialog is displayed, beginning with **Step 1**.



Step 1: Applies to the following entities

Use this page of the **Edit Initiation Policy** dialog to apply the policy to entities. You can assign any of the following entities: Agent, Workgroup, Role, Station, or Line.

Applying Policies to Entities

You can apply this policy to all entities *or* you can select specific entities to apply the policy to.

Apply policy to all entities

To apply this policy to all entities:

1. In the **Name** field, type a descriptive name for the policy.
2. In the **Step 1: Applies to the following entities** box, the **Filter** legend lists the entity types and their icons. To apply this policy to all entities, select the **Applies to all entities** check box.

   In the **Policy description** pane, the entity description, **This policy applies to everyone** is displayed.

Apply policy to specific entities

To apply this policy to specific entities:

1. In the **Name** field, type a descriptive name for the policy.
2. Be sure the **Applies to all entities** check box is clear.
3. In the **Step 1: Applies to the following entities** box, the **Filter** legend lists the entity types and their icons: **Agent**, **Workgroup**, **Role**, **Station**, and **Line**. To reduce the number of entities returned in the search results, clear the check boxes for the entities you do not want to include

in the search. For example, if you know the entity you are searching is a Role, clear the other check boxes.

4. To apply this policy to specific entities, click in the **Search for entities** field.
5. In the **Search for entities** field, begin typing an entity name, for example the name of an **Agent**, **Workgroup**, **Role**, **Station**, or **Line**. Entity names that match are displayed in a pop-up window. Note that the entity type icon is displayed next to the entity name.
6. In the pop-up window, click the entity to apply this policy to. The entity is displayed in the entity list box.

   In the **Policy description** pane, the entity is added below the **This policy applies to the following entities** descriptor.
7. Continue adding entities using the **Search for entities** field.

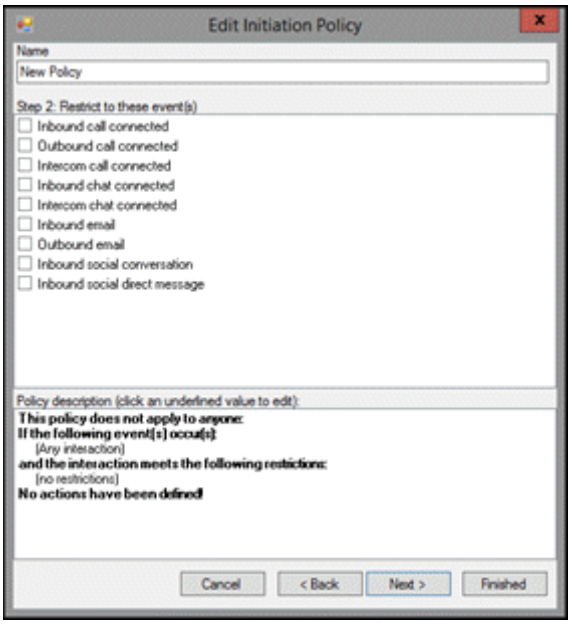
Removing Entities from a Policy

To remove an entity from this policy, from the entity list box, select an entity and click **Remove**. The entity is removed from the list box and also removed from the policy descriptor **This policy applies to the following entities** in the **Policy description** pane.

Completing applying entities

The **Policy description** pane is updated as Initiation Policy settings are added and updated.

When the **Policy description** for applying Initiation Policies to entities is complete, click **Next**. The **Edit Initiation Policy** dialog, **Step 2: Restrict to these events** is displayed.



Step 2: Restrict to these events

Use this page of the **Edit Initiation Policy** dialog to select the type of interactions to be recorded. Interactions for the following events are recorded by default: Inbound call connected, Outbound call

connected, Intercom call connected, Inbound chat connected, Intercom chat connected, Inbound e-mail, Outbound email, Inbound social conversation, and Inbound social direct message. Use Step 2 to restrict the recording of the interactions for these events.

Recording Any Interaction

To record any interaction, be sure **(Any interaction)** is displayed in the **Policy description** pane, below the **If the following events occur**. For **Any interaction** to be recorded, all check boxes for the events in Step 2 must be clear.

Restricting Recording to Specific Events

You can restrict recording to certain interactions by selecting specific events in the **Step 2: Restrict to these events** box. To restrict the recording to specific events:

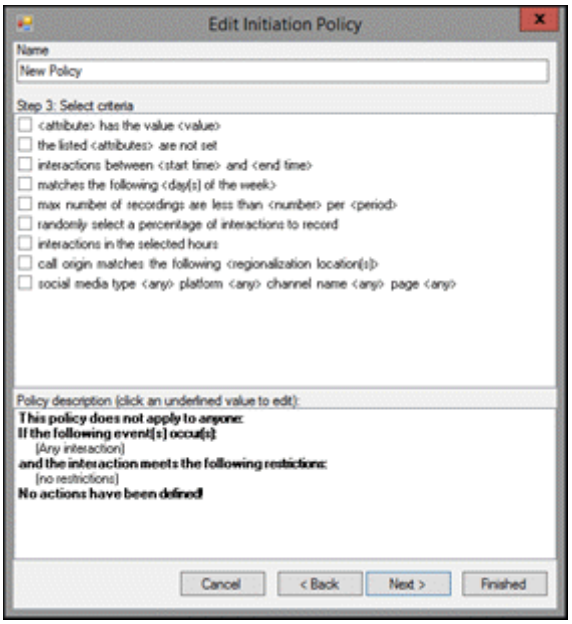
1. In the **Step 2: Restrict to these events** box, select the events check boxes for the type of interaction you want to record. For example, if you select **Inbound call connected**, all inbound call interactions will be recorded. You can select one or more events for the types of interactions you want to record.
   In the **Policy description** pane, the interactions to record are added below the **If the following events occur** descriptor.
2. Continue selecting events for which you want to record interactions.

Completing Interactions to be Recorded

When you have completed configuring the settings for interactions to be recorded, verify that the interactions you want to record are listed in the **Policy description** pane under the **If the following events occur** descriptor. Depending on your selections, the following events are displayed:

- Inbound call
- Outbound call
- Intercom call
- Inbound chat
- Intercom chat
- Inbound email
- Outbound email
- Inbound social conversation
- Inbound social direct message

After you have verified your selections, click **Next**. The **Edit Initiation Policy** dialog, **Step 3: Select criteria** is displayed.



Step 3: Select criteria

Use this page of the **Edit Initiation Policy** dialog to select criteria to restrict which interactions are recorded. The criteria that can be selected to restrict the recording of interactions are:

- <attribute> contains the value <value>
- the listed <attributes> are not set
- interactions between <start time> and <end time>
- matches the following <day(s) of the week>
- max number of recordings are less than <number> per <period>
- randomly select <percent> of interactions per <period> per <user/system>, limiting to <max> interactions
- interactions in the selected hours
- call origin matches the following <regionalization location(s)>
- social media type <any> platform <any> channel name <any> page <any>

Use this step to select criteria to restrict the recording of interactions.

Note You are not required to select criteria in Step 3. If no restrictions for recording interactions are required, do not select any check boxes.

Selecting Criteria for Restricting Recordings

To select criteria that restricts the recording of interactions:

1. In the **Step 3: Select criteria** box, select the check box for the criteria to use to determine when an interaction is recorded.

In the **Policy description** pane, the criteria is added below the **and the interaction meets the following restrictions** descriptor.

2. In the **Policy description** pane, configure the criteria by clicking the variable. When you click a variable, a pop-up window is displayed to enter a value for the variable.

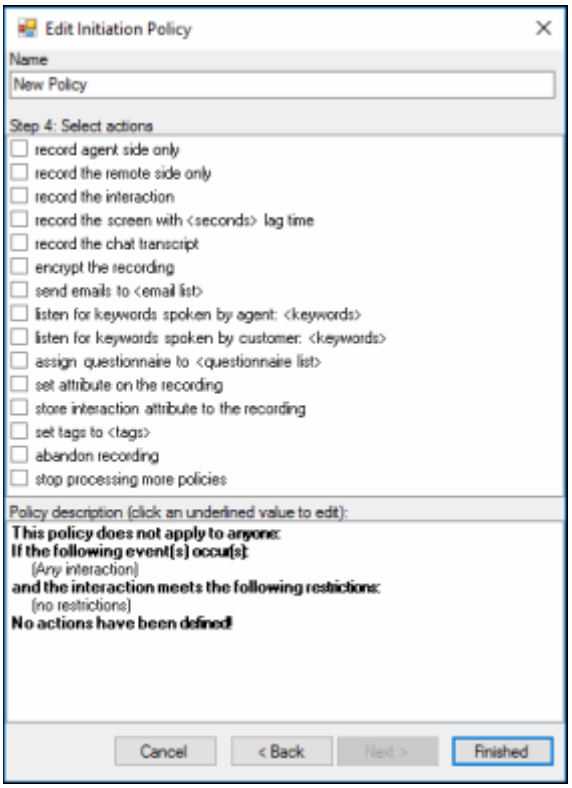
   Note When configuring a variable, to view a table with descriptions for the Criteria values, press F1 to display the Help.

3. Continue selecting criteria check boxes and configuring them in the **Policy description** pane.

Completing Criteria Selection

When you have completed configuring the recording criteria settings, verify that the criteria you want for recording interactions are listed in the **Policy description** pane under the **and the interaction meets the following restrictions** descriptor. Also be sure that the value for each criterion is configured.

After you have verified your selections, click **Next**. The **Edit Initiation Policy** dialog, **Step 4: Select actions** is displayed.



Step 4: Select Actions

Use this page of the **Edit Initiation Policy** dialog to apply **Actions** to interactions. Actions define how a Policy executes. If an action is not defined for an initiation Policy, a warning message is displayed when you are creating the Policy. If no actions are defined for a Policy, an **ERROR** message is displayed in the Policy Editor status bar.

The actions that can be selected to apply to interactions are:

- record agent side only
- record the remote side only
- record the interaction
- record the screen with <seconds> lag time
- record the chat transcript
- encrypt the recording
- send emails to <email list>
- listen for keywords spoken by agent: <keywords>
- listen for keywords spoken by customer: <keywords>
- assign questionnaire to <questionnaire list>
- set attribute on the recording
- store interaction attribute to the recording
- set tags to <tags>
- abandon recording
- stop processing more policies

Selecting Actions for Interactions

Select actions to apply to interactions in the **Step 4: Select actions** box.

To select actions to apply to interactions:

1. In the **Step 4: Select actions** box, select the check box for the action to apply to an interaction.

   In the **Policy description** pane, the action is added below the **perform the following actions** descriptor.

2. If a selected action requires configuring, a variable is displayed in the **Policy description** pane. To configure the value, click the variable and a pop-up window is displayed.

   Note When configuring a variable, to view a table with descriptions for the Criteria values, press F1 to display the Help.

3. Continue selecting action check boxes and configuring them in the **Policy description** pane.

Completing Action Selection

When you have completed configuring the action settings, verify that the actions you want for interactions are listed in the **Policy description** pane under the **perform the following actions** descriptor. Also be sure that the value for each criterion is configured.

After you have verified your selections, click **Finished**. The New Policy name is displayed in italics and selected in the **Policy** pane, and the complete description is displayed in the **Policy description** pane.

Initiation Policy Overview

Click **Overview** to analyze the currently active Initiation policies to be sure your Initiation policies are recording and evaluating the policy entities: Users, Stations, Roles, Workgroups, and Lines. Running Overview also ensures all the users specified in your Initiation policies are licensed for Interaction Recorder access. And the Overview process warns you if your Initiation policies contain **Abandon Recording** or **Stop Processing** actions. When running this process, the Initiation Policy Overview dialog displays status information in **Overview Progress**, and presents the analysis results in the **Licensing Overview** and the **Recorded Overview** tabs. For more information on Overview analysis, see Initiation Policy Overview.

Saving a Policy

When you have completed creating a new Initiation Policy, and there are no errors, click **Apply** to save the Policy. When you click Apply, the Policies are saved and the italics are removed from the name in the Policy list.

Next, see Updating a Policy for more information on configuring Policies.

