Access Review 2.5.2

Administrative Guide

Table of Contents

Introduction

1.1 Purpose

This guide describes administrative usage of ForgeRock AccessReview, including overviews and instructions for administrative tasks occurring within the application, focusing on the Management Dashboard. It is not intended to document end-user processes interacting with administrative tasks described herein.

1.2 Intended Audience

This guide is written for ForgeRock AccessReview administrators performing actions in certification campaigns and Segregation-of-Duty (SOD) violation processes.

2 Installation

2.1 Provided Files

The installer is provided in the AReview-2.5.2.zip archive. The top-level directory contains the following files and directories:

- **install.sh**: Linux installer
- **install.bat**: Windows installer
- **governance.groovy**: Common installer, invoked by both Linux and Windows installers
- **governance.properties**: Properties file that can be used in place of interactive input with the installers
- **openidm**: Files to be installed in the IDM home directory. These files include configuration files, scripts, workflows, CLI tools, user interface configuration and file fragments that will be injected into existing files.

2.2 Installation Instructions

IDM must be started prior to running the installer

1. Unzip the AReview-2.5.2.zip to a temporary directory then navigate to the directory that was unzipped

2. Run the following command to initiate the installer:

For Windows:
install.bat [--properties filename | -p filename]

For Linux:
./install.sh [--properties filename | -p filename]

The command can be run with the following optional argument:

- **--properties or –p <location/of/properties/file>:** Provides a properties file for script input. If no properties file is specified, the user must input the following properties at run time.

The following input is used for the installer:

- **openidm_location**: File location of IDM home directory
- **project_location**: File location of IDM project directory, if used. *This is an optional property that will default to the openidm_location if left blank.*
- **ldg_installer_location:** *Location where the installer is being run from*
- **openidm_url**: URL where IDM can be reached. *This will often be the localhost.*
- **openidm_version**: The version of IDM. *This will either be 5.0, 5.5, 6.0, or 6.5*
- **openidm_admin**: User ID for user with openidm-admin role
- **openidm_admin_password**: Password for IDM administrator
- **openidm_database_type**: 'MsSQL' or 'MySQL' only for ForgeRock AccessReview 2.5.1

Note: Names are those found in the properties file. If a properties file is not used, equivalent input will be gathered directly from the installer.

The installer will print updates to the console until successful completion

3. After installation completes, the IDM server must be restarted

4. Enable Audit Event Handler: repo

    a. Log into IDM as an IDM administrator
    b. Navigate to the Admin View
    c. Click on Configure System Preferences
    d. Under the Event Handlers section of the Audit tab, click edit for the RepositoryAuditEventHandler

e. Click Enabled
f. Click Submit
g. Click Save

2.3 Clustered Environment

Currently, the installer script can only be run once per environment. In a clustered environment, manual steps will need to be taken to copy over artifacts to subsequent nodes once the installer has run on the initial node. The following requires replication on each node after the first:

1. Copy the following files from the installer zip into the IDM installation directory:
    a. Everything in the ./openidm/script directory, copied into the script directory of the installation
    b. Everything in the ./openidm/conf directory, copied into the conf directory of the installation
    c. Everything in the ./openidm/workflow directory, copied into the workflow directory of the installation
    d. Everything in the ./openidm/tools directory, copied into the tools directory of the installation
    e. Everything in the ./openidm/bundle directory, copied into the bundle directory of the installation
    f. The entire ./openidm/governance directory, copied into the openidm installation directory
    g. The entire ./legal-notices directory, copied into the openidm installation directory
2. Copy the following files from the first node's IDM installation directory:
    a. openidm/script/access.js
    b. openidm/conf/managed.json
    c. openidm/conf/repo.jdbc.json
    d. openidm/conf/policy.json
    e. openidm/conf/IDG-queries.json
    f. openidm/bin/defaults/script/ui/onDelete-user-cleanup.js
    g. openidm/ui/admin/default/configAppConfiguration.js
    h. openidm/ui/selfservice/default/configAppConfiguration.js

2.4 Post-Installation Instructions

Additional configuration is needed on each node as described to support the following use cases:

- Event-Driven Certifications

    1. Navigate to openidm/tools/idg directory of the IDM installation
    2. Run the following command to enable event-driven certifications:

       For Windows:
       ./enableEventBasedCerts.bat

       For Linux:
       ./enableEventBasedCerts.sh

    3. You will be prompted for the file location of the IDM home directory. Enter the absolute path.
    4. You will be given the option to choose which types of certifications to enable event-based certifications for:
        a. 1) ALL - This option will enable event-based certifications for all supported certification types listed below
        b. 2) USER - This option will enable event-based certifications for user certs-only. The script will update the user object configuration in the managed.json config file.
        c. 2) ASSIGNMENT - This option will enable event-based certifications for assignment certs-only. The script will update the assignment object configuration in the managed.json config file.

- Reactive Policy Scans:

    1. Navigate to openidm/tools/idg directory of the IDM installation
    2. Run the following command to enable event-driven certifications:

       For Windows:
       ./enableReactiveScans.bat

       For Linux:
       ./enableEventReactiveScans.sh

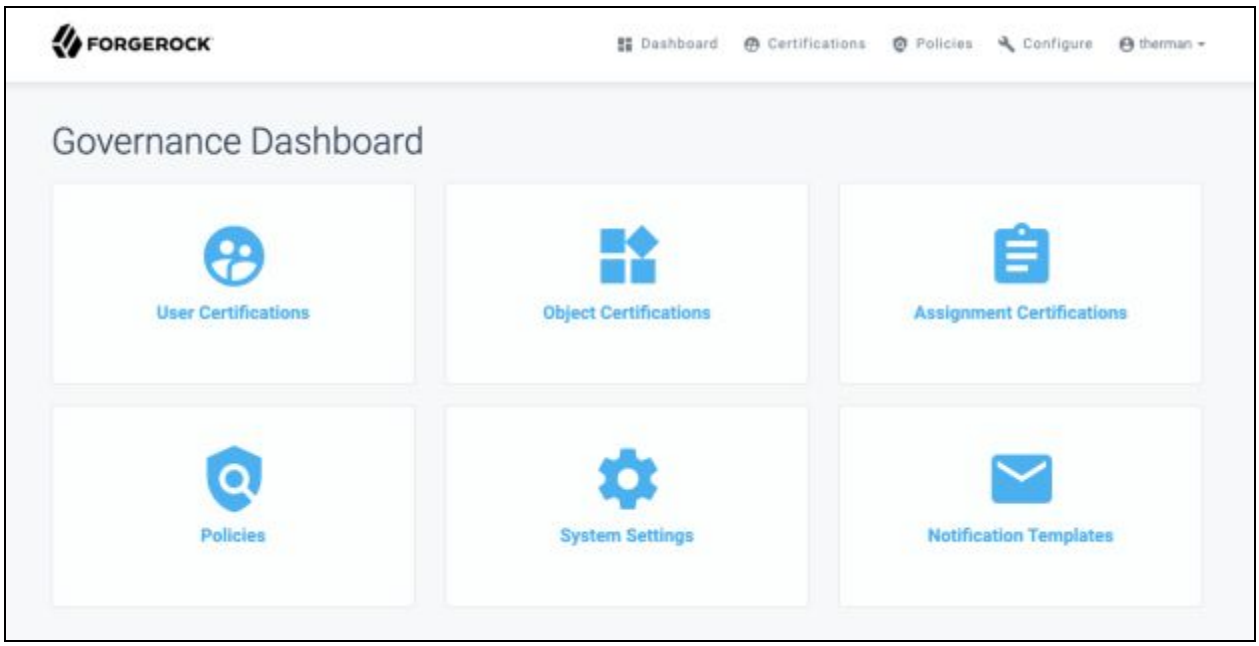
    3. You will be prompted for the file location of the IDM home directory. Enter the absolute path.
    4. The script will update the 'out of the box' script at openidm/bin/defaults/script/role/postOperation-roles.js

- **NOTE**: After installation steps are complete, it is recommended that the installer ZIP and the created installation folders and files be removed from the server.

3 Management Dashboard

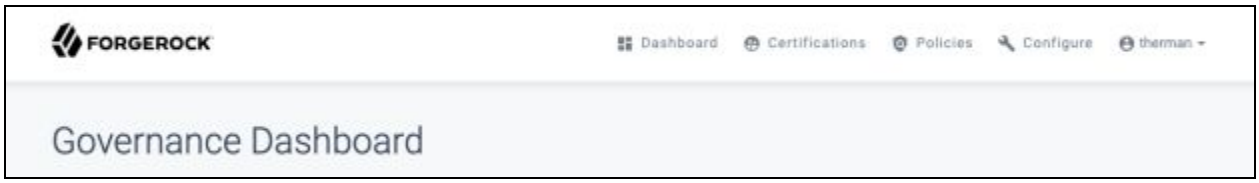
Governance Management Dashboard details the following options for configuration to the administrator:

1. User Certifications
2. Object Certifications
3. Assignment Certifications
4. Policies
5. System Settings
6. Notification Templates



3.1 Navigating to the Management Dashboard

To access the Governance Management Dashboard, log into the Governance Dashboard as a user with the governance-administrator authorization role. Select '**Configure**' in the navigation menu at the top of the screen.



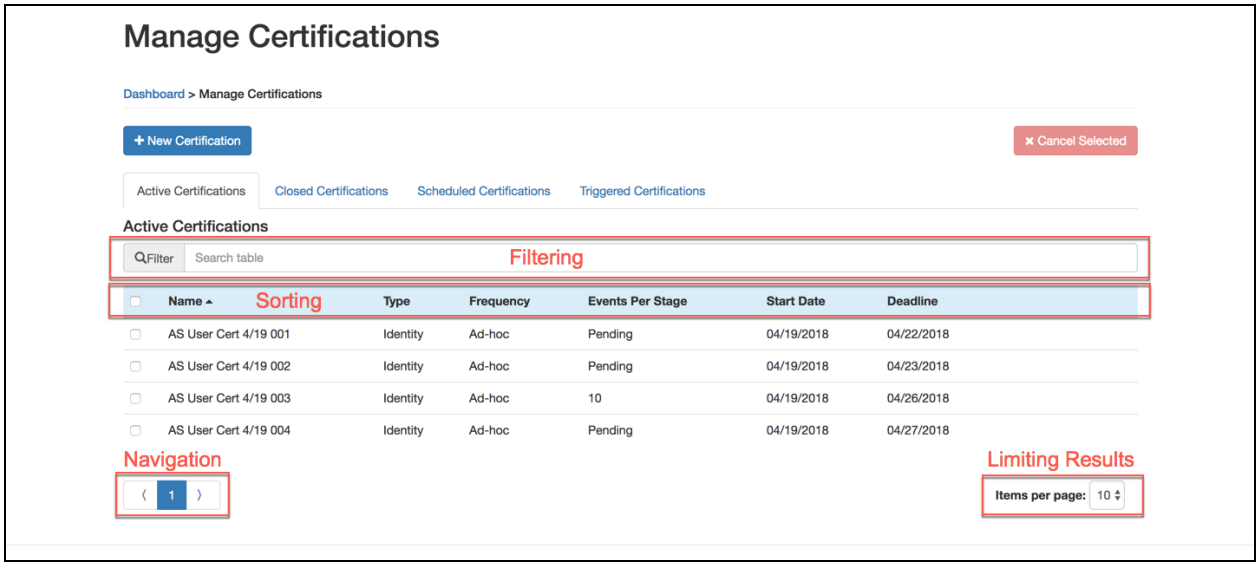
To return to the Governance Dashboard, select '**Dashboard**' from the same menu

3.2 Common Interfaces

The following sections detail functionality common throughout the Identity Governance Management Dashboard

3.2.1 Tables

Throughout the management dashboard, information is often stored in tables with a common set of properties, including the following options:



- **Filtering:** Allows the administrator to filter results in the list. The filter details all rows where matching values exist and updates results as the value are entered.
- **Sorting:** Selecting column headers sorts information in a table

Note: Selecting multiple times adjusts the order from descending to ascending for the field selected

- **Limiting results per page:** (Items per page) Identifies the number of results made visible at a specific time within the table. Values may include 5, 10, 25, 50, 100, 200 or all.
- **Navigating results:** Allows navigation within the table when results exceed the number specified in the field Items per page

3.2.2 Comments

Comments appear throughout review screens for certifications, violations, and exceptions, identifying actions taken against these objects. Once one or more actions have occurred, the following information details the history of events leading up to the current state of an object:

- **Time:** Time an action was taken
- **Action:** Action is taken when evaluating the line item. Values may include 'Comment', 'Revoked' or 'Signed-off'.
- **Username:** Username of user who performed the action
- **Message:** Details comments entered by the user when performing the action

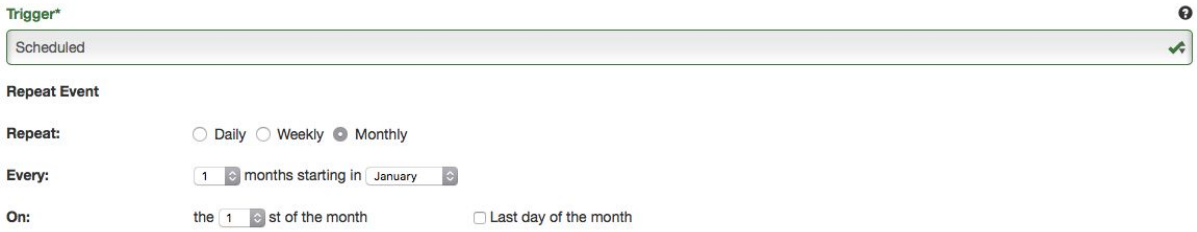
3.2.3 Metadata

Metadata, in the form of glossary entries, can be created for various object and attribute values. Each metadata entry can contain any number of extended attributes, defined independently from other entries. There will be an icon in the row to indicate if such metadata exists for an individual line item in a certification task, allowing the certifier to select to view metadata. In some cases, this metadata may even substitute the value that is displayed to the certifier. Additional information is detailed in Section 9.6.

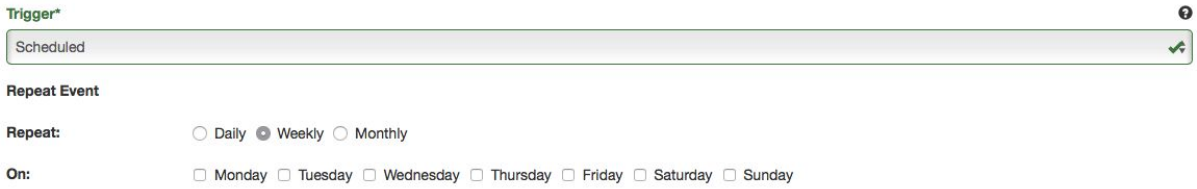
3.2.4 Scheduling Events

Events can be scheduled for generating certifications or running policy scans. To determine the duration between actions, the following options are available:

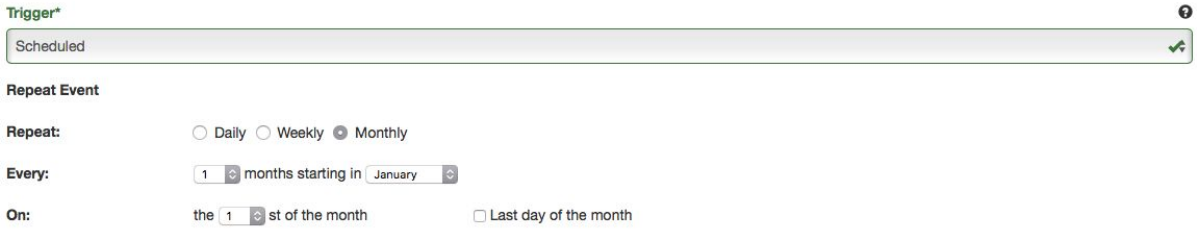
- **Daily:** Allows the administrator to generate a certification every specified number of days, starting on a specified day of the month



- **Weekly:** Allows the administrator to generate a certification on specified days of the week



- **Monthly:** Allows the administrator to generate a certification every specified number of months starting on a specified month. Day of the month for the certification generation can also be specified, with 'Last day of the month' as an option.



3.2.5 Remediation Tasks

Remediation Tasks complete revocations resulting from certifications or violations, including reference to workflow defined in OpenIDM for completion following certification or violation completion. The following workflows are provided with AccessReview; however, it is recommended that these be modified or replaced to adhere to custom policy:

- **None:** Skips automatic remediation to allow manual intervention from an administrator
- **AssignmentRemediation:** (Assignment Certification) Removes attributes revoked during certification from the target assignment
- **ObjectAssignmentRemediation:** (Object Certification) Removes assignments revoked during certification from the target object
- **RevokeResources:** (User Certification) Disables user targeted in the certification if the user was revoked. All applications and attributes assigned to the user revoked during the certification will also be removed.
- **ViolationRevokeResources:** (Violation) Removes any roles or resources that caused the violation to trigger from the user targeted in the violation. If an attribute value caused the violation, it is updated on the user by appending a specified value.

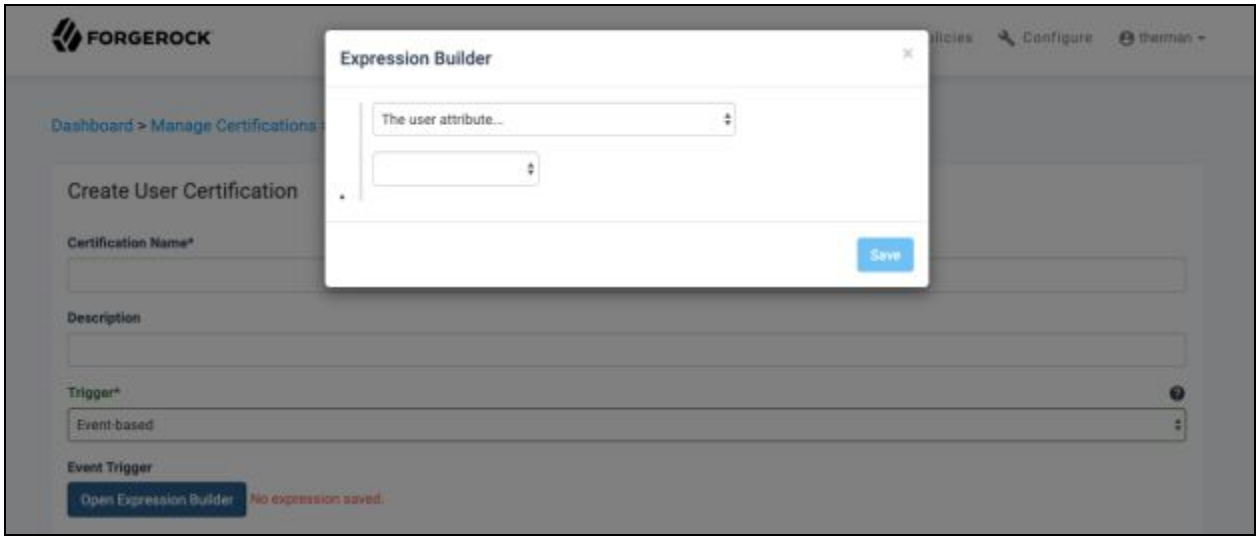
3.2.6 Expression Builder

Expression Builder identifies criteria for filters in certification definitions policy rules. The criteria identify attribute constraints for target users. If a user is otherwise considered for a certification or violation but fails to meet the criteria specified in the Expression Builder, the action against the user is ignored.

To build an expression, select one of the following options: *Each option presents either another tier for additional criteria or identifies an attribute / managed object to serve as a base for the trigger.*

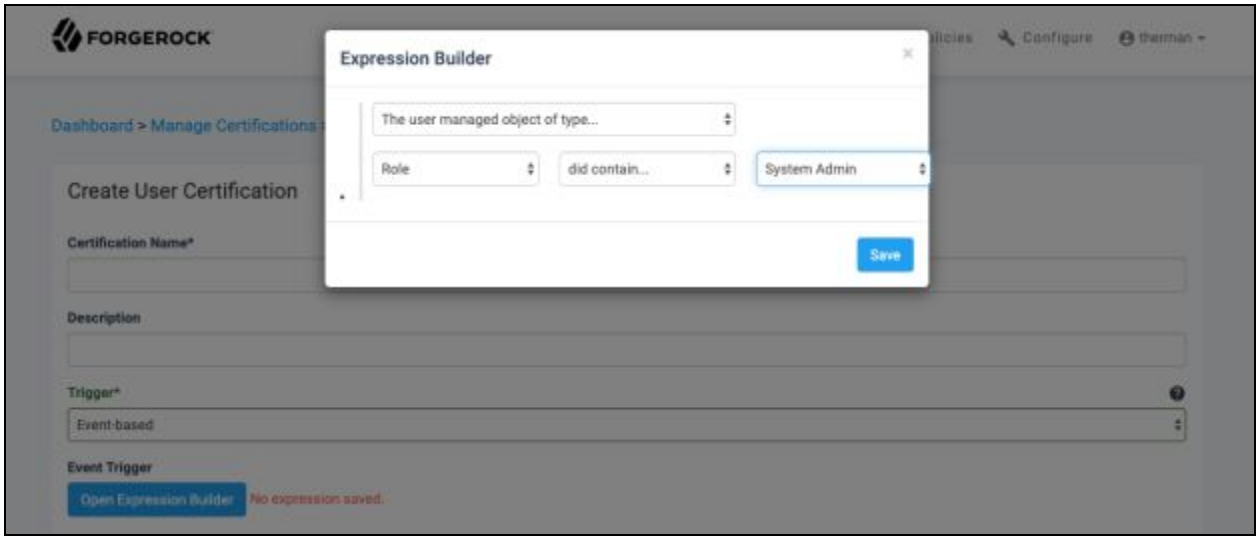
- **The user attribute:** Allows the administrator to specify an attribute and evaluate its value. The administrator can specify whether to evaluate the previous value of the attribute (was), the new value of the attribute (is) or changed state of the attribute (changed). If the conditions are met, certification is generated.

  In the example below, a certification will be generated after a user's 'Username' is updated



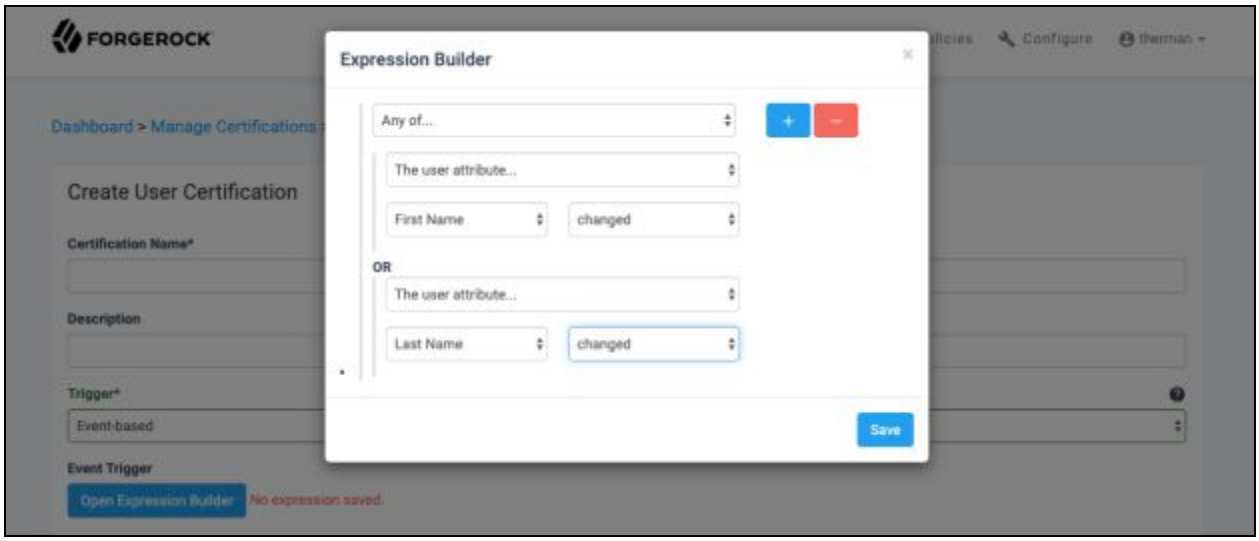
- **The user manage object of type:** Allows the administrator to specify a managed object and evaluate whether a user has been assigned. The administrator can specify the type of object (e.g. Role, Assignment, custom multi-valued attribute), whether the user was assigned the object prior to the transaction (did contain) or is currently assigned the object (does contain) and the value of the object.

A certification will be generated after a user is updated if the user has the Role certification-administrator, as seen in the example below



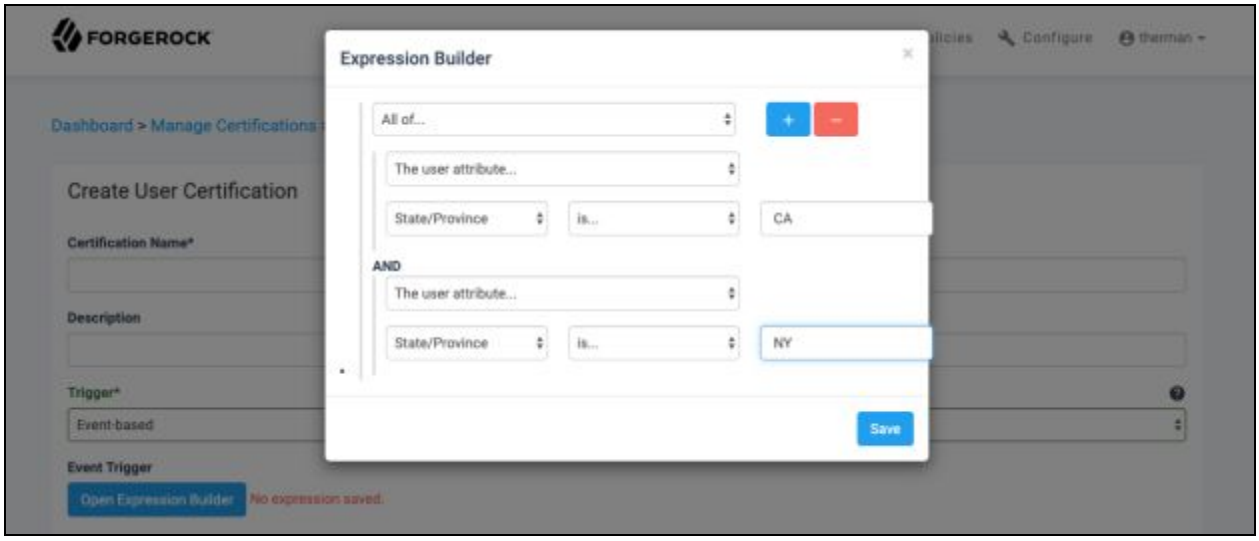
- **Any of:** Allows the administrator to specify multiple expressions concatenated by 'OR' conditions. If any of the contained expressions are true following an update, a certification is generated. Selecting '**+**' appends additional expressions while selecting '**-**' removes expressions from the end.

A certification will be generated after a user's name is updated, as seen in the example below



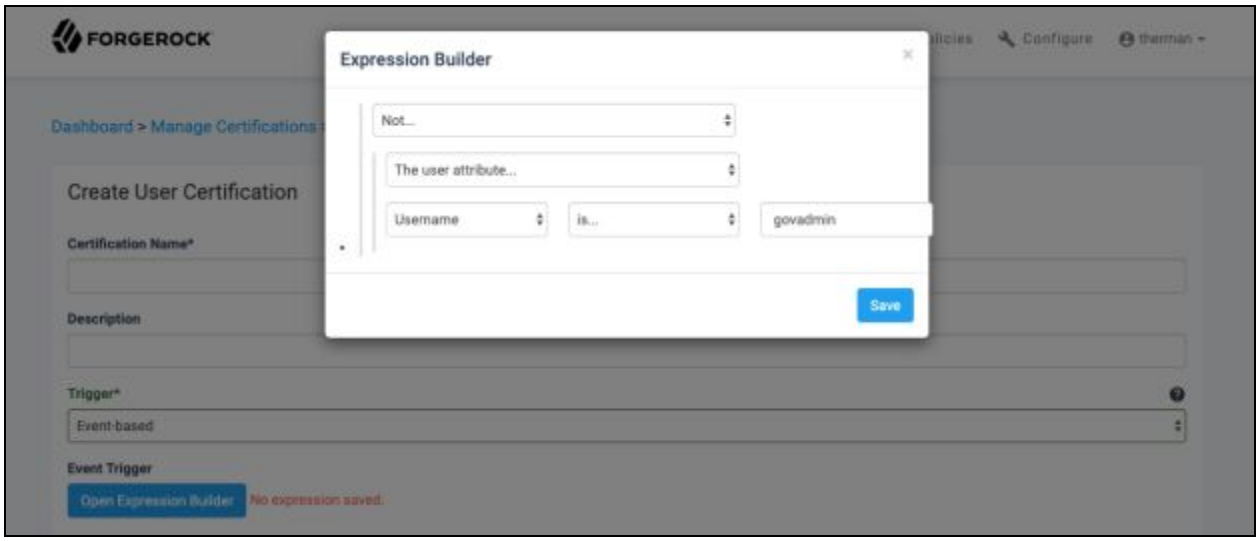
- **All of:** Allows the administrator to specify multiple expressions concatenated by 'AND' conditions. If all of the contained expressions are true following an update, a certification is generated. Selecting '**+**' appends additional expressions while selecting '**-**' removes expressions from the end.

A certification will be generated after a user is updated for relocation, as seen in the example below



- **Not:** Allows the administrator to specify an expression and negate its value. If the contained expression is false following an update, a certification is generated.

  A certification will be generated after a user is updated if their username is not 'govadmin', as seen in the example below



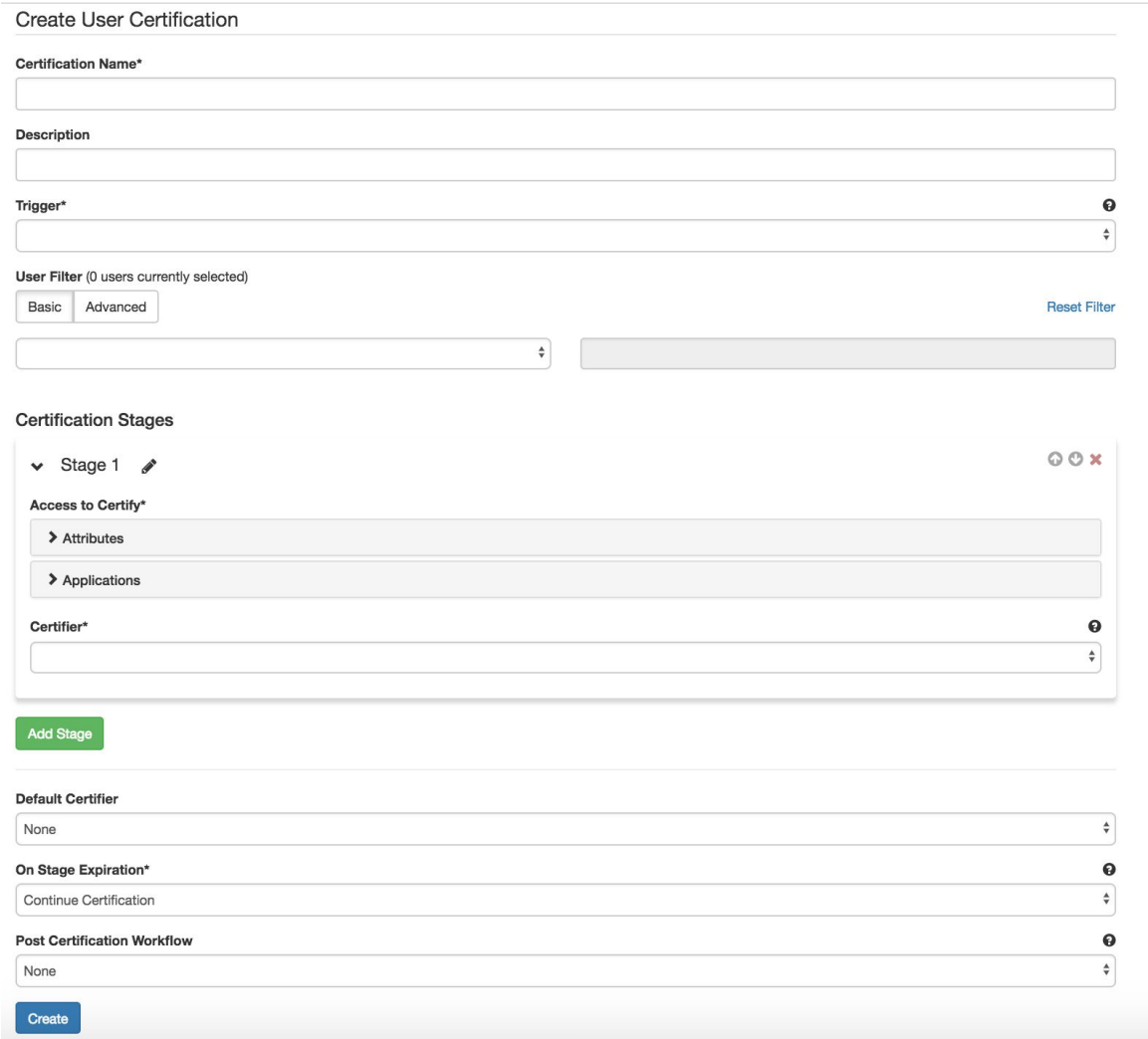
4 User Certifications

User certifications target individual users for certification. Certifications allow one or more certifiers to review a user's attributes and access to applications, as well as sign-off or revoke reviewed objects.

4.1 Creating New Certification Definitions

1. For User Certifications, navigate to Manage Certifications, located in the Management Dashboard under User Certifications

2. From the Manage Certifications page, select '**New Certification**'



3. On the Create Certification page, fill in each of the required fields. Additional details on the available fields are given below:

   - **Certification Name:** *(Required)* Title for the certification that will appear on all summary pages
   - **Description:** Provides additional details about the purpose of the certification for certifiers
   - **Trigger:** *(Required)* Identifies when the certification is created. Options are:
     - **Ad-Hoc:** Generates a new certification immediately after submitting the current form and can only be triggered once
     - **Scheduled:** Generates a new certification each time a specified time duration has passed. When selecting the '**Scheduled**' option, additional fields become available, allowing duration to be specified.

       Note: For more information on scheduling events, refer to section 3.2.4

     - **Event-based:** Generates a certification based upon criteria evaluated when a user's attributes or managed object is updated. After selecting an Event-based trigger, select '**Open Expression Builder**' under Event Trigger to identify the criteria for triggering certification generation.

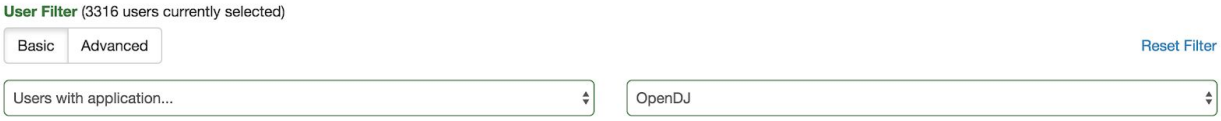
Note: For more information on building expressions, refer to section 3.2.6

- **User Filter:** *(Required)* Identifies filter for limiting the users returned for the certification. The current number of users that are currently targeted by the given expression is displayed next to the 'User Filter' text. The 'Reset Filter' option is available on the right-hand side of the filter, which will restore the filter to its default state. The filter uses the two following categories:

  - **Basic:** Upon selecting, the left dropdown is populated with the following options:

    - **User:** Allows certification to be filtered to a specified user. Upon selecting, the right input box becomes available to enter in a username

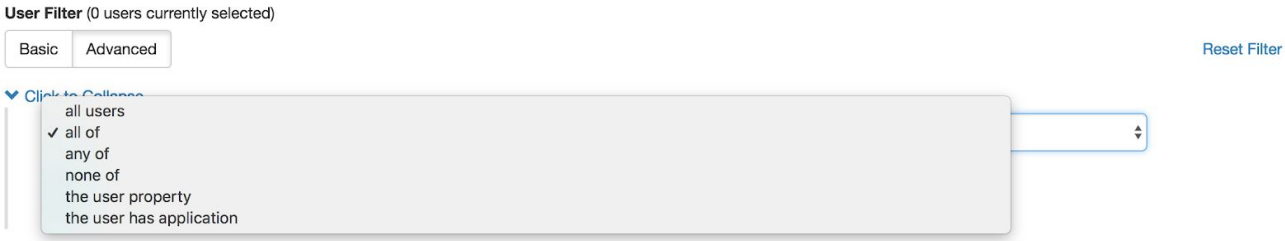
    - **Users with manager:** Allows certification to be filtered to any user with a specified manager. Upon selecting, the right input box becomes available to enter in a username corresponding to the manager.



    - **Users with application:** Allows certification to be filtered to any user assigned to a specified application. Upon selecting, the right select box becomes available to select the name of the connected application.

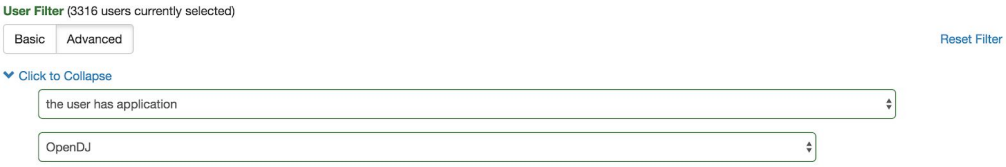
    - **All Users:** Allows certification to be run with no filter and target all users

- **Filter by provisioning/authorization role:** Allows certification to be filtered to any user assigned to a specified instance of either a provisioning role or an authorization role. Upon selecting, the right input box becomes available to enter in the name of the role.