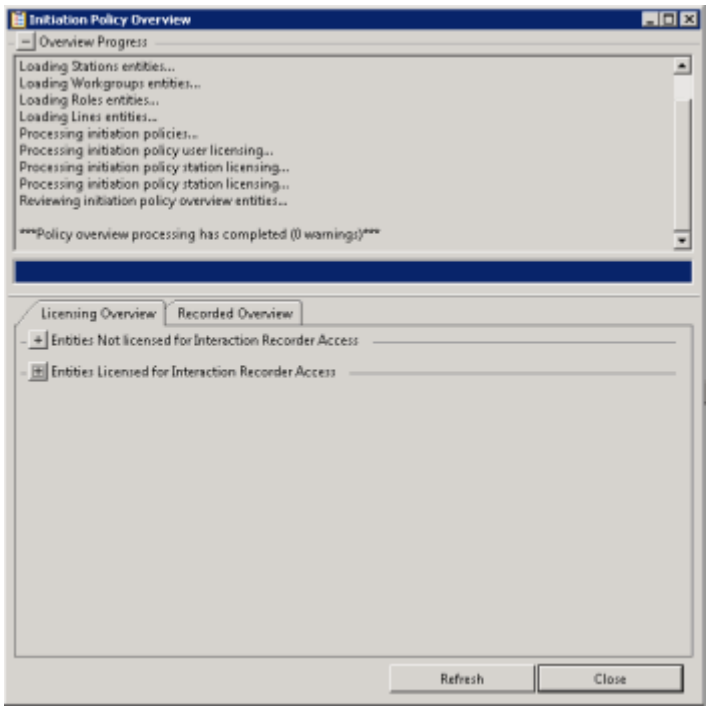
Related Topics

Actions

Initiation Criteria Descriptions

Initiation Policy Overview

After you have created your Initiation Policies, clicking **Overview** displays the Initiation Policy Overview dialog.

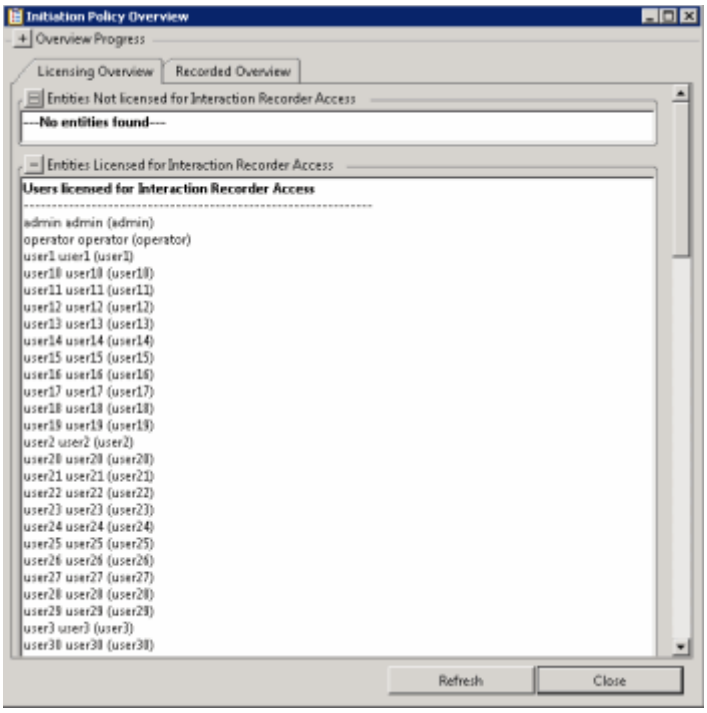


Overview Progress

The Overview Progress box is at the top of the dialog and displays each step in the policy analysis along with any warnings. Warnings are displayed if any entities are not licensed or not recorded. Warnings are also displayed if your Initiation policies contain **Abandon Recording** or **Stop Processing** actions. A warning also appears if Policy Editor is run against an older server, stating that the licensing information is unavailable. When no warnings occur, the Overview Progress box is collapsed.

Licensing Overview

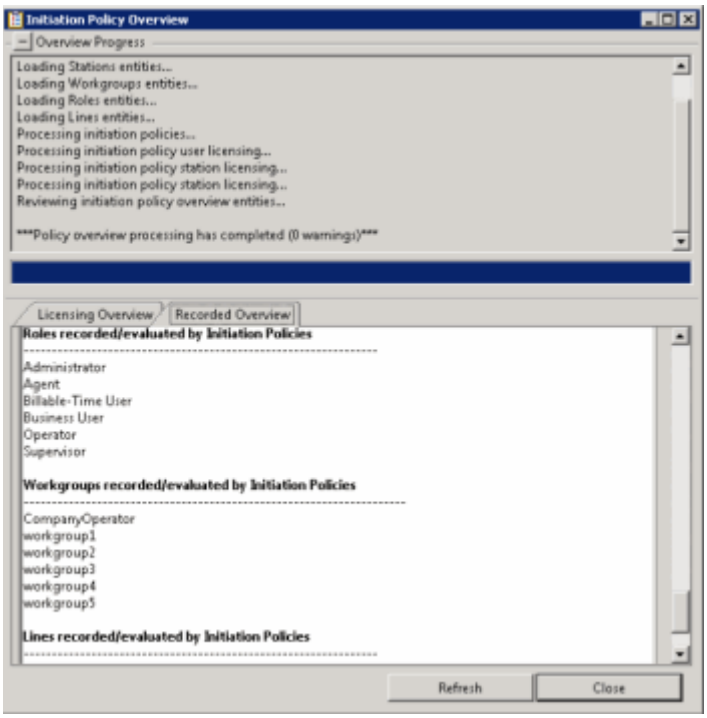
The Licensing Overview tab lists every user and station by type on the server, in the **Entities Licensed for Interaction Recorder Access** box or **Entities Not Licensed for Interaction Recorder Access** box.



If any entities are *not* licensed, the **Entities Not Licensed for Interaction Recorder Access** box is open and the **Entities Licensed for interaction Recorder Access** box is collapsed. Otherwise, the **Entities Licensed for interaction Recorder Access** box is open and the **Entities Not Licensed for Interaction Recorder Access** box is collapsed.

Recorded Overview

The Recorded Overview tab lists all Users, Stations, Roles, Workgroups, and Lines, by type on the server, in the **Entities Recorded/Evaluated by Initiation Policies** box or **Entities Not Recorded/Evaluated by Initiation Policies** box.

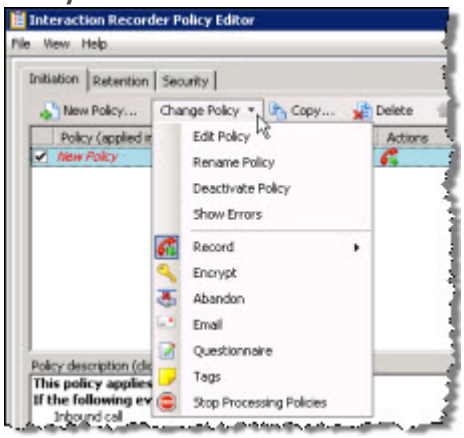


If any entities are *not* licensed, the **Entities Not Recorded/Evaluated by Initiation Policies** box is open and the **Entities Recorded/Evaluated by Initiation Policies** box is collapsed. Otherwise, the **Entities Recorded/Evaluated by Initiation Policies** box is open and the **Entities Not Recorded/Evaluated by Initiation Policies** box is collapsed.

Note No criteria is analyzed when determining which entities will be recorded. All entities that are specified in an Initiation Policy containing a record action are added to the **Entities Recorded/Evaluated by Initiation Policies** box. Recording actions that are supported include: *record interaction, record agent side only,* and *record chat transcript*.

Updating a Policy

Use the **Change Policy** menu to make updates to a Policy or quickly add Actions to a Policy. To display the Change Policy dialog, in the Policy Pane select a Policy and on the Policy Editor toolbar, click **Change Policy**.



The commands on the **Change Policy** menu allow you to:

- Edit a Policy
- Rename a Policy
- Deactivate a Policy
- Show Policy errors
- Add an Action to a Policy

The Actions on the **Change Policy** menu allow you to add the following Actions to a Policy, based on the Policy Type you are configuring:

- Record
- Encrypt
- Abandon
- E-mail
- Questionnaire
- Tags
- Location
- Retention
- Delete
- Score
- Play
- Retrieve
- Stop Processing Policies

Edit a Policy

To edit a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Edit Policy**. The Edit Policy dialog is displayed.
3. Use the Edit Policy dialog to make your changes.

You can also double-click a Policy in the Policy pane to display the Edit Policy dialog.

Rename a Policy

To rename a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.

2. On the Change Policy menu click **Rename Policy**. The Rename Policy dialog is displayed.
3. In the name field, type your new name, and click **OK**.

Deactivate/Activate a Policy

To Deactivate a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Deactivate Policy**. In the Policy pane, the check box for the Policy is cleared.

> You can also deactivate a Policy by clicking the selected check box in the Policy pane. The check is cleared and the Policy is deactivated.

To Activate a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Activate Policy**. In the Policy pane, the check box for the Policy is selected.

> You can also activate a Policy by selecting the Policy check box in the Policy pane.

Show Errors

When there are errors in a Policy, to display the errors:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Show Errors**. A window is displayed listing the **Type** of error and an explanation of the error.

> You can also display the errors for a Policy by right-clicking the Policy and on the shortcut menu click **Show Errors**.

Adding Actions to a Policy

To quickly add Actions to an existing Policy:

1. Select the Policy in the Policy pane and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu, select an Action to apply to the Policy.

When you have completed updating a Policy, and there are no errors, click **Apply** to save the Policy. When you click Apply, the Policies are saved and the italic is removed from the name in the Policy list. When updating Security Policies, the changes take effect immediately when the Security Policy is applied.

Related Help

For additional information on updating policies, including using the toolbar buttons, see the Help for:

Interaction Recorder Policy Editor Initiation page

Interaction Recorder Policy Editor Retention page

Interaction Recorder Policy Editor Security page

Initiation Criteria Descriptions

When selecting criteria and configuring variables for Initiation policies, refer to the following tables for descriptions of criteria and variable values.

Initiation Policy Step 3 Criteria Descriptions

The following table describes the details for configuring variables when setting criteria values in the **Policy description** pane. Variables are configured in a pop-up window when you click the variable below the **and the interaction meets the following restrictions** descriptor. The following criteria appear in the Policy description pane when the criterion is selected.

Criteria for Step 3: Select criteria

Criterion	Description	
<attribute> contains the value **<value>**	**Attribute**	Configure the **attribute** variable to select which interactions are recorded. In the **Edit Attribute** pop-up window, use the drop-down list to select a custom attribute to configure for this criterion.
	Value	In the **Edit Value** pop-up window, enter a value for the attribute selected for this criterion.
	To add additional attributes and values for this criterion, click **[Add]**. To remove an attribute and value for this criterion, click **[Remove]**.	
the following attributes are not set **<Attribs>**	**Attribs**	Configure the **Attribs** variable to select which interactions are recorded when a custom attribute is not set. In the **Attributes Editor** pop-up window, use the **Enter an attribute** drop-down list to select a custom attribute, and then click **Add**. The attribute is added to the attribute list. To remove an attribute from the list, select the attribute in the list and click **Remove**.

interactions between **12:00 AM** and **12:00 AM**	Configure the time variables to set the start and stop times for the recording of interactions.	
	12:00 AM	In the **Time Editor** pop-up window, in the **Time** box, use the up and down arrows to set the hours and minutes to start recording.
	12:00 AM	In the **Time Editor** pop-up window, in the **Time** box, use the up and down arrows to set the hours and minutes to stop recording.
matches **0 days(s)** in the week	Configure the **days** variable to select which days of the week interactions are recorded. In the **Select days of week** pop-up window, select the check boxes next to the days of the week to record interactions.	
max number of recordings is less than **<count>** per **Hour** per **system**	Use this criterion to restrict the number of interactions recorded during a period of time by system or agent.	
	count	In the **Edit Count** pop-up window, type a number for the maximum number of interactions to be recorded for this policy.
	Hour	In the **Select Period** pop-up window, in the **Select the period** box, choose the time period to record interactions for the **count** specified in this criterion. The available time periods are: **Hour**, **Day**, **Week**, **Month**, or **Year**.
	system	Use the **system** toggle variable to switch between recording interactions by **system** or **agent**.
randomly select **100%** of interactions per **hour** per **system**, limiting to **1** interactons	Use this criterion to randomly select a number of interactions to record during a period of time by system or agent.	
	100%	In the **Edit Percent** pop-up window, type a number for the percent of random interactions to be recorded for this policy.
	hour	In the **Select Period** pop-up window, in the **Select the period** box, choose the time period to record interactions for the **percent** specified in this criterion. The available time periods are: **Hour**, **Day**, **Week**, **Month**, or **Year**.

	system	Use the **system** toggle variable to switch between recording interactions by **system** or **agent**.
	1 (edit max)	In the **Edit Max** pop-up window, type a number for the total number of expected interactions for the time period set for this criterion.
matches **0 hour(s)** in a day	Use this criterion to configure the exact hours to record interactions in a day. In the **Select hours** pop-up window, select the specific hours in a day to record interactions.	
call origin matches regionalization locations: **<locations>**	Configure the locations variable to select which locations are recorded. In the **Locations** dialog, in the **Available Locations** box, select the locations, and click **Add**. The locations are displayed in the **Selected Locations** box.	
social media type <any> platform <any> channel name <any> page <any>	Select the value for Social Media: **type**, **platform**, **channel name**, or **page**. For social media **type**, the values are: **Any**, **Conversation**, or **Direct Message**. For Social Media **platform**, the values are: **Any**, **Facebook**, or **Twitter**. For social media **channel name**, specify the social media channel configuration value or leave the field empty for any channel configuration. For social media **page**, specify the social media page configuration value or leave the field empty for any page configuration. **Note:** The social media **page** value is only available for Facebook, and it is limited to the standard 75 characters. If Twitter platform is selected, the page value is Not Available For more information, see the *Social Media Technical Reference* in the PureConnect Documentation Library.	
(no restrictions)	This is the default setting for Step 3. If no restrictions for recording interactions are required, and you have not selected any check boxes, **no restrictions** is displayed under the descriptor for this step.	

Initiation Policy Step 4 Action Descriptions

The following table describes the details for configuring variables when setting action values in the **Policy description** pane. Variables are configured in a pop-up window when you click the variable below the **perform the following actions** descriptor. The following criteria appear in the Policy description pane when the action is selected.

Actions for Step 4: Select actions	
Action	**Description**
record agent side only	When this action is selected, only the agent's side of the interaction is recorded.
record remote side only	When this action is selected, only the remote side of the interaction is recorded.
record the interaction	This action records both sides of the interaction.
record the agent's screen with the **Default** lag time	When this action is selected, the agent's screen is recorded. The default lag time is set in Interaction Recorder Screen Recording in Interaction Administrator. Use this action to set a lag time by recording. To set a lag time, click **Default**. On the **Edit Lag Time** dialog, clear the **Use Default** check box. Enter a Lag time value in the **Lag time is** field.
record the chat transcript	This action records the chat
encrypt the recording	When this action is selected the recording is encrypted. If a call is being recorded using Proactive Recording with no encryption, the call cannot be encrypted using an Initiation Policy. When an Initiation Policy tries to encrypt a Proactive Recording, a warning is registered in the system event log. See the following note for details. **Note** When **Use Proactive Recording** is selected in Interaction Administrator Line Configuration, the **Encrypt Recordings** setting overrides the Interaction Recorder Policy Editor Initiation Policy action, **Encrypt the Recording**. For example, if an Interaction Recorder Initiation Policy is *not* configured to **Encrypt the Recording** and the Interaction Administrator Line Configuration is set to **Use Proactive Recording** and **Encrypt Recordings** is selected, the line

	configuration setting overrides the Interaction Recorder Initiation Policy setting and the recording *is* encrypted. Conversely, if an Interaction Recorder Initiation Policy *is* configured to **Encrypt the Recording** and the Interaction Administrator Line Configuration is set to **Use Proactive Recording** but **Encrypt Recordings** is *not* selected, the line configuration setting overrides the Interaction Recorder Initiation Policy setting and the recording is *not* encrypted. A conflicting record call request logs a Configuration Error warning message in the Application log.
send emails to **<email list>**	This action sends a notification to an e-mail list that an interaction was recorded. On the **Edit EMail List** pop-up window, click **To** or **CC** to create an e-mail distribution list for this action. Click **Reply** to specify an e-mail address to reply to. **Note** If the Initiation Policy is set to send an e-mail, but no recording is made for the interaction, an e-mail is sent with a recording ID of "No Recording Produced."
listen for keywords spoken by agent: **<none>**	During a call, this action listens for keywords that are spoken by an agent. Configure this action to specify which keyword sets to use for the policy. When you click the variable **none**, the **Agent Analyzer Keyword Sets** dialog is displayed. From the list of **Available Keyword Sets**, add keyword sets to the **Selected Keyword Sets** list for this action. The Agent Analyzer Keyword Sets for this action are only selecting keyword sets for the Agent. Information about cumulative Keyword sets, keyword sets that include *both* Agent and Customer keywords, are displayed in the bottom pane of the dialog. This information includes: Language, Agent Keywords, Customer Keywords, Total Keyword Count, and Exceeds Keyword Count Limit. The **Total keyword counts** for a policy is limited to 50 keywords. The total keyword count for a **Language** is the combination of the keyword counts from all of the Keyword Sets selected in this Agent action *plus* the keyword counts from the

Customer action, if included in the policy.

For information on creating Keyword Sets, see the *Interaction Analyzer Technical Reference* in the Documentation Library.

Important Notes

1. Initiation policies that include Analyzer Keyword Sets are combined when a call is received. For example, if Policy A has a keyword set Polite Phrases for the Agent and Policy B has a keyword set Rude Phrases for the Agent and both polices apply to a call, Agents on that call will be spotted with the keyword sets Polite Phrases and Rude Phrases. If the combination of Keyword Sets from multiple Initiation policies causes the keyword count to exceed the configured maximum keywords per language, an error is logged and no keyword spotting occurs. The default Analyzer Maximum Keyword Count server parameter default value is 50. The value for this server parameter can be changed in Interaction Administrator.

- If a keyword count configuration on a call exceeds the maximum allowed, an error is logged in one or two places: an error is logged in the recorder server trace logs for every call whose configuration exceeds the maximum keyword count, and a Windows Event Log error is logged once an hour. For example, if during the course of 8 hours there were 100 calls per hour that had configurations that exceeded the maximum keyword count, then at the end of those 8 hours there would be 800 errors in the recorder server trace logs and 8 errors logged in the Windows Event Log.
- When a policy turns keyword spotting on for a call, it remains on for the duration of the recording, even if a call is transferred. Policies can be configured to turn off keyword spotting by using the default keyword set selection <none>. If the Policy action value is set to **<none>** for either the Agent or the Customer and no other policy that applies to the call contains Keyword Sets for the Agent or

	Customer, then the <none> selection forces keyword spotting off, and no keywords are added to the combined Initiation Policies. To turn keyword spotting off when a call is transferred to a specific agent, station, role, or workgroup, set the Policy action to **<none>**. • Intercom call keyword spotting behaves differently than keyword spotting for inbound and outbound calls. Intercom calls consist of two internal users: the user initiating the call and the user receiving the call. CIC does not support applying both users' keyword spotting policies for intercom calls. For intercom calls, CIC applies the receiving user's keyword spotting policies. As a result, only the keyword sets that were configured by the receiving user's policy actions **listen for keywords spoken by agent** and **listen for keywords spoken by customer** are used to listen for keywords spoken during intercom calls. When the receiving user's keyword spotting actions are applied, the receiving user is spotted for **agent** keywords, and the initiating user is spotted for **customer** keywords. • For details on identifying recordings for evaluation based on Spotted Keywords and Phrases, see "Appendix F: Identify Recordings by Spotted Keywords and Phrases for Evaluation" in the *Interaction Recorder Technical Reference* in the PureConnect Documentation Library.
listen for keywords spoken by customer: **<none>**	During a call, this action listens for keywords that are spoken by a customer. Configure this action to specify which keyword sets to use for the policy. When you click the variable none, the **Agent Analyzer Keyword Sets** dialog is displayed. From the list of **Available Keyword Sets**, add keyword sets to the **Selected Keyword Sets** list for this action. The Customer Analyzer Keyword Sets for this action are only selecting keyword sets for the Customer. Information about cumulative Keyword sets, keyword sets that include both Agent and Customer keywords, are displayed in the bottom pane of the dialog. This information includes: Language, Agent Keywords,

Customer Keywords, Total Keyword Count, and Exceeds Keyword Count Limit. The **Total keyword counts** for a policy is limited to 50 keywords. The total keyword count for a **Language** is the combination of the keyword counts from all of the Keyword Sets selected in this Customer action plus the keyword counts from the Agent action, if included in the policy.

For information on creating Keyword Sets, see the *Interaction Analyzer Technical Reference* in the PureConnect Documentation Library.

Important Notes

2. Initiation policies that include Analyzer Keyword Sets are combined when a call is received. For example, if Policy A has a keyword set Polite Phrases for the Agent and Policy B has a keyword set Rude Phrases for the Agent and both polices apply to a call, Agents on that call will be spotted with the keyword sets Polite Phrases and Rude Phrases. If the combination of Keyword Sets from multiple Initiation policies causes the keyword count to exceed the configured maximum keywords per language, an error is logged and no keyword spotting occurs. The default Analyzer Maximum Keyword Count server parameter default value is 50. The value for this server parameter can be changed in Interaction Administrator.

- If a keyword count configuration on a call exceeds the maximum allowed, an error is logged in one or two places: an error is logged in the recorder server trace logs for every call whose configuration exceeds the maximum keyword count, and a Windows Event Log error is logged once an hour. For example, if during the course of 8 hours there were 100 calls per hour that had configurations that exceeded the maximum keyword count, then at the end of those 8 hours there would be 800 errors in the recorder server trace logs and 8 errors logged in the Windows Event Log.
- When a policy turns keyword spotting on for a call, it remains on for the duration of the

	recording, even if a call is transferred. Policies can be configured to turn off keyword spotting by using the default keyword set selection <none>. If the Policy action value is set to **<none>** for either the Agent or the Customer and no other policy that applies to the call contains Keyword Sets for the Agent or Customer, then the <none> selection forces keyword spotting off, and no keywords are added to the combined Initiation Policies. To turn keyword spotting off when a call is transferred to a specific agent, station, role, or workgroup, set the Policy action to **<none>**. • Intercom call keyword spotting behaves differently than keyword spotting for inbound and outbound calls. Intercom calls consist of two internal users: the user initiating the call and the user receiving the call. CIC does not support applying both users' keyword spotting policies for intercom calls. For intercom calls, CIC applies the receiving user's keyword spotting policies. As a result, only the keyword sets that were configured by the receiving user's policy actions **listen for keywords spoken by agent** and **listen for keywords spoken by customer** are used to listen for keywords spoken during intercom calls. When the receiving user's keyword spotting actions are applied, the receiving user is spotted for **agent** keywords, and the initiating user is spotted for **customer** keywords. • For details on identifying recordings for evaluation based on Spotted Keywords and Phrases, see "Appendix F: Identify Recordings by Spotted Keywords and Phrases for Evaluation" in the *Interaction Recorder Technical Reference* in the PureConnect Documentation Library.
assign questionnaire to **<questionnaire list>**	This action assigns an active questionnaire to the questionnaire list associated with a recording. In the **Assign Questionnaire** dialog, select the questionnaire from the questionnaire list. To select this questionnaire for calibration, select the

	Mark for calibration check box. To require the scored user's signature for the completed questionnaire, select the **Require agent signoff** check box. Next, to assign the questionnaire to a scoring user, in the **Select scoring user** box, in the **Search for entities** field, begin typing the name of an entity: Agent, Workgroup, or Role. Entity names that match are displayed in a pop-up window. Note that the entity type icon is displayed next to the entity name. A **Filter** legend lists the entity types and their icons. To reduce the number of entities returned in the search results, clear the check boxes for the entities you do not want to include in the search. In the pop-up window, click the entity to apply this questionnaire to. The entity is displayed in the entity list box. Continue adding entities using the Search for entities field. These entities will be selected by round-robin. To remove an entity from the list, select an entity and click **Remove**.	
set attribute **<attribute> on the recording to <value>**	Configure this action to set a custom attribute for a recording.	
	attribute	In the **Edit Attribute** pop-up window, type or select a name for the custom attribute.
	value	In the **Edit Value** pop-up window, enter a value for the attribute selected for this

		action.
store interaction attribute **<attribute>** to the recording	Configure this action to assign a custom attribute to the recording. In the **Edit Attribute** pop-up window, type or select a name for the custom attribute to be stored with the recording.	
set tags to **<Tags>**	Use this action to create tags for an interaction recording. In the **Tags Editor** pop-up window, type or select a tag name and click **Add**. All the tags created in the **Tags Editor** list are displayed in the Policy description pane.	
abandon recording	Select the abandon recording action to specify that certain users, workgroups, or roles should not be recorded. If an interaction matches multiple policies, and one of the policies has the abandon recording action, the interaction will *not* be recorded.	
stop processing more policies	Add this action to a Policy to stop processing policies that follow it. The order of a policy is set in the Policy pane, using the up and down arrows.	