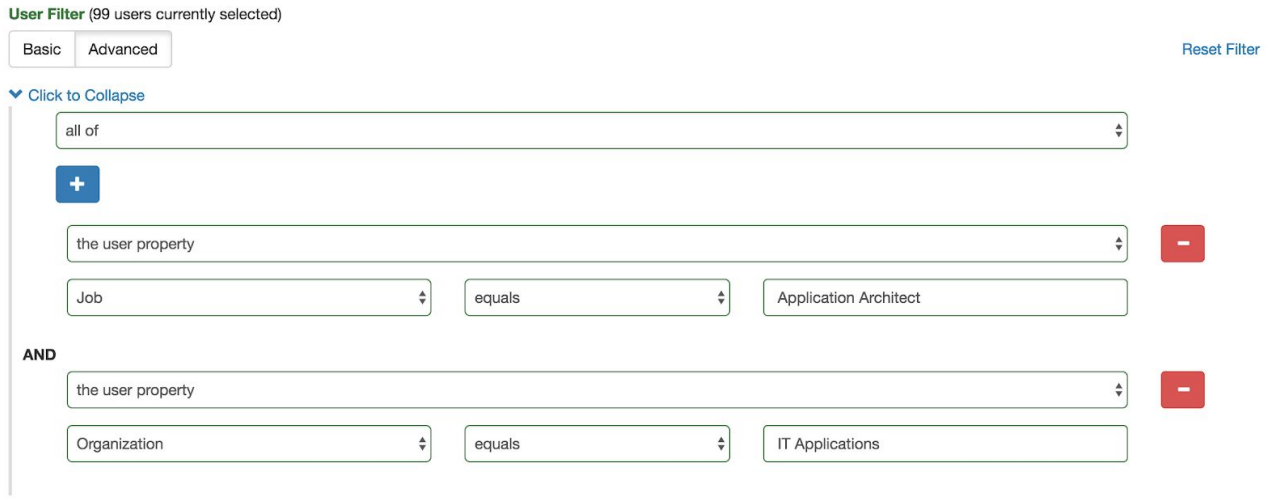


- **Advanced:** Upon selecting, the advanced expression builder is displayed. The top level select box offers the above options for starting an expression.

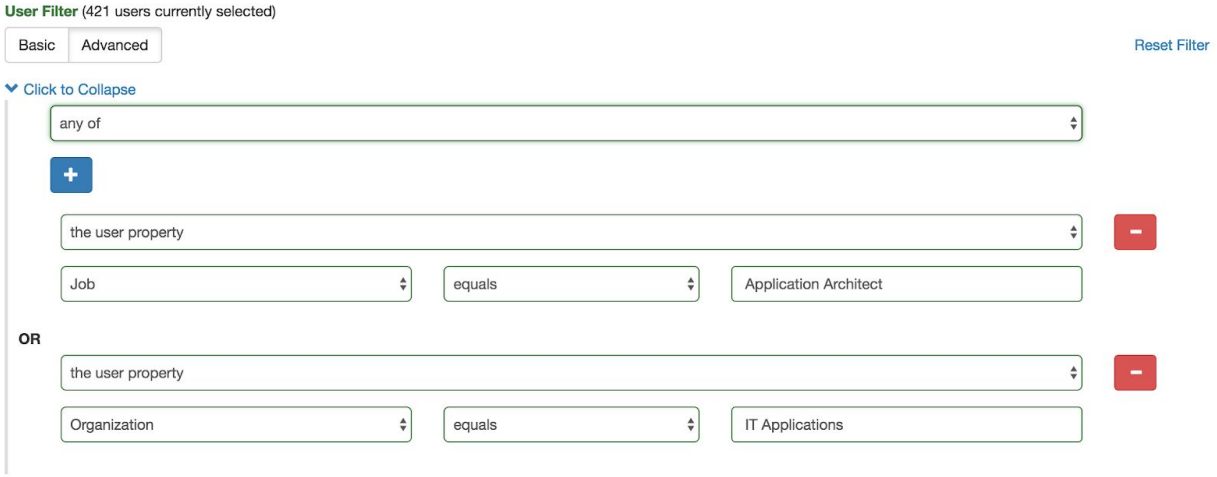
- **User property:** Allows choice of any IDM attribute to be selected in the leftmost input, a modifier (equals, contains…) in the middle input, and value in the right most input.



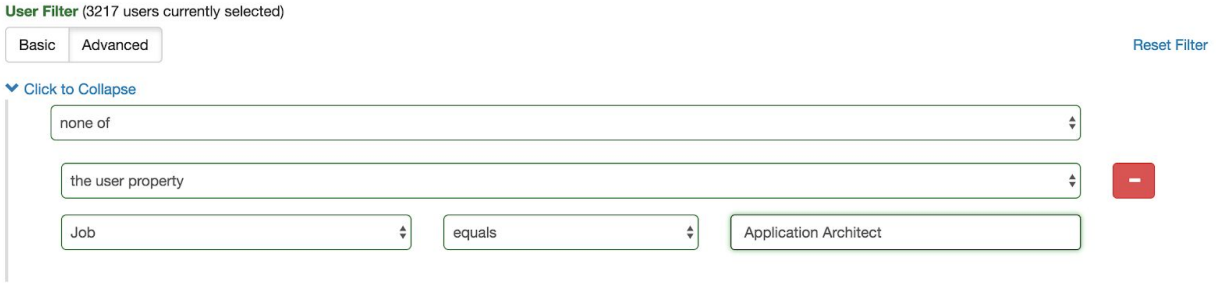
- **User application:** Allows choice of any connected application to be selected from the dropdown menu



- **All of:** Creates a nested level within the expression of which all the following criteria must be satisfied in order to match the filter.



- **Any of:** Creates a nested level within the expression of which any of the following criteria can be satisfied in order to match filter.

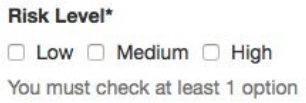


- **None of:** Creates a singleton nested level within the expression for which the negation of the one following criteria is a match for the filter

- **Certification Stages:** A certification may have one or more stages. Each certifier is responsible for one stage, and additional stages may be added as

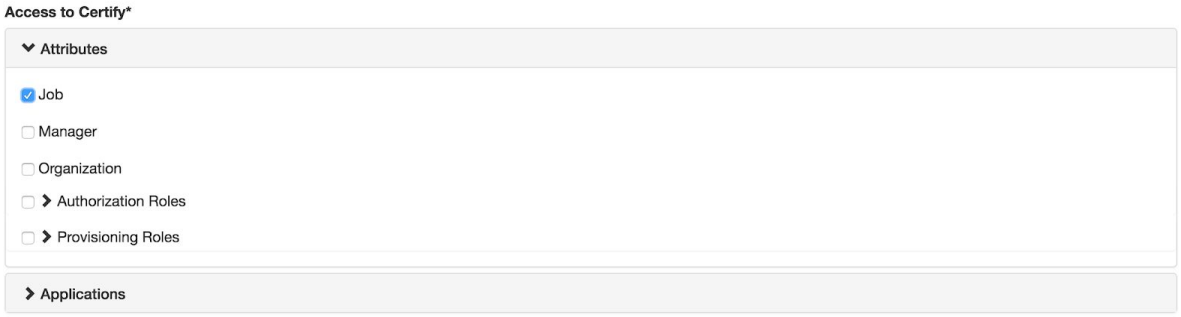
needed (by selecting the 'Add Stage' button.), while selecting. Optionally, stage names may be modified by selecting the pencil icon next to a stage name.

- **Stage icons:**
  - *Up / Down arrows (at the top right of each stage)*: Change the stage order
  - *Red 'X' icon*: remove a specific stage
  - *Caret**: (**at the top left of each stage**)**:* collapse/expand details for a given stage
  - *Pencil icon (to the right of the stage name)*: Rename a specific stage

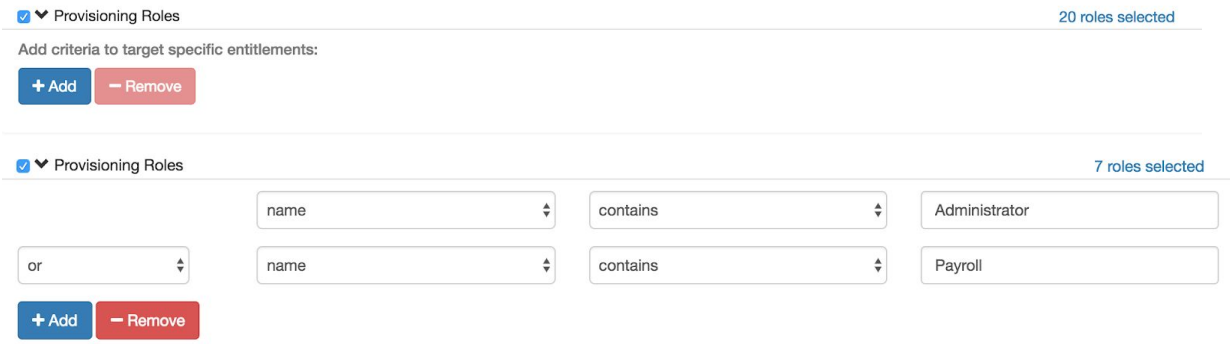


- **Risk Level:** Specifies a filter for the entitlements within the given stage. Only certifications with entitlements that match the specified levels of risk will be generated, with a minimum of one option selected to generate any certifications. Any chosen entitlements within a stage that do NOT have a risk level assigned will not appear in the certification. (Note: Risk Level can be enabled/disabled in settings.)

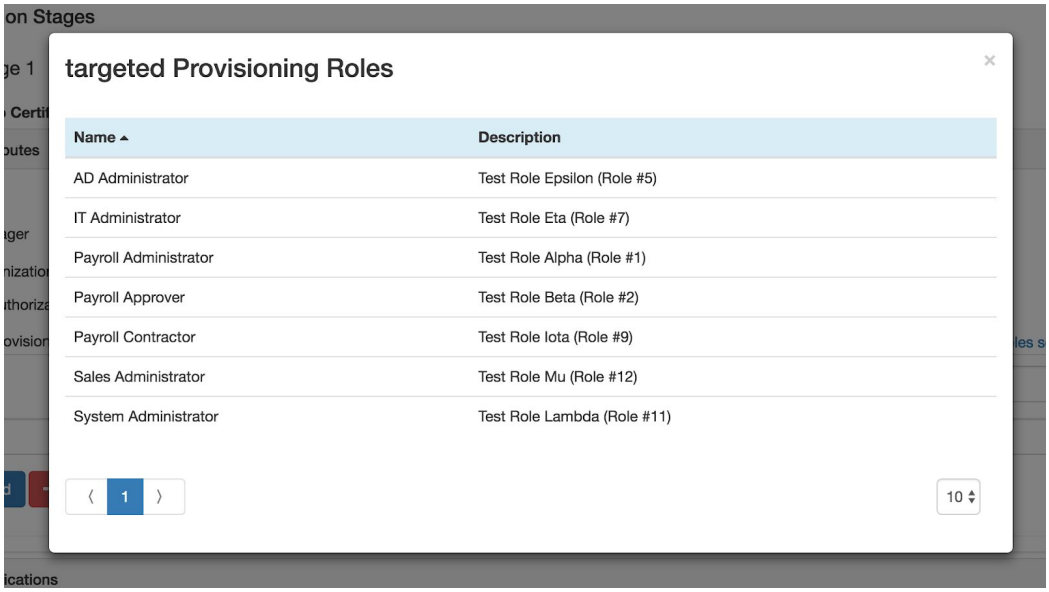
- **Access to Certify:** Specifies the entitlements/access that will appear to certifiers within the given stage. The attributes/applications that appear in these sections correspond to those that are selected as certifiable within the system settings.



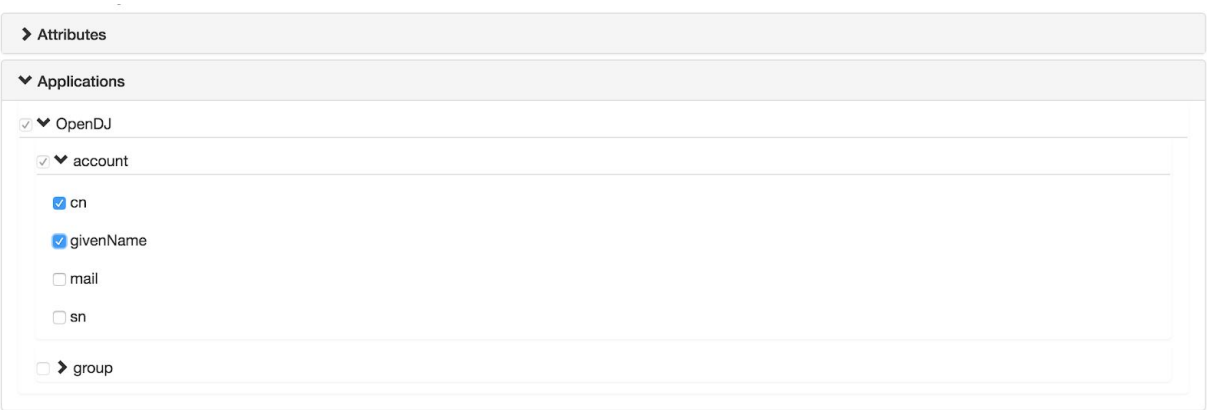
- **Attributes:** The entitlements on the user that are tracked and stored within IDM. Basic attributes and single object relationships are included in a certification stage via a basic checkbox. Multi-valued relationship objects are shown below:



- **Relationships:** When a relationship attribute is selected, add and remove buttons appear below the attribute name, allowing a complex target expression to be built. The number of objects currently selected is displayed to the right. If no expression is specified, all possible options are selected.



  - **Selected Modal:** Clicking on the number of objects currently selected will display the targeted modal, displaying the names and descriptions of the items selected.



- **Applications:** The external applications and user data that is connected to IDM

- **Certifier:** *(Required)* Identifies to whom the certification stage will be assigned once generated, with the following available options:

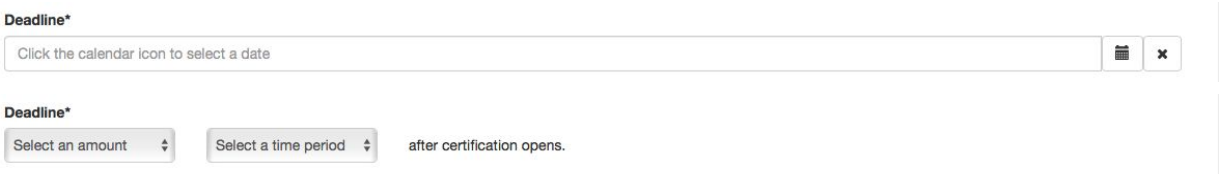
- **User:** *(Required)* User certifier will assign the generated certification stage to a specific user and a single user will certify all targets. When specifying a user, autocomplete will help identify the user login for the assignment.

- **Authorization Role:** *(Required)* Certifier assigns generated certification stage to a group of specified users. All targets will be certified by users with the given authorization role attribute. To specify an authorization role, select an available role in the Authorization Role drop-down menu.

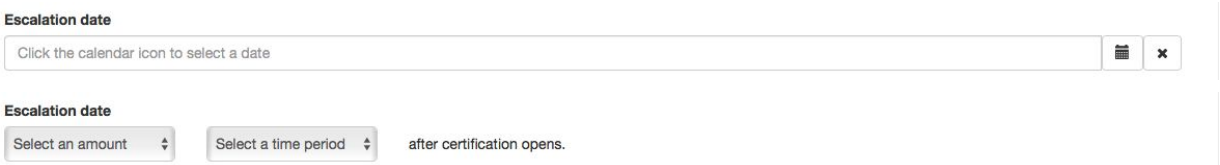
- **User Manager:** Certifier assigns generated certification stage to users designated by the Manager attribute. Their managers will certify all targets.

- **Previous Certifier's Manager:** Certifier assigns generated certification to the manager of the user specified in the preceding stage. *Note that this option will be disabled for the first stage in the sequence, or if the preceding stage has the Certifier field set to 'Authorization Role.'*

- **Entitlement Owner:** Certifier assigns generated certification to the entitlement owner of the included entitlements. The certification targets for the stage will be split among the users/roles who are set as the owner of the entitlement in the AccessReview settings. This option will allow for multiple certifiers to be assigned a subset of entitlements for a given certification within a stage.



- **Deadline:** *(Required)* Specifies how long certification stage should remain active. After the specified date or duration, certification stage will expire. Certification will then either 1) move to the next stage or 2) expire and becomes unavailable for modification, based on which option has been specified for the 'On Stage Expiration' field.



- **Escalation date:** Specifies if / when an escalation should occur prior date specified in the Deadline. After the specified date or duration, notification will be sent to the user / role specified.

Escalation Owner: *(Required)* If specifying an escalation date, the fields become available to specify the escalation user or role to send a notification:

- **User:** Notifies a specified user when an escalation occurs
  Choose User: *(Required)* Identifies a single user to target as escalation owner. The field is open with autocomplete and requires a username.

- **Authorization Role:** Notifies a specified group of users when an escalation occurs
  Authorization Role: *(Required)* Identifies a group of users to target as escalation owner. The field is a dropdown, offering existing authorization roles as options.

- **Certifier Manager:** Notifies the managers of users assigned to the certification

- **Default Certifier:** Specifies a default certifier for the entire campaign. If a default certifier is set, then stage events with no owner will be assigned to that certifier. If no default certifier is set, events with no owner will receive the status 'No Certifier.'

- **On Stage Expiration:** If a stage is not completed before the deadline, the events of that stage will be marked as expired. The 'On Stage Expiration' field determines how the same events in subsequent stages are affected.
  - **Continue Certification:** The expired event(s) will not be affected in the next stage of the campaign; the next certifier will be able to take action as they would normally
  - **Expire Throughout:** The event(s) will be expired for all future stages within the campaign. This will prevent any future certifiers of the campaign to take action on the event.

- **Post Certification Workflow:** Identifies an automated remediation task for handling revocations from the certification

  Note: For more information on remediation tasks, refer to section 3.2.5

4.2 Modifying Certification Definitions

1. For User Certifications, navigate to Manage Certifications, located in the Dashboard Management Dashboard under User Certifications

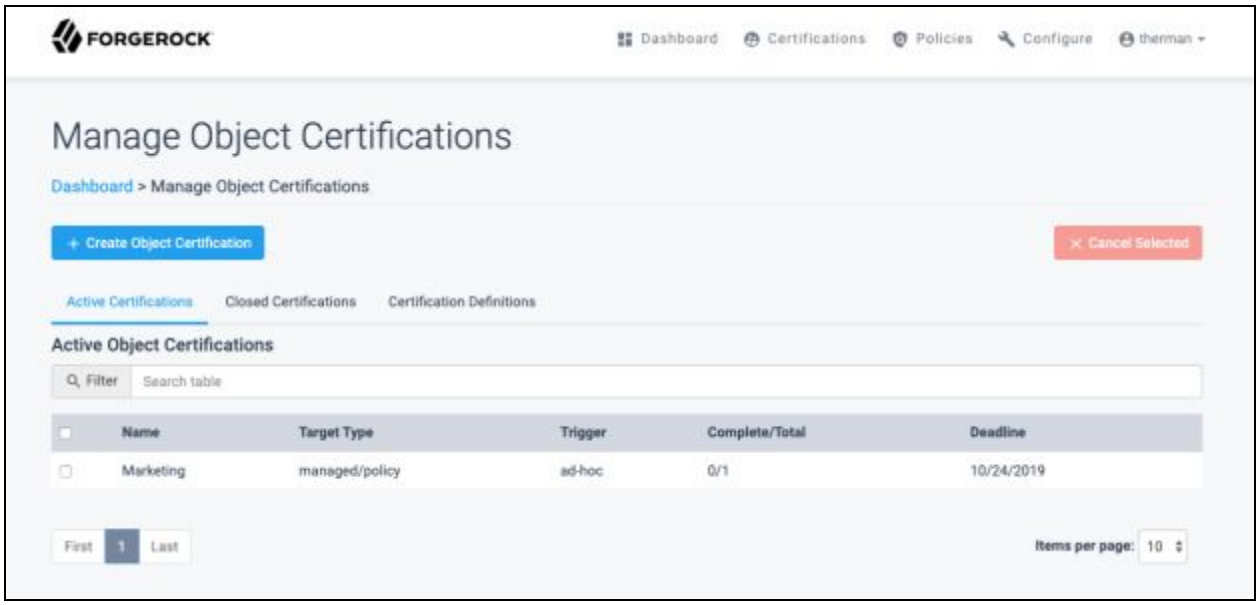
2. View contents under the Scheduled Certification and Triggered Certification tabs
   - **Certification Definitions:** Contains all existing Scheduled or Event-Based certification definitions. Ad-hoc certification definitions cannot be modified. Each line contains a summary of certification definition with the following details:
     - **Delete Selected:** Allows the administrator to delete a certification definition, while not affecting existing certifications. To utilize, select the checkboxes next to the Certification Definitions to delete, then select '**Delete Selected**'.
     - **Name:** Details certification by the name given when creating the Certification Definition
     - **Next Run Date:** *(Scheduled certifications only)* The next date which this campaign is scheduled to run

3. To display additional information about the certification, select a certification definition from the Certification Definitions list (from either the Schedule Certifications or Triggered Certifications tab)

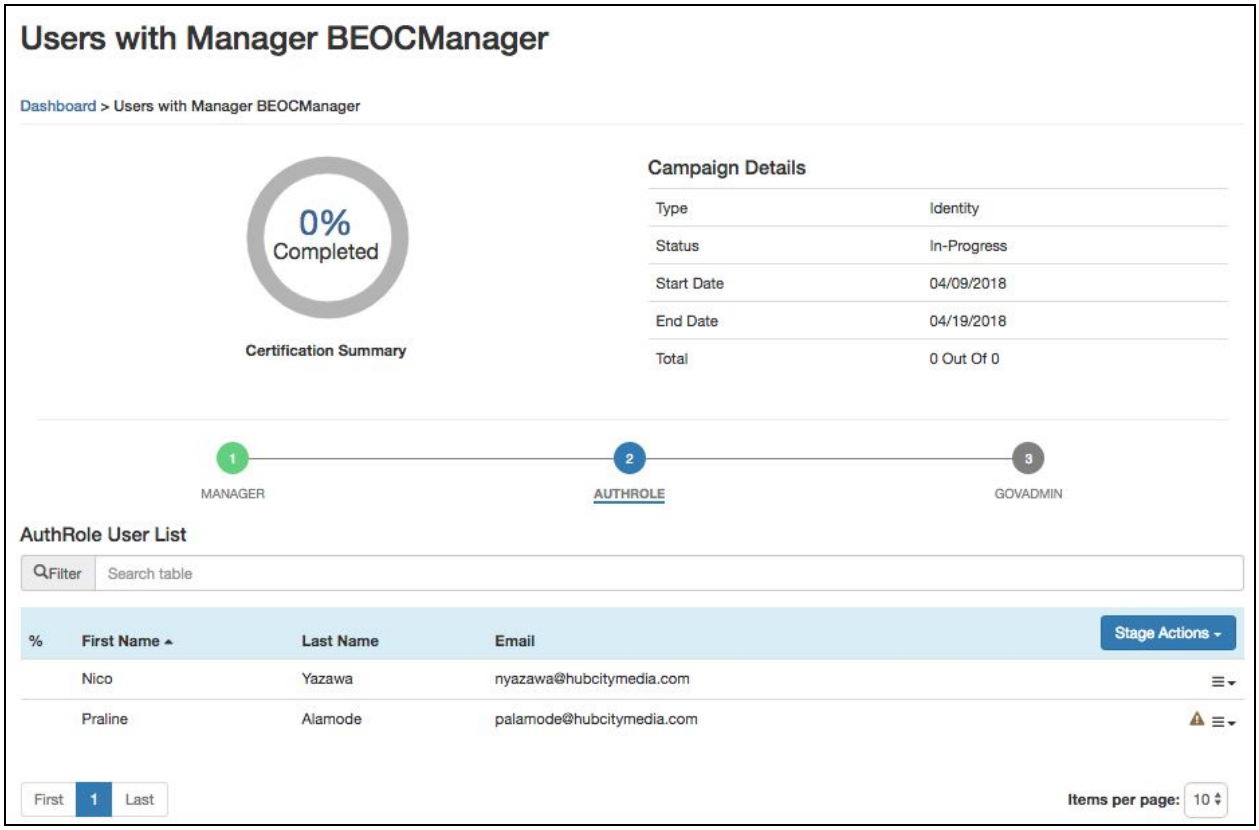
Note: For additional information on fields to update on this form, refer to section 3.1 step 3

4.3 Reviewing Active Certifications

1. For User Certifications, navigate to Manage Certifications, located in the Dashboard Management Dashboard under User Certifications



1. View contents under the tab Active Certifications:
   - **Active Certifications:** Contains all active user certifications. Each line displays a summary of a certification, with the following information:
     - **Cancel Selected:** Allows the administrator to change a certification to an inactive state, removing from assignees' queues. To utilize, select the checkboxes next to the certifications, then select '**Cancel Selected**'.
     - **Name:** Details certification by name given when creating the Certification Definition
     - **Frequency:** Details frequency used to create the certification. Values may include Ad-hoc, Scheduled or Event-based.
     - **Total Event Count:** Details the number of events required to complete the certification stage
     - **Start Date:** Details the date the certification became active
     - **Deadline:** Details the date the certification becomes expired and inactive

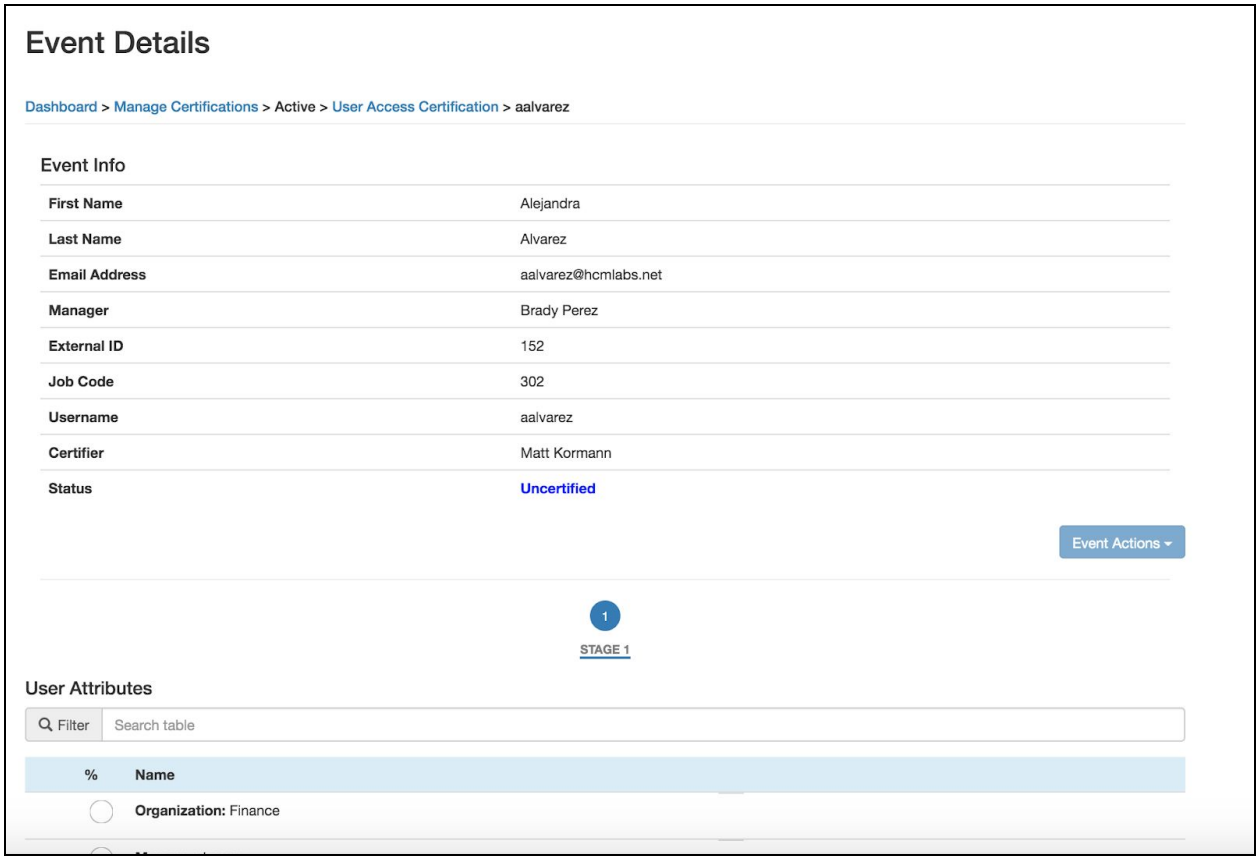


2. Select a certification from the Active Certifications list to display additional information. The following details will be displayed:
   - **Certification Summary:** Identifies the percentage complete for the entire certification stage. Note that this chart is only displayed when accessing a certification from the User Dashboard, not from the Admin Dashboard.
   - **Campaign Details:** Displays a summary of the certification with the following information:
     - **Status:** Identifies the current state of the certification. Values may include Open or In-Progress.
     - **Certifier:** Identifies the certifier for the given campaign. If it is a single user or group, their name will be displayed. If it is a certifier type that is dependent on the user (e.g. manager, entitlement owner), then that type will be displayed.
     - **Start Date:** Identifies the date that the certification became active
     - **End Date:** *(Active Certifications only)* Identifies the deadline of the selected campaign stage
     - **Completion Date:** Identifies the completion date of the certification. While viewing Active Certifications, this field will appear blank.
   - **Stage Indicator:** Indicates the certification stages. By selecting a stage node, the page will be updated to reflect data for the selected stage. Additional information is conveyed by the state and appearance of each node in the stage indicator. Note that this information will differ depending on whether certification is being viewed from the Admin Dashboard or not.

- **Non-admin View:** This view is primarily intended to reflect information that is relevant to the current user's responsibilities. As such, stage indicator nodes may be displayed in one of the following states:
  - *Selected:* the selected stage will have its name displayed in bold, underlined text
  - *Active:* the active stage's node will be blue. This state is intended to illustrate on which stage is the current user needs to take action.
  - *Completed:* Completed stage nodes will be green. A stage is considered complete when an action has been taken on all stage events, and the stage has received the certifier(s) sign-off.

- **Admin View:** This view is intended to communicate information about the certification as a whole, rather than in relation to a specific stage. Therefore, only the selected stage is available in Admin View:
  - *Selected:* The selected stage node will be blue, and the stage name will be displayed in bold, underlined text

- **User List:** List containing all targets for the certification. Each line contains a summary of the targeted user with the following information:
  - **%:** Graphical representation of the percentage complete for the target evaluation. An empty circle indicates no progress, whereas a green checkmark indicates the target evaluation is complete.
  - **First Name:** Identifies the first name of the target for certification
  - **Last Name:** Identifies the last name of the target for certification
  - **E-mail:** Identifies contact information for the user
  - **Risk Score:** *(If 'Configure Risk Level' is enabled in System Settings)* Identifies the risk level of the user on a 1 - 10 scale. A risk score of 1 indicates a low-risk target for the certification, whereas a risk score of 10 indicates high risk.



- Select a user from the User List to display additional information about the selected user's certification status. The following details will be displayed:
- **User Details:** Details a summary of the target user with the following information. Note that more attributes may appear (as shown above) if the option to do so is selected in the system settings:
    - **Username:** Login name for the target user
    - **First Name:** First name of the target user
    - **Last Name:** Last name of the target user
    - **Email Address:** Contact information of the target user
    - **Certifier:** Lists the user or group that is responsible for this individual user event. In cases where the certifier type is entitlement owner, the certifier for each individual item will appear on each line with the table below.
    - **Status:** Current status of the target within the certification stage. Values may include Uncertified, Certified, or Revoked.

- **Attributes:** Contains attributes to be certified for the target user. Attributes that are single-valued will be listed in a Name: Value format, while attributes that are multi-valued will appear underneath a parent row with the attribute name listed.
    - **+/-:** Identifies a row containing information about a multi-valued attribute. Selecting '**+**' displays values for individually certifiable attributes. Selecting '**-**'collapses values.

  - **%:** Graphical representation of the percentage complete for the attribute evaluation. An empty circle indicates no progress, whereas a blue circle indicates the attribute evaluation is complete. A row marked with +/- indicates overall progress for the attribute. Otherwise, the field indicates if a value has been certified.
  - **Name:** Identifies the name of the attribute in a field marked with +/-. Otherwise, the field identifies the value of the attribute to be certified.
  - **Metadata:** Identifies whether metadata has been set for this attribute in the glossary
  - **Risk Level:** *(If 'Configure Risk Level' is enabled in System Settings)* Identifies risk level of value for an attribute on a 1 - 10 scale. A risk score of 1 indicates a low-risk target for the certification, whereas a risk score of 10 indicates high risk. This field will appear blank in rows marked with +/-.
- **Applications:** Contains applications to be certified for the target user.
  - **+/-:** Identifies a row containing information about an application. Selecting '**+**' displays attributes for the application for additional reference. Selecting '**-**' collapses the attributes.
  - **%:** Graphical representation of the percentage complete for the application evaluation. An empty circle indicates no progress, whereas a green checkmark indicates the application evaluation is complete. A red x indicates the application was revoked. This field only appears in rows marked by +/-.
  - **Attribute:** Identifies the name of the application being certified in rows marked by +/-. Otherwise, the field identifies the name of an attribute within the application to be certified.
  - **Value:** Identifies the name of the application being certified in rows marked by +/-. Otherwise, the field identifies the value of an attribute name in the Attribute column on the same row.
  - **Metadata:** Identifies whether metadata has been set for this attribute in the glossary
  - **Risk Level:** *(If 'Configure Risk Level' is enabled in System Settings)* Identifies risk level of value for an attribute on a 1 - 10 scale. A risk score of 1 indicates a low-risk attribute within the application for the certification, whereas a risk score of 10 indicates high risk. This field will appear blank in rows marked with +/-.
  - **Comments:** Identifies additional information around actions taken when certifying an application. This field will only appear on rows marked with +/-.

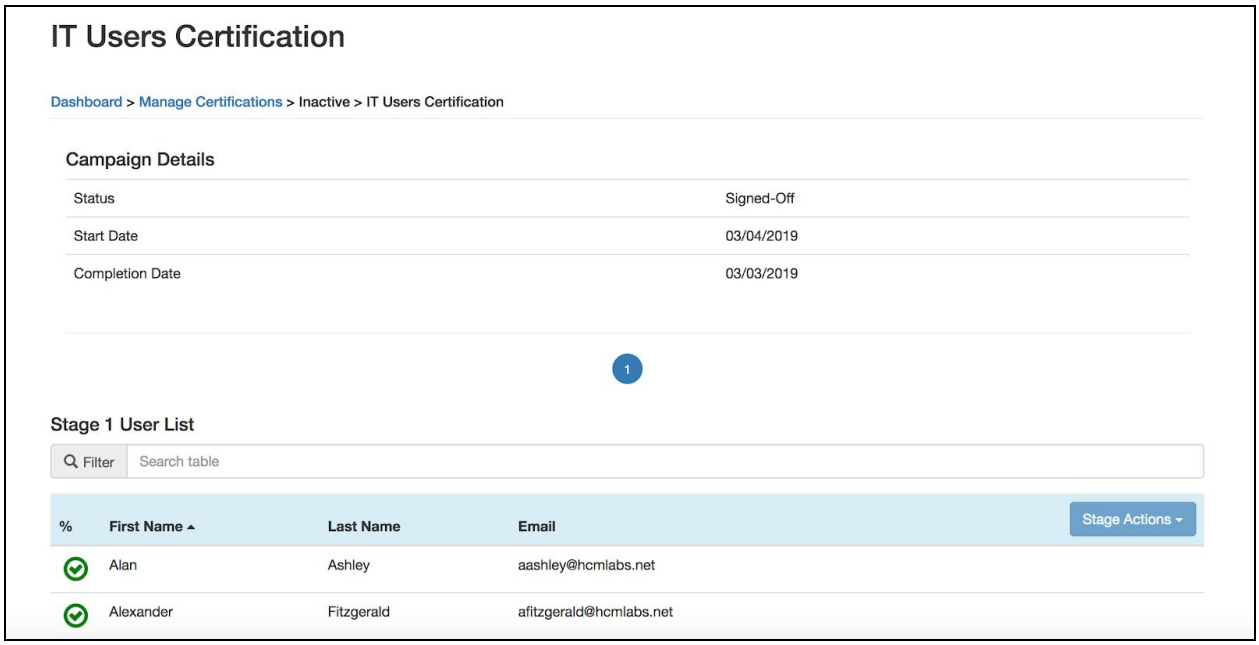
Note: For more information on Comments, refer to section 2.2.2

- **Quick View Mode:** The Event Details page provide a 'Quick View' option in order to more easily previous certifiers' responses for a particular Event Details attribute. Select the Quick View action to bring up the corresponding modal. Note that for nested attributes, this option is only available for items in the lowest nested group.
    - **Quick View Stage Indicator:** Indicates the certification's stages. When the Quick View option is selected for an attribute, the Stage Indicator displayed in the resulting modal is scoped to that attribute. For completed stages, the attribute's Stage Indicator icon will match the attribute's outcome in that stage. The actions, comments, and certifier for a completed stage can be viewed by selecting the stage.