Related Topics

Creating an Initiation Policy

Retention Policy

About Retention Policy

A Retention Policy tells Interaction Recorder *Where* recordings are stored and archived and how long they are retained. Retention policies are created in the Interaction Recorder Policy Editor on the **Retention** page. To learn more about Retention polices, see Creating a Retention Policy.

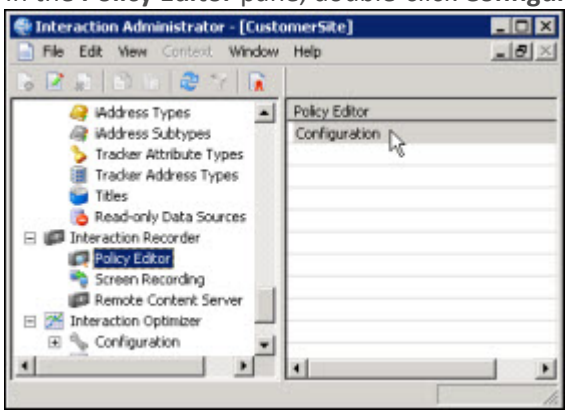
Creating a Retention Policy

Create Retention Policies to configure where recordings are stored, when they should be archived, and how long they are retained. After Retention Policies evaluate a recording, in order for the recording to be re-evaluated by the Retention Policies, be sure to create a Retention Policy with the re-evaluation action. This action allows the recording to be re-evaluated by Retention Policies. Retention policies are

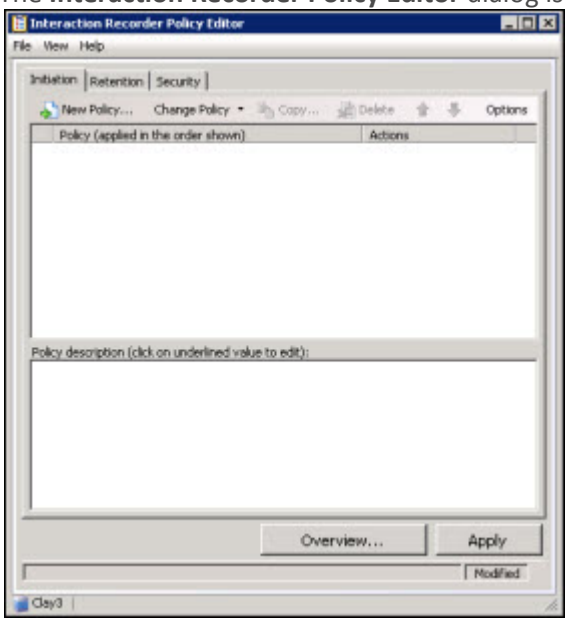
created in Interaction Administrator under Interaction Recorder on the Policy Editor Configuration dialog, on the **Retention** page. Here's how to create a Retention Policy.

Start Policy Editor

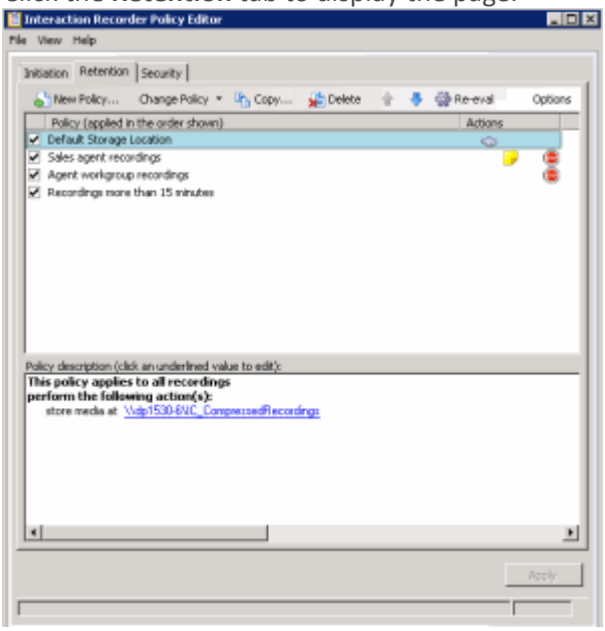
1. From **Interaction Administrator** under **Interaction Recorder**, click **Policy Editor**.
2. In the **Policy Editor** pane, double-click **Configuration**.



3. The **Interaction Recorder Policy Editor** dialog is displayed.



4. Click the **Retention** tab to display the page.

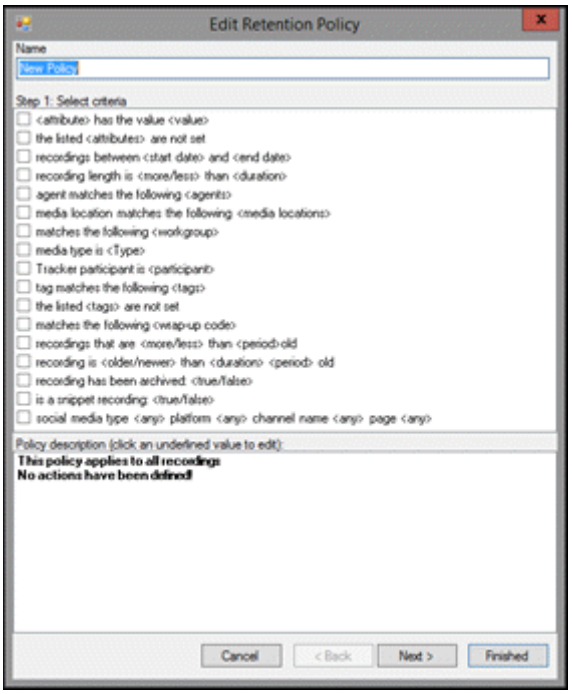


The Retention page is displayed, showing the Default Storage Location Policy.

Create a New Retention Policy

To create a new Retention Policy, on the **Retention** page toolbar, click **New Policy** 

.
The **Edit Retention Policy** dialog is displayed, beginning with **Step 1**.



Step 1: Select criteria

Use this page of the **Edit Retention Policy** dialog to select retention criteria for a recorded interaction. The criteria that can be selected to retain a recorded interaction are:

- <attribute> contains the value <value>
- the listed <attributes> are not set
- recordings between <start date> and <end date>
- recording length is <more/less> than <duration>
- agent matches the following <agents>
- media location matches the following <media locations>
- matches the following <workgroup>
- media type is <Type>
- Tracker participant is <participant>
- tag matches the following <tags>
- the listed <tags> are not set
- matches the following <wrapup code>
- recordings that are <more/less> than <period> old
- recording is <older/newer> than <duration> <period> old
- recording has been archived: <true/false>
- is a snippet recording: <true/false>
- social media type <any> platform <any> channel name <any> page <any>

Note If no criteria are selected, the policy applies to all recordings.

Selecting Criteria for Retaining Recordings

Select the retention criteria for recordings in the **Step 1: Select criteria** box.

To select retention criteria for interaction recordings:

1. In the **Name** field, type a descriptive name for the policy.
2. In the **Step 1: Select criteria** box, select the check box for the criteria to use for retention settings for recorded interactions.

   In the **Policy description** pane, the criteria is added below the **if the interaction meets the following criteria** descriptor.
3. In the **Policy description** pane, configure the criteria by clicking the variable. When you click a variable, a pop-up window is displayed to enter a value for the variable.

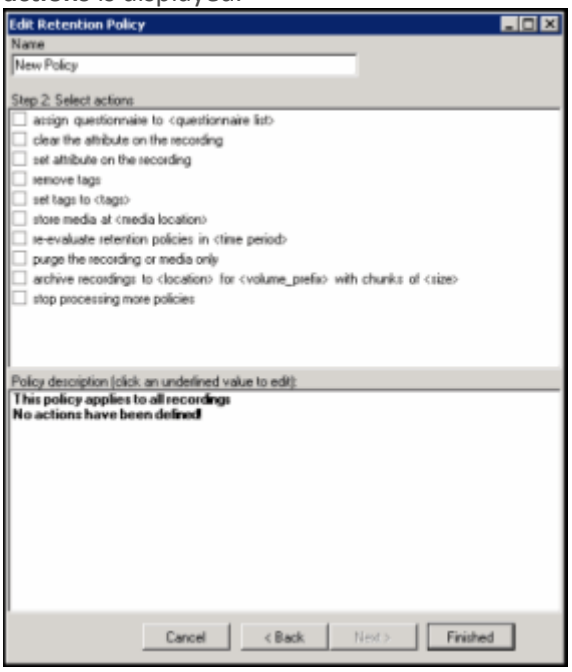
   Note When configuring a variable, to view a table with descriptions for the Criteria values, press F1 to display the Help.

4. Continue selecting criteria check boxes and configuring them in the **Policy description** pane.

Completing Criteria Selection

When you have completed configuring the retention criteria settings, verify that the criteria you want for retaining recording interactions are listed in the **Policy description** pane under the **if the interaction meets the following criteria** descriptor. Also be sure that the value for each criterion is configured.

After you have verified your selections, click **Next**. The **Edit Retention Policy** dialog, **Step 2: Select actions** is displayed.



Step 2: Select actions

Use this page of the **Edit Retention Policy** dialog to apply retention **Actions** to recordings. Actions define how a Policy executes. If an action is not defined for a retention Policy, a warning message is displayed when you are creating the Policy. If no actions are defined for a Policy, an **ERROR** message is displayed in the Policy Editor status bar.

The retention actions that can be selected to apply to recordings are:

- assign questionnaire to <questionnaire list>
- clear the attribute on the recording
- set attribute on the recording
- remove tags
- set tags to <tags>
- store media at <media location>
- re-evaluate retention policies in <time period>
- purge the recording or media only
- archive recordings to <location> for <volume_prefix> with chunks of <size>

- stop processing more policies

Selecting Actions for Recordings

Select retention actions to apply to recordings in the **Step 2: Select actions** box.

To select actions to apply to recordings:

1. In the **Step 2: Select actions** box, select the check box for the retention action to apply to a recording.

   In the **Policy description** pane, the action is added below the **perform the following actions** descriptor.

2. If a selected action requires configuring, a variable is displayed in the **Policy description** pane. To configure the value, click the variable and a pop-up window is displayed.

   Note When configuring a variable, to view a table with descriptions for the Criteria values, press F1 to display the Help.

3. Continue selecting action check boxes and configuring them in the **Policy description** pane.

Completing Action Selection

When you have completed configuring the action settings, verify that the retention actions you want for recordings are listed in the **Policy description** pane under the **perform the following actions** descriptor. Also be sure that the value for each criterion is configured.

After you have verified your selections, click **Finished**. The New Policy name is displayed and selected in the **Policy** pane, and the complete description is displayed in the **Policy description** pane.

Saving a Policy

When you have completed creating a new Retention Policy, and there are no errors, click **Apply** to save the Policy. When you click Apply, the Policies are saved and the italics are removed from the name in the Policy list.

Next, see Updating a Policy for more information on configuring Policies.

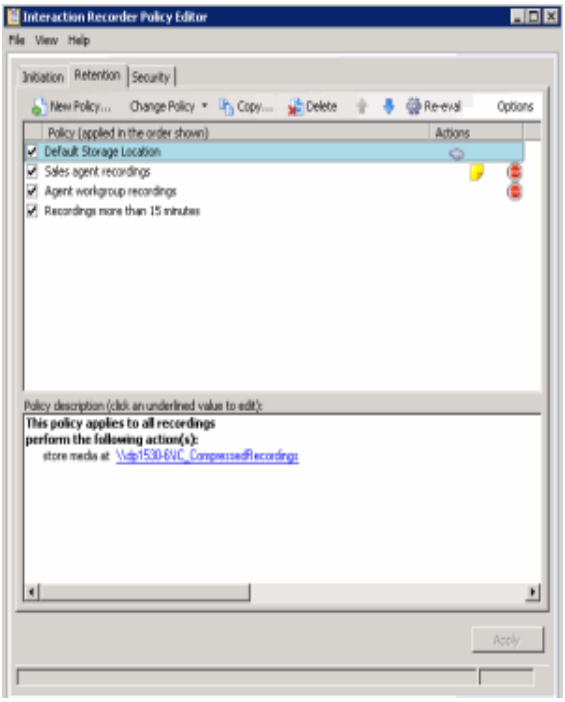
Related Topics

Actions

Retention Criteria Descriptions

Default Storage Location Policy

If you used IC Setup Assistant to configure the Default Storage Location, the directory you specified is configured in a Default Storage Location Retention policy. This Retention policy was created automatically, and is displayed on the Retention page.



To change the default storage for compressed and processed recordings, edit the value for **store media at** in the Policy description pane.

Note We highly recommend that the stored recordings media location be a valid UNC path. This is necessary because there might be multiple CIC Servers and Interaction Recorder servers requesting recording files from one another. To set the **<media location>** variable to a valid UNC path, on the Select Folder pop-up window, type a UNC path.

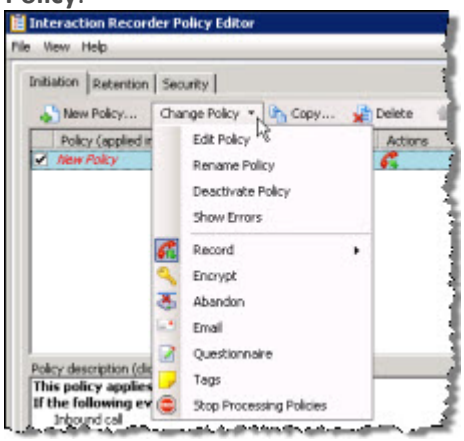
Related Topics

Creating a Retention Policy

Updating a Policy

Use the **Change Policy** menu to make updates to a Policy or quickly add Actions to a Policy. To display the Change Policy dialog, in the Policy Pane select a Policy and on the Policy Editor toolbar, click **Change**

Policy.



The commands on the **Change Policy** menu allow you to:

- Edit a Policy
- Rename a Policy
- Deactivate a Policy
- Show Policy errors
- Add an Action to a Policy

The Actions on the **Change Policy** menu allow you to add the following Actions to a Policy, based on the Policy Type you are configuring:

- Record
- Encrypt
- Abandon
- E-mail
- Questionnaire
- Tags
- Location
- Retention
- Delete
- Score
- Play
- Retrieve
- Stop Processing Policies

Edit a Policy

To edit a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Edit Policy**. The Edit Policy dialog is displayed.
3. Use the Edit Policy dialog to make your changes.

You can also double-click a Policy in the Policy pane to display the Edit Policy dialog.

Rename a Policy

To rename a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Rename Policy**. The Rename Policy dialog is displayed.
3. In the name field, type your new name, and click **OK**.

Deactivate/Activate a Policy

To Deactivate a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Deactivate Policy**. In the Policy pane, the check box for the Policy is cleared.

You can also deactivate a Policy by clicking the selected check box in the Policy pane. The check is cleared and the Policy is deactivated.

To Activate a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Activate Policy**. In the Policy pane, the check box for the Policy is selected.

You can also activate a Policy by selecting the Policy check box in the Policy pane.

Show Errors

When there are errors in a Policy, to display the errors:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Show Errors**. A window is displayed listing the **Type** of error and an explanation of the error.

You can also display the errors for a Policy by right-clicking the Policy and on the shortcut menu click **Show Errors**.

Adding Actions to a Policy

To quickly add Actions to an existing Policy:

1. Select the Policy in the Policy pane and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu, select an Action to apply to the Policy.

When you have completed updating a Policy, and there are no errors, click **Apply** to save the Policy. When you click Apply, the Policies are saved and the italic is removed from the name in the Policy list. When updating Security Policies, the changes take effect immediately when the Security Policy is applied.

Related Help

For additional information on updating policies, including using the toolbar buttons, see the Help for:

Interaction Recorder Policy Editor Initiation page

Interaction Recorder Policy Editor Retention page

Interaction Recorder Policy Editor Security page

Retention Criteria Descriptions

When selecting criteria and configuring variables for Retention policies, refer to the following tables for descriptions of criteria and variable values.

Retention Policy Step 1 Criteria Descriptions

The following table describes the details for configuring variables when setting retention criteria values in the **Policy description** pane. Variables are configured in a pop-up window when you click the variable below the **if the interaction meets the following criteria** descriptor. The following criteria appear in the Policy description pane when the criterion is selected.

Criteria for Step 1: Select Criteria		
Criterion	**Description**	
<attribute> contains the value, **<value>**	**Attribute**	Configure the **attribute** variable to select which recordings apply to this retention policy. In the **Edit Attribute** pop-up window, use the drop-down list to select a custom attribute to configure for this criterion.
	Value	In the **Edit Value** pop-up window, enter a value for the attribute selected for this criterion.

	To add additional attributes and values for this criterion, click **[Add]**. To remove an attribute and value for this criterion, click **[Remove]**.	
the following attributes are not set **<Attribs>**	**Attribs**	Configure the **Attribs** variable to select which recordings apply to this policy when a custom attribute is not set. In the **Attributes Editor** pop-up window, use the **Enter an attribute** drop-down list to select a custom attribute, and then click **Add**. The attribute is added to the attribute list. To remove an attribute from the list, select the attribute in the list and click **Remove**.
recordings between **<start date>** and **<end date>**	Configure the variables for this criterion to select which recordings, within a date range, apply to this retention policy.	
	start date	In the **Date Editor** pop-up window, select a start date from the drop-down calendar.
	end date	In the **Date Editor** pop-up window, select an end date from the drop-down calendar.
recording length is **less than 0 seconds**	Configure this variable to apply this retention policy to recordings with a specific length. In the **Compare Recording Length** pop-up window, configure the first part of this setting. In the **Recording length is** drop-down list, select either **less than** or **greater than**. To configure the next setting for this criterion, in the **seconds** box, type the number of seconds or use the up and down arrows to select a number.	
agent matches one of the following **[Modify]**	Configure this variable to select which agents to apply this retention policy to. In the **Select Agents** pop-up window, begin typing an agent name in the **Search for agents** box. Agent names that match are displayed in a pop-up window. When you select an agent in the pop-up, it is added to the agent list.	
media location matches the following **<media locations>**	Configure this variable to apply this retention policy to recordings that are located in a specific folder. In the **Select Folder** pop-up window, select a folder from the drop-down list. You can also browse for a folder using the ellipsis button.	
matches following **<workgroup>**	Configure the **<workgroup>** variable to select which workgroups to apply this retention policy to. In the **Select Workgroups** pop-up window, begin typing a workgroup name in the **Search for workgroups** box. Workgroup names that match are displayed in a pop-up window. When you select a workgroup in the	

	pop-up, it is added to the workgroup list.
media type is **<media type>**	Configure this variable to apply this retention policy to recordings with specific media types. In the **Select Media type** pop-up window, select the media type. Multiple media types can be selected. The available media types are: **Call**, **Chat**, **Chat Transcript, Email**, **Screen, Social Conversation,** and **Social Direct Message**.
matches one of the following Tracker participants **[Modify]**	Configure this variable to select which Tracker participants to apply this retention policy to. In the **Select Remote Parties** pop-up window. A **Filter** legend lists the remote party types and their icons. To reduce the number of entities returned in the search results, clear the check boxes for the entities you do not want to include in the search. Begin typing a name in the **Search for remote parties** box. Names that match are displayed in a pop-up window. Note that the remote party type icon is displayed next to the remote party name. When you select a remote party in the pop-up, it is added to the remote parties list.
tag matches the following **<Tags>**	Configure the **<Tags>** variable to select Tags, which are associated with recordings that you want to apply this retention policy to. In the **Tags Editor** pop-up window, in the **Enter a tag** box, type or select a tag name, and click **Add** to include the name in the Tags Editor list. All the tags created in the **Tags Editor** list are displayed in the Policy description pane.
the following tags are not set **<Tags>**	Configure this variable to apply this retention policy to recordings that *do not* have these tags associated with them. In the **Tags Editor** pop-up window, in the **Enter a tag** box, type or select a tag name, and click **Add** to include the name in the Tags Editor list. All the tags created in the **Tags Editor** list are displayed in the Policy description pane.
wrapup code is **<wrapup codes>**	Configure the variable for this criterion to select which wrap-up codes apply to this retention policy. In the **Select Wrapup Codes** pop-up window, select the wrap-up codes to apply to this retention policy.
recordings that are **older than today**	Configure the variable for this criterion to select which recordings, within a date range, apply to this retention policy. To configure the first field in the **Select Date Range** pop-up window, in the drop-down list, select either **older than** or **within.** To configure the second field in the **Select Date Range** pop-up window, in the drop-down list, select the period of time. The available options are: **today**, **this week**, **this month**, **this quarter**, **this year**.
recording is **older than 0 day**	Configure the variables for this criterion to select which recordings are within or older than the specified period of time. In the **Compare Recording Age** first

old	drop-down list, select **older than** or **within**. In the next box, type a number for the period of time. In the last drop-down list, select the period of time. The options are: **Hour**, **Day**, **Week**, **Month**, or **Year**.
recording has been archived: **false**	Configure the variable for this criterion to select which recordings have or have not been archived. Click the variable and toggle to **true** or **false**.
is a snippet recording: **false**	Configure the variable for this criterion to apply this retention policy for snippet recordings. To apply the policy to snippet recordings, click the variable and toggle to **true**.
social media type <any> platform <any> channel name <any> page <any>	Select the value for Social Media: **type**, **platform**, **channel name**, or **page**. For social media **type**, the values are: **Any**, **Conversation**, or **Direct Message**. For Social Media **platform**, the values are: **Any**, **Facebook**, or **Twitter**. For social media **channel name**, specify the social media channel configuration value or leave the field empty for any channel configuration. For social media **page**, specify the social media page configuration value or leave the field empty for any page configuration. **Note:** The social media **page** value is only available for Facebook, and it is limited to the standard 75 characters. If Twitter platform is selected, the page value is Not Available. For more information, see the *Social Media Technical Reference* in the PureConnect Documentation Library.

Retention Policy Step 2 Action Descriptions

The following table describes the details for configuring variables when setting retention action values in the **Policy description** pane. Variables are configured in a pop-up window when you click the variable below the **perform the following actions** descriptor. The following criteria appear in the Policy description pane when the action is selected.