4.4 Reviewing Closed Certifications

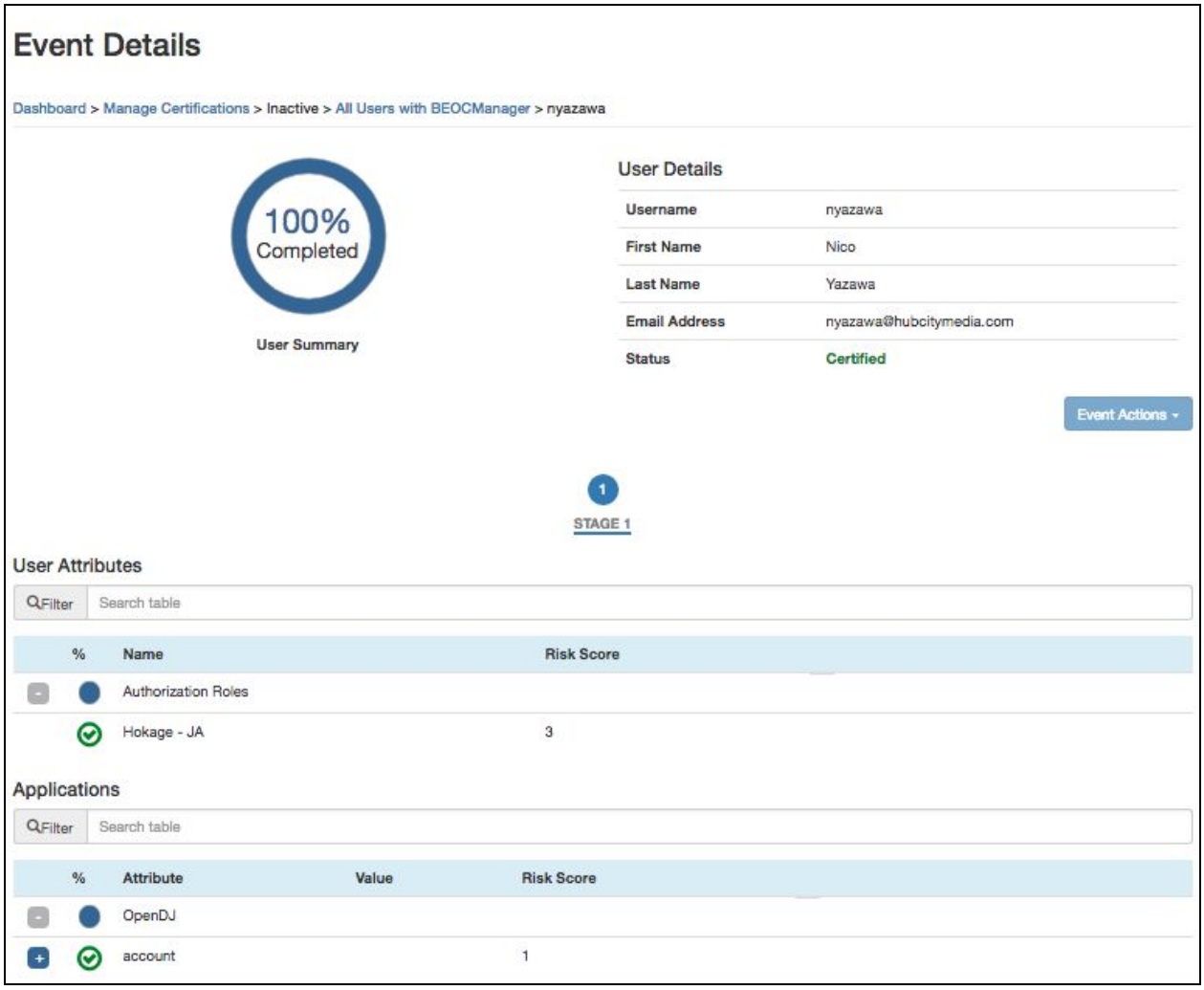
1. For User Certifications, navigate to Manage Certifications, located in the Dashboard Management Dashboard under User Certifications

2. View contents under the Closed Certifications tab
   - **Closed Certifications:** Contains all inactive user certifications. Each line displays a summary of a certification with the following information:
     - **Name:** Identifies certification by name given when creating the certification definition
     - **Frequency:** Identifies frequency used to create the certification. Values may include Ad-hoc, Scheduled or Event-based.
     - **Events Per Stage:** Identifies the number of events required to complete the certification stage
     - **Start Date:** Identifies the date the certification became active
     - **Deadline:** Identifies date the certification expires and becomes inactive
     - **Completion Date:** Identifies date the certification is marked as complete. If the certification expired before completion, the field will indicate the date as Incomplete.



3. To display additional information about the certification, select '**Certification**' from the Closed Certifications list. The following details will be displayed:
   - **Campaign Details:** Displays summary of the certification with the following information:
     - **Status:** Identifies current state of certification. Values may include Expired, Cancelled or Signed-off.

    - **Start Date:** Identifies the date the selected certification stage became active
    - **Completion Date:** Identifies date the certification is marked as complete. If the certification expired before completion, the field will indicate the date as Incomplete.
  - **Stage Indicator:** Indicates the certification stages. By selecting a stage node, the page will be updated to reflect data for the selected stage. Additional information is conveyed by the state and appearance of each node in the stage indicator.
- **User List:** Contains all targets for the certification. Each line contains a summary of the targeted user with the following information.
    - **%:** Graphical representation of the percentage complete for the target evaluation. An empty circle indicates no progress, whereas a green checkmark indicates that the target evaluation is complete.
    - **Target Name:** Name of the target for certification. For User Certifications, this will be the user's full name.
    - **E-mail:** Contact information for the user
    - **Risk Score:** *(If 'Configure Risk Level' is enabled in System Settings)* Identifies risk level of the user on a 1 - 10 scale. A risk score of 1 indicates low risk target for the certification, whereas a risk score of 10 indicates high risk.



4. To display additional information about selected user's certification status, select a user from the User List. The following details will be displayed:
   - **User Details:** Displays summary of the target user with the following information:
     - **Username:** Login name for the target user
     - **First Name:** First name of the target user
     - **Last Name:** Last name of the target user
     - **Email Address:** Contact information of the target user
     - **Status:** Current status of the target within the certification. Values may include Uncertified or Certified.
   - **Stage Indicator:** Indicates the certification stages. By selecting a stage node, the page will be updated to reflect data for the selected stage. Additional information is conveyed by the state and appearance of each node in the stage indicator.
   - **Attributes:** Contains multi-valued attributes to be certified for the target user, including Provisioning Roles, Authorization Roles and custom objects. This section may contain data for User Certifications of Type Identity or Attribute only.

  - **+/-:** Identifies rows containing information about a multi-valued attribute. Selecting '**+**' displays values for the individually certifiable attributes Selecting '**-**' collapses the values
  - **%:** Graphical representation of the percentage complete for the attribute evaluation. An empty circle indicates no progress, whereas a blue circle indicates the attribute evaluation is complete. A gray circle indicates that the event was cancelled. A red x indicates that the attribute was revoked. A row marked with +/- indicates overall progress for the attribute. Otherwise, the field indicates if a value has been certified.
  - **Name:** Name of the attribute in a field marked with +/-. Otherwise, the field identifies the value of the attribute to be certified.
  - **Risk Score:** *(If 'Configure Risk Level' is enabled in System Settings)* Risk level of a value for an attribute on a 1 - 10 scale. A risk score of 1 indicates low risk target for the certification, whereas a risk score of 10 indicates high risk. This field will appear blank in rows marked with +/-.
- **Applications:** Contains applications to be certified for the target user. This section may contain data for User Certifications of Type Identity or Application only.
  - **+/-:** Identifies a row containing information about an application. Selecting '**+**' displays attributes for the application for additional reference. Selecting '**–**' collapses the attributes.
  - **%:** Graphical representation of the percentage complete for the application evaluation. An empty circle indicates no progress, whereas blue circle indicates the application evaluation is complete. A gray circle indicates that the event was cancelled. A red x indicates the application was revoked. This field only appears in rows marked by +/-.
  - **Attribute:** Name of the application being certified in rows marked by +/-. Otherwise, the field identifies the name of an attribute within the application to be certified.
  - **Value:** Name of the application being certified in rows marked by +/-. Otherwise, the field identifies the value of an attribute name in the Attribute column on the same row.
  - **Risk Level:** *(If 'Configure Risk Level' is enabled in System Settings)* Risk level of a value for an attribute on a 1 - 10 scale. A risk score of 1 indicates low risk attribute within the application for the certification, whereas a risk score of 10 indicates high risk. This field will appear blank in rows marked with +/-.
  - **Comments:** Additional information around actions taken when certifying an application. This field will only appear on rows marked with +/-.

Note: For more information on Comments, refer to section 2.2.2

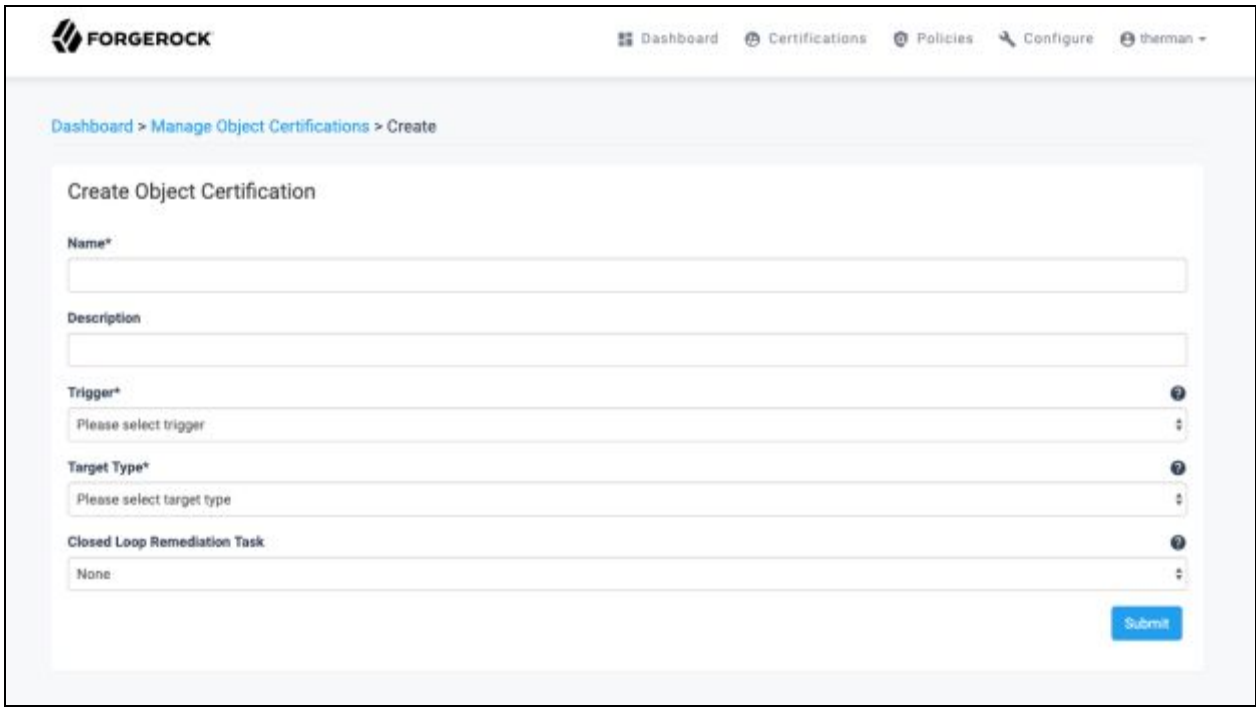
5 Object Certifications

Object certifications target managed objects for certification. Certifications allow a certifier to review an object's risk level and assignments, as well as sign-off or revoke assignments concerning those objects.

5.1 Creating New Certifications

1. For Object Certifications, navigate to Manage Certifications, located in the Dashboard Management Dashboard under Object Certifications

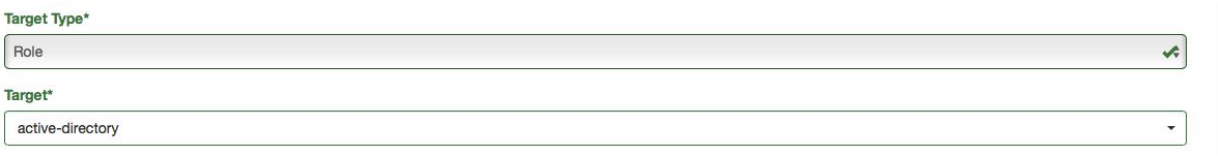
2. From the Manage Certifications page, select '**New Certification**'



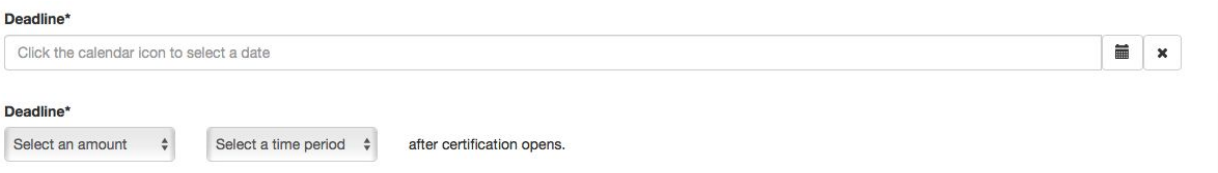
3. On the Create Certification page, fill in each required field. Additional details on the available fields are given below:
   - **Create Object Certification:** Fields required to define an object certification:
     - **Name:** *(Required)* Title for the certification, appears on all summary pages
     - **Description:** Additional details about the purpose of the certification to certifiers
     - **Trigger:** *(Required)* Identifies when the certification is created. Options are described below:
       - **Ad-Hoc:** Generates new certification immediately after submitting the current form and can only be triggered once
       - **Scheduled:** Generates new certification when a specified time duration has passed. Additional fields become available when selecting the '**Scheduled**' option to allow duration to be specified.

         Note: For more information on scheduling events, refer to section 3.2.4.

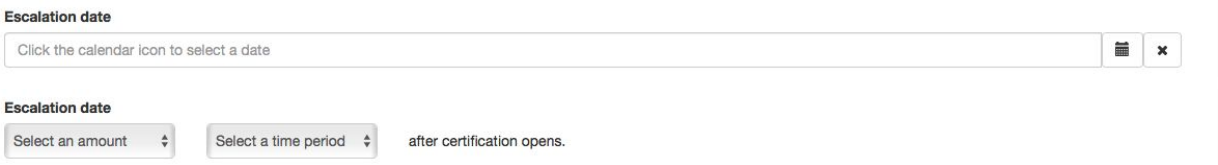
- **Event-based:** Generates certification based on an update to the objects specified in Target Type field



- **Target Type:** *(Required)* Type of object targeted for certification. Values may include Role or a custom managed object.
- **Target:** *(Required)* Object instance targeted for certification



- **Deadline:** *(Required)* Specifies how long certification should remain active. After specified date or duration, the certification expires and becomes unavailable for modification.



- **Escalation:** Specifies if / when an escalation should occur prior to the date specified in the Deadline. After the specified date or duration, a notification will be sent to the user or role specified in the Escalation Owner field. This field becomes available upon selecting an Escalation Date.
  Escalation Owner: *(Required)* If specifying an escalation date, the following fields become available to identify the escalation user or role to send a notification. The following options are available:

- **User:** Notifies specified user when an escalation occurs

- **Authorization Role:** Notifies specified group of users when an escalation occurs

- **Certifier Manager:** Notifies managers of users assigned to the certification

- **Closed Loop Remediation Task:** Identifies automated remediation task for handling revocations from the certification

  Note: For more information on remediation tasks, refer to section 3.2.5

5.2 Modifying Certification Definitions

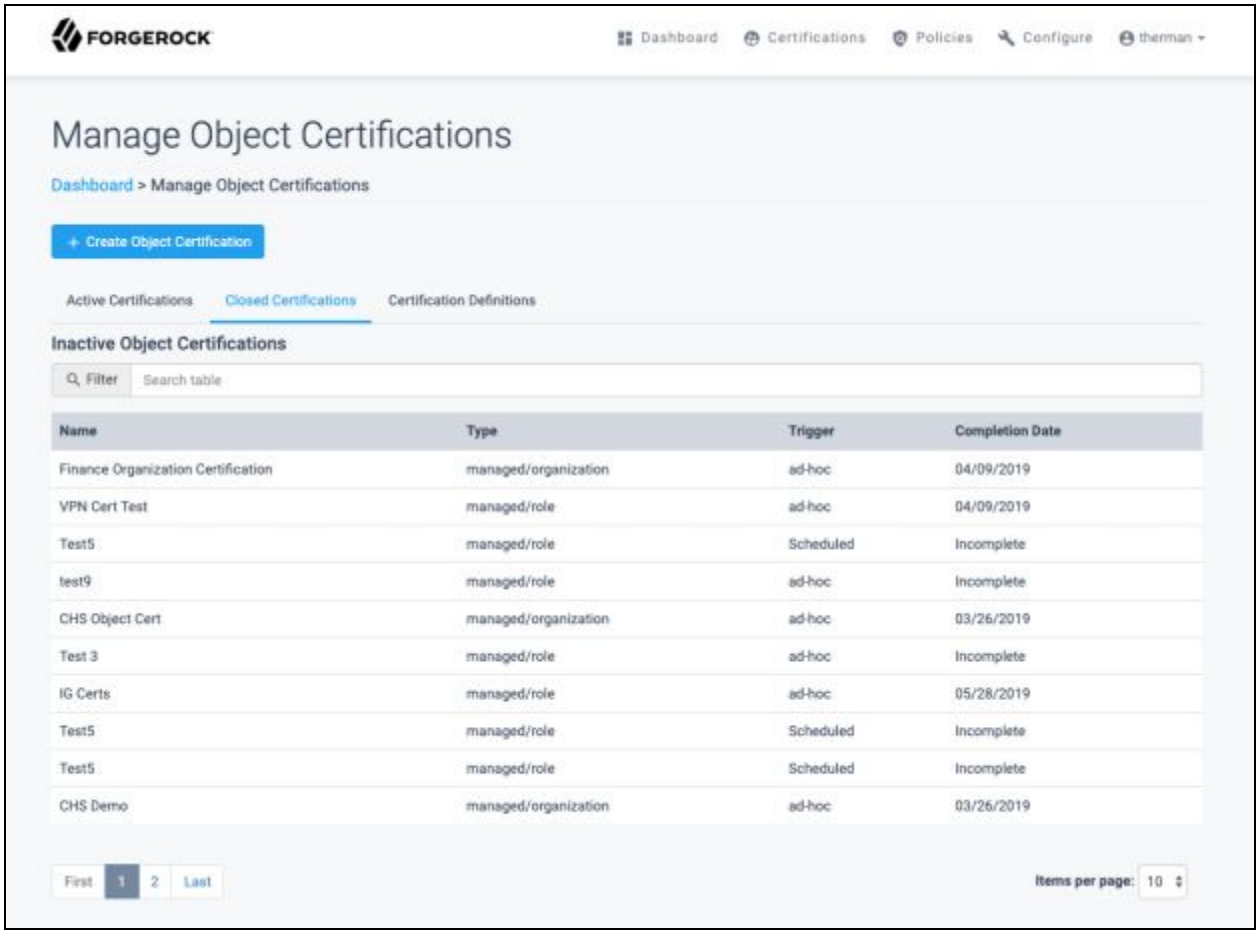
1. Navigate to Manage Object Certifications for Certifications. This is located in the Dashboard Management Dashboard under Object Certifications.

2. View the contents under the tab Certification Definitions
   - **Object Certification Definitions:** Contains all existing certification definitions that are Scheduled or Event-based. Ad-hoc certification definitions cannot be modified. Each line contains a summary of certification definition with the following details:
     - **Delete Selected:** Allows the administrator to delete a certification definition, while not affecting existing certifications. To utilize, select the checkboxes next to the certification definitions to delete, then select Delete Selected.
     - **Trigger:** Trigger used to create the certification. Values may include Scheduled or Event-based.
     - **Name:** Identifies the certification by the name given when creating the certification definition
     - **Target Type:** Type of object targeted for certification. Values may include Role or a custom managed object.
     - **Target Name:** Object instance targeted for certification

3. Select a certification definition from the Object Certification Definitions list to display additional information about the certification. For additional information on the fields to update on this form, refer to section 4.1 step 3.

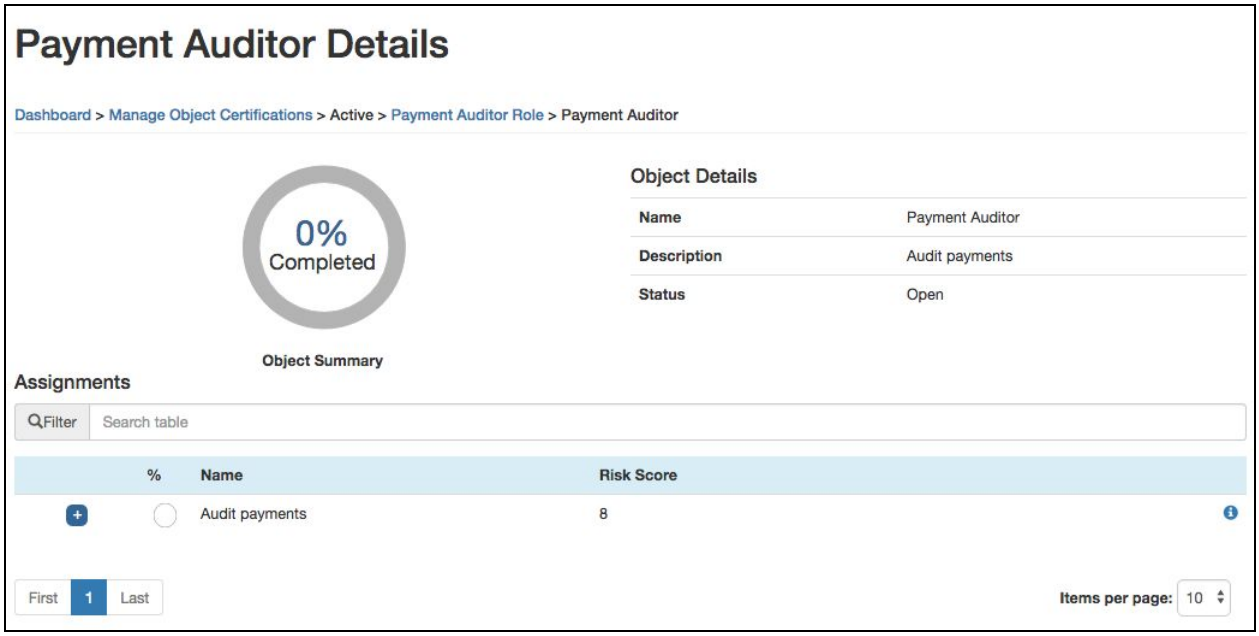
5.3 Reviewing Active Certifications

1. For Object Certifications, navigate to Manage Certifications, located in the Dashboard Management Dashboard under Object Certifications



2. View the contents under the Active Certifications tab
   - **Active Object Certifications:** Details all active object certifications. Each line displays a summary of certification with the following information:
     - **Cancel Selected:** Allows the administrator to change a certification to an inactive state, removing from assignees' queues. To utilize, select the checkboxes next to the certifications to cancel, then select '**Cancel Selected**'.
     - **Name:** Identifies certification by the name given when creating the certification definition
     - **Type:** Type of certification. Values may include managed / object, where object is the type of object (e.g. role or custom object).
     - **Trigger:** Trigger used to create the certification. Values may include Ad-hoc, Scheduled or Event-based.
     - **Complete / Total:** Number of completed events and the total number of events required to complete the certification
     - **Deadline:** Date that causes the certification to become expired and inactive

3. To display additional information about the certification, select a certification from the Active Object Certifications list. The following details are displayed:
   - **Object Certification Summary:** Identifies percentage complete for the entire certification
   - **Object List:** All objects targeted for certification. Each line displays a summary of certification with the following information:
     - **%:** Graphical representation of the percentage complete for the object evaluation. An empty circle indicates no progress, whereas a green checkmark indicates the object evaluation is complete.
     - **Object Name:** Name of the object for certification
     - **Risk Score:** *(If 'Configure Risk Level' is enabled in System Settings)* Risk level of the object on a 1 - 10 scale. A risk score of 1 indicates a low-risk target for the certification, whereas a risk score of 10 indicates high risk.

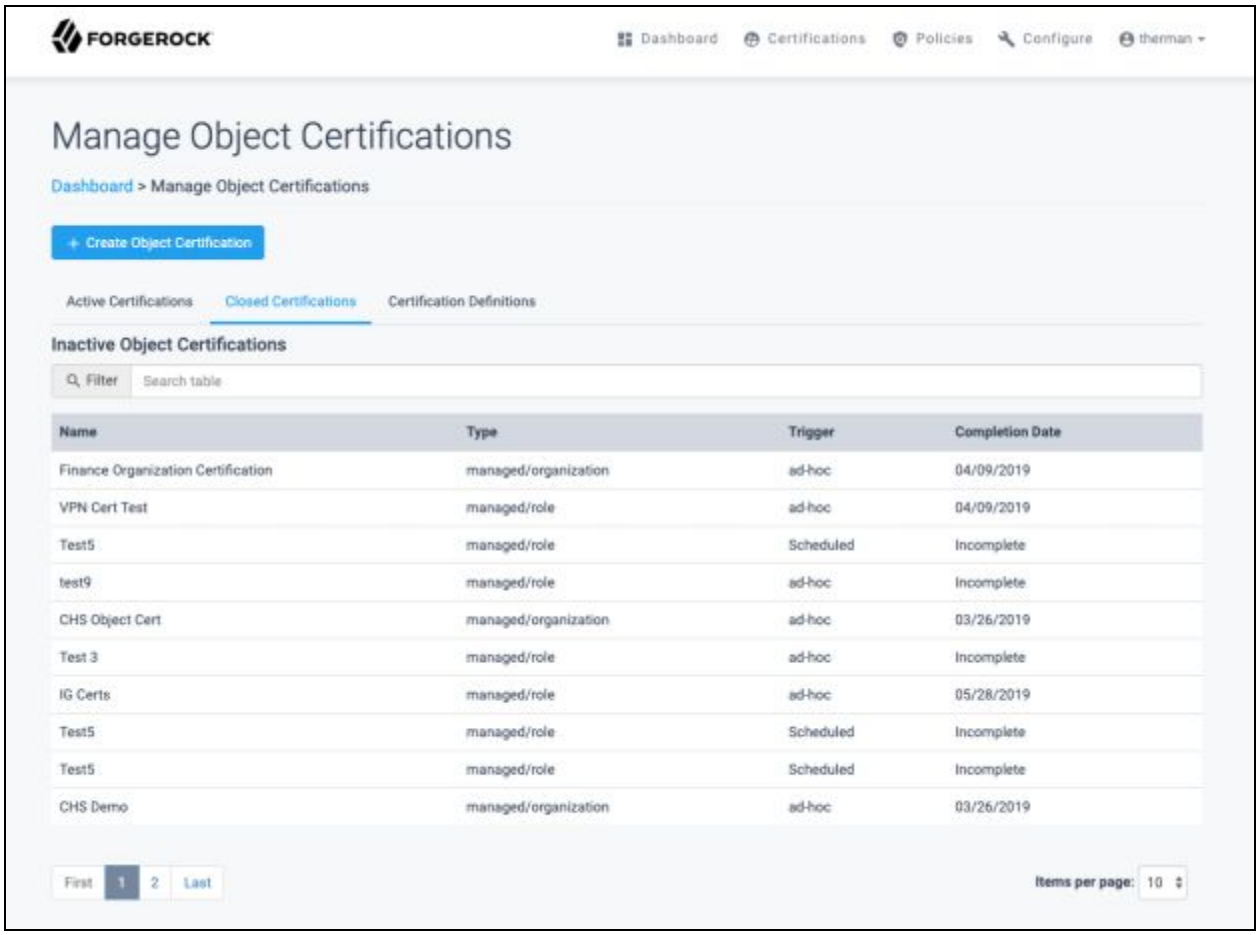


4. To display additional information about the selected object's certification status, select an object from the Object List. The following details are displayed:
   - **Object Summary:** Percentage complete for the assignment list
   - **Object Details:** Summary of the target object with the following details:
     - **Name:** Name of the object for certification
     - **Description:** Description of the object as identified in the object
     - **Status**: Current state of the certification. Values may include Open or In Progress and may also contain comments.

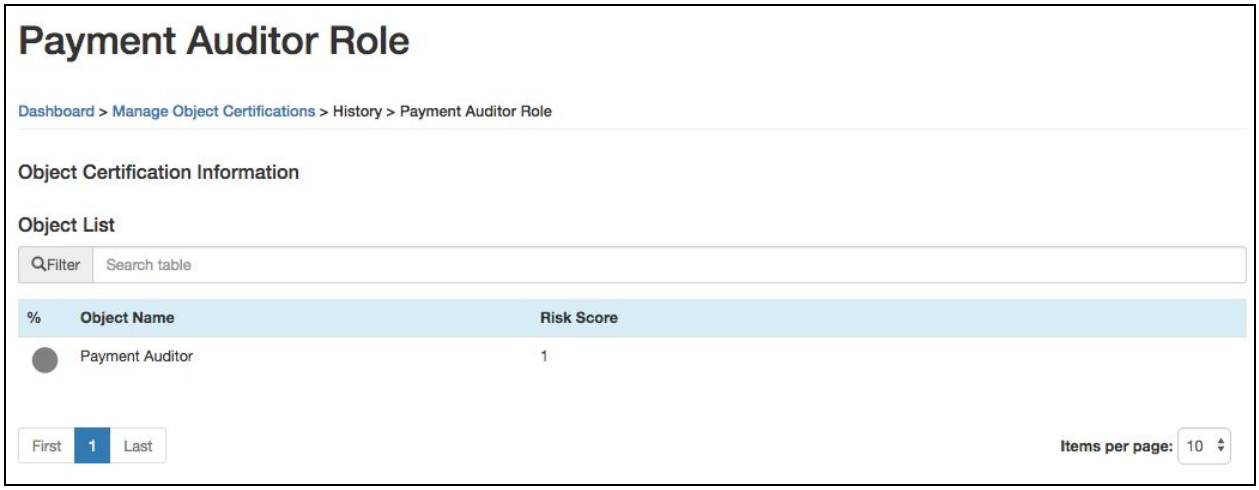
- **Assignments:** Information about the targeted assignment within the certification. Each line displays a summary of an object instance with the following information:
    - **%:** Graphical representation of the percentage complete for the assignment evaluation. An empty circle indicates no progress, whereas a green checkmark indicates the assignment evaluation is complete. A red x indicates that the assignment was revoked.
    - **Name:** Name of the assignment for certification
    - **Risk Level:** *(If 'Configure Risk Level' is enabled in System Settings)* Risk level of the object on a 1 - 10 scale. A risk score of 1 indicates ow risk target for the assignment, whereas a risk score of 10 indicates high risk.
    - **🛈:** Additional information about attributes provided by the assignment. Information is a list of paired values with the following details:
        - **Attribute:** Name of an attribute provisioned through the assignment
        - **Value:** Value of the attribute provisioned through the assignment

5.4 Reviewing Inactive Certifications

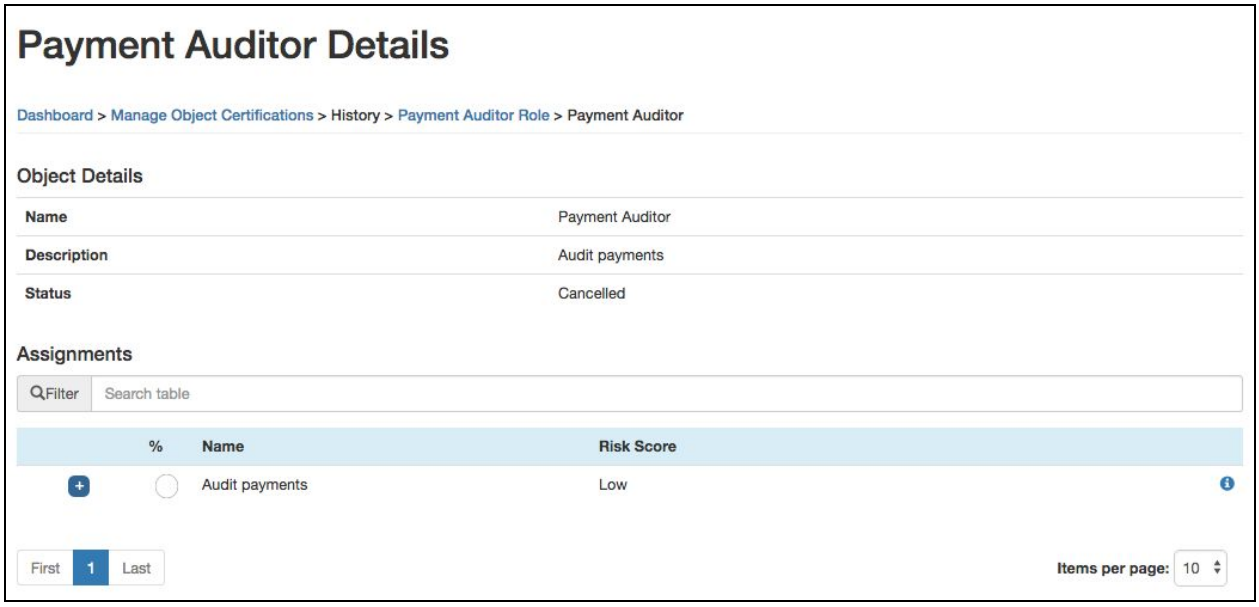
1. For Object Certifications, navigate to Manage Certifications, located in the Dashboard Management Dashboard under Object Certifications



2. View contents under the tab Closed Certifications
   - **Inactive Object Certifications:** List containing all of the inactive object certifications. Each line displays a summary of a certification with the following information.
     - **Name:** Identifies certification by name given when creating the certification definition
     - **Type:** Type of certification. Values may include managed / object, where object is the type of object (e.g. role or custom object).
     - **Trigger:** Trigger used to create the certification. Values may include Ad-hoc, Scheduled or Event-based.
     - **Completion Date:** Identifies date the certification is marked as complete. If the certification expired before completion, field will indicate the date as Incomplete.



3. To display additional information about the certification, select a certification from the Inactive Object Certifications list. The following details will be displayed:
   - **Object List:** All objects targeted for certification. Each line displays a summary of a certification with the following information:
     - **%:** Graphical representation of the percentage complete for the object evaluation. An empty circle indicates no progress, whereas a green checkmark indicates the object evaluation is complete.
     - **Object Name:** Name of the object for certification
     - **Risk Score:** *(If 'Configure Risk Level' is enabled in System Settings)* Identifies risk level of the object on a 1 - 10 scale. A risk score of 1 indicates low risk target for the certification, whereas a risk score of 10 indicates high risk.



4. To display additional information about the selected object's certification status, select an object from the Object List. The following details are displayed:

- **Object Details:** Identifies a summary of the target object with the following details:
    - **Name:** Name of the object for certification
    - **Description:** Description of the object as identified in the object
    - **Status**: Current state of the certification. Values may include Cancelled or Signed-off and may also contain comments.

- **Assignments:** Details information about the targeted assignment within the certification. Each line displays a summary of an object instance with the following information:
    - **%:** Graphical representation of the percentage complete for the assignment evaluation. An empty circle indicates no progress made, whereas a green checkmark indicates that the assignment evaluation is complete. A red x indicates that the assignment was revoked.
    - **Name:** Name of the assignment for certification
    - **Risk Level:** *(If 'Configure Risk Level' is enabled in System Settings)* Risk level of the object on a 1 - 10 scale. A risk score of 1 indicates a low-risk target for the assignment, whereas a risk score of 10 indicates high risk.
    - **🛈:** Additional information about attributes provided by the assignment. Information is a list of paired values with the following details:
        - **Attribute:** Name of an attribute provisioned through the assignment
        - **Value:** Value of the attribute provisioned through the assignment

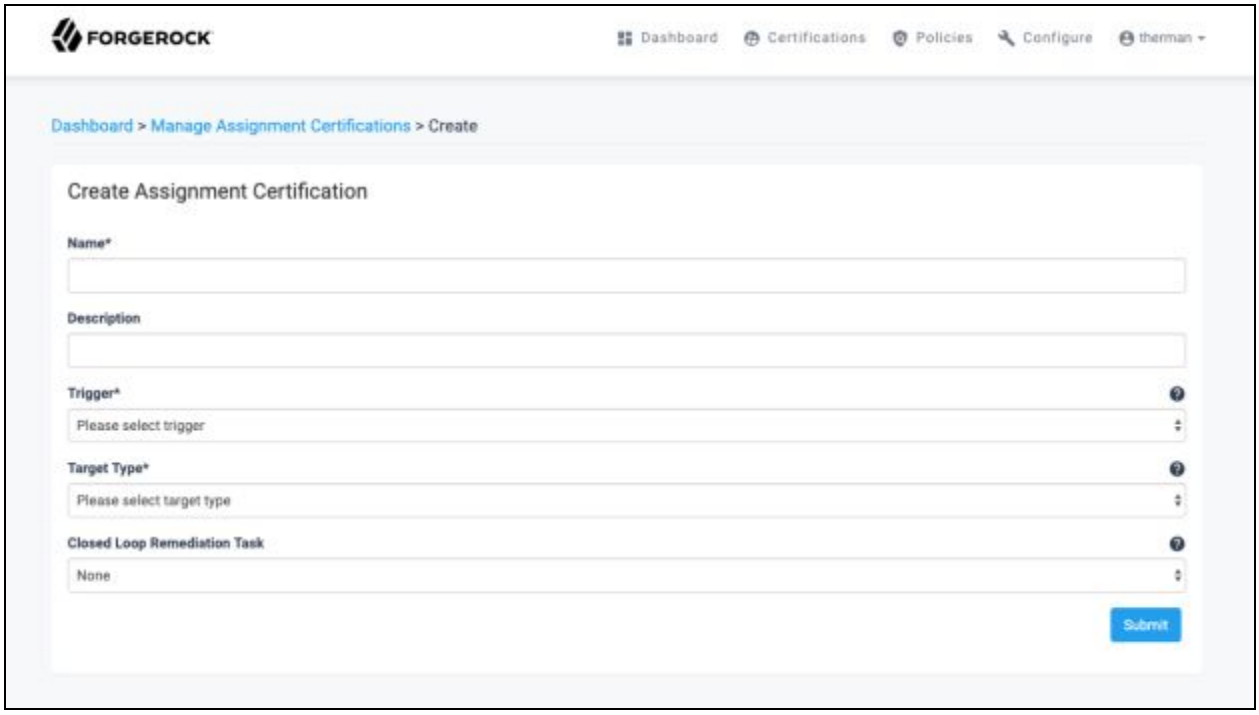
6 Assignment Certifications

Assignment certifications target individual assignments for certification. The certifications allow a certifier to review an assignment's provisioning attributes, as well as sign-off or revoke targeted assignments.