Actions for Step 2: Select actions	
Action	**Description**
assign questionnaire to **<questionnaire list>**	This action assigns an active questionnaire to the questionnaire list associated with a recording. In the **Assign Questionnaire** dialog, select the questionnaire from the questionnaire

	list. To select this questionnaire for calibration, select the **Mark for calibration** check box. To require the scored user's signature for the completed questionnaire, select the **Require agent signoff** check box. Next, to assign the questionnaire to a scoring user, in the **Select scoring user** box, in the **Search for entities** field, begin typing the name of an entity: Agent, Workgroup, or Role. Entity names that match are displayed in a pop-up window. Note that the entity type icon is displayed next to the entity name. A **Filter** legend lists the entity types and their icons. To reduce the number of entities returned in the search results, clear the check boxes for the entities you do not want to include in the search. In the pop-up window, click the entity to apply this questionnaire to. The entity is displayed in the entity list box. Continue adding entities using the Search for entities field. These entities will be selected by round-robin. To remove an entity from the list, select an entity and click **Remove**. **Note** When assigning a Role, the maximum number of Roles that can be configured for a Retention policy is 300.
clear attribute **<attribute>** on the recording	Configure this action to remove a custom attribute from recordings. In the **Edit Attribute** type or select a name of the custom attribute to be removed from recordings. To add an additional criterion to clear an attribute from a recording, click **[Add]**. To remove the criteria list, click **[Remove]**.
set attribute **<attribute>** on the recording to **<value>**	Configure this action to set a custom attribute for a recording.

	attribute	In the **Edit Attribute** pop-up window, type or select a name for the custom attribute.
	value	In the **Edit Value** pop-up window, enter a value for the attribute selected for this action.
remove the following tags **<tags>**	Use this action to remove tags from an interaction recording. In the **Tags Editor** pop-up window, type or select a name for the tag to be removed, and click **Add**. The name of the tag to be removed from recordings is added to the list. This is a list of tags that will be removed from recordings for this policy.	
set tags to **<Tags>**	Use this action to create tags for an interaction recording. In the **Tags Editor** pop-up window, type or select a tag name and click **Add**. All the tags created in the **Tags Editor** list are displayed in the Policy description pane.	
store media at **<media location>**	Configure this variable to store a recording in a specific folder, or to select an Amazon S3 location to store your recording. In order to view a screen recording in the	

	playback window, the action **Store Media at** executes before the action **Archive Recording to** when both actions are in the same Retention Policy. **Note** All Amazon S3 communication uses HTTPS protocol. Also note, the S3 Bucket name cannot contain periods as Amazon's SSL wildcard certificate only matches buckets that do not contain periods. **Select a Folder** To select a specific folder to store the recording, click the **media location** variable, and in the **Select Folder** pop-up window select a folder from the drop-down list. You can also browse for a folder using the ellipsis button. **Notes** - We highly recommend that the stored recordings media location be a valid UNC path. This is necessary because there might be multiple CIC Servers and Interaction Recorder servers requesting recording files from one another. To set the **<media location>** variable to a valid UNC path, on the Select Folder pop-up window, type a UNC path. - If a Retention policy includes both the "store media at" action *and* the "purge the media only" action, the "store media at" action is not executed. - If no Interaction Recorder Remote Content Servers are configured, specifying local storage paths might unexpectedly result in performance issues with the CIC server, specifically when drive storage is limited. If Interaction Recorder Remote Content Servers *are* configured and you experience connection or network access issues, specifying local storage paths can result in recording storage to unexpectedly fall back to the CIC server. Performance issues can occur on the CIC

server when drive storage becomes limited. We recommend specifying network or shared paths for optimal performance.

Amazon S3 location

To store a recording using Amazon Simple Storage Service (Amazon S3), select the check box **Amazon S3 location**.

Next, select a **Bucket** from the drop-down list and in the **Subfolder** field type a name for the subfolder where the recordings will be stored.

Configure Amazon S3 Bucket

Configure in Interaction Administrator
Amazon S3 location buckets are configured in Interaction Administrator and are available in the Bucket list. For more information see "Cloud Services Configuration" in the *Interaction Recorder and Interaction Quality Manager Technical Reference.*

Configure in Policy Editor
You can also configure a new Amazon S3 bucket in Policy Editor from the Bucket drop-down list. To do this:
- Select **<Configure>** and on the **S3 Bucket Configuration** dialog, add the Amazon **Account ID** and **Secret Key** information for the new Bucket.
- In the **Region Endpoint** list, select the region where recordings are stored or accessed.
- If the **Region Endpoint** is not in the list, you can select **Specify custom S3 Endpoint** and click **Configure**. In the **Specify Custom Endpoint** dialog, enter the endpoint information. When adding a custom region and endpoint, the display name must match the region name defined for the given endpoint. Endpoints are defined in Amazon S3.

	The endpoint information helps reduce data latency when you access or store recordings with the Amazon S3 service. Click **Test** to validate the proper access level for the specified account credentials. For information on Amazon Simple Storage Service, see Amazon Web Services at http://aws.amazon.com/s3.
re-evaluate retention policies in **Never**	After Retention Policies evaluate a recording, in order for the recording to be re-evaluated by the Retention Policies, be sure to create a Retention Policy with the re-evaluation action. This action allows the recording to be re-evaluated by Retention Policies. Configure this variable to set the re-evaluation time period for a recording. In the **Edit Re-evaluation Period** pop-up window, select the time period from the drop-down list. The available re-evaluation time periods are: **Never** or **Duration**. When you select **Duration**, values are displayed. You can set the re-evaluation duration by **Minutes**, **Hours**, **Days**, **Weeks**, **Months**, **Quarters**, or **Years**. **Note** A month is defined as 31 days, a quarter is defined as 93 days, and one year is defined as 365 days. **Note** When a recording matches multiple Retention Policies, the policy with the shortest re-evaluation time interval is used to re-evaluate the recording. For example if a recording matches three retention policies, one with a 3-day re-evaluation interval, another with a 30-day re-evaluation interval, and another policy matches with a 1-year re-evaluation interval, the recording will be re-evaluated in 3 days.
purge the **recording and**	Configure this variable to purge a recording and media for a recording, or

media	to only purge the media for a recording. *Media* refers to the actual audio or video recording, and *recording and media* refers to the audio or video recording and the database records. If you purge the media only, the database records remain for reporting purposes. To purge the audio or video and the database records, click the variable and toggle to **recording and media**. To purge only the audio or video recording, click the variable and toggle to **media only**.
archive recording to **<media location>** for **<volume prefix>** with chunks of **0 MB**	Configure these variables to archive recordings to a specific volume folder, or to select an Amazon S3 location to archive a recording. In order to view a screen recording in the playback window, the action **Store Media** at executes before the action **Archive Recording** to when both actions are in the same Retention Policy. **Note** For information on automatically archiving recordings using Interaction Recorder Policy Editor, see "Appendix D: Archive Recordings" in the *Interaction Recorder and Interaction Quality Manager Technical Reference* in your PureConnect Documentation Library. **Select a Folder** To select a specific folder to archive a recording, click the **media location** variable and in the **Archive storage location** pop-up window, specify a valid non-local shared UNC path. Click the **volume prefix** variable, and in the **Archive volume prefix** pop-up window, specify a prefix string for the archive volume name. Click the **0 MB** variable, and in the **Edit Storage size** pop-up window, type the

	maximum storage size for each archive volume folder. Click the **MB** box to toggle between **MB** and **GB**. **Notes** - When entering the storage size for an archive volume folder in an Archive action, the Edit Storage size dialog shows a red error rectangle around the storage size field and the OK button is not available, if the field is empty or 0 is specified. The Edit Storage Size dialog shows a yellow warning rectangle around the storage size field when the storage size is determined to be risky and outside of the normal storage range. A tooltip is displayed explaining the error or warning. - If no Interaction Recorder Remote Content Servers are configured, specifying local storage paths might unexpectedly result in performance issues with the CIC server, specifically when drive storage is limited. If Interaction Recorder Remote Content Servers *are* configured and you experience connection or network access issues, specifying local storage paths can result in recording storage to unexpectedly fall back to the CIC server. Performance issues can occur on the CIC server when drive storage becomes limited. We recommend specifying network or shared paths for optimal performance. **Amazon S3 location** To archive a recording using amazon Simple Storage Service (Amazon S3), click the **media location** variable, and in the **Archive storage location** pop-up window select the check box **Amazon S3 location**. **Note** All Amazon S3

communication uses HTTPS protocol.

Next, select a **Bucket** from the drop-down list and in the **Subfolder** field type a name for the subfolder where the recordings will be archived.

Click the **volume prefix** variable, and in the **Archive volume prefix** pop-up window, specify a prefix string for the archive volume name.

Click the **0 MB** variable, and in the **Edit Storage size** pop-up window, type the maximum storage size for each archive volume folder. Click the **MB** box to toggle between **MB** and **GB**.

Amazon S3 location

To store a recording using Amazon Simple Storage Service (Amazon S3), select the check box **Amazon S3 location**.

Next, select a **Bucket** from the drop-down list and in the **Subfolder** field type a name for the subfolder where the recordings will be stored.

Configure Amazon S3 Bucket

Configure in Interaction Administrator
Amazon S3 location buckets are configured in Interaction Administrator and are available in the Bucket list. For more information see "Cloud Services Configuration" in the *Interaction Recorder and Interaction Quality Manager Technical Reference.*

Configure in Policy Editor
You can also configure a new Amazon S3 bucket in Policy Editor from the Bucket drop-down list. To do this:
- Select **<Configure>** and on the **S3 Bucket Configuration** dialog, add the Amazon **Account ID** and **Secret Key** information for the new Bucket.
- In the **Region Endpoint** list, select the region where recordings are stored or

	accessed. **-** If the **Region Endpoint** is not in the list, you can select **Specify custom S3 Endpoint** and click **Configure**. In the **Specify Custom Endpoint** dialog, enter the endpoint information. When adding a custom region and endpoint, the display name must match the region name defined for the given endpoint. Endpoints are defined in Amazon S3. The endpoint information helps reduce data latency when you access or store recordings with the Amazon S3 service. Click **Test** to validate the proper access level for the specified account credentials. For information on Amazon Simple Storage Service, see Amazon Web Services at http://aws.amazon.com/s3.
stop processing more policies	Add this action to a Policy to stop processing policies that follow it. The order of a policy is set in the Policy pane, using the up and down arrows.

Related Topics

Creating a Retention Policy

Security Policy

About Security Policy

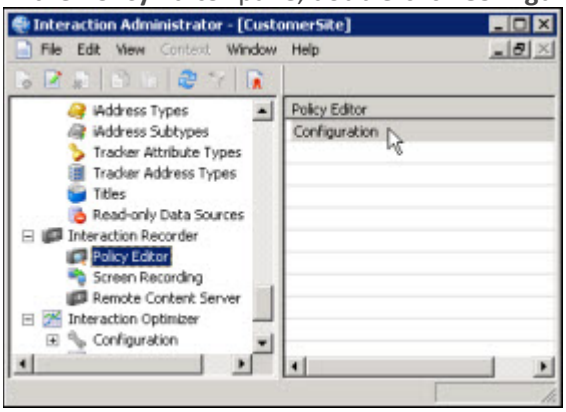
A Security Policy tells Interaction Recorder *Who* can access, play, score, export, and archive recordings. Security policies are created in the Interaction Recorder Policy Editor on the **Security** page. To learn more about Security polices, see Creating a Security Policy.

Creating a Security Policy

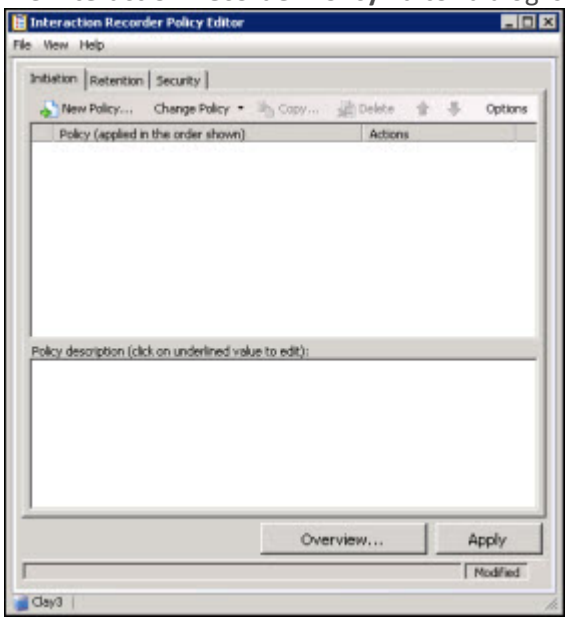
Create a Security Policy to specify which actions specific users are allowed to perform on selected recordings. Security policies apply to Agents and Roles. Security policies are created in Interaction Administrator under Interaction Recorder on the Policy Editor Configuration dialog, on the **Security** page. Here's how to create a Security Policy.