6.1 Creating New Certifications

1. For Object Certifications, navigate to Manage Certifications, located in the Dashboard Management Dashboard under Object Certifications

2. From the Manage Certifications page, select '**New Assignment Certification**'



3. On the Create Certification page, fill in each required field. Details on the available fields are given below:

- **Create Assignment Certification:** Fields required to define an assignment certification
  - **Name:** *(Required)* Title for the certification that will appear on all summary pages
  - **Description:** Additional details about the purpose of the certification to certifiers
  - **Trigger:** *(Required)* Identifies when certification will get created. Options are described below:
    - **Ad-Hoc:** Generates new certification immediately after submitting the current form and can only be triggered once
    - **Scheduled:** Generates a new certification when each time duration specified has passed. Additional fields become available when selecting the '**Scheduled**' option to allow duration to be specified.

      Note: For more information on scheduling events, refer to section 3.2.4

    - **Event-based:** Generates certification based upon an update to the assignments specified in the Target Type field
  - **Target Type:** *(Required)* Identifies filter for the targets to be certified. The following options are available:

    - **All Assignments:** Allows all assignments for applications to be targeted for certification. When selecting, the following filter becomes available:

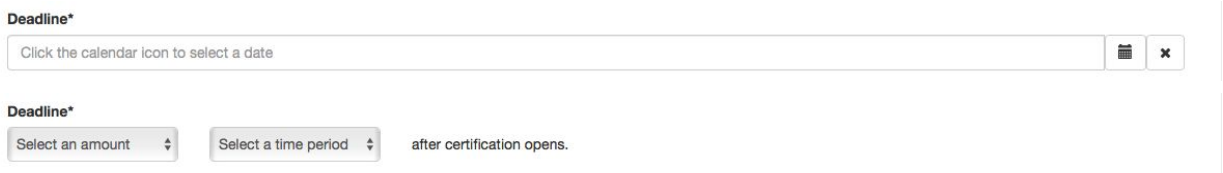
      Risk Level: *(Required)* Specifies filter for the certifications. Only certifications with specified levels of risk will be generated, and a minimum of one option must be selected to generate any certifications. This setting may be hidden if risk score has been disabled from the global settings, in which case it will treat the certification as if all options were selected.

    - **All Assignments Under Application:** Allows all assignments under a specified application to be targeted for certification. When selecting, the following filter becomes available:

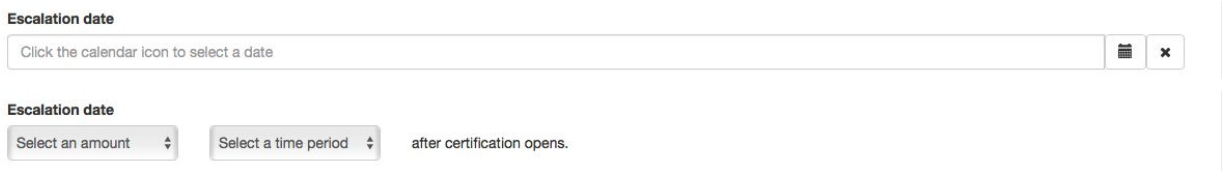
Target: *(Required)* Specifies filter for certifications. A dropdown making certifiable applications becomes available. Any assignments affecting the specified application will be considered for certification.

- **Assignment:** Allows only the specified assignment as a target for certification. When selecting, the following filter becomes available:

Target: *(Required)* Specifies filter for the certifications. A dropdown making certifiable assignments becomes available. Any assignments within the specified application will be considered for certification.



- **Deadline:** *(Required)* Specifies if / when an escalation should occur prior to the date specified in the Deadline. After the specified date or duration, a notification will be sent to the user or role specified.



- **Escalation:** Specifies if / when an escalation should occur prior to the date specified in the Deadline. After the specified date or duration, a notification will be sent to the user or role specified.
- **Escalation Owner:** *(Required)* When specifying an escalation date, the following fields become available to specify the escalation user or role to send a notification:

- **User:** Notifies specified user when an escalation occurs

- **Authorization Role:** Notifies specified group of users when an escalation occurs

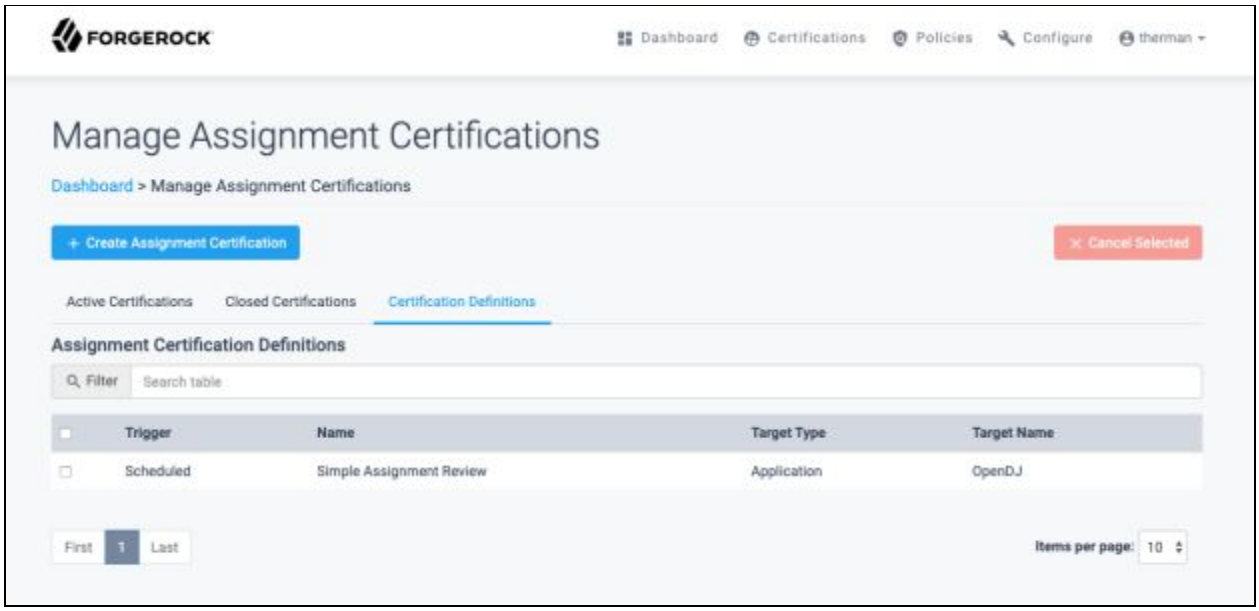
- **Certifier Manager:** Notifies managers of users assigned to the certification

o **Closed Loop Remediation Task:** Automated remediation task for handling revocations from the certification

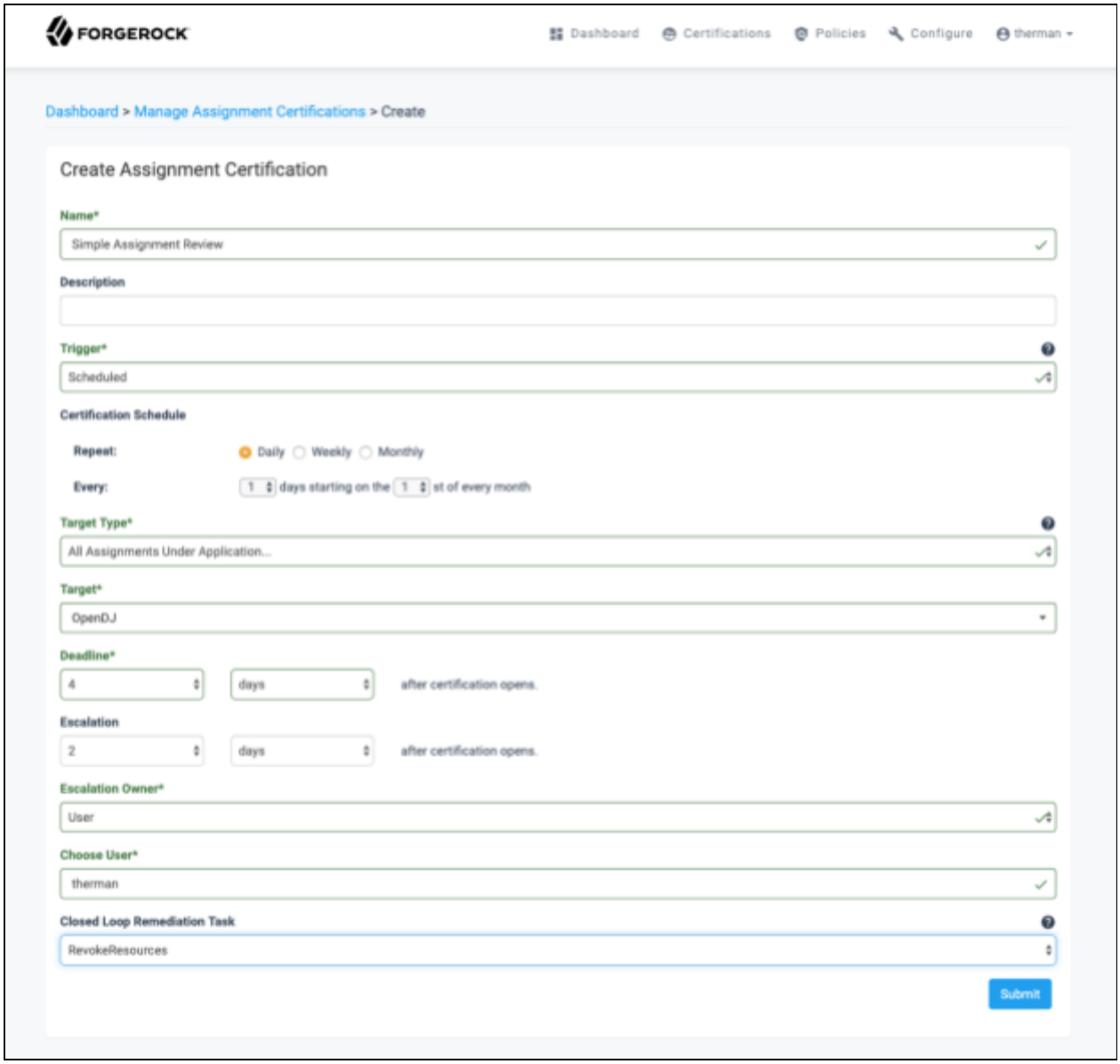
Note: For more information on remediation tasks, refer to section 3.2.5

6.2 Modifying Certification Definitions

1. For Assignment Certifications, navigate to Manage Assignment Certifications, located in the Dashboard Management Dashboard under Assignment Certifications



2. View the contents under the Assignment Certification Definitions tab
   - **Assignment Certification Definitions:** Details all existing certification definitions, Scheduled or Event-based. Ad-hoc certification definitions cannot be modified. Each line contains a summary of certification definition with the following details:
     - **Remove Selected:** Allows the administrator to delete a certification definition, while not affect existing certifications. To utilize, select the checkboxes next to the certification definitions to delete, then select '**Remove Selected**'.
     - **Trigger:** Identifies when the certification will get created
     - **Name:** Name given when creating the certification definition
     - **Target Type:** Type of the target named in the Target Name field. Values may include application, assignment and All.
     - **Target Name:** Name of the target for the certification. If All is specified, all assignments are considered for the certification.

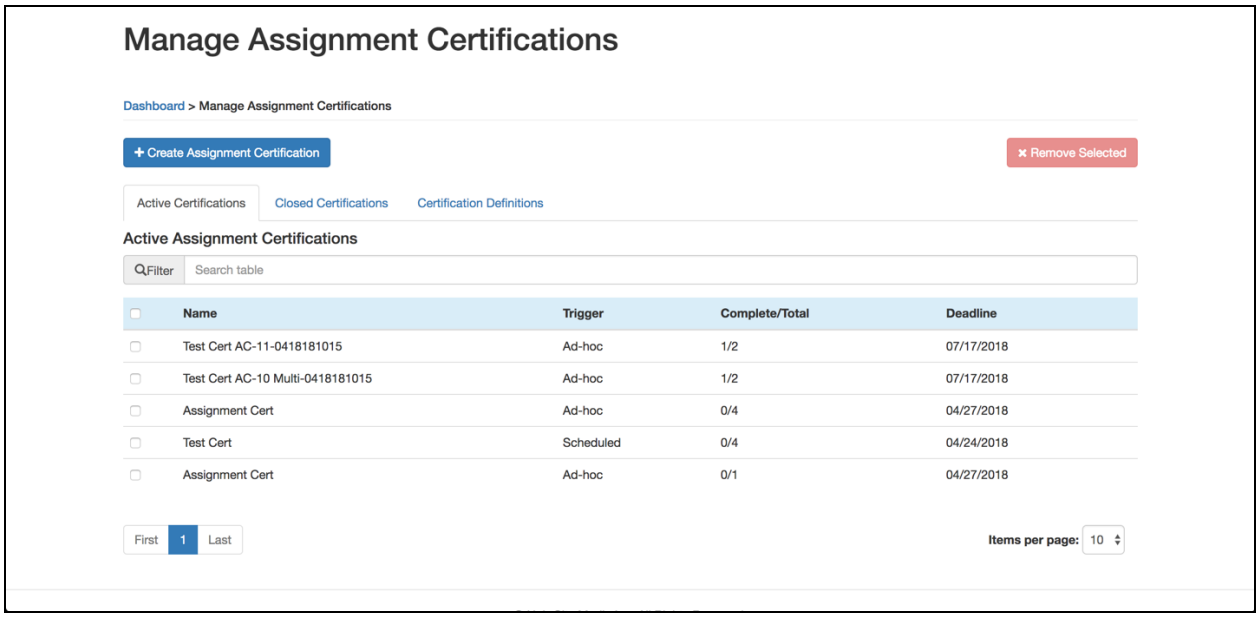


3. To display additional information about the certification, select a certification definition from the Assignment Certification Definitions list

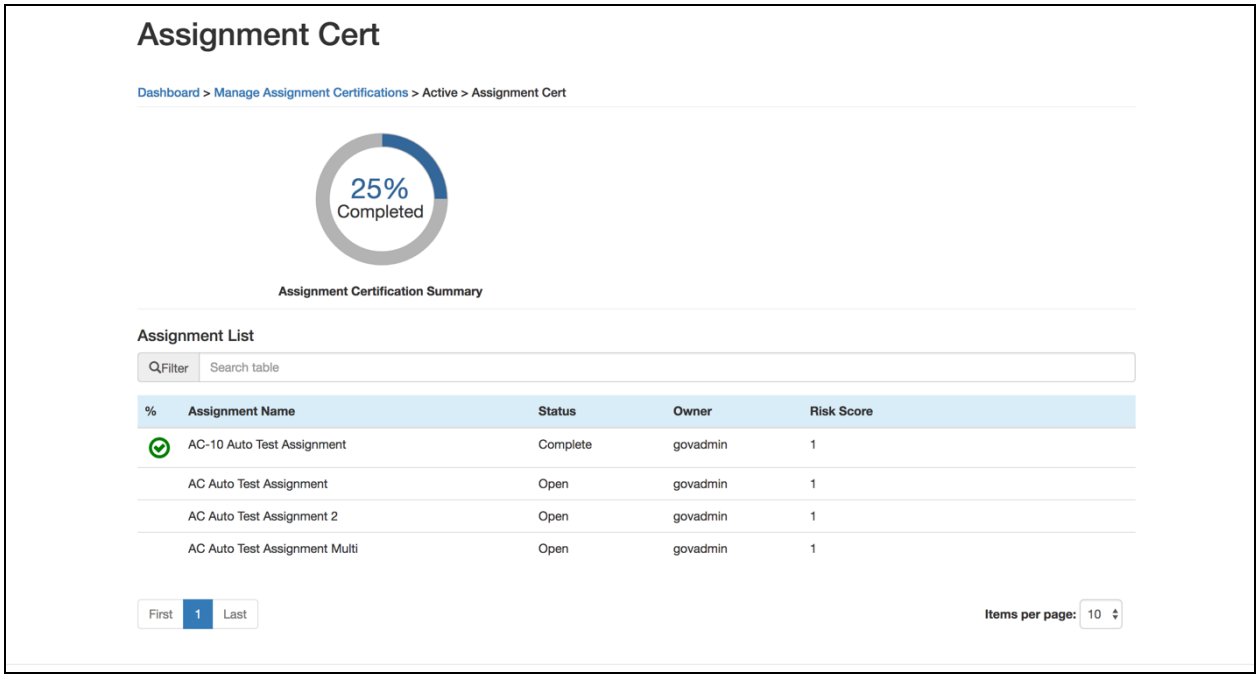
Note: For additional information on the fields to update on this form, refer to section 5.1 step 3

6.3 Reviewing Active Certifications

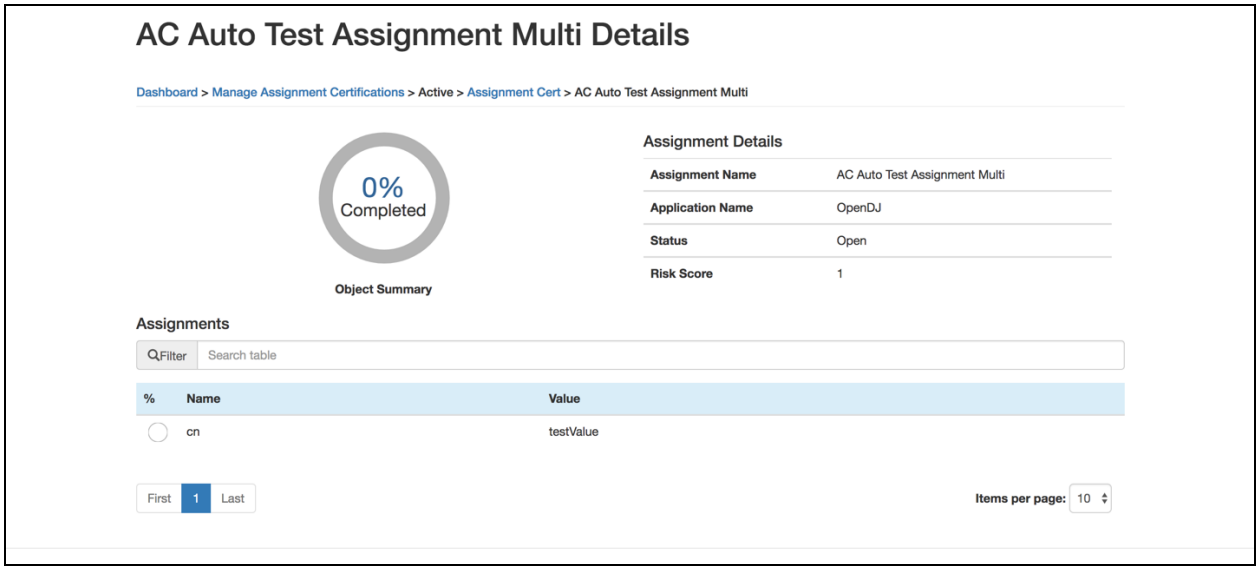
1. For Assignment Certifications, navigate to Manage Certifications, located in the Dashboard Management Dashboard under Assignment Certifications



2. View contents under the Active Certifications tab
   - **Active Assignment Certifications:** Details all active object certifications. Each line displays a summary of a certification with the following information:
     - **Remove Selected:** Allows the administrator to change a certification to an inactive state, removing from assignees' queues. To utilize, select the checkboxes next to the certifications to cancel, then select '**Cancel Selected**'.
     - **Name:** Details certification by name given when creating the certification definition
     - **Type:** Type of certification. Values may include managed / object, where object is the type of object (e.g. role or custom object).
     - **Trigger:** Trigger used to create the certification. Values may include Ad-hoc, Scheduled or Event-based.
     - **Complete / Total:** Number of completed events and total number of events required to complete the certification
     - **Deadline:** Date that causes the certification to become expired and inactive



3. To display additional information about the certification, select a certification from the Active Assignment Certifications list. The following details are displayed:
   - **Assignment Certification Summary:** Percentage complete for the entire certification
   - **Assignment List:** All assignments targeted for certification. Each line displays a summary of certification with the following information:
     - **%:** Graphical representation of percentage complete for the assignment evaluation. An empty circle indicates no progress, whereas a green checkmark indicates the object evaluation is complete. A red x indicates that the attribute was revoked.
     - **Assignment Name:** Name of the assignment for certification
     - **Status:** Status of the certification. Values may include Open, In Progress, Revoked or Signed-Off.
     - **Owner:** Owner for the assignment, responsible for the certification
     - **Risk Score:** Identifies the risk level of the certification on a 1 - 10 scale. A risk score of 1 indicates a low-risk target for the certification whereas a risk score of 10 indicates high risk. This column may not be visible if the risk score has been disabled from the global settings.

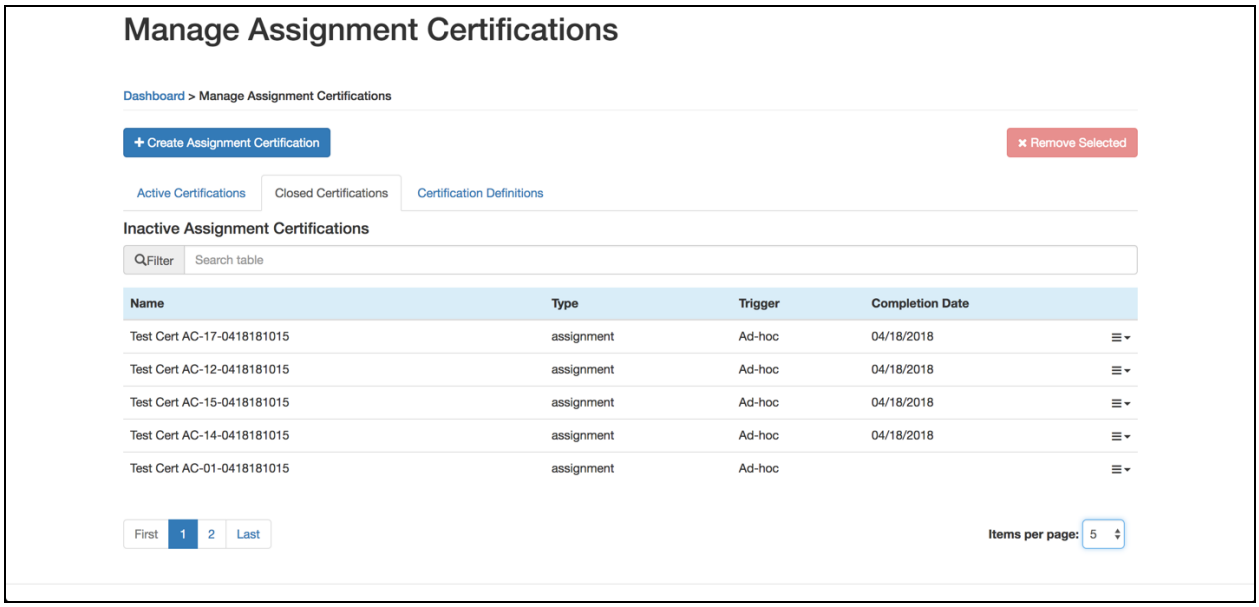


4. To display additional information about the selected object's certification status, select an object from the Assignments List
   - **Object Summary:** Percentage complete for the Assignments list
   - **Assignment Details:** Summary of details for the assignment, as well as status for this portion of the certification
     - **Assignment Name:** Name of the assignment for certification
     - **Risk Score:** Risk level of the assignment on a 1 - 10 scale. A risk score of 1 indicates low risk target for the certification, whereas a risk score of 10 indicates high risk. This column may not be visible if risk score has been disabled from the global settings.
     - **Application Name:** Name of the application affected by the assignment
     - **Status:** Status of the certification. Values may include Open, In Progress, Revoked or Signed-Off.

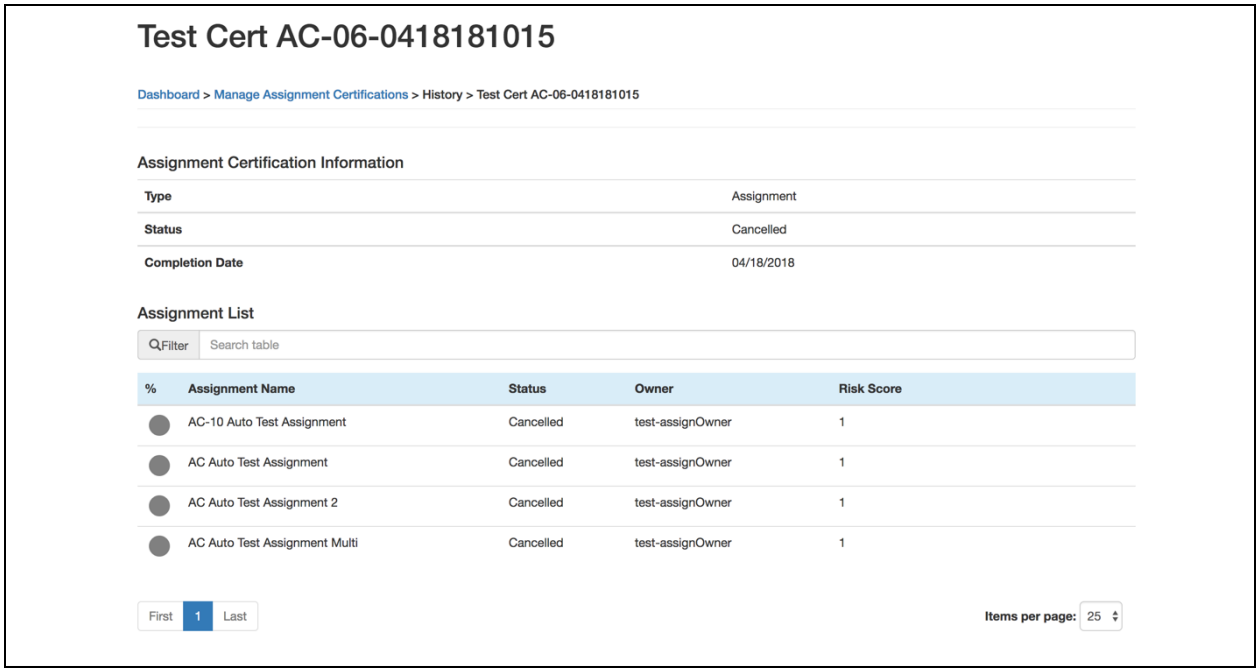
   - **Assignments:** Identifies additional information about the attributes of the assignment targeted for certification
     - **%:** Graphical representation of the percentage complete for the attribute evaluation. An empty circle indicates no progress, whereas a green checkmark indicates that the object evaluation is complete. A red x indicates that the attribute was revoked.
     - **Name:** Identifies name of the attribute to be certified
     - **Value:** Identifies value of the attribute to be certified

6.4 Reviewing Closed Certifications

1. For Assignment Certifications, Navigate to Manage Certifications, located in the Dashboard Management Dashboard under Assignment Certifications

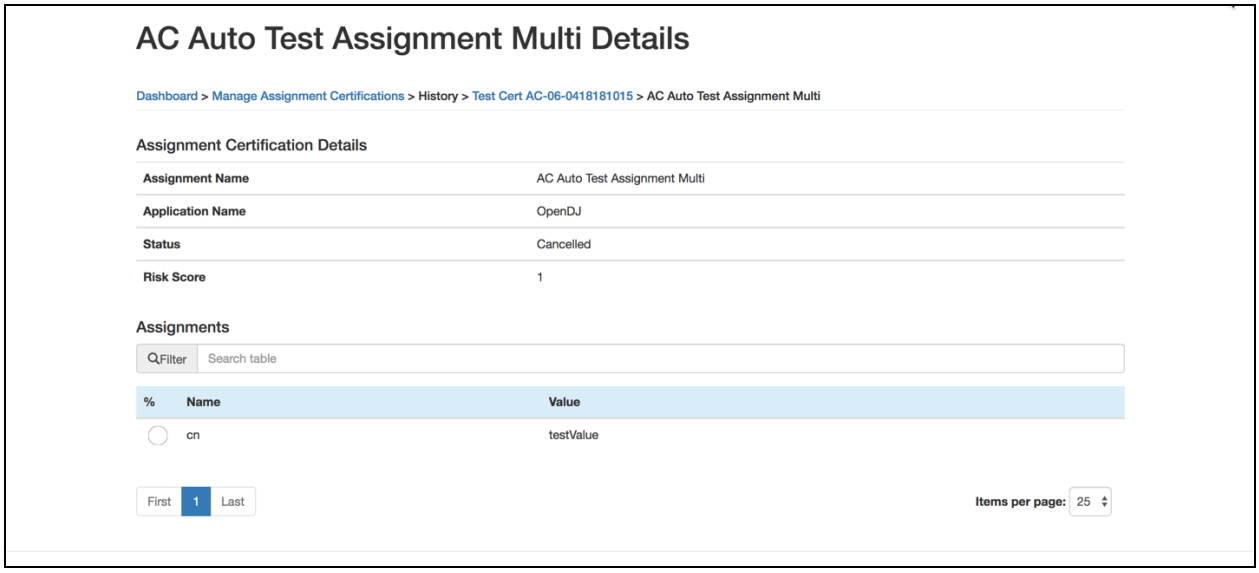


2. View contents under the Closed Certifications tab
   - **Inactive Assignment Certifications:** Details all active object certifications. Each line displays a summary of a certification with the following information:
     - **Name:** Name given when creating the certification definition
     - **Type:** Type of the target named in the Target Name field. Values may include application, assignment and All.
     - **Trigger:** Trigger used to create the certification. Values may include Ad-hoc, Scheduled or Event-based.
     - **Completion Date:** Date the certification becomes inactive



3. To display additional information about the certification, select a certification from the Active Object Certifications list. The following details will be displayed:
   - **Assignment Certification Information:** Percentage complete for the entire certification
     - **Type:** Type of target named in the Target Name field. Values may include application, assignment and All.
     - **Status:** Status of the certification. Values may include Signed-Off or Cancelled.
     - **Complete Date:** Date the certification becomes inactive

- **Assignment List:** Details all objects targeted for certification. Each line displays a summary of certification with the following information:
    - **%:** Graphical representation of the percentage complete for the object evaluation. An empty circle indicates no progress, whereas a green checkmark indicates that the object evaluation is complete. A red x indicates that the attribute was revoked.
    - **Assignment Name:** Name of the object for certification
    - **Status:** Status of this portion of the certification. Values may include Expired or Signed-Off.
    - **Owner:** Owner for the assignment, responsible for the certification
    - **Risk Score:** Risk level of the object on a 1 - 10 scale. A risk score of 1 indicates a low-risk target for the certification, whereas a risk score of 10 indicates high risk. This column may not be visible if the risk score has been disabled from the global settings.



4. To display additional information about the selected object's certification status, select an object from the Object List. The following details are displayed:
   - **Assignment Certification Details:**
     - **Assignment Name:** Name of the assignment for certification
     - **Risk Score:** Risk level of the assignment on a 1 - 10 scale. A risk score of 1 indicates a low-risk target for the certification, whereas a risk score of 10 indicates high risk. This column may not be visible if the risk score has been disabled from the global settings.
     - **Application Name:** Name of the application affected by the assignment
     - **Status:** Status of this portion of the certification. Values may include Expired, Cancelled or Signed-Off.
   - **Assignments:** Additional information about the attributes of the assignment targeted for certification
     - **%:** Graphical representation of the percentage complete for the object evaluation. An empty circle indicates no progress, whereas a green checkmark indicates that the object evaluation is complete. A red x indicates that the attribute was revoked.
     - **Name:** Name of the attribute to be certified
     - **Value:** Value of the attribute to be certified

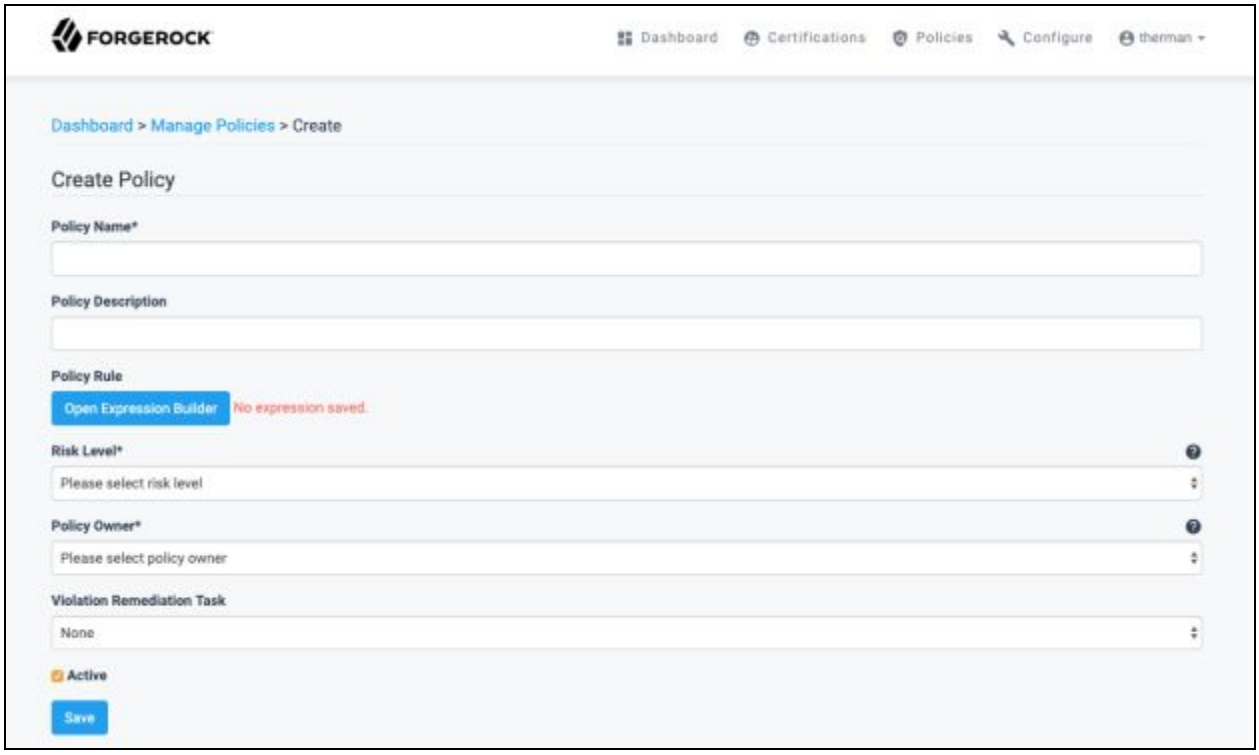
7 Policies

Policies allow the administrator to define a set of criteria and schedule to determine violations within OpenIDM, as well as providing the ability to grant exceptions. To manage violations, the administrator should create a policy to determine criteria for the violation, create a policy scan to generate those violations and monitor any exceptions granted from certifiers. Configure scheduled policy scans to scan for violations on a regular basis or configure reactive policy scans to scan a user for violations whenever a user is updated.

7.1 Creating a New Policy

1. Navigate to the Manage Policies page, located in the Dashboard Management Dashboard under Policies

2. From the Manage Policies page, select '**New Policy**'



3. On the Create Policy page, fill in each of the required fields. Additional details on the available fields are given below:
   - **Create Policy:** (Edit Policy) Fields required to define a policy
     - **Policy Name:** *(Required)* Reference name of the policy
     - **Policy Description:** Additional details describing the purpose of the policy

- **Policy Rule:** *(Required)* Rule for triggering a violation from the policy. If an event causing the rule to evaluate is true, a violation is created.

  Note: For more information on building expressions, refer to section 3.2.6

- **Risk Level:** *(Required)* Risk level for the policy on a 1 - 10 scale. A risk score of 1 indicates low-risk target for the certification, whereas a risk score of 10 indicates high risk.

- **Policy Owner:** *(Required)* Owner for the policy. If a violation is raised, the owner is responsible for remediation.

  - **User:** Allows policy to be assigned to a specified user as owner. Selecting details the following options:

Choose User: *(Required)* User, as owner of the policy. The field is open with autocomplete and requires a username.

  - **Authorization Role:** Allows policy to be assigned to a specified authorization role as owner. Selecting details the following options:

Authorization Role: *(Required)* Role, as owner of the policy. The field is a dropdown, with all available authorization roles.

- **Violation Remediation Task:** An automated remediation task for handling revocations from violation acceptance

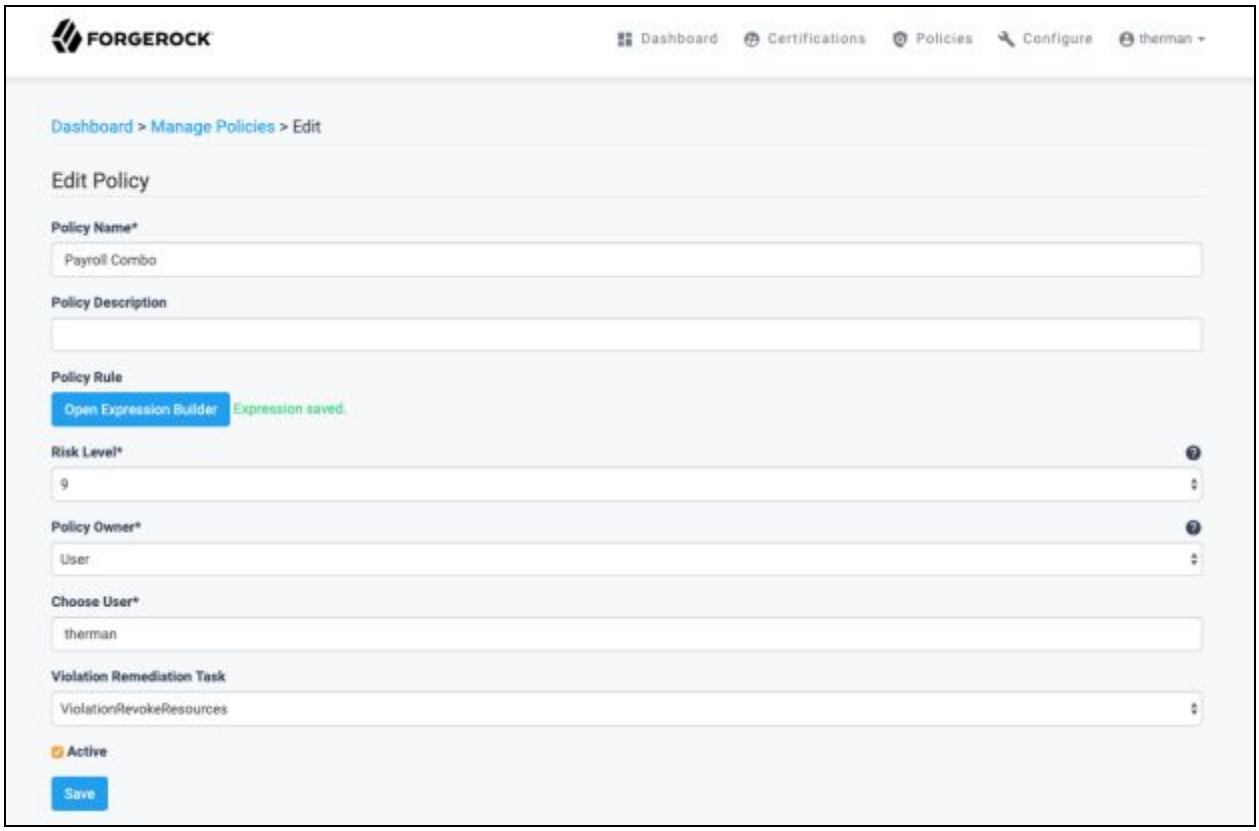
  Note: For more information on remediation tasks, refer to section 3.2.5

- **Active:** Identifies whether the policy is active or inactive. If unchecked, the policy will not be evaluated on updates.

7.2 Modifying Policies

1. Navigate to the Manage Policies page, located in the Dashboard Management Dashboard under Policies

2. View the contents under the tab Policies
   - **Policies:** Details information about existing policies, displaying policy summary with the following information:
     - **Delete Selected**: Allows the administrator to delete a policy while not affecting existing violations. To utilize, select the checkboxes next to the policies to delete, then select '**Delete Selected**'.
     - **Name:** Name of the policy
     - **Risk Level:** Identifies risk level assigned to the policy on a 1 - 10 scale. A risk score of 1 indicates low risk target for the certification, whereas a risk score of 10 indicates high risk.
     - **Status:** Identifies whether the policy is active or inactive. Values may include Active or Inactive.



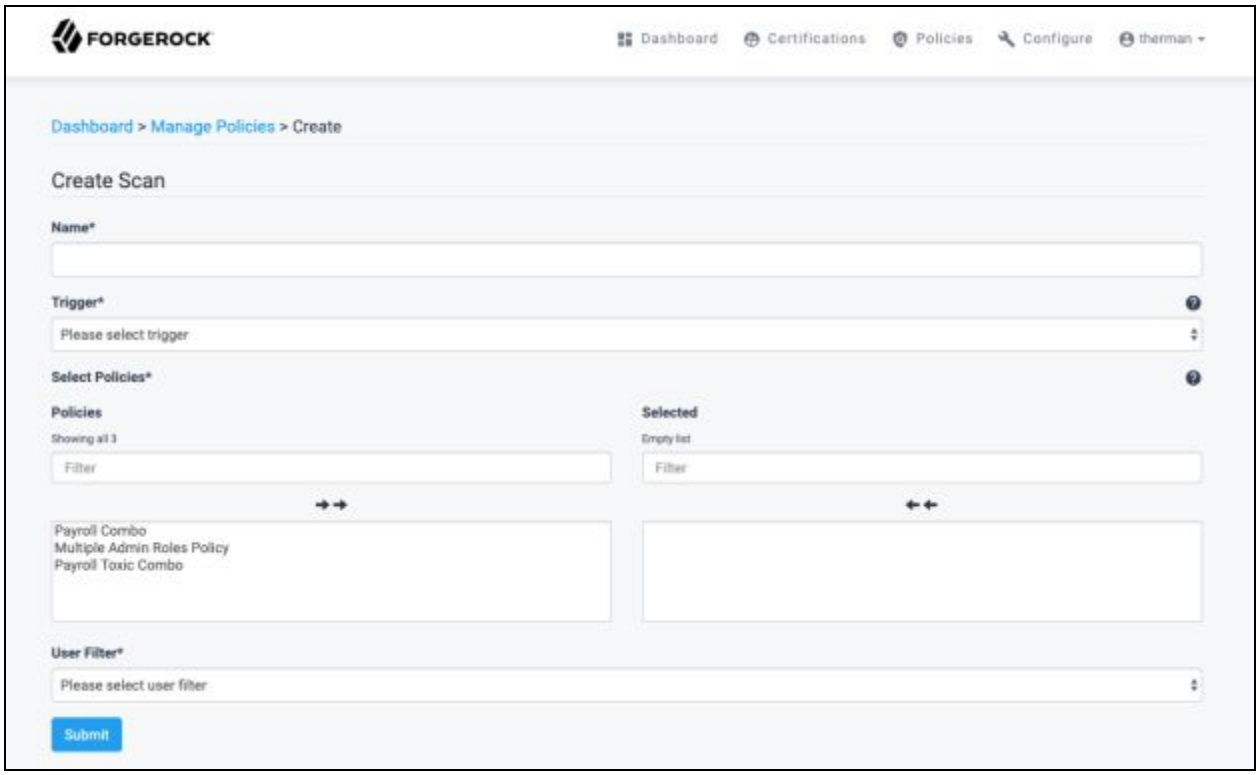
3. Select a policy from the Policies list. The Edit Policy page appears with details about the policy.

Note: For additional information on the fields to update on this form, refer to section 6.1 step 3

7.3 Creating a New Policy Scan

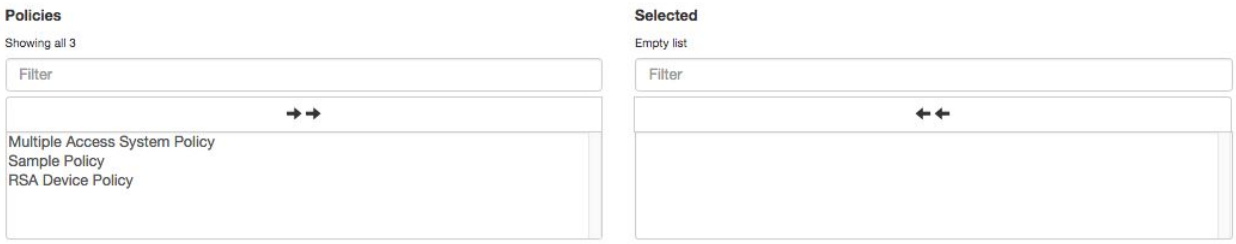
1. Navigate to the Manage Policies page, located in the Dashboard Management Dashboard under Policies

2. From the Manage Policies page, navigate to the Policy Scans tab and select '**New Scan**'



3. On the Create Scan page, fill in each of the required fields. Additional details on available fields are given below:
   - **Create Scan:** Fields required to define a policy scan
     - **Name:** *(Required)* Name of the policy scan
     - **Trigger:** *(Required)* When the policy scan will run. Options are described below:
       - **Ad-hoc:** Triggers a policy scan immediately after submitting the current form and can only be triggered once
       - **Scheduled:** Triggers a policy scan when a specified time duration has passed. Additional fields become available when selecting the '**Scheduled**' option to allow specific durations.

         Note: For more information on scheduling events, refer to section 3.2.4



- **Select Policies:** *(Required)* Policies that will be triggered by the scan. The field consists of side-by-side lists, with the left side containing available policies and the right side containing policies to be triggered in the scan. Selecting a policy in either list will move the policy to the opposite list.

- **User Filter:** *(Required)* Filter for users to scan. The following options are available:

  - **User:** Allows scan to be filtered to a specified user. Selecting provides the following option:

    Choose User: *(Required)* Identifies single user to target for the scan. The field is open with autocomplete and requires a username.

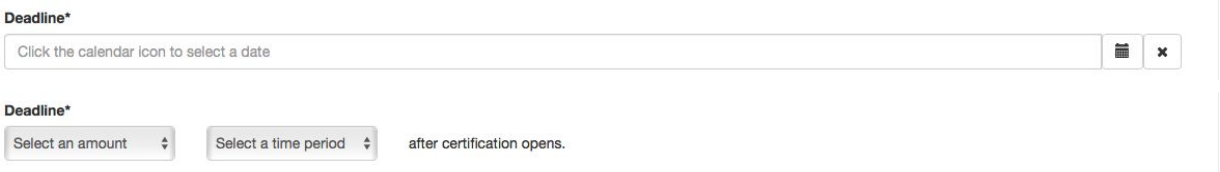
  - **Users with manager:** Allows scan to be filtered to any user with a specified manager. Selecting provides the following option:

    Choose Manager: *(Required)* Identifies a user, with the user's subordinates targeted for the scan. The field is open with autocomplete and requires a username.

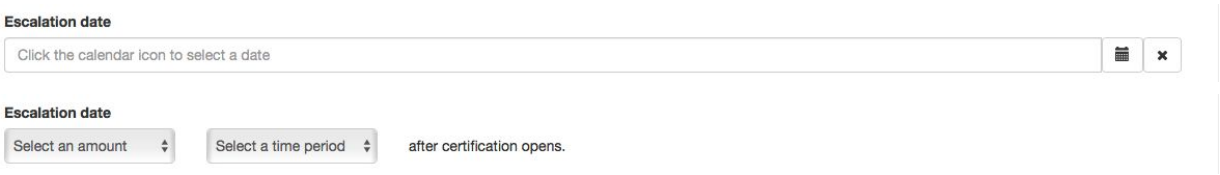
  - **All Users:** Allows scan to be run with no filter, targeting all users

- **Filter by user attribute:** Allows scan to be filtered to any user assigned to a specified instance of an attribute. Selecting provides the following option:

Attribute Value: *(Required)* Identifies attribute value for the specified attribute in the User Filter field, with users assigned the specified attribute value targeted for the scan. The Attribute Value field is a dropdown allowing certifiable attribute values to be specified.



- **Expiration Date:** *(Required)* Specifies how long a violation should remain active. After the specified date or duration, the violation expires and becomes unavailable for modification.



- **Escalation Date:** Specifies if / when an escalation should occur prior to the date specified in the Expiration Date field. After the specified date or duration, a notification will be sent to the user or role specified.

Escalation Owner: *(Required)* If specifying an escalation date, the following fields become available to specify the escalation user or role to send a notification:

- **User:** Notifies specified user when an escalation occurs

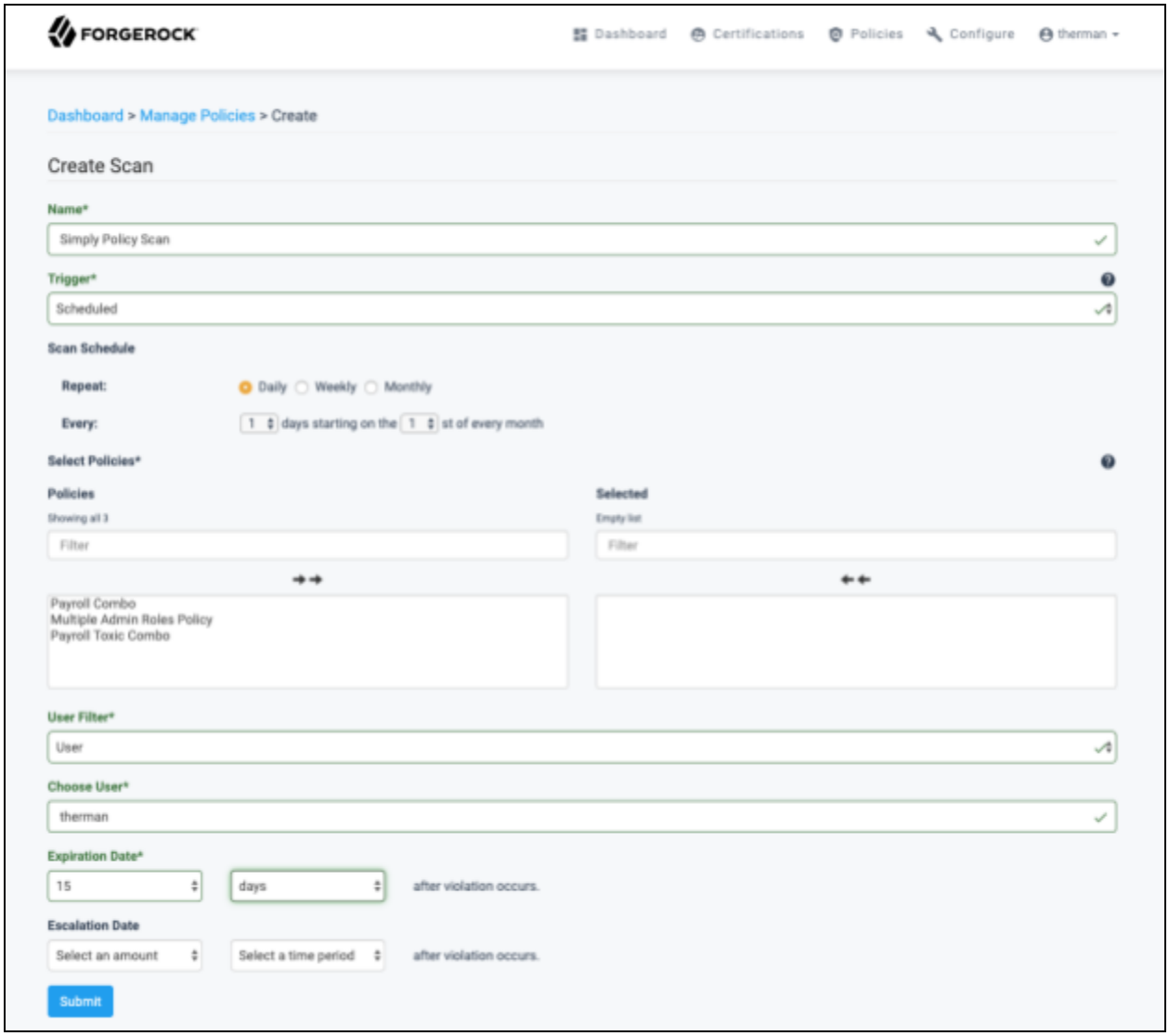
- **Authorization Role:** Notifies specified group of users when an escalation occurs

- **Policy Owner Manager:** Notifies managers of the policy owners

7.4 Modifying Scheduled Policy Scans

1. Navigate to the Manage Policies page, located in the Dashboard Management Dashboard under Policies

2. View the contents under the tab Policies
   - **Scheduled Scans:** Details information about policy scans that run on a scheduled basis. Each line displays a summary of a policy scan with the following information:
     - **Delete Selected:** Allows the administrator to delete a policy scan while not affecting existing violations. To utilize, select the checkboxes next to the policy scans to delete, then select '**Delete Selected.**'
     - **Scan Name:** Name of the policy scan
     - **Filter Type:** Type of target for the policy scan. Values may include All Users, User, Users with manager and attribute.
     - **Filter Value:** Target value for the type specified in the Filter Type field

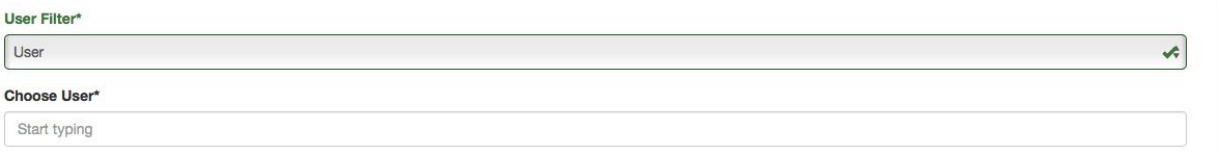


3. Select a Scan from the Scheduled Scans list
   - **Edit Scan:** Fields required to define a policy scan
     - **Name:** *(Required)* Name used to reference the policy scan
     - **Scan Schedule:** Triggers a policy scan each time a specified duration has passed. Additional fields become available when selecting the '**Scheduled**' option to allow duration to be specified.

       Note: For more information on scheduling events, refer to section 3.2.4

     - **Select Policies:** *(Required)* Policies triggered by the scan. The field consists of side-by-side lists, with the left side containing available policies and the right side containing policies to be triggered in the scan. Selecting a policy in either list will move the policy to the opposite list.

- **User Filter:** *(Required)* Filter for users to scan. The following options are available:



  - **User:** Allows scan to be filtered to a specified user. Selecting provides the following options:

    Choose User: *(Required)* Identifies single user to target for the scan. The field is open with autocomplete and requires a username.

  - **Users with manager:** Allows scan to be filtered to any user with a specified manager. Selecting provides the following option:

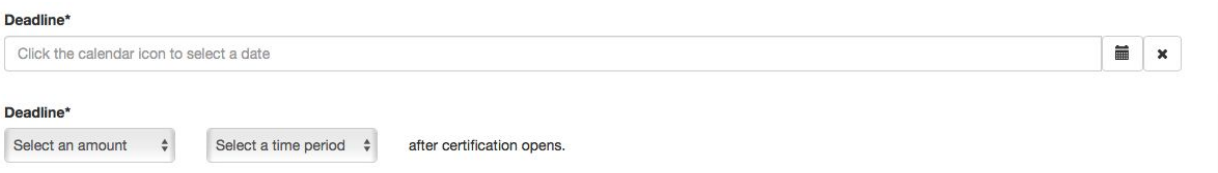
    Choose Manager: *(Required)* Identifies a user, with the user's subordinates targeted for the scan. The field is open with autocomplete and requires a username.

  - **All Users:** Allows the scan to be run with no filter, targeting all users

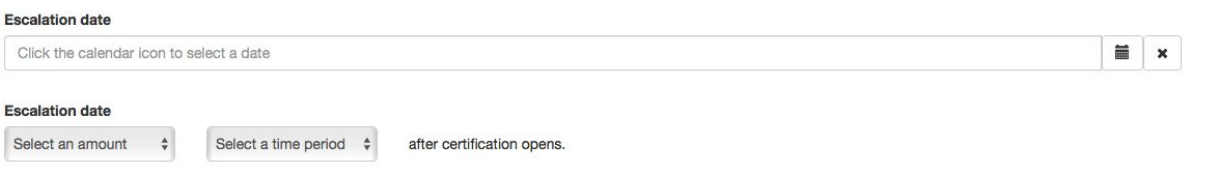
  - **Filter by user attribute:** Allows scan to be filtered to any user assigned to a specified instance of an attribute. Selecting provides the following option:

    Attribute Value: *(Required)* Attribute value for the specified attribute in the User Filter field, with users assigned the specified attribute value targeted for the scan. The Attribute Value field

is a dropdown allowing certifiable attribute values to be specified.



- **Expiration Date:** *(Required)* Specifies how long a violation should remain active. After the specified date or duration, the violation expires and becomes unavailable for modification.



- **Escalation Date:** Specifies if / when an escalation should occur prior to the date specified in the Expiration Date field. After the specified date or duration, a notification will be sent to the user or role specified.

Escalation Owner: *(Required)* If specifying an escalation date, the following fields become available to specify the escalation user or role to send a notification:

- **User:** Notifies specified user when an escalation occurs

- **Authorization Role:** Notifies specified group of users when an escalation occurs

- **Policy Owner Manager:** Notifies managers of policy owners

7.5 Reviewing Active Policy Scans

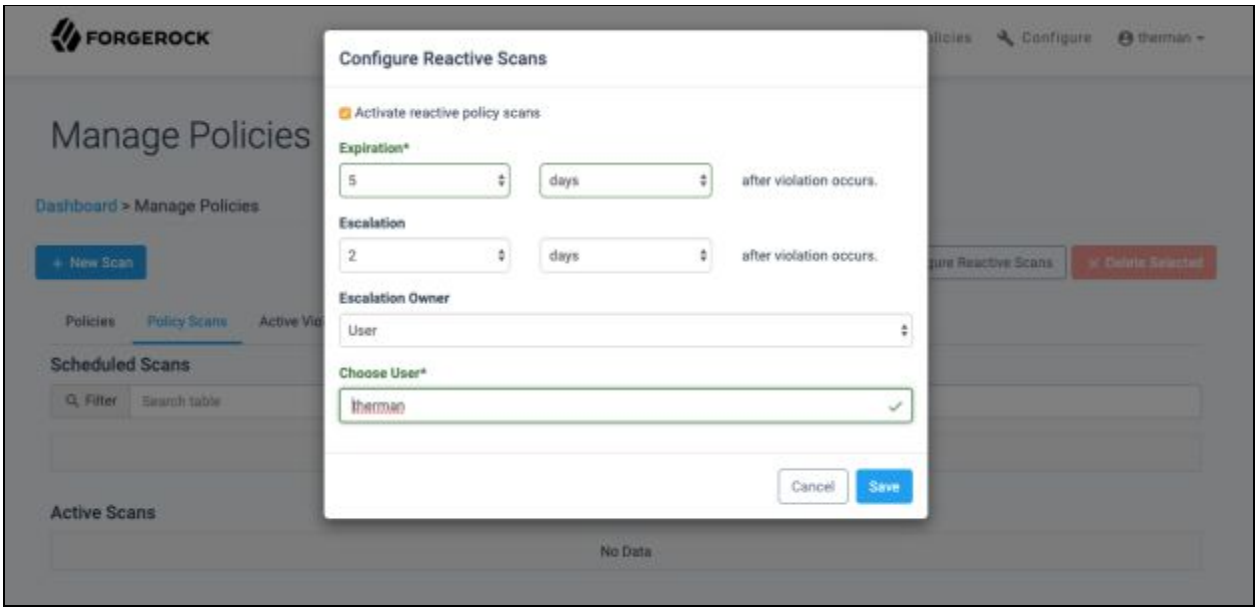
1. Navigate to the Manage Policies page, located in the Dashboard Management Dashboard under Policies

2. View the contents under the tab Policy Scans
   - **Active Scans:** Details information about running policy scans. Each line displays a summary of a policy scan with the following information:
     - **Scan Name:** Name of the running policy scan
     - **Scan Type:** Type of policy scan running. Values may include Ad-hoc or Scheduled.
     - **Policies:** Number of policies affected by the scan
     - **Scan Target Type:** Filter on users the scan is running. Values may include User, Users with manager, Users with application, All users or *attribute*.
     - **Scan Target Name:** Value of the filter specified in the Scan Target Type field. Only users matching the criteria are considered in the scan.
     - **Scan Progress:** Percentage complete for the scan

7.6 Configure Reactive Policy Scans

1. Navigate to the Manage Policies page, located in the Dashboard Management Dashboard under Policies

2. Select '**Configure Reactive Scans**' under the Policies Scans tab.



The following options become available:

- **Activate reactive policy scans:** Identifies if reactive policy scans are active or inactive. If unchecked, reactive scans will not run.
- **Expiration:** *(Required)* Specifies how long a violation should remain active. After the specified duration, a violation expires and becomes unavailable for modification.
- **Escalation:** Specifies if / when an escalation should occur prior to the date specified in the Expiration field. After the specified duration, a notification will be sent to the specified user or role.
- **Escalation Owner:** Target user or role for an escalation of a violation. The field is a dropdown with the following options:
    - **User:** Allows user to be specified as the escalation owner. The specified user will be notified for any escalations of reactive scan violations. Selecting details the following option:

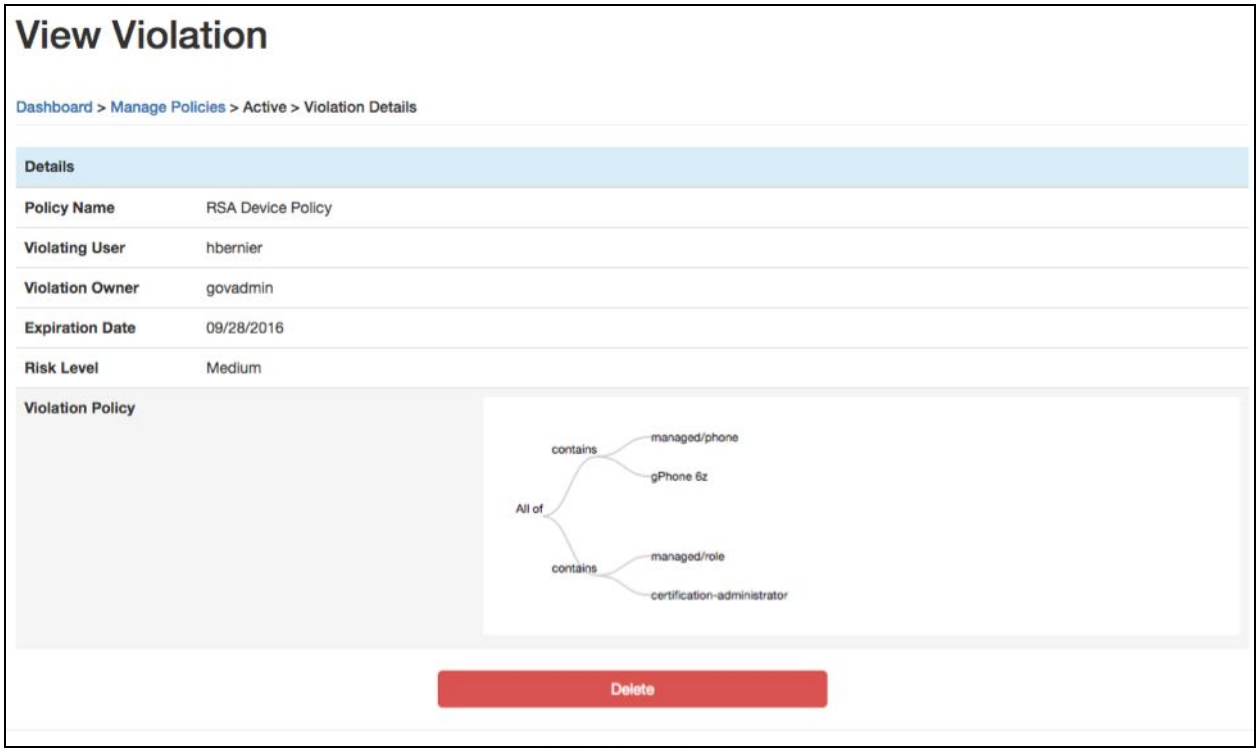
      Choose User: *(Required)* Identifies single user as the escalation owner. The field is open with autocomplete and requires a username.
    - **Policy Owner-Manager:** Provisions managers of policy owners affected by the policy scan escalation owners. All managers will be notified for any escalations of reactive scan violations.
    - **Authorization Role:** Allows an authorization role to be specified as the escalation owner. All users assigned the specified authorization role will be notified for any escalations of reactive scan violations. Selecting details the following option:

Authorization Role: *(Required)* Identifies authorization role as the escalation owner. The Authorization Role field is a dropdown, allowing authorization role values to be specified.

7.7 Modifying Active Violations

1. Navigate to the Manage Policies page, located in the Dashboard Management Dashboard under Policies

2. View the contents under the tab Active Violations
   - **Active Violations:** Details information about active violations requiring manual remediation. Each line displays a summary of a violation with the following information:
     - **Delete Selected:** Allows the administrator to delete a violation. To utilize, select the checkboxes next to the policy scans to delete, then select '**Delete Selected.**'
     - **Policy:** Policy that generated the violation
     - **User:** User targeted by the violation
     - **Owner:** User responsible for the violation as specified in generating the policy
     - **Risk Level:** Risk level for the violation as specified in generating the policy on a 1 - 10 scale. A risk score of 1 indicates low risk target for the certification, whereas a risk score of 10 indicates high risk.
     - **Expiration Date:** Specifies how long a violation should remain active as specified by generating the policy scan. After the specified duration, a violation expires and becomes unavailable for modification.

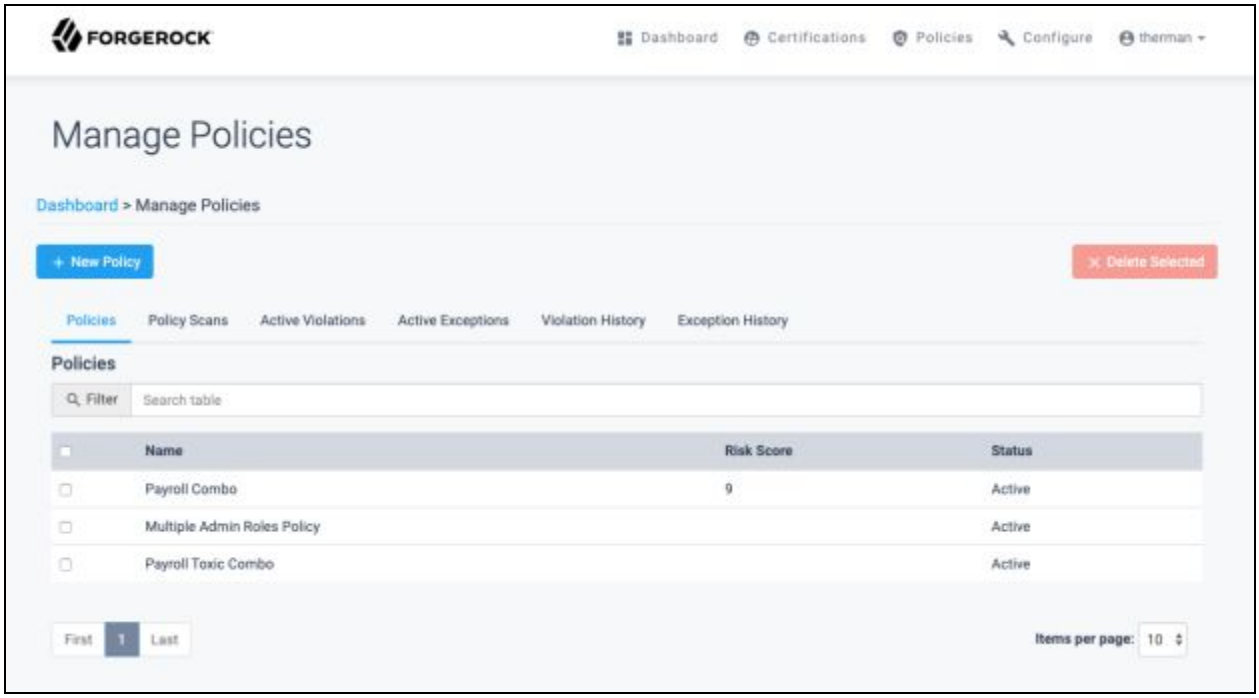


3. Select a Violation from the Active Violations list
   - **Details:** Information regarding a selected violation

  - **Policy Name:** Policy that generated the violation
  - **Violating User:** User targeted by the violation
  - **Violation Owner:** User responsible for the violation as specified in generating the policy
  - **Expiration Date:** Specifies how long a violation should remain active as specified by generating the policy scan. After the specified duration, a violation expires and becomes unavailable for modification.
  - **Risk Level:** Risk level for the violation as specified in the generating policy on a 1 - 10 scale. A risk score of 1 indicates low risk target for the certification, whereas a risk score of 10 indicates high risk.
  - **Violation Policy:** Graphical representation of the violation policy as specified with the Expression Builder in generating the policy
- **Delete:** Allows the administrator to delete the violation

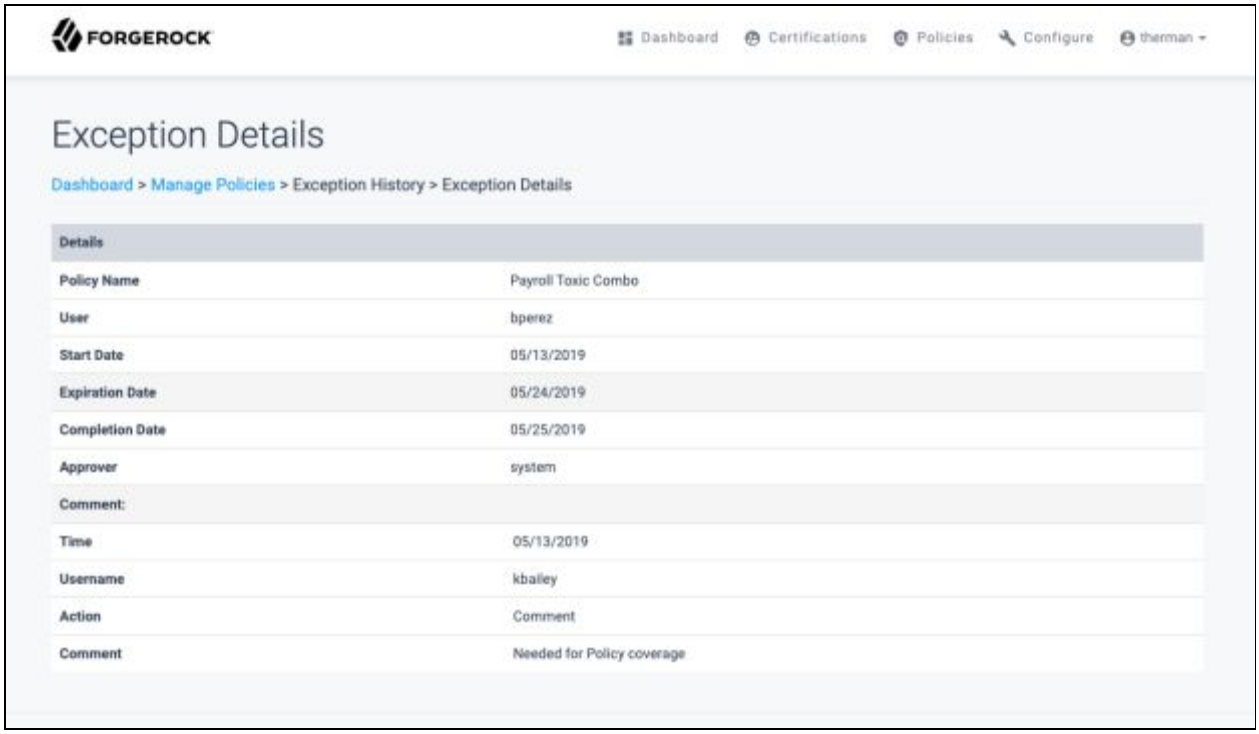
7.8 Modifying Active Exceptions

1. Navigate to the Manage Policies page, located in the Dashboard Management Dashboard under Policies



2. View contents under the Active Exceptions tab
   - **User-Owned Exceptions:** Details information about exceptions currently assigned to specified users. Each line displays a summary of an exception with the following information:
     - **User:** User targeted by the exception
     - **Policy:** Policy that generated the violation requiring the exception
     - **Complete Date:** Date the exception becomes inactive

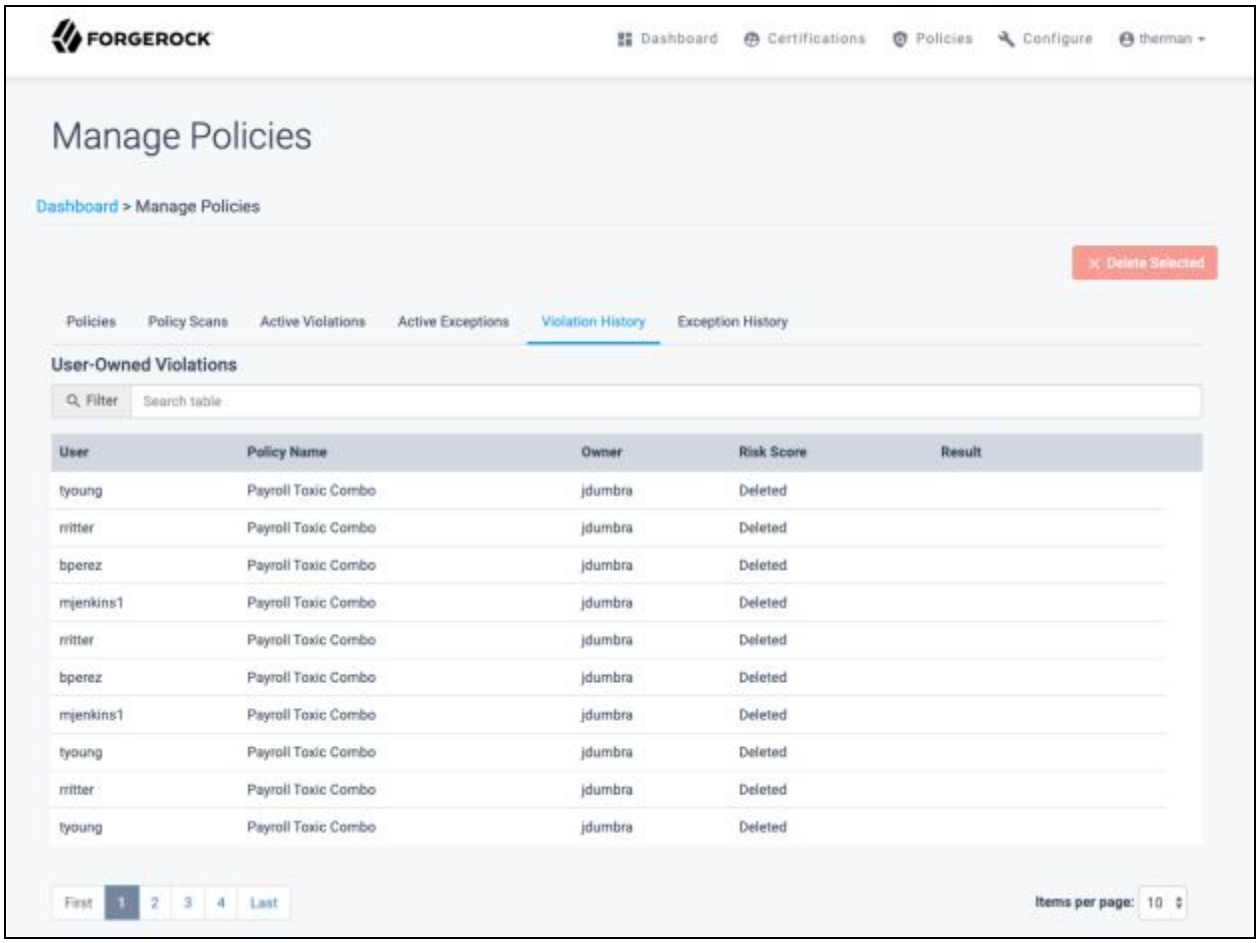
- **Role-Owned Exceptions:** Details information about exceptions currently assigned to specified roles. Each line displays a summary of an exception with the following information:
    - **User:** User targeted by the exception
    - **Policy:** Policy that generated the violation requiring the exception
    - **Complete Date:** Date the exception becomes inactive



3. Select an Exception from the User-Owned Exceptions or Role-Owned Exceptions lists
    - **Details:** Information regarding a selected violation
        - **Policy Name:** Policy that generated the violation requiring the exception
        - **User:** User targeted by the violation
        - **Start Date:** First effective date of the exception
        - **Expiration Date:** Date the exception is targeted becomes inactive
        - **Approver:** User who generated the exception
    - **Cancel:** Allows an administrator to cancel an exception. After selecting, the exception becomes inactive and the user is once again eligible for violation by the targeted policy.