Start Policy Editor

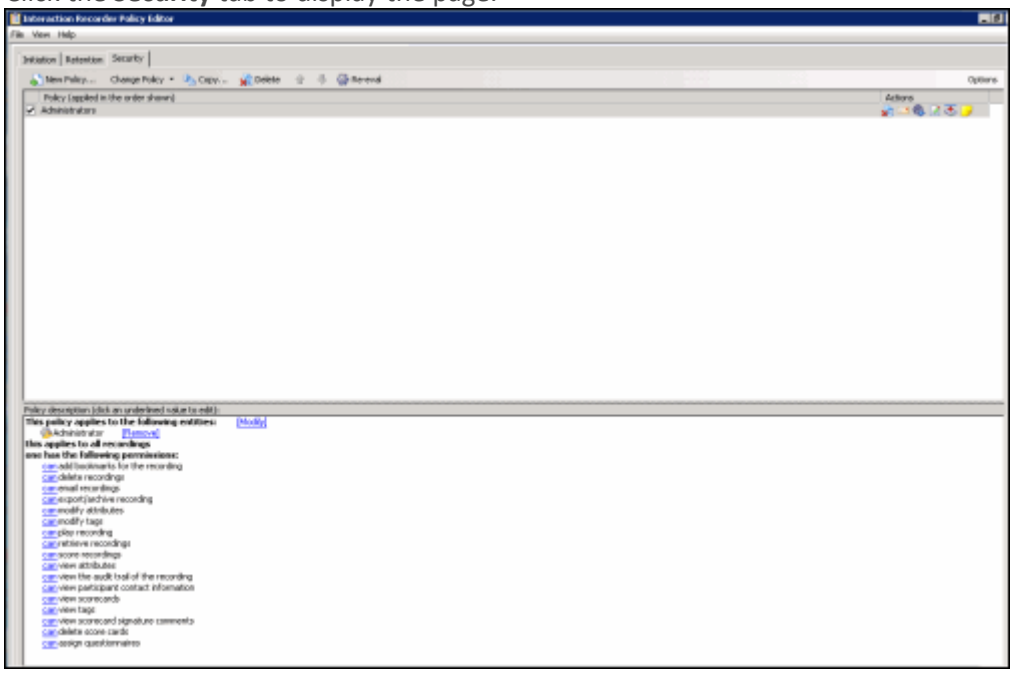
1. From **Interaction Administrator** under **Interaction Recorder**, click **Policy Editor**.
2. In the **Policy Editor** pane, double-click **Configuration**.



3. The **Interaction Recorder Policy Editor** dialog is displayed.



4. Click the **Security** tab to display the page.



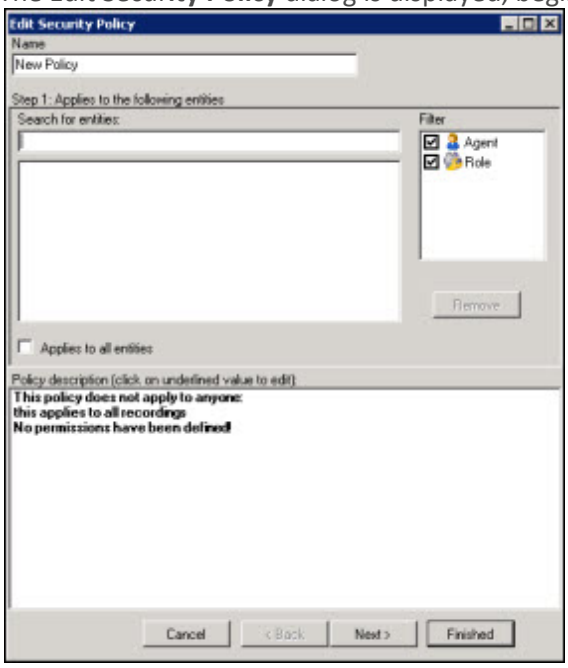
The Security page is displayed, showing the **Administrators** Security Policy. The Administrators security policy is provided, giving all Security permissions to users who are assigned the Administrator Role.

Create a New Security Policy

To create a new Security Policy, on the Security page toolbar, click New Policy 

.

The Edit Secur**ity Policy** dialog is displayed, beginning with **Step 1**.



Step 1: Applies to the following entities

Use this page of the **Edit Security Policy** dialog to apply the policy to entities. You can assign the following entities:

- Agent
- Role

Applying Policies to Entities

You can apply this policy to all available entities *or* you can select specific entities to apply the policy to.

Apply policy to all entities

To apply this policy to all entities:

1. In the **Name** field, type a descriptive name for the policy.
2. In the **Step 1: Applies to the following entities** box, the **Filter** legend lists the entity types and their icons. To apply this policy to all entities, select the **Applies to all entities** check box.

   In the **Policy description** pane, the entity description, **This policy applies to everyone** is displayed.

Apply policy to specific entities

To apply this policy to specific entities:

1. In the **Name** field, type a descriptive name for the policy.
2. Be sure the **Applies to all entities** check box is clear.

3. In the **Step 1: Applies to the following entities** box, the **Filter** legend lists the entity types and their icons, **Agent** and **Role**. To reduce the number of entities returned in the search results, clear the check boxes for the entities you do not want to include in the search. For example, if you know the entity you are searching is a Role, clear the Agent check box.
4. To apply this policy to specific entities, click in the **Search for entities** field.
5. In the **Search for entities** field, begin typing an entity name, for example the name of an **Agent** or **Role**. Entity names that match are displayed in a pop-up window. Note that the entity type icon is displayed next to the entity name.
6. In the pop-up window, click the entity to apply this policy to. The entity is displayed in the entity list box.

   In the **Policy description** pane, the entity is added below the **This policy applies to the following entities** descriptor.
7. Continue adding entities using the **Search for entities** field.

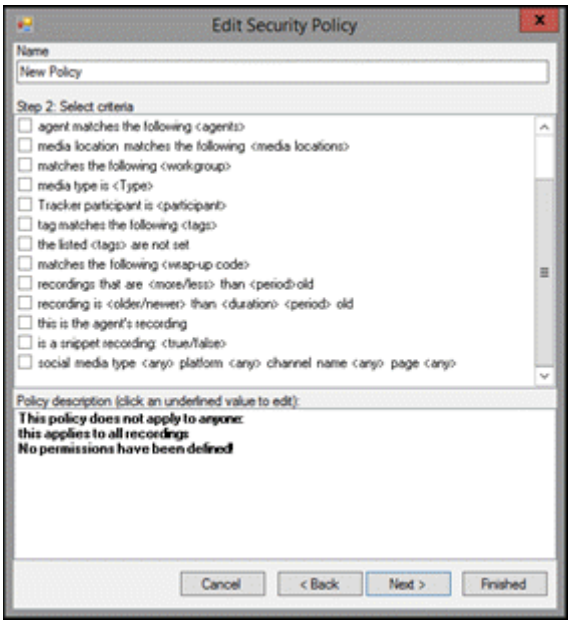
Removing Entities from a Policy

To remove an entity from this policy, from the entity list box, select an entity and click **Remove**. The entity is removed from the list box and also removed from the policy descriptor **This policy applies to the following entities** in the **Policy description** pane.

Completing applying entities

The **Policy description** pane is updated as Security Policy settings are added and updated.

When the **Policy description** for applying Security Policies to entities is complete, click **Next**. The **Edit Security Policy** dialog, **Step 2: Select criteria** is displayed.



Step 2: Select criteria

Use this page of the **Edit Security Policy** dialog to select criteria for applying this security policy to specific recordings.

The criteria that can be selected to apply this policy to recordings are:

- <attribute> contains the value <value>
- the listed <attributes> are not set
- recordings between <start date> and <end date>
- agent matches the following <agents>
- media location matches the following <media locations>
- matches the following <workgroup>
- media type is <Type>
- Tracker participant is <participant>
- tag matches the following <tags>
- the listed <tags> are not set
- matches the following <wrapup code>
- recordings that are <more/less> than <period> old
- recording is <older/newer> than <duration> <period> old
- this is the agent's recording
- is a snippet recording: <true/false>
- social media type <any> platform <any> channel name <any> page <any>

Note If no criteria are selected, the policy applies to all recordings.

Selecting Criteria for Recordings

Select the criteria for recordings, for this security policy, in the **Step 2: Select criteria** box.

To select criteria for interaction recordings:

1. In the **Step 2: Select criteria** box, select the check box for the criteria to use for applying security settings to recorded interactions.

   In the **Policy description** pane, the criteria is added below the **if the interaction meets the following criteria** descriptor.

2. In the **Policy description** pane, configure the criteria by clicking the variable. When you click a variable, a pop-up window is displayed to enter a value for the variable.

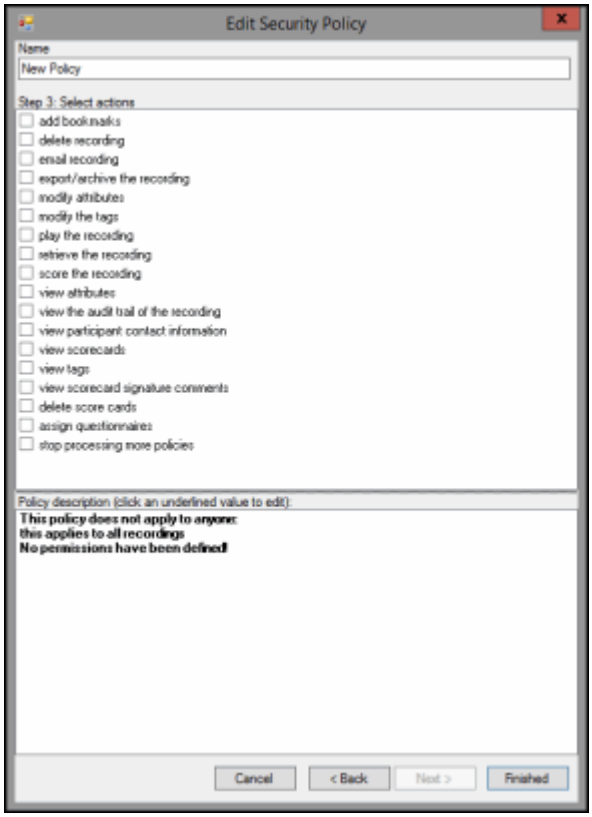
   Note When configuring a variable, to view a table with descriptions for the Criteria values, press F1 to display the Help.

3. Continue selecting criteria check boxes and configuring them in the **Policy description** pane.

Completing Criteria Selection

When you have completed configuring the criteria settings, verify that the criteria you want for applying security settings to recorded interactions are listed in the **Policy description** pane under the **if the interaction meets the following criteria** descriptor. Also be sure that the value for each criterion is configured.

After you have verified your selections, click **Next**. The **Edit Security Policy** dialog, **Step 3: Select actions** is displayed.



Step 3: Select actions

Use this page of the **Edit Security Policy** dialog to select **Actions** for user security permissions for this policy. Actions define how a Policy executes. If an action is not defined for a security Policy, a warning message is displayed when you are creating the Policy. If no actions are defined for a Policy, an **ERROR** message is displayed in the Policy Editor status bar.

Available actions for this Security Policy are:

- add bookmarks
- delete recording
- email recording
- export/archive the recording
- modify attributes
- modify the tags

- play the recording
- retrieve the recording
- score the recording
- view attributes
- view the audit trail of the recording
- view participant contact information
- view scorecards
- view tags
- view scorecard signature comments
- delete scorecards
- assign questionnaires
- stop processing more policies

Selecting Actions for a Security Policy

Select actions for security permissions to apply to recordings in the **Step 2: Select actions** box.

To select actions to apply to recordings:

1. In the **Step 3: Select actions** box, select the check box for the actions for the security permissions to apply to a recording.

   In the **Policy description** pane, the action is added below the **one has the following permissions** descriptor.

2. If a selected action requires configuring, a variable is displayed in the **Policy description** pane. To configure the value, click the variable and a pop-up window is displayed.

   Note When configuring a variable, to view a table with descriptions for the Criteria values, press F1 to display the Help.

3. Continue selecting action check boxes and configuring them in the **Policy description** pane.

Completing Action Selection

When you have completed configuring the action settings, verify that the actions for security permissions you want for recordings are listed in the **Policy description** pane under the **one has the following permissions** descriptor. Also be sure that the value for each criterion is configured.

After you have verified your selections, click **Finished**. The New Policy name is displayed and selected in the **Policy** pane, and the complete description is displayed in the **Policy description** pane.

Saving a Policy

When you have completed creating a new Security Policy, and there are no errors, click **Apply** to save the Policy. When you click Apply, the Policies are saved and the italics are removed from the name in the Policy list. The changes take effect immediately when the Security Policy is applied.

Next, see Updating a Policy for more information on configuring Policies.

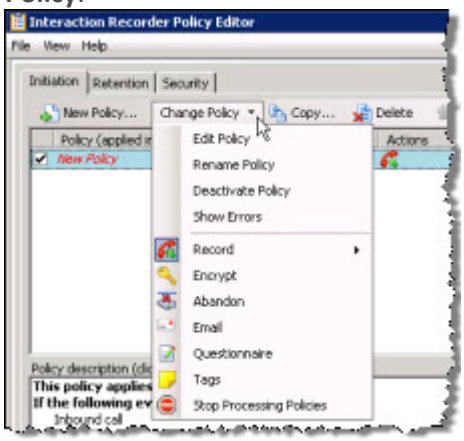
Related Topics

Actions

Security Criteria Descriptions

Updating a Policy

Use the **Change Policy** menu to make updates to a Policy or quickly add Actions to a Policy. To display the Change Policy dialog, in the Policy Pane select a Policy and on the Policy Editor toolbar, click **Change Policy**.