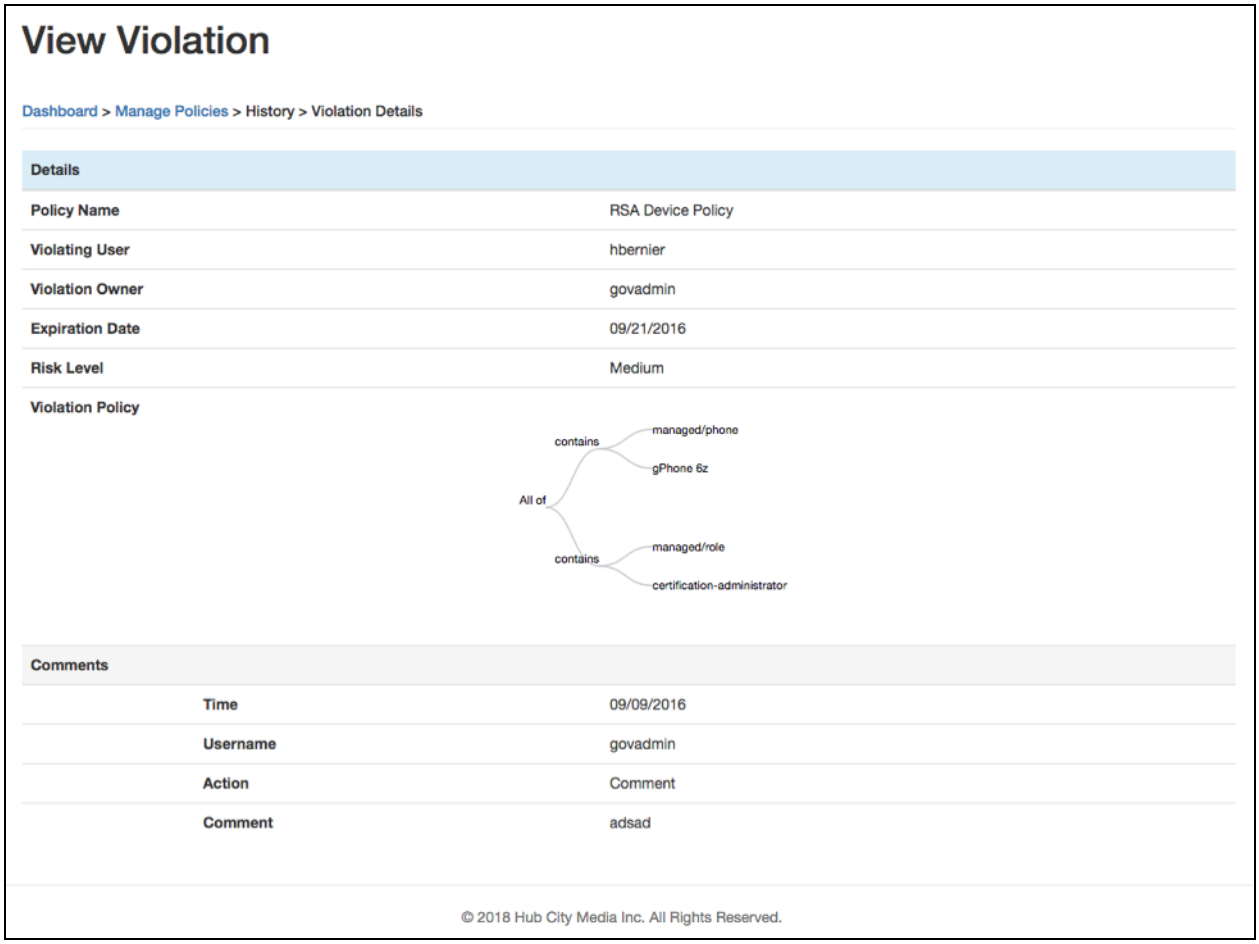
7.9 Reviewing Violation History

1. Navigate to the Manage Policies page, located in the Dashboard Management Dashboard under Policies



2. View contents under the Violation History tab
   - **User-Owned Violations:** Details information about violations previously assigned to specified users. Each line displays a summary of a violation with the following information:
     - **User:** User targeted by the violation
     - **Policy Name:** Policy that generated the violation
     - **Owner:** User responsible for the violation as specified in generating the policy
     - **Risk Level:** Risk level for the violation as specified in generating the policy on a 1 - 10 scale. A risk score of 1 indicates low risk target for the certification, whereas a risk score of 10 indicates high risk.
     - **Result:** Action taken on the violation. Values may include Exception or Remediated.

- **Group-Owned Violations:** Details information about violations previously assigned to specified roles. Each line displays a summary of a violation with the following information:
    - **User:** User targeted by the violation
    - **Policy Name:** Policy that generated the violation
    - **Owner:** User responsible for the violation as specified in generating the policy
    - **Risk Level:** Risk level for the violation as specified in generating the policy on a 1 - 10 scale. A risk score of 1 indicates low risk target for the certification, whereas a risk score of 10 indicates high risk.
    - **Result:** Action taken on the violation. Values may include Exception or Remediated.

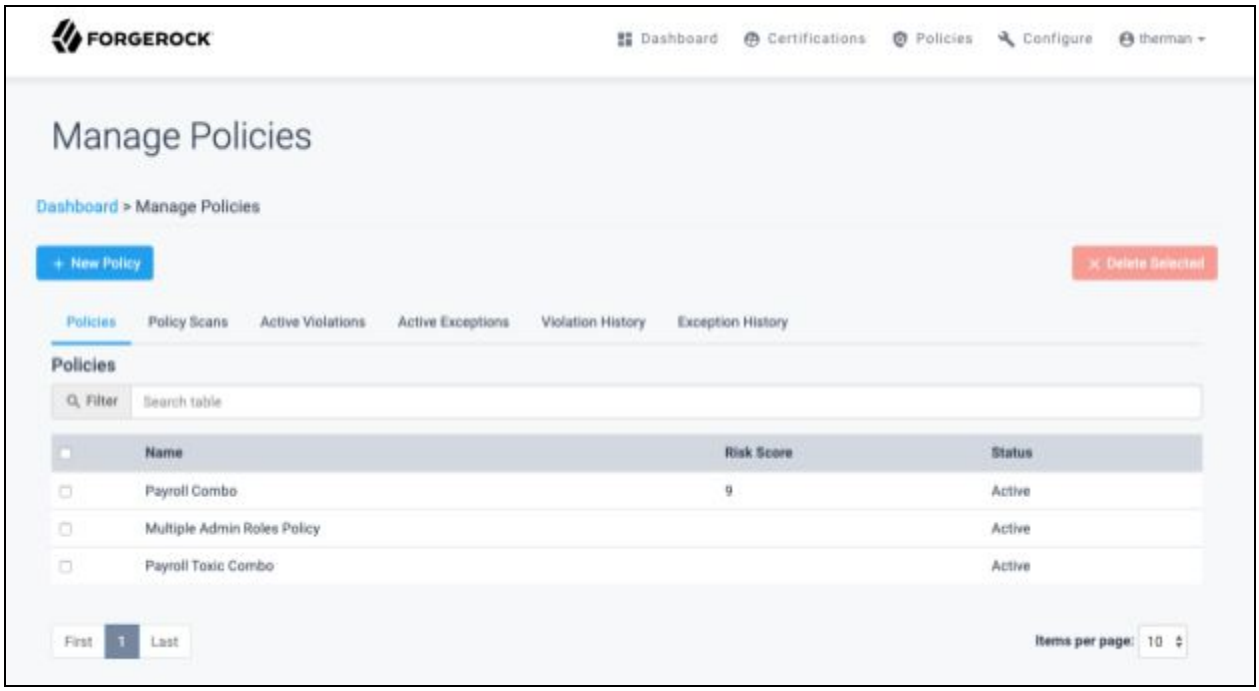


3. Select a Violation from the User-Owned Violations or Group-Owned Violations list
    - **Details:** Information regarding a selected violation
        - **Policy Name:** Policy that generated the violation
        - **Violating User:** User targeted by the violation
        - **Violation Owner:** User responsible for the violation as specified in generating the policy

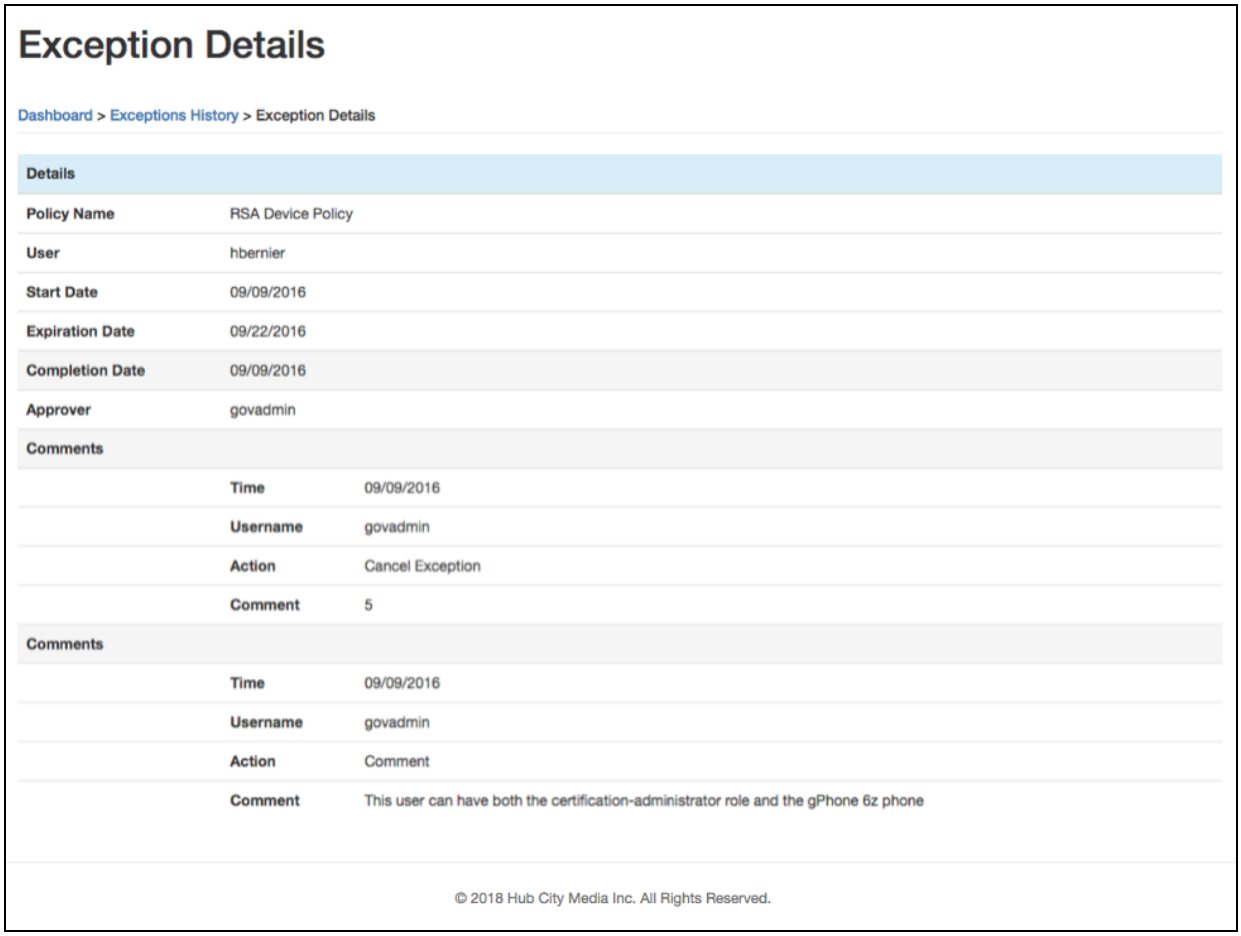
- **Expiration Date:** Last date a violation should have remained active as specified by generating the policy scan
- **Risk Level:** Risk level for the violation as specified in generating the policy on a 1 - 10 scale. A risk score of 1 indicates low-risk target for the certification, whereas a risk score of 10 indicates high risk.
- **Violation Policy:** Policy that generated the violation

7.10 Reviewing Exception History

1. Navigate to the Manage Policies page, located in the Dashboard Management Dashboard under Policies



2. View contents under the tab Exception History
   - **User-Owned Exceptions:** Details information about exceptions previously assigned to specified users. Each line displays a summary of an exception with the following information:
     - **User:** User targeted by the exception
     - **Policy:** Policy that generated violation requiring the exception
     - **Complete Date:** Date the exception becomes inactive
   - **Group-Owned Exceptions:** Details information about exceptions previously granted by specified roles. Each line displays a summary of an exception with the following information:
     - **User:** User targeted by the exception
     - **Policy:** Policy that generated violation requiring the exception
     - **Complete Date:** Date the exception becomes inactive



Exception Details

Dashboard > Exceptions History > Exception Details

Details		
Policy Name	RSA Device Policy	
User	hbernier	
Start Date	09/09/2016	
Expiration Date	09/22/2016	
Completion Date	09/09/2016	
Approver	govadmin	
Comments		
	Time	09/09/2016
	Username	govadmin
	Action	Cancel Exception
	Comment	5
Comments		
	Time	09/09/2016
	Username	govadmin
	Action	Comment
	Comment	This user can have both the certification-administrator role and the gPhone 6z phone

3. Select an Exception from the User-Owned Exceptions or Group-Owned Exceptions list
   - **Details:** Information regarding a selected violation
     - **Policy Name:** Policy that generated violation requiring the exception
     - **User:** User targeted by violation
     - **Start Date:** First effective date of the exception
     - **Expiration Date:** Date the exception was targeted to become inactive
     - **Completion Date:** Date the exception actually became inactive
     - **Approver:** User who generated the exception

8 System Settings

8.1 Global

8.1.1 General

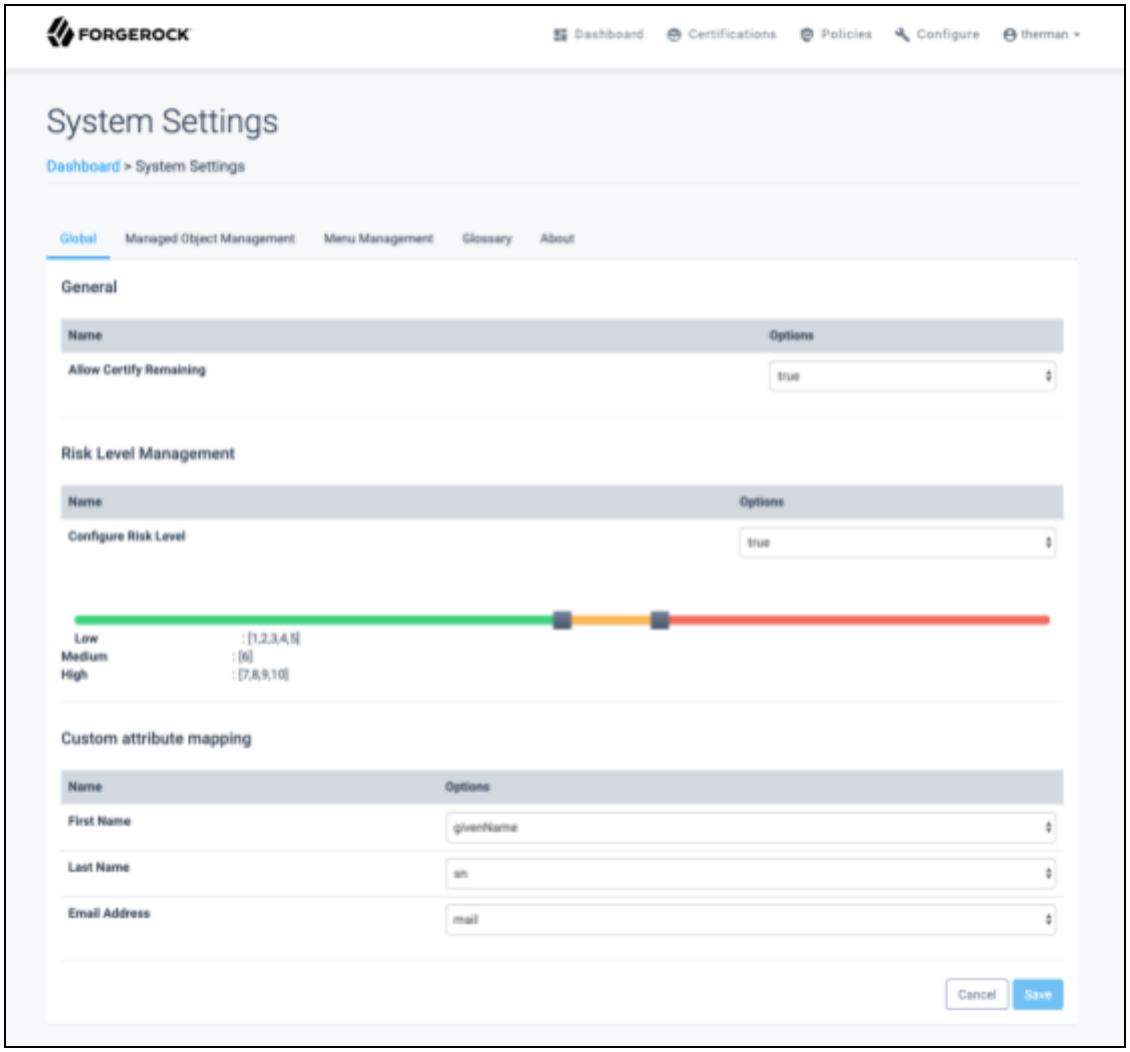
Allow Bulk Stage Actions: If set to **True,** certifiers are able to certify all users at once for a specific campaign. If set to **False,** certifiers will need to certify each user individually.

Note: It is best practice to set the Allow Bulk Stage Actions option to False as it prevents 'rubber stamping'

8.1.2 Risk Level Management

Risk level Management allows an administrator to adjust levels of risk defined as Low, Medium and High.

1. Navigate to the System Settings page, located in the Dashboard Management Dashboard under System Settings



2. View contents under the Risk Level Management header

Configure Risk Level: Allows for the Risk Level to be turned on or off. When **False** the Risk Level scores are ignored and will not be filtered for any certifications.

Risk Level Management: Bar associates levels of risk (1 - 10) with types (Low - Green / Medium - Yellow / High - Red). Drag tabs to adjust the levels of risk. As tabs move, the adjustment is reflected in the table below the bar.

8.1.3 Custom Attribute Mapping

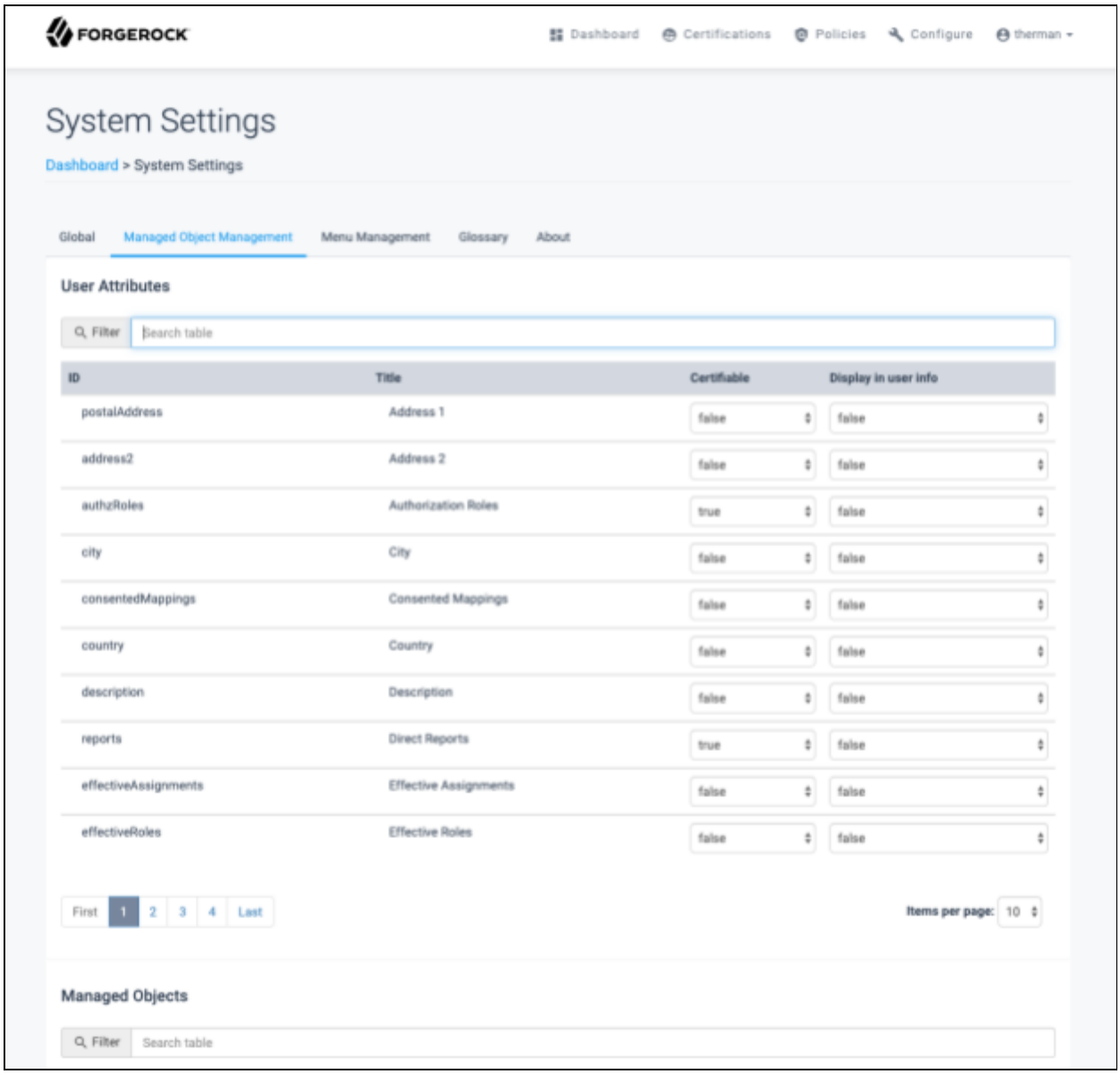
Custom attribute mapping

Name	Options
First Name	givenName
Last Name	sn
Email Address	mail

In order to display user information throughout the user interface, ForgeRock AccessReview relies on the values stored in the out-of-the-box IDM attributes username, givenName, sn, and email. However, to accommodate those implementations that use alternative custom attributes to store this basic information, an administrator can choose to map those attributes to the values available in this setting.

8.2 Managed Object Management

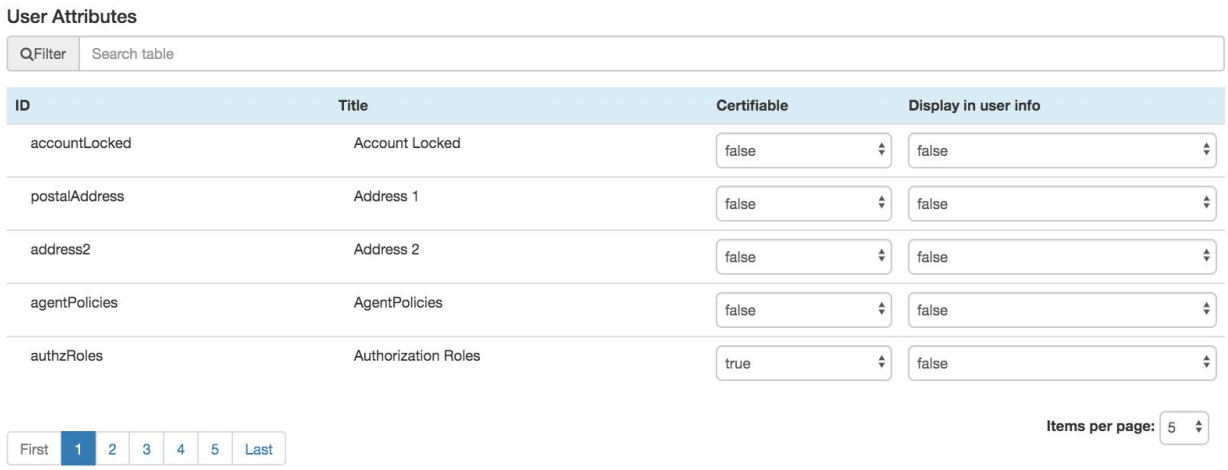
The Managed Object Management tab under System Settings allows an administrator to define risk level, certifiers and the ability to certify specific targets within the system



8.2.1 User Attribute Management

User Attribute Management allows an administrator to adjust user attributes and associated risk level instances to certifiable

1. Navigate to the System Settings page, located in the Dashboard Management Dashboard under System Settings



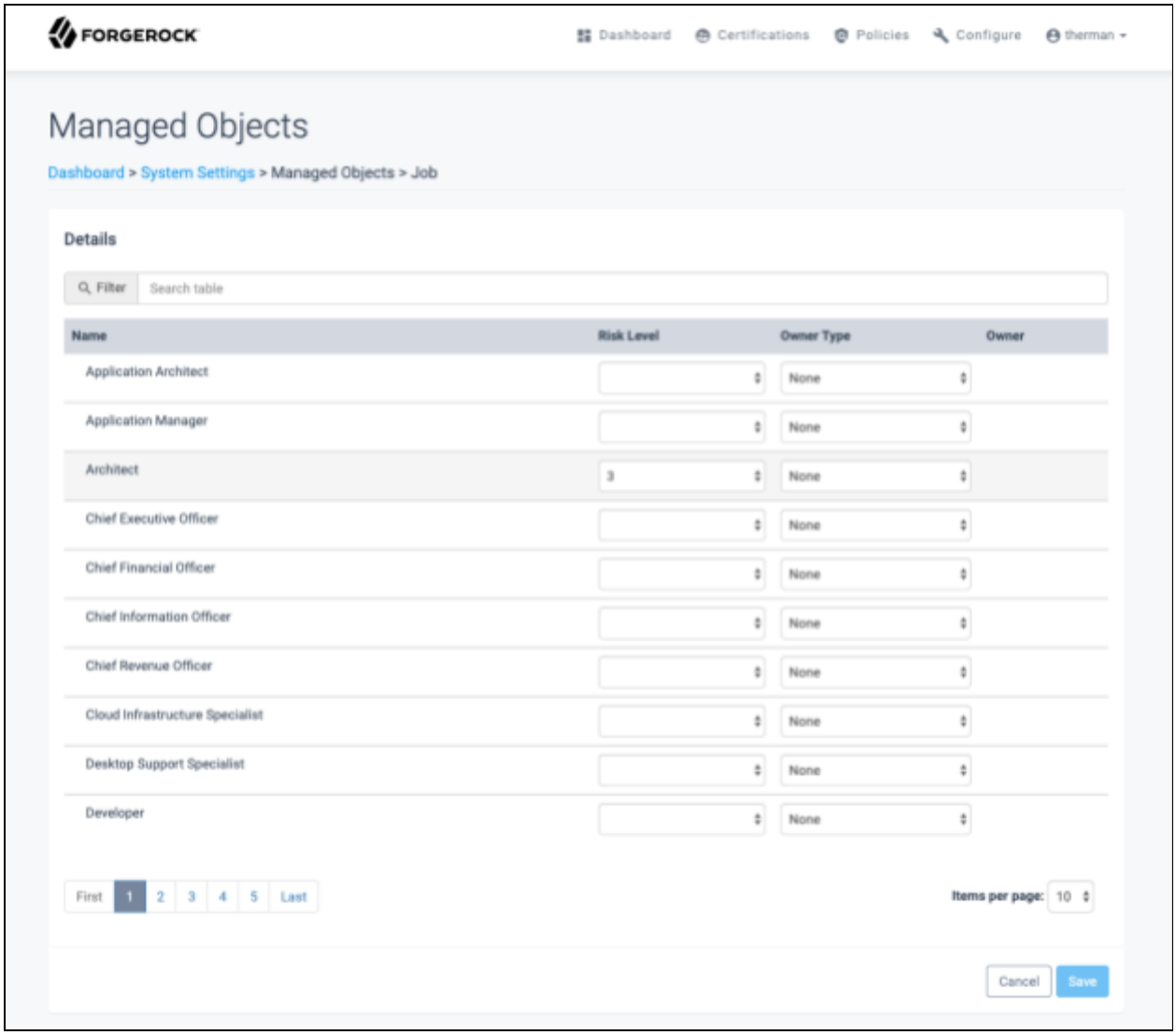
2. View the contents under the tab Managed Object Management
   - **User Attributes:** Details information about user attributes that can be marked as certifiable. Each line displays a summary of a user attribute with the following information:
     - **ID:** IID for the certifiable attribute
     - **Title:** Name for the certifiable attribute
     - **Certifiable:** Identifies if attribute is certifiable. Values may include true or false. If true, further options are available by selecting the row of the attribute.
     - **Display in user info:** Determines if the attribute will display in the user certification list and user event details page for user certifications. Note the following two caveats:
       - The attributes givenName, sn, and mail will always display in the user table regardless of this setting. If you use different attributes to track these values, please use the Custom Attribute Mapping in the Global section of the System Settings.
       - Relationship attributes on a user are not currently supported for this option. Those attributes are selectable, but will not display in a readable format for your end users. The one exception to this is the 'manager' attribute which will display the user's name.

8.2.2 Managed Object Management

Managed Object Management allows an administrator to adjust the risk level and owner associated with a managed object, e.g. assignment, role or custom object

1. Navigate to the System Settings page, located in the Dashboard Management Dashboard under System Settings

2. View the contents under the Managed Object Management tab
   - **Managed Objects:** Details information on managed objects available for certification. Note that in order to access and edit information about individual objects of each type, you *must* set an export key for the object type on the glossary page (see section 8.4.)
     - **ID:** ID of the certifiable object
     - **Title:** Name of the certifiable object



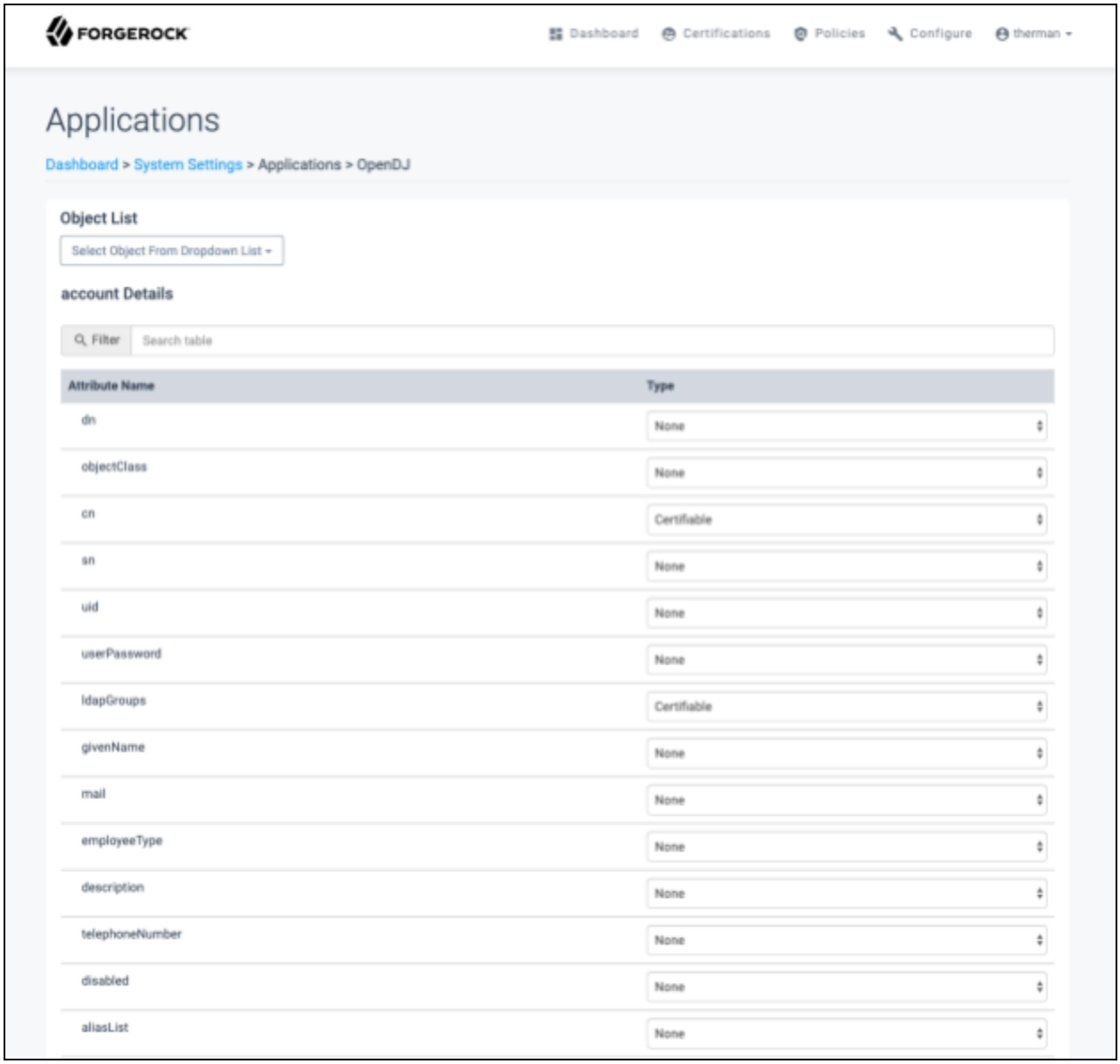
3. In order to view, add, or edit the managed object options, a key for the managed object in question must be set in advance. (See section 8.4.3)
4. Select a managed object from the Managed Objects list. Additional details are displayed with the following information:
   - **Details:** Details information on instances of the selected object, allowing the administrator to adjust risk level and owner for each instance
     - **Name:** Name of the instance to be certified
     - **Risk Level:** Risk level associated with the object instance. Values may include a level between 1 - 10. A risk score of 1 indicates low risk target for the assignment, whereas a risk score of 10 indicates high risk.
     - **Owner Type:** Type of owner for the object instance. The value of this field will affect options for Owner.
       - **None:** Does not assign owner to the object instance
       - **User:** Assigns a specific user as owner. Selecting makes the Owner field open with autocomplete.
       - **Role:** Assigns a role as owner. Selecting makes the Owner field a drop-down with available roles.
     - **Owner:** Identifies owner of the object. Value is used to determine who receives an object certification for the object instance completion as well as who is responsible for certifying the object in user certifications when the certifier is set to ‘Entitlement Owner.’

8.2.3 Application Management

Application Management allows an administrator to define which applications are certifiable and at what risk level they are certifiable. In addition, an administrator can adjust visibility with ability to certify at an attribute level for each application.

1. Navigate to the System Settings page, located in the Dashboard Management Dashboard under System Settings

2. View contents under the tab Managed Object Management
   - **Applications:** Details information on applications available for certification, allowing the administrator to adjust risk level and certifiable properties of the application
     - **Name:** Name of the application to be certified
     - **Certifiable:** Identifies whether the application is certifiable. Values may include true or false. If true, further options are available by selecting the row of the application.
     - **Risk Level:** Risk level associated with the application. Values may include a level between 1 - 10. A risk score of 1 indicates low risk target for the assignment, whereas a risk score of 10 indicates high risk.
     - **Owner Type:** Type of owner for the object instance. The value of this field will affect options for Owner.
       - **None:** Does not assign owner to the object instance
       - **User:** Assigns a specific user as owner. Selecting makes the Owner field open with autocomplete.
       - **Role:** Assigns a role as owner. Selecting makes the Owner field a drop-down with available roles.
     - **Owner:** Identifies owner of the application. Value is used to determine who is responsible for certifying application related attributes in user certifications when the certifier is set to ‘Entitlement Owner’.



3. Select an application from the Applications list. The Certifiable field must be marked as true to continue. Additional details are displayed with the following information:
   - **Object List:** Controls the details to be displayed in the Object Details section. An account option should always be available to certify the single-valued attributes of the application. Each multi-valued attribute will appear as a separate option in the list. Fields can be adjusted in the object Details section for multiple options before being saved.
   - **object Details:** Details information about the attributes associated with the object identified in the Object List section, allowing the administrator to view the visibility and certifiable properties of an attribute or attribute instance within an application.
     - **Attribute Name:** Name of an attribute or attribute instance to be certified or displayed within a certification

- **Type:** Visible and certifiable properties of the attribute within a certification
  - **None:** Makes attribute non-certifiable and hidden in a certification
  - **Certifiable:** Makes attribute available for certification
  - **Displayable:** Makes attribute non-certifiable, but visible for reference within a certification

8.3 Menu Management

Menu Management allows an administrator to add / remove links to the top-right user dropdown menu. Follow the steps below to access the menu management page.