The commands on the **Change Policy** menu allow you to:

- Edit a Policy
- Rename a Policy
- Deactivate a Policy
- Show Policy errors
- Add an Action to a Policy

The Actions on the **Change Policy** menu allow you to add the following Actions to a Policy, based on the Policy Type you are configuring:

- Record
- Encrypt
- Abandon
- E-mail
- Questionnaire
- Tags
- Location

- Retention
- Delete
- Score
- Play
- Retrieve
- Stop Processing Policies

Edit a Policy

To edit a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Edit Policy**. The Edit Policy dialog is displayed.
3. Use the Edit Policy dialog to make your changes.

You can also double-click a Policy in the Policy pane to display the Edit Policy dialog.

Rename a Policy

To rename a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Rename Policy**. The Rename Policy dialog is displayed.
3. In the name field, type your new name, and click **OK**.

Deactivate/Activate a Policy

To Deactivate a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Deactivate Policy**. In the Policy pane, the check box for the Policy is cleared.

You can also deactivate a Policy by clicking the selected check box in the Policy pane. The check is cleared and the Policy is deactivated.

To Activate a Policy:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Activate Policy**. In the Policy pane, the check box for the Policy is selected.

You can also activate a Policy by selecting the Policy check box in the Policy pane.

Show Errors

When there are errors in a Policy, to display the errors:

1. Select the Policy in the Policy pane, and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu click **Show Errors**. A window is displayed listing the **Type** of error and an explanation of the error.

> You can also display the errors for a Policy by right-clicking the Policy and on the shortcut menu click **Show Errors**.

Adding Actions to a Policy

To quickly add Actions to an existing Policy:

1. Select the Policy in the Policy pane and click **Change Policy**. The Change Policy menu is displayed.
2. On the Change Policy menu, select an Action to apply to the Policy.

When you have completed updating a Policy, and there are no errors, click **Apply** to save the Policy. When you click Apply, the Policies are saved and the italic is removed from the name in the Policy list. When updating Security Policies, the changes take effect immediately when the Security Policy is applied.

Related Help

For additional information on updating policies, including using the toolbar buttons, see the Help for:

Interaction Recorder Policy Editor Initiation page

Interaction Recorder Policy Editor Retention page

Interaction Recorder Policy Editor Security page

Security Criteria Descriptions

When selecting criteria and configuring variables for Security policies, refer to the following tables for descriptions of criteria and variable values.

Security Policy Step 2 Criteria Descriptions

The following table describes the details for configuring variables when setting criteria values in the **Policy description** pane. Variables are configured in a pop-up window when you click the variable below the **if the interaction meets the following criteria** descriptor. The following criteria appear in the Policy description pane when the criterion is selected.

Criteria for Step 2: Select Criteria	
Criterion	**Description**

<attribute> contains the value, **<value>**	**Attribute**	Configure the **attribute** variable to select which recordings apply to this security policy. In the **Edit Attribute** pop-up window, use the drop-down list to select a custom attribute to configure for this criterion.
	Value	In the **Edit Value** pop-up window, enter a value for the attribute selected for this criterion.
	To add additional attributes and values for this criterion, click **[Add]**. To remove an attribute and value for this criterion, click **[Remove]**.	
the following attributes are not set **<Attribs>**	**Attribs**	Configure the **Attribs** variable to select which recordings apply to this policy when a custom attribute is not set. In the **Attributes Editor** pop-up window, use the **Enter an attribute** drop-down list to select a custom attribute, and then click **Add**. The attribute is added to the attribute list. To remove an attribute from the list, select the attribute in the list and click **Remove**.
recordings between **<start date>** and **<end date>**	Configure the variables for this criterion to select which recordings, within a date range, apply to this security policy.	
	start date	In the **Date Editor** pop-up window, select a start date from the drop-down calendar.
	end date	In the **Date Editor** pop-up window, select an end date from the drop-down calendar.
agent matches one of the following **[Modify]**	Configure this variable to select which agents' recordings to apply this security policy to. In the **Select Entities** pop-up window, begin typing an agent name in the **Search for agents** box. Agent names that match are displayed in a pop-up window. When you select an agent in the pop-up, it is added to the agent list.	
media location matches the following **<media locations>**	Configure this variable to apply this security policy to recordings that are located in a specific folder. In the **Select Folder** pop-up window, select a folder from the drop-down list. You can also browse for a folder using the ellipsis button.	
matches following **<workgroup>**	Configure the **<workgroup>** variable to select which workgroups' recordings to apply this security policy to. In the **Select Entities** pop-up window, begin typing a workgroup name in the **Search for workgroups** box. Workgroup names that	

	match are displayed in a pop-up window. When you select a workgroup in the pop-up, it is added to the workgroup list.	
media type is <**media type**>	Configure this variable to apply this security policy to recordings with specific media types. In the Select **Media type** pop-up window, select the media type. Multiple media types can be selected. The available media types are: **Call**, **Chat**, **Chat Transcript, Email**, **Screen, Social Conversation,** and **Social Direct Message**.	
matches one of the following Tracker participants **[Modify]**	Configure this variable to select which Tracker participants' recordings to apply this security policy to. In the **Select Entities** pop-up window. A **Filter** legend lists the remote party types and their icons. To reduce the number of entities returned in the search results, clear the check boxes for the entities you do not want to include in the search. Begin typing a name in the **Search for remote parties** box. Names that match are displayed in a pop-up window. Note that the remote party type icon is displayed next to the remote party name. When you select a remote party in the pop-up, it is added to the remote parties list.	
tag matches the following **<Tags>**	**Tags**	Configure the **<Tags>** variable to select Tags, which are associated with recordings, that you want to apply this security policy to. In the **Tags Editor** pop-up window, in the **Enter a tag** box, type or select a tag name, and click **Add** to include the name in the Tags Editor list. All the tags created in the **Tags Editor** list are displayed in the Policy description pane.
the following tags are not set **<Tags>**	**Tags**	Configure this variable to apply this security policy to recordings that *do not* have these tags associated with them. In the **Tags Editor** pop-up window, in the **Enter a tag** box, type or select a tag name, and click **Add** to include the name in the Tags Editor list. All the tags created in the **Tags Editor** list are displayed in the Policy description pane.
recordings that are **older than today**	Configure the variable for this criterion to select which recordings, within a date range, apply to this security policy.	
	older than	To configure the first part of this setting, in the **Select Date Range** pop-up window, in the drop-down list, select either **older than** or **within.**
	today	To configure the second part of this setting, in the drop-down list select period of time. The

		available options are: **today**, **this week**, **this month**, **this quarter**, **this year**.
wrapup code is **<wrapup codes>**	Configure the variable for this criterion to select which wrap-up codes apply to this security policy. In the **Select Wrapup Codes** pop-up window, select the wrap-up codes to apply to this security policy.	
Recording is **older than 0** day old	Configure the variables for this criterion to select which recordings are within or older than the specified period of time. In the **Compare Recording Age** first drop-down list, select **older than** or **within**. In the next box, type a number for the period of time. In the last drop-down list, select the period of time. The options are: **Hour**, **Day**, **Week**, **Month**, or **Year**.	
this is the agent's recording	Select this check box if you want to control which actions an agent can perform on his or her own recordings.	
is a snippet recording: **false**	Configure the variable for this criterion to apply this security policy for snippet recordings. To apply the policy to snippet recordings, click the variable and toggle to **true**.	
social media type <any> platform <any> channel name <any> page <any>	Select the value for Social Media: **type**, **platform**, **channel name**, or **page**. For social media **type**, the values are: **Any**, **Conversation**, or **Direct Message**. For Social Media **platform**, the values are: **Any**, **Facebook**, or **Twitter**. For social media **channel name**, specify the social media channel configuration value or leave the field empty for any channel configuration. For social media **page**, specify the social media page configuration value or leave the field empty for any page configuration. **Note:** The social media **page** value is only available for Facebook, and it is limited to the standard 75 characters. If Twitter platform is selected, the page value is Not Available. For more information, see the *Social Media Technical Reference* in the PureConnect Documentation Library.	

Security Policy Step 3 Action Descriptions

The following table describes the details for configuring variables when setting action values in the **Policy description** pane. Variables are configured in a pop-up window when you click the variable below the **one has the following permissions** descriptor. The following criteria appear in the Policy description pane when the action is selected.

Actions for Step 3: Select actions	
Action	**Description**
can add bookmarks for the recording	Configure this action to allow specific users to add bookmarks to a recording. Use the **can** toggle variable to allow or deny users permission to add bookmarks to a recording by selecting **can** or **can NOT**.
can delete recordings	Configure this action to allow specific users to delete recordings. Use the **can** toggle variable to allow or deny users permission to delete recordings by selecting **can** or **can NOT**.
can email recordings	Configure this action to allow specific users to e-mail recordings. Use the **can** toggle variable to allow or deny users permission to e-mail recordings by selecting **can** or **can NOT**.
can export/archive recording	Configure this action to allow specific users to export a recording. Use the **can** toggle variable to allow or deny users permission to export or archive a recording by selecting **can** or **can NOT**.
can modify attributes	Configure this action to allow specific users to modify attributes of a recording. Use the **can** toggle variable to allow or deny users permission to modify attributes of a recording by selecting **can** or **can NOT**.
can modify tags	Configure this action to allow specific users to modify tags of a recording. Use the **can** toggle variable to allow or deny users permission to modify tags of a recording by selecting **can** or **can NOT**.
can play recording	Configure this action to allow specific users to play a recording.

	Use the **can** toggle variable to allow or deny users permission to play a recording by selecting **can** or **can NOT**.
can retrieve recordings	Configure this action to allow specific users to retrieve recordings. Use the **can** toggle variable to allow or deny users permission to retrieve recordings by selecting **can** or **can NOT**.
can score recordings	Configure this action to allow specific users to score recordings. Use the **can** toggle variable to allow or deny users permission to score recordings by selecting **can** or **can NOT**.
can view attributes	Configure this action to allow specific users to view attributes of a recording. Use the **can** toggle variable to allow or deny users permission to view attributes of a recording by selecting **can** or **can NOT**.
can view the audit trail of the recording	Configure this action to allow specific users to view the audit trail of a recording. Use the **can** toggle variable to allow or deny users permission to view the audit trail of a recording by selecting **can** or **can NOT**.
can view participant contact information	Configure this action to allow specific users to view participant contact information for a recording. Use the **can** toggle variable to allow or deny users permission to view participant contact information for a recording by selecting **can** or **can NOT**.
can view scorecards	Configure this action to allow specific users to view scorecards for a recording. Use the **can** toggle variable to allow or deny users permission to view scorecards for a recording by selecting **can** or **can NOT**.
can view tags	Configure this action to allow specific users to view tags of a recording.

	Use the **can** toggle variable to allow or deny users permission to view tags of a recording by selecting **can** or **can NOT**.
can view scorecard signature comments	Configure this action to allow specific users to view scorecard signature comments. Use the **can** toggle variable to allow or deny users permission to view scorecard signature comments by selecting **can** or **can NOT**.
can delete scorecards	Configure this action to allow specific users to delete scorecards. Use the **can** toggle variable to allow or deny users permission to delete scorecards by selecting **can** or **can NOT**.
can assign questionnaires	Configure this action to allow specific users to assign questionnaires. Use the **can** toggle variable to allow or deny users permission to assign questionnaires by selecting **can** or **can NOT**.
stop processing more policies	Add this action to a Policy to stop processing policies that follow it. The order of a policy is set in the Policy pane, using the up and down arrows. A Security Policy with the **stop processing more policies** action only takes effect when *both* the User entities *and* Recording Criteria match the recording being evaluated. If *either* the User entity *or* the recording criteria in the Security policy with the Stop processing more policies action does not match the recording being evaluated, the evaluation of the current recording does not stop, and policy evaluation continues through the remainder of the policies, until stopped.

Related Topics

Creating a Security Policy