1. Navigate to the System Settings page located in the Management Dashboard. Select the **'Menu Management'** tab (reference the screenshot below).

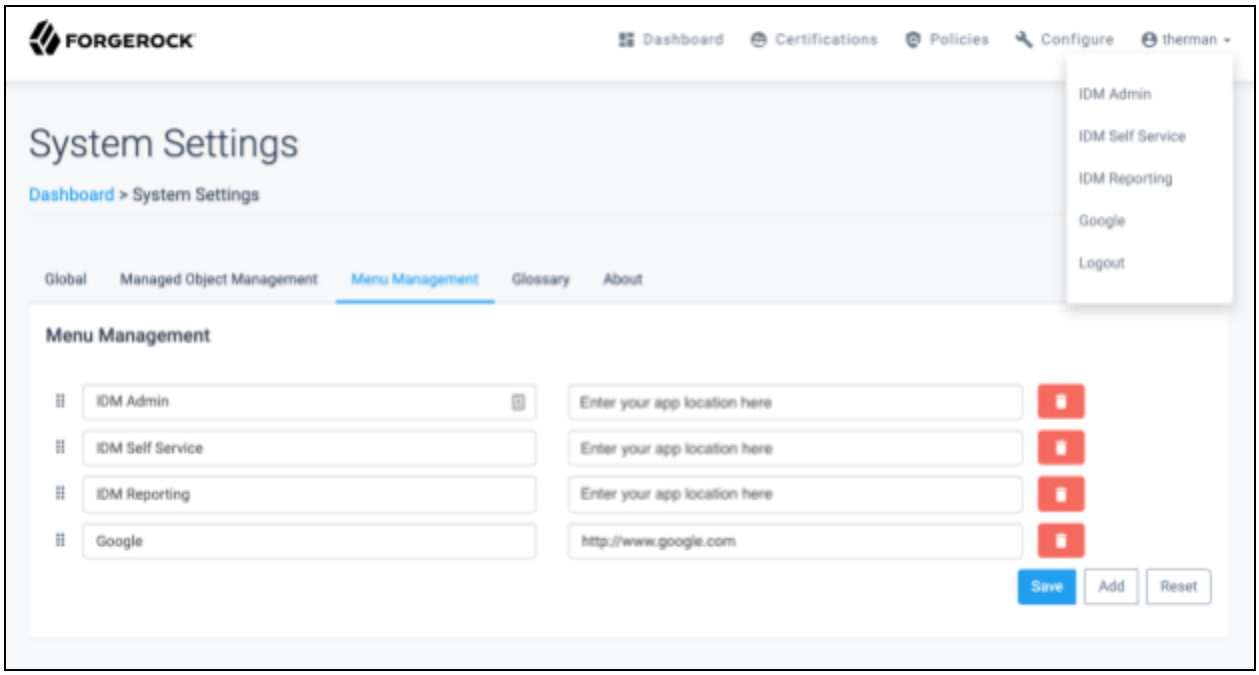
2. To add links to the menu, select **'Add'** A new blank row to be filled in will appear.

3. Enter the name of the link and the URL in the respective fields

4. When complete, select **'Save'**. A success message will appear

5. A new link is now available at any time on the top right dropdown menu

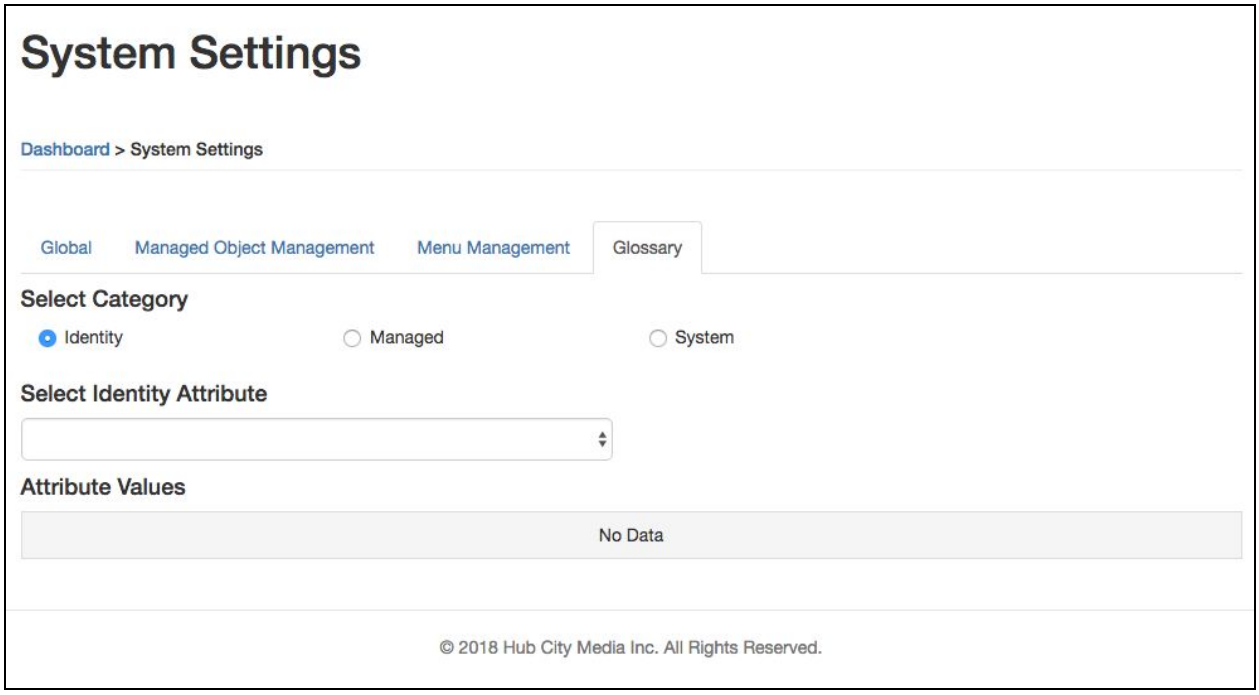
6. You can add/remove multiple links at once and save when complete



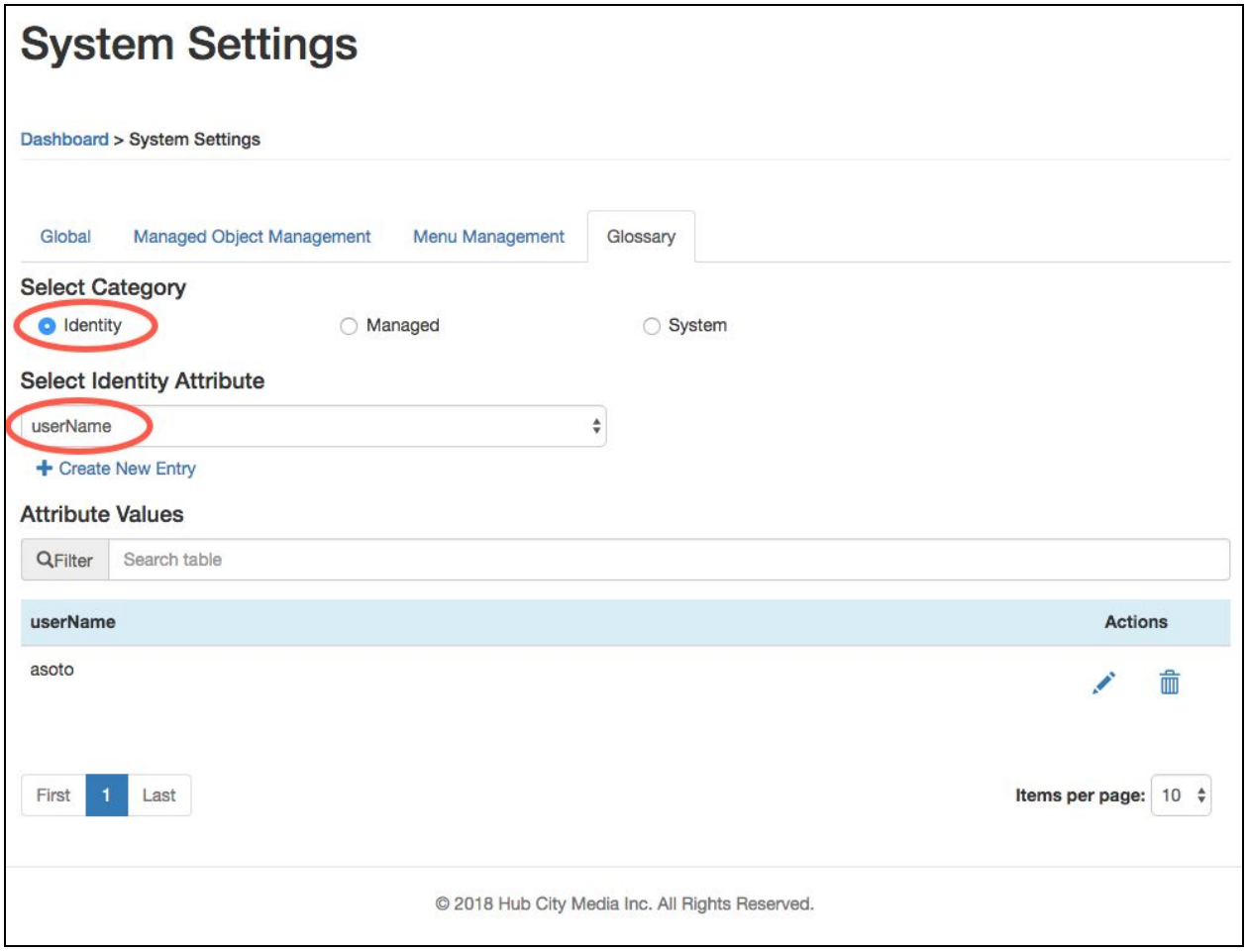
8.4 Glossary

The Glossary feature allows an admin to create metadata for a user, objects, or application attributes

1. Navigate to the System Settings page located in the Management Dashboard then select **'Glossary'** (reference screenshot below).

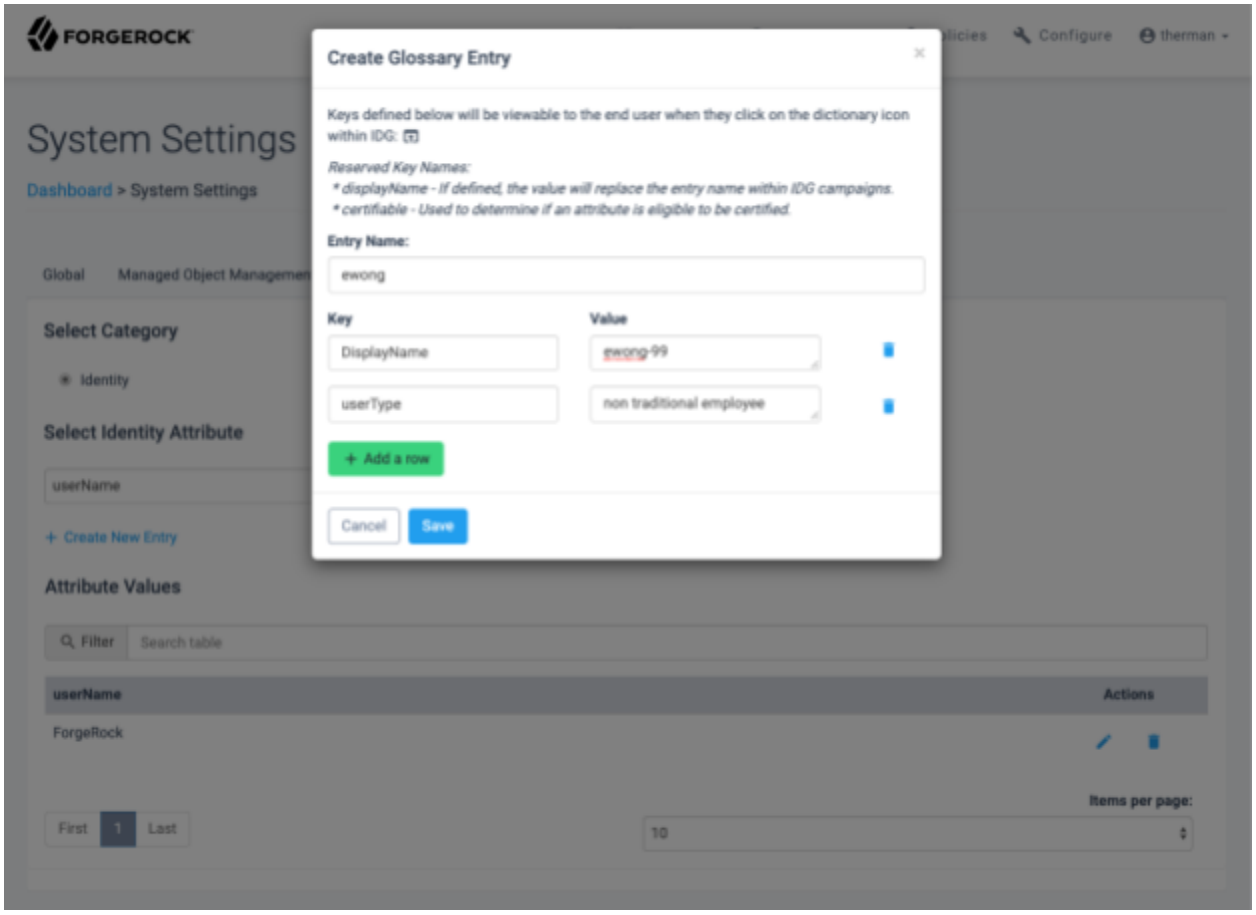


2. Adding glossary data to **<u>Identity</u>** attributes
   2.1. Under **'Select Category'**, select **'Identity',** and then select an attribute from the dropdown menu. A table with the current glossary data already added to the attribute selected (if any) or a message that says 'No Data'. Reference screenshot below.



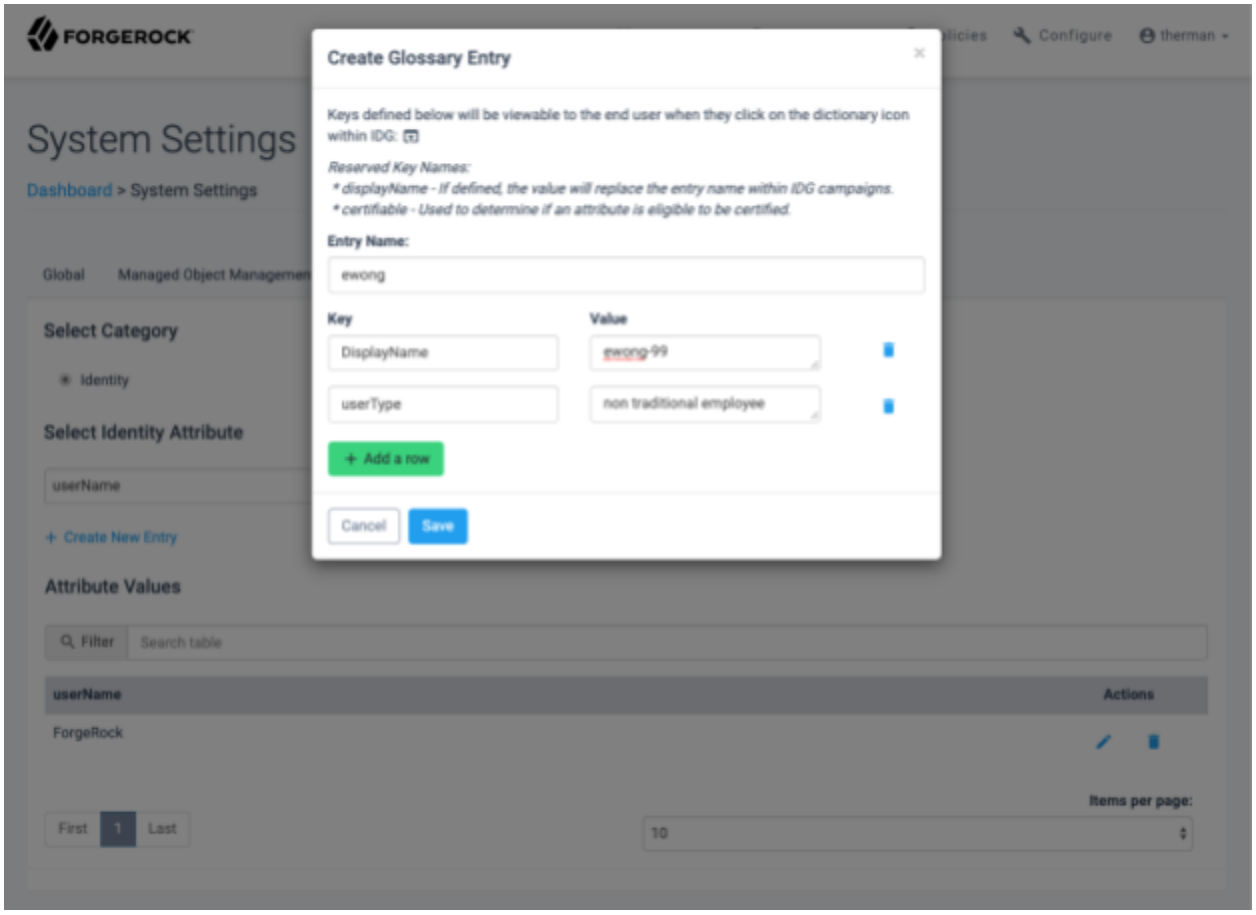
2.2. Select the button under the dropdown labeled **'+ Create New Entry'**. A modal window with the required form fields is displayed. Add additional rows as required. Complete all fields; then select **'Save'** when done. The modal will be dismissed and your new entry will show up on the table.

Note: 'displayName' - If defined as 'Key', the value will replace the entry name within AccessReview campaigns



After selecting **'Save'**, a new entry will display on the table

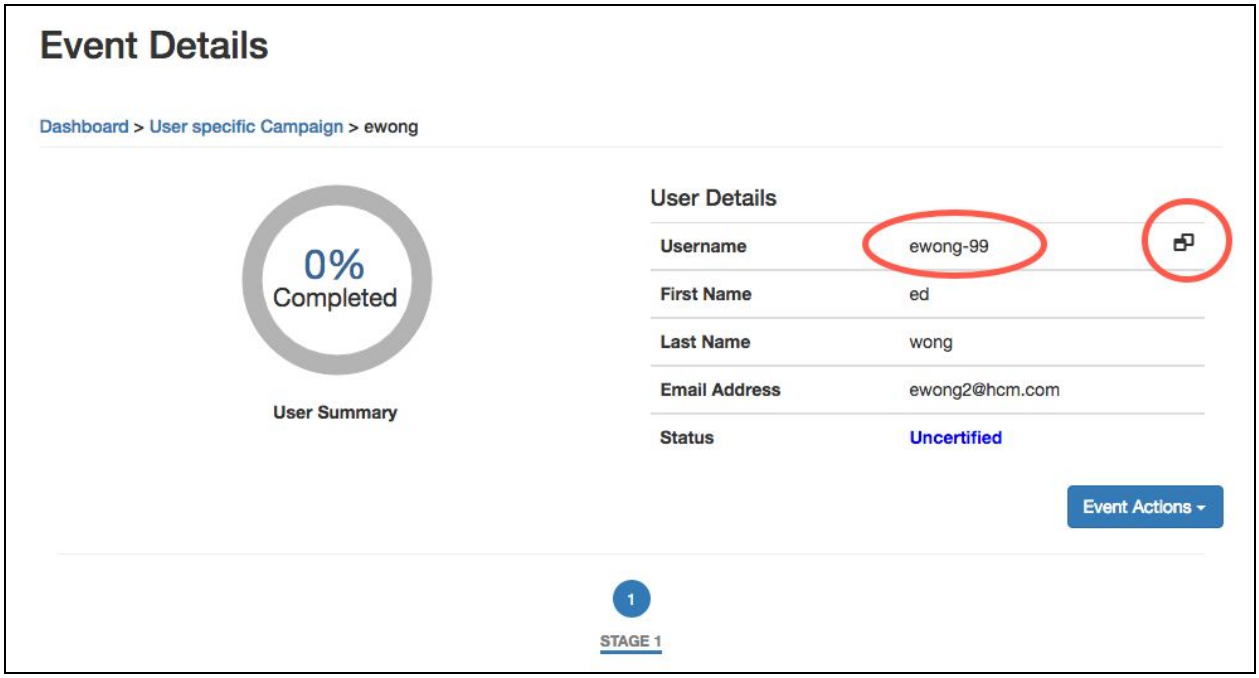
2.3. To edit an existing entry, select the pencil icon under the 'Actions' column. The same modal will show up with a few key changes:
   2.3.1. The title says 'Edit Glossary Entry'
   2.3.2. The entry Name field is un-editable
   2.3.3. Fields will be populated with existing data



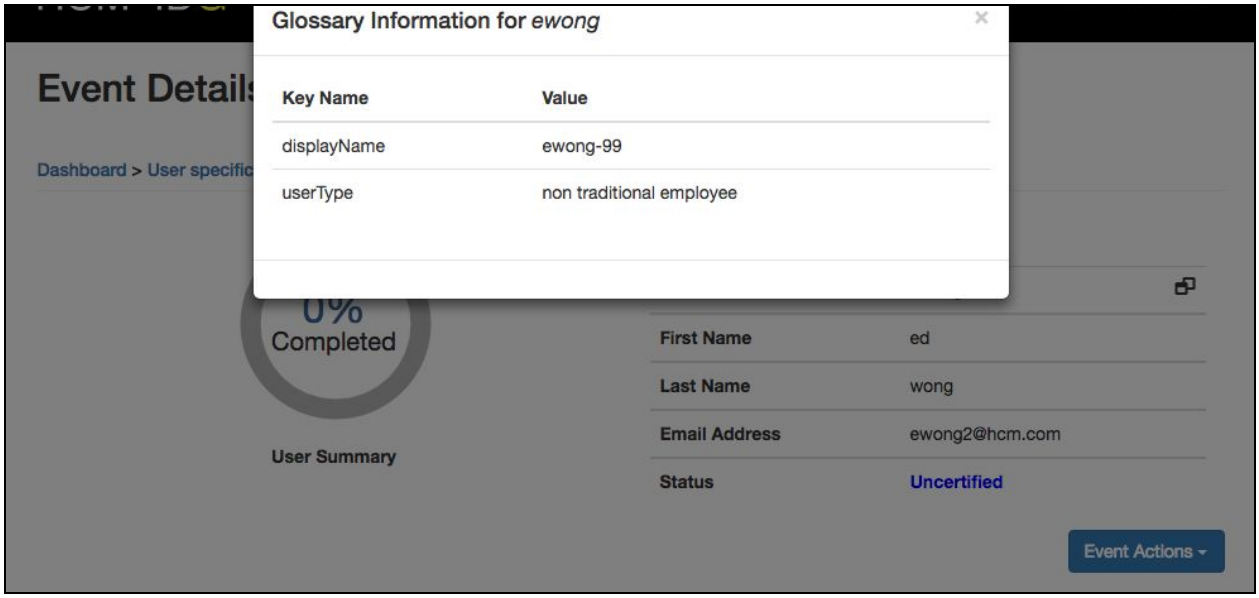
Make changes as needed and select **‘Save’** when done

2.4. To delete entries, select the trashcan icon under ‘Actions’ column
2.5. To view the Identity glossary entry just created in a campaign, navigate to a campaign and select on an event with the name of the user associated with the glossary data. An icon next to the user attribute will be displayed.

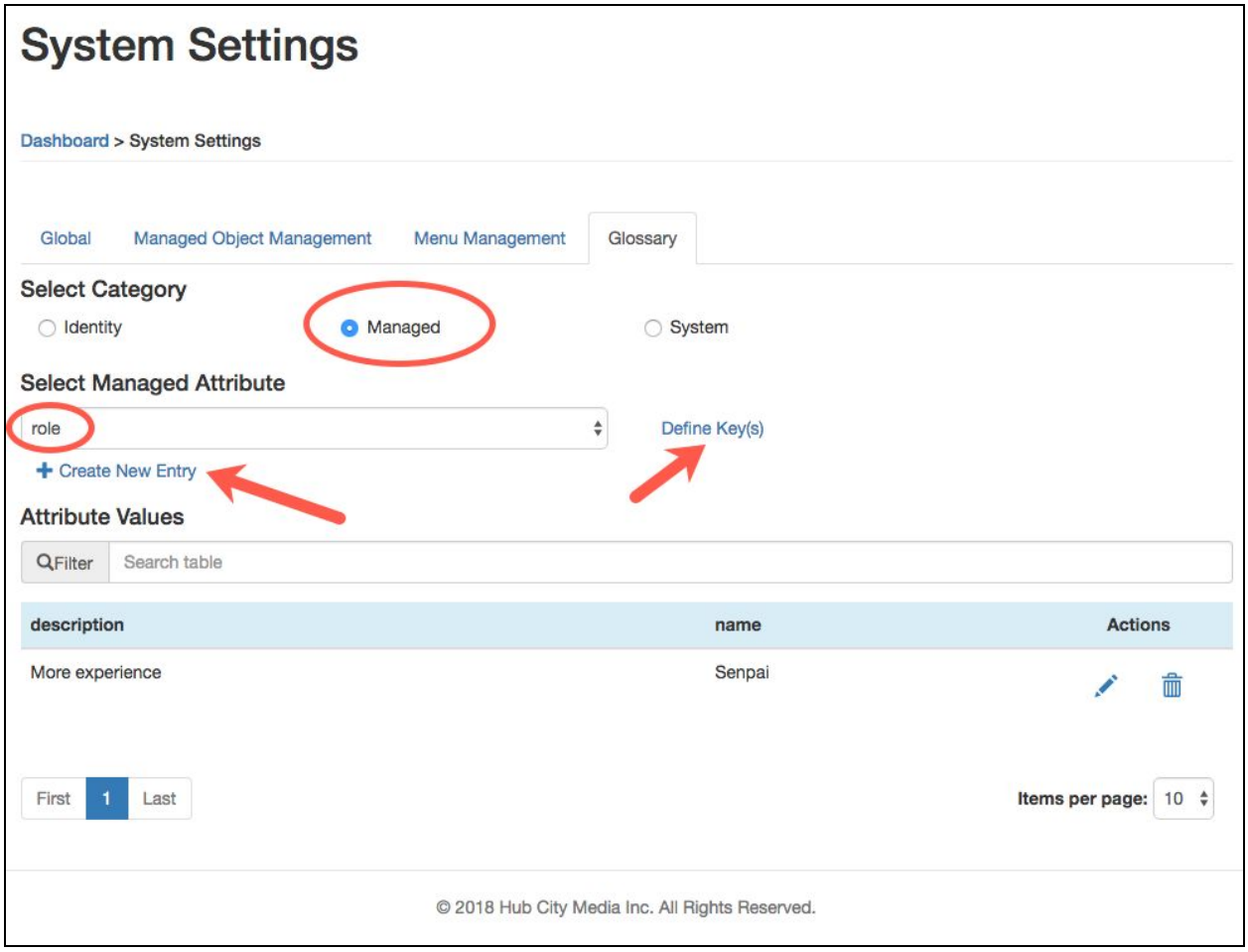
If ‘displayName’ was a key in glossary data, the actual attribute name will be replaced with the key value.



2.6. Select the icon to open the glossary modal. The modal displays the following information:
   2.6.1. The title of the modal 'Glossary Information for ewong'
   2.6.2. A table displaying 'Key Name' and 'Value' for each glossary entry

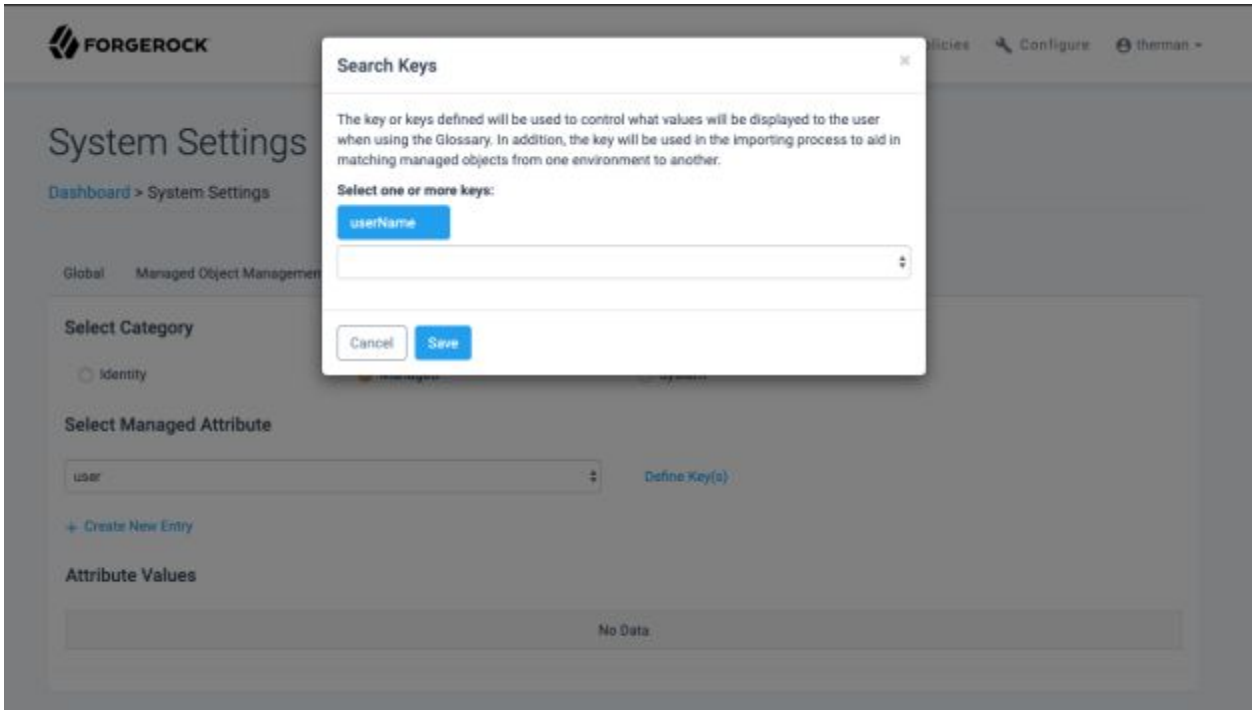


3. Adding glossary data to **Managed Object** attributes
   3.1. Under 'Select Category', select **'Managed'** and select a value from the dropdown

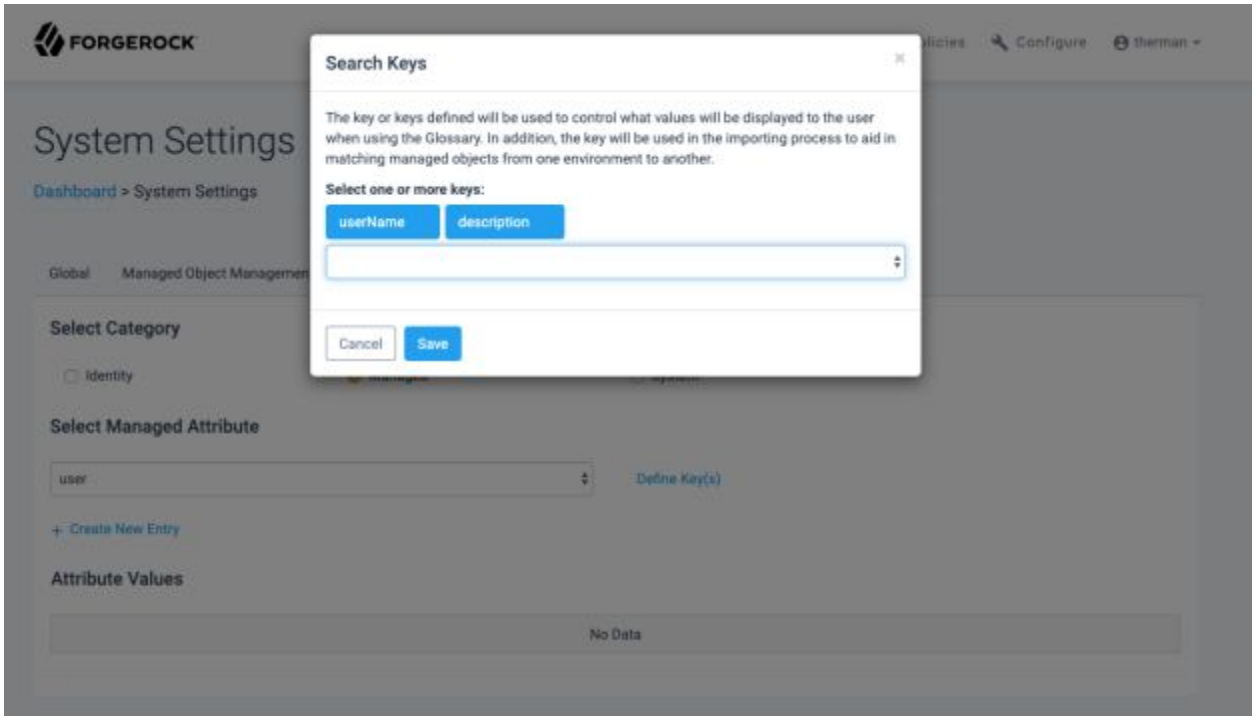


3.2. At this point, select either '**+ Create New Entry**' or **'Define Key(s)'**

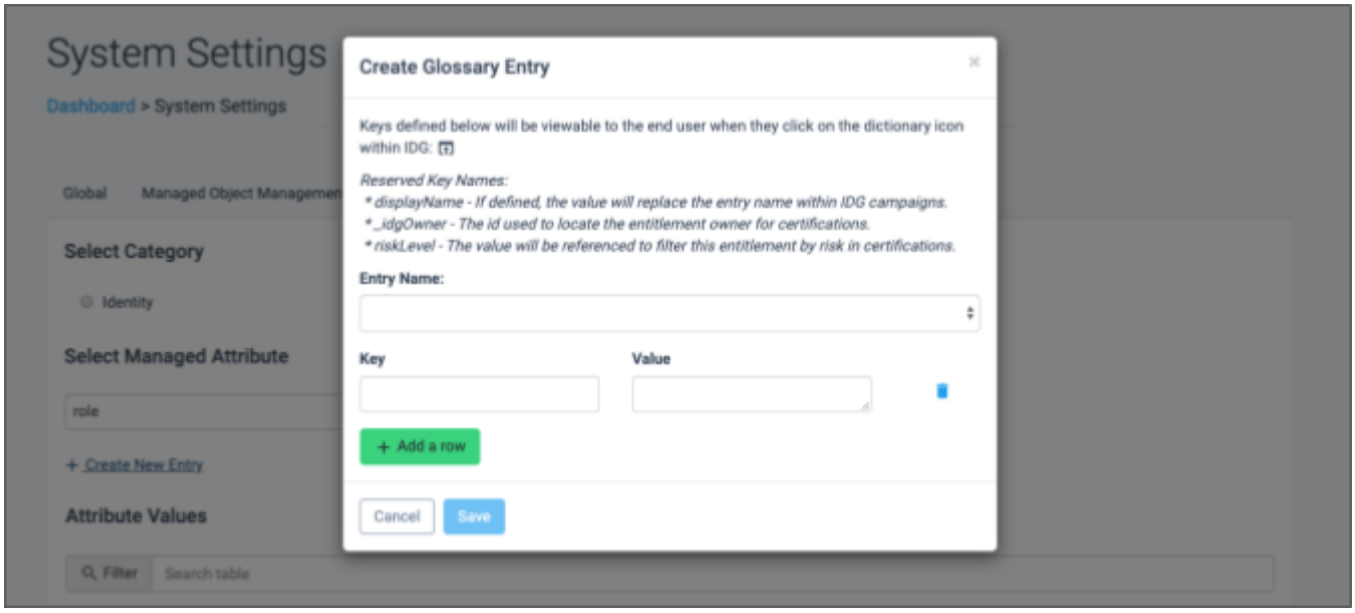
3.3. Once an option is selected from the dropdown, you are allowed to define keys for that object. Select **'Define Key(s)'**.



3.4. One key must be selected in order to be able to create a new glossary entry for a managed object. Once selected, select Save to apply changes.

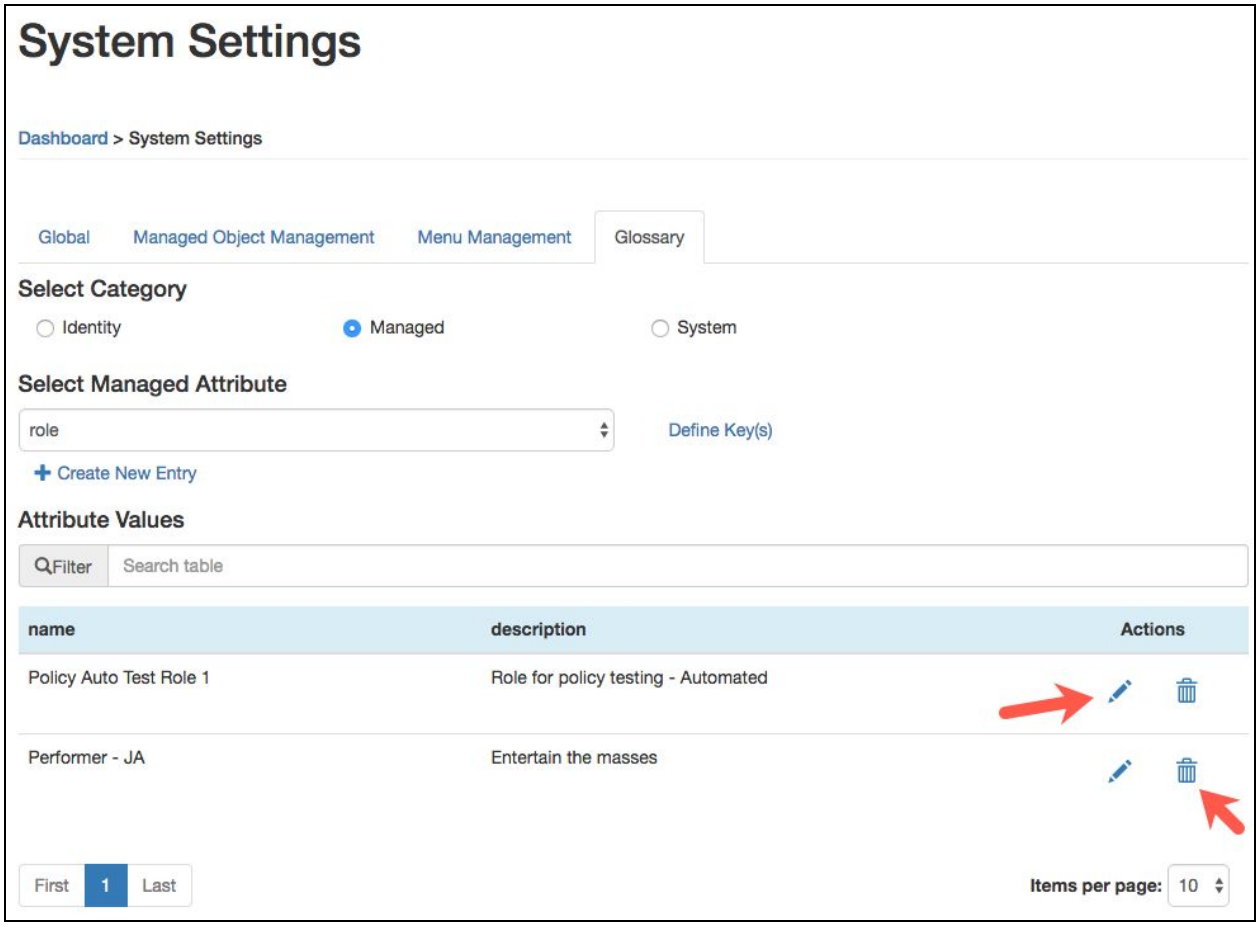


3.5. Create a new glossary entry by selecting **'+ Create New Entry'**, the following modal will display

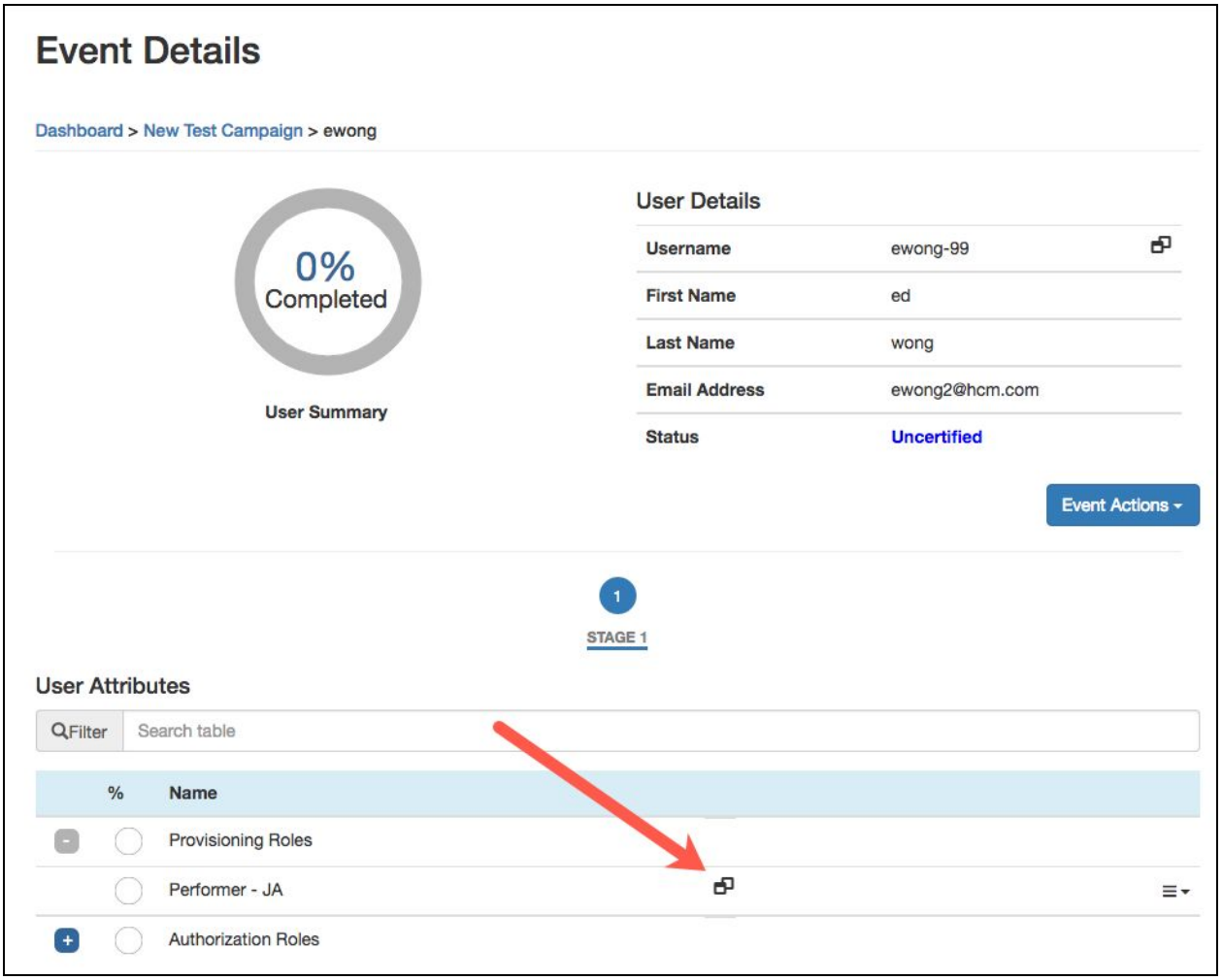


3.6. Select a value from the 'Entry Name' dropdown and define as many key/value pairs as required. When complete, select **'Save'**. The modal will close and the new entry will show on the table.

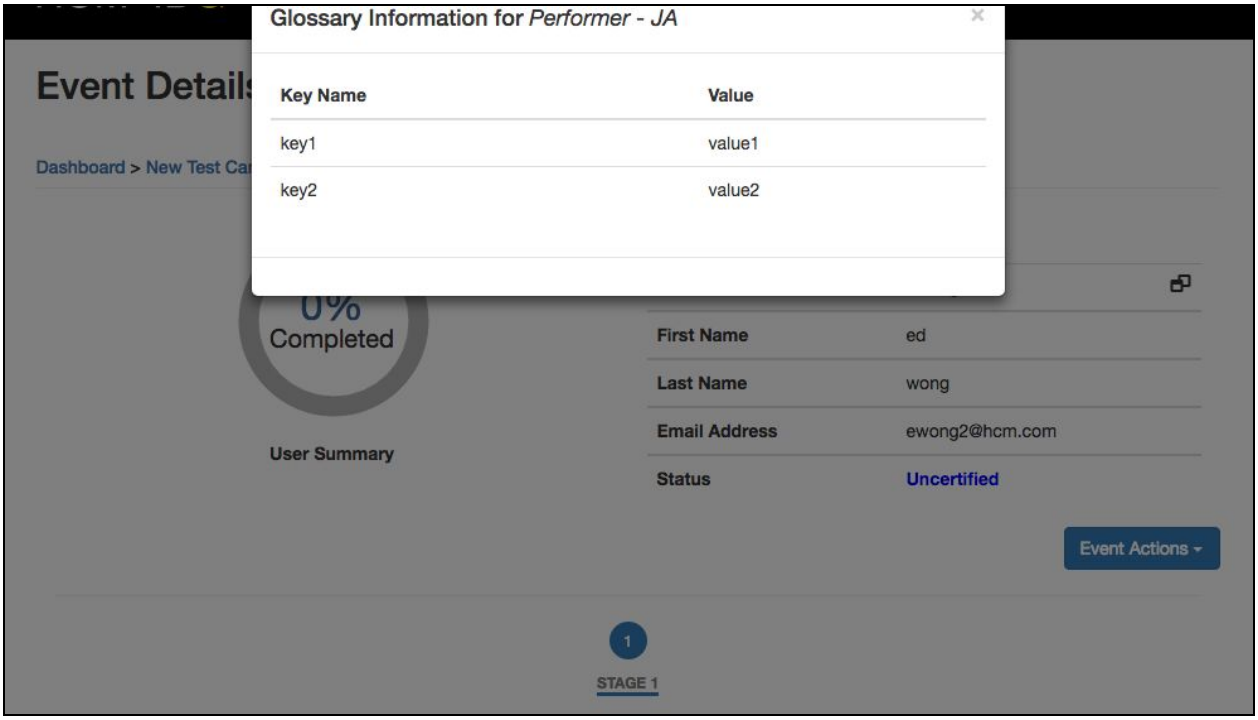
3.7. Edit the entry by selecting the pencil icon or delete an entry by selecting the garbage can icon.



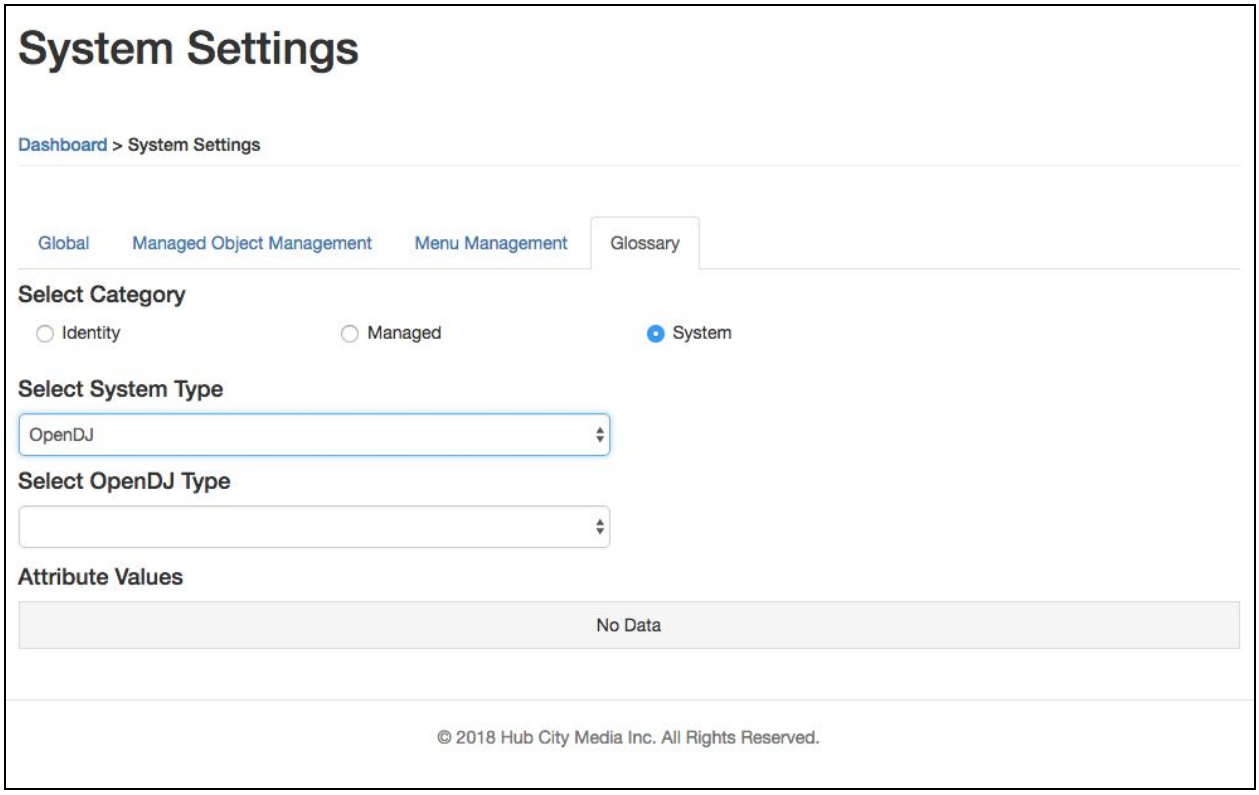
3.8. To view a new entry in a campaign, navigate to a campaign and select an event with a username that owns the role glossary data was created for.

3.9. 

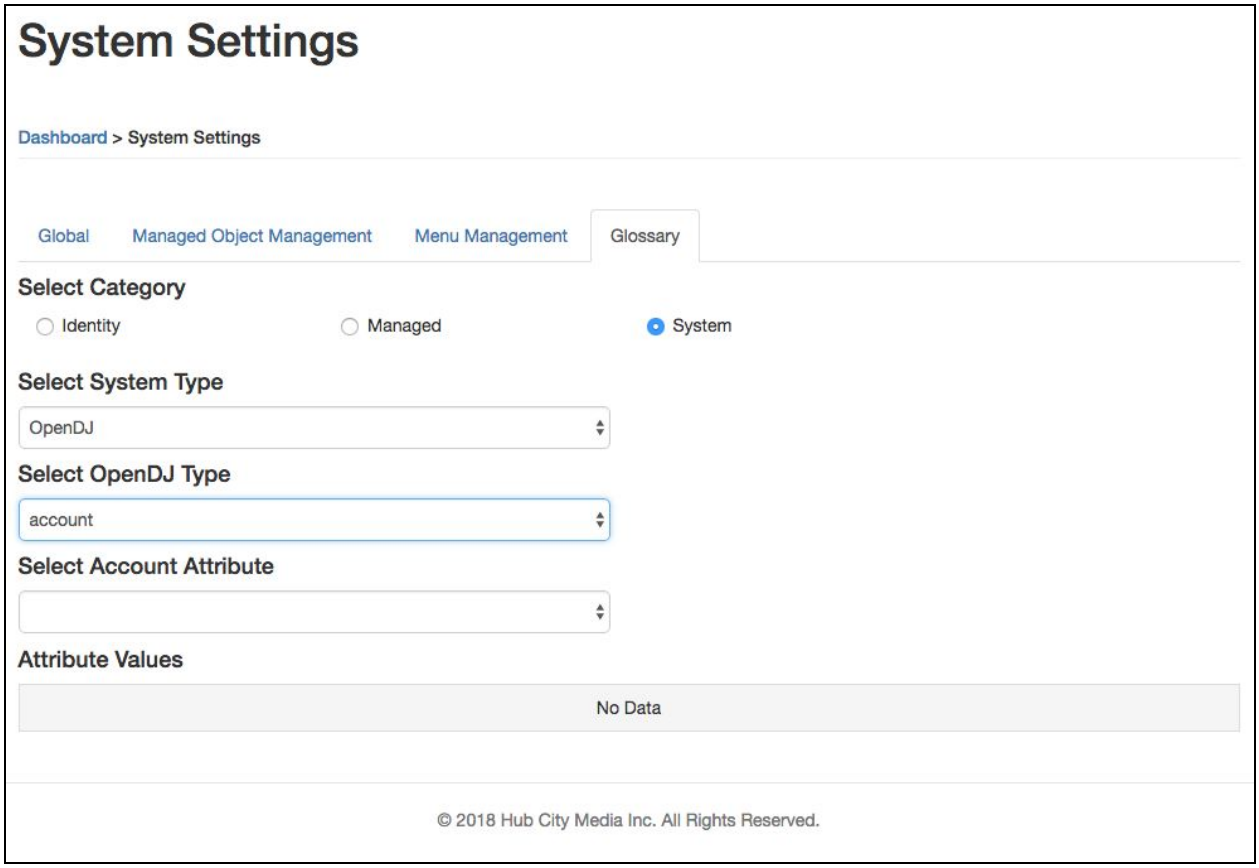
3.10. Select the icon to reveal the modal with the glossary

3.11. 

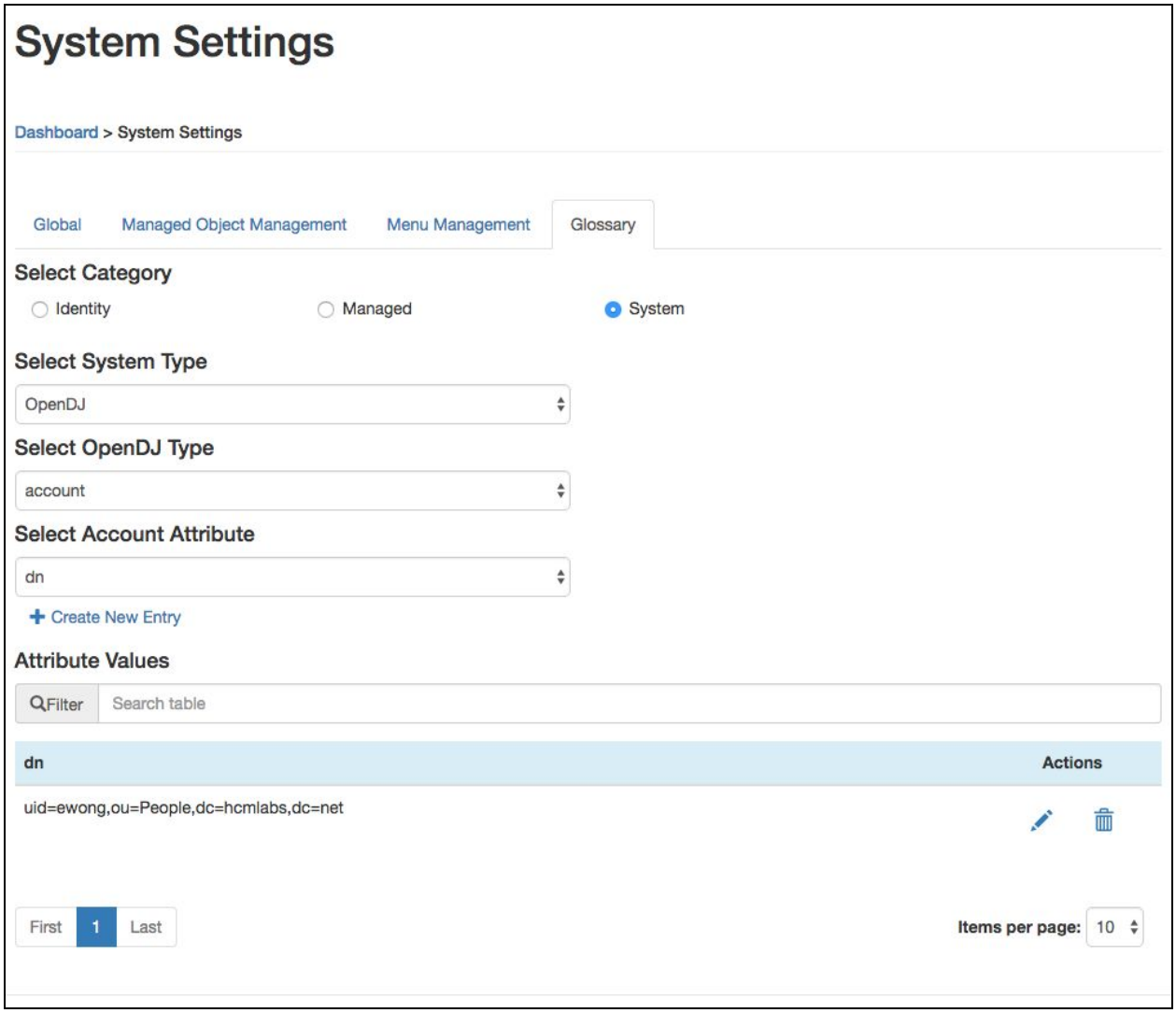
4. Adding glossary data to Applications
   4.1. Under 'Select Category', select **'System'** and choose a value from the dropdown



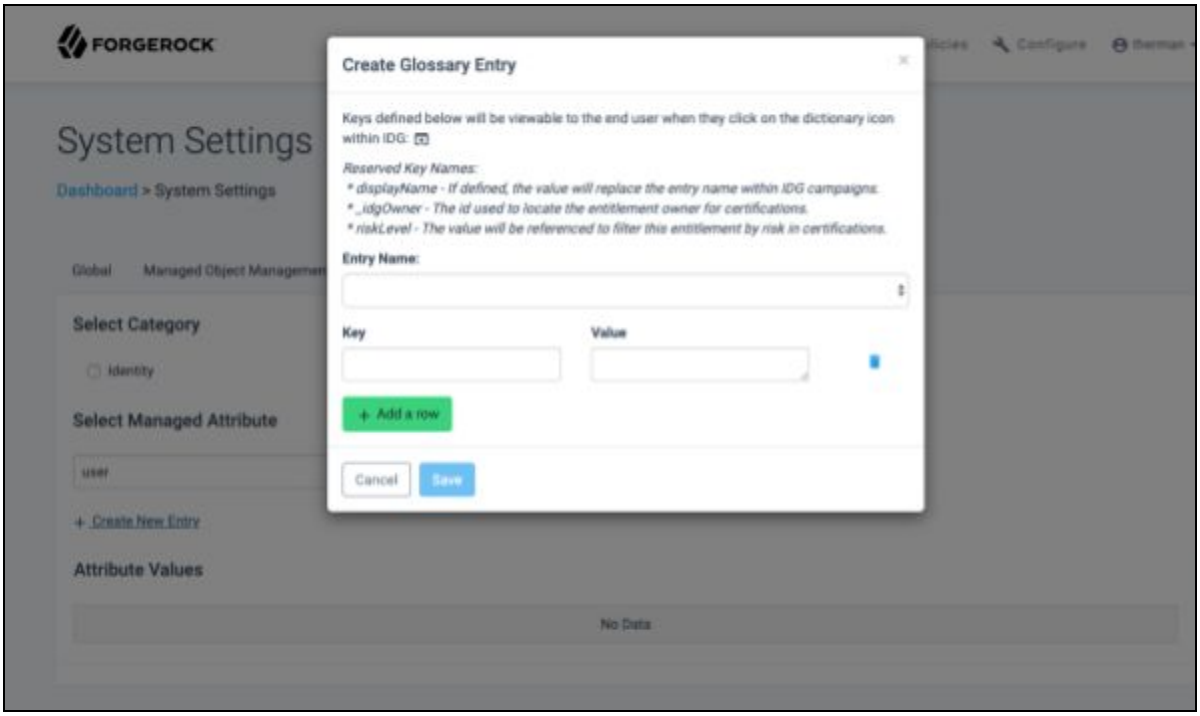
4.2. Another dropdown will appear to select a ‘type’ for the application. Make a selection.



4.3. A third dropdown will display to select the attribute for the selected type. Make a selection (if existing data is there it will be displayed).

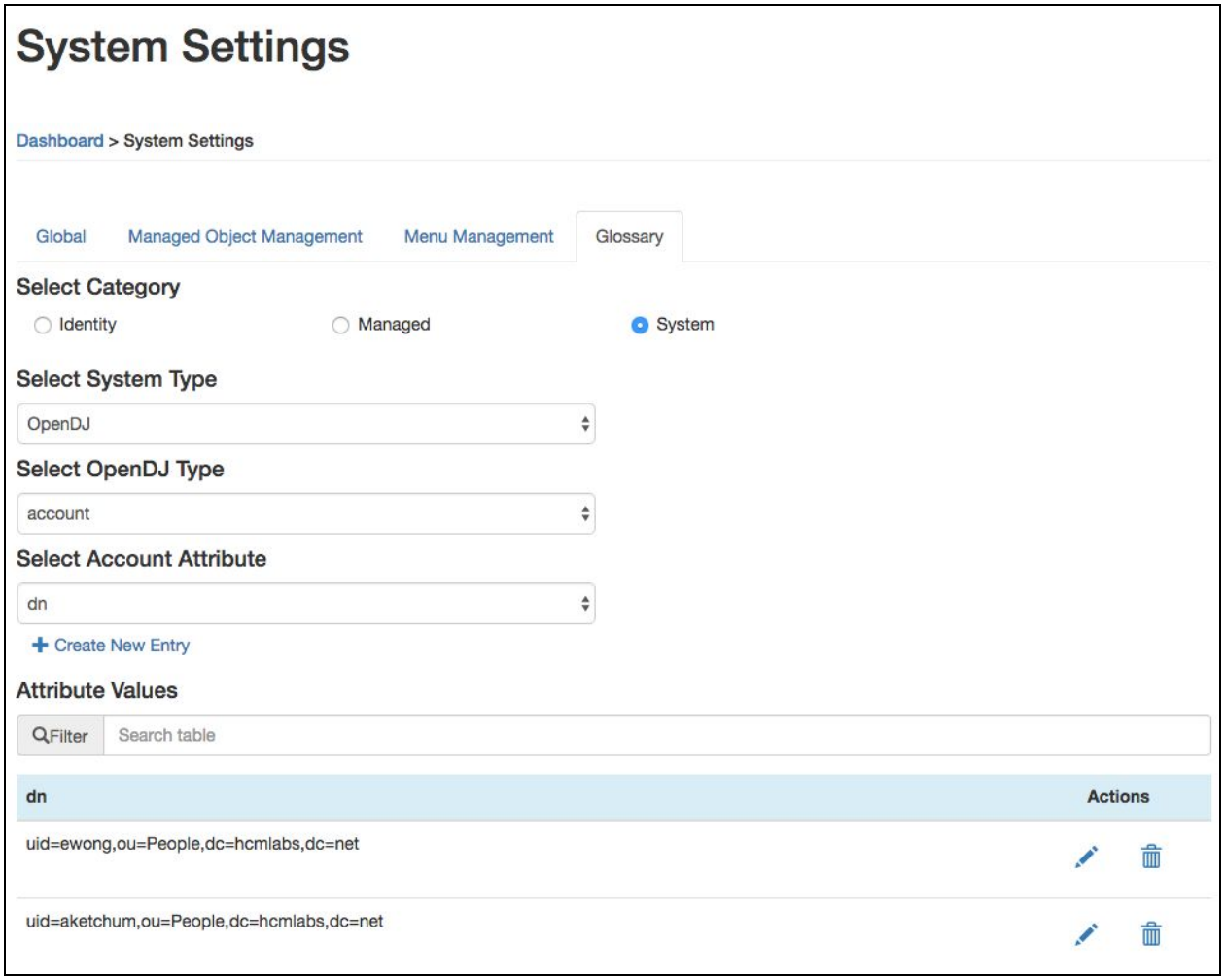

System Settings
Dashboard > System Settings
Global
Managed Object Management
Menu Management
Glossary
Select Category
Identity
Managed
System
Select System Type
OpenDJ
Select OpenDJ Type
account
Select Account Attribute
dn
Create New Entry
Attribute Values
Filter
Search table
dn
Actions
uid=ewong,ou=People,dc=hcmlabs,dc=net
First
1
Last
Items per page:
10

4.4. Create a new entry by selecting **'+Create New Entry'**. Fill in all the fields

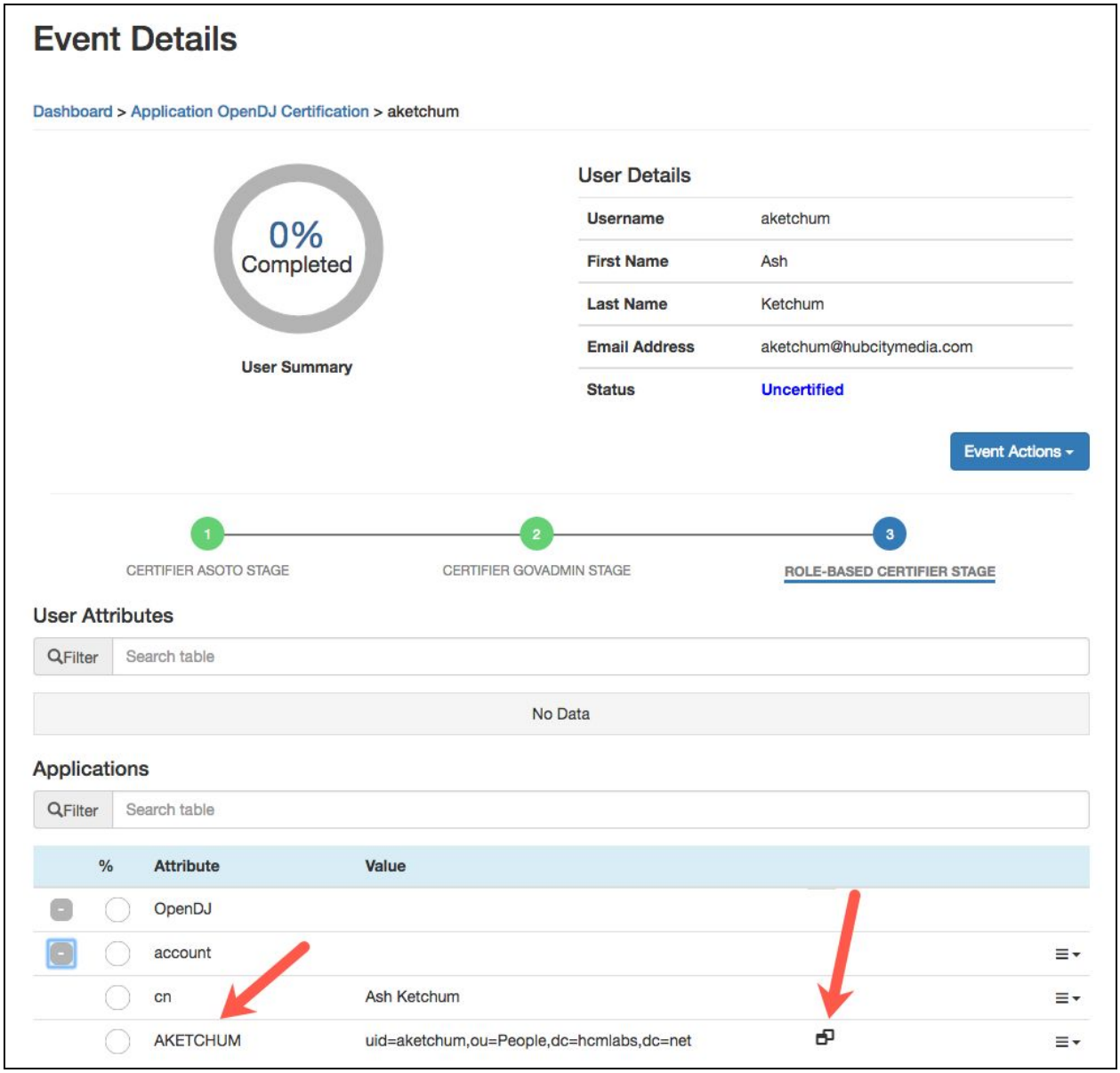


(required).

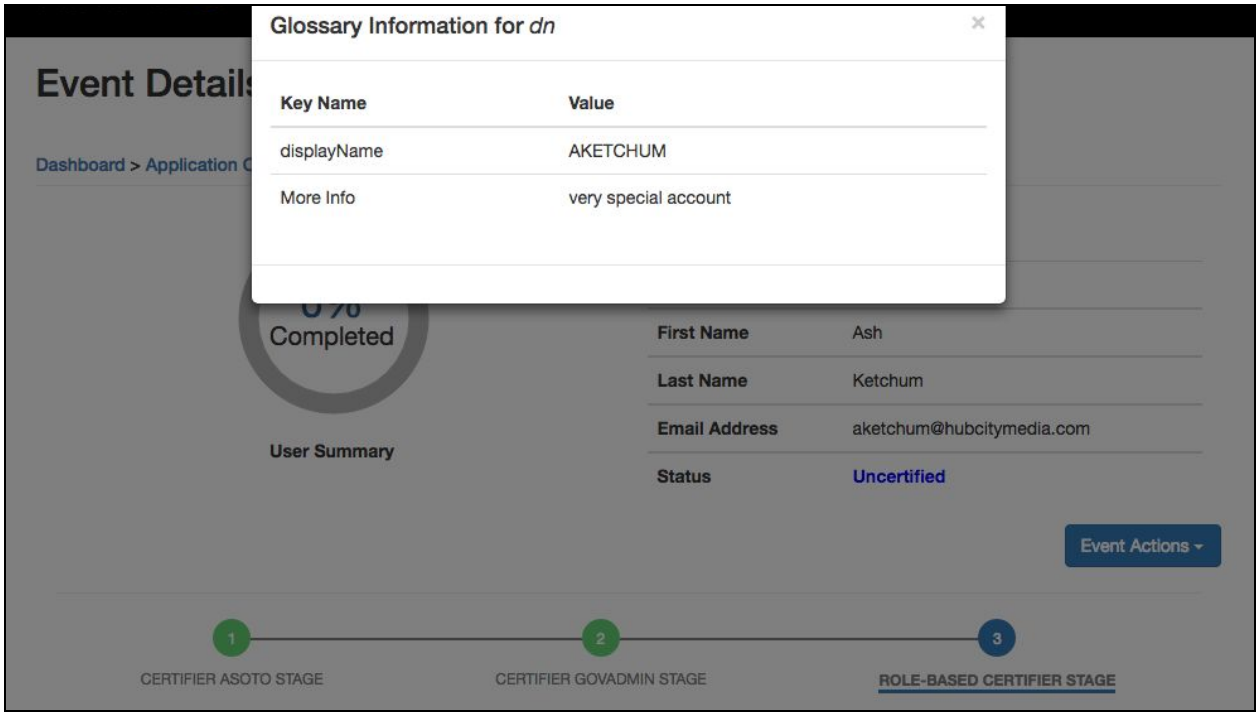
4.5. Select **'Save'** when done. The new entry should now appear in the table.



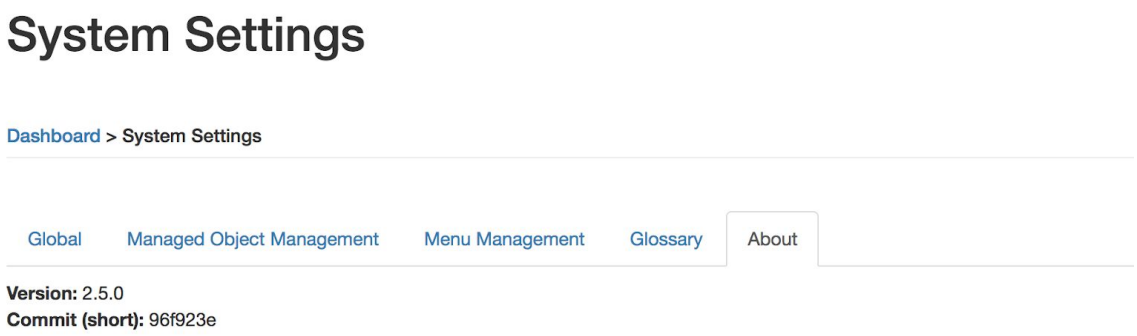
4.6. To view an entry on a campaign, navigate to any campaign's event that has the application and attribute that glossary data was for. There will be a glossary icon next to it (the name of the property will be replaced if you defined 'displayName' key in glossary data).



4.7. Select the icon to reveal a modal with the glossary data defined



8.5 About



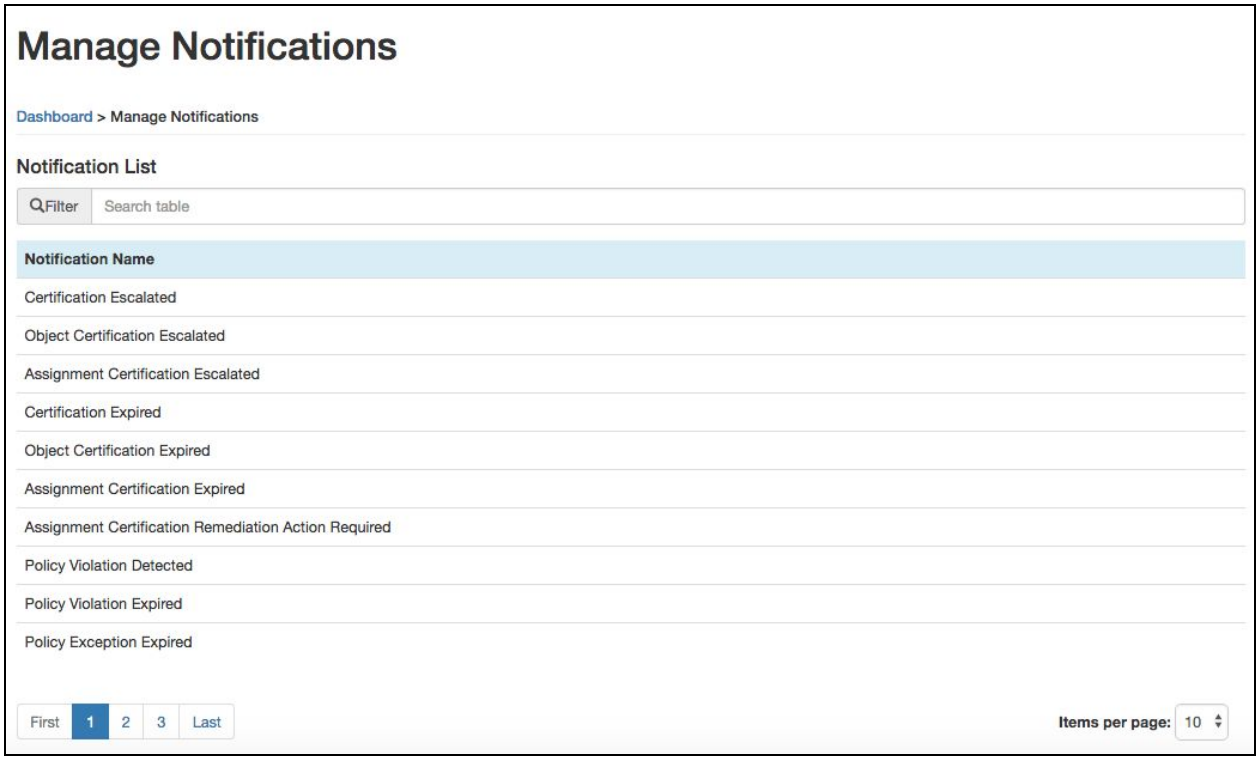
The about tab of the System Settings allows the user to see some basic information about the current version of the product that is installed. This information can be useful in debugging or diagnosing any issues or bugs.

9 Notification Templates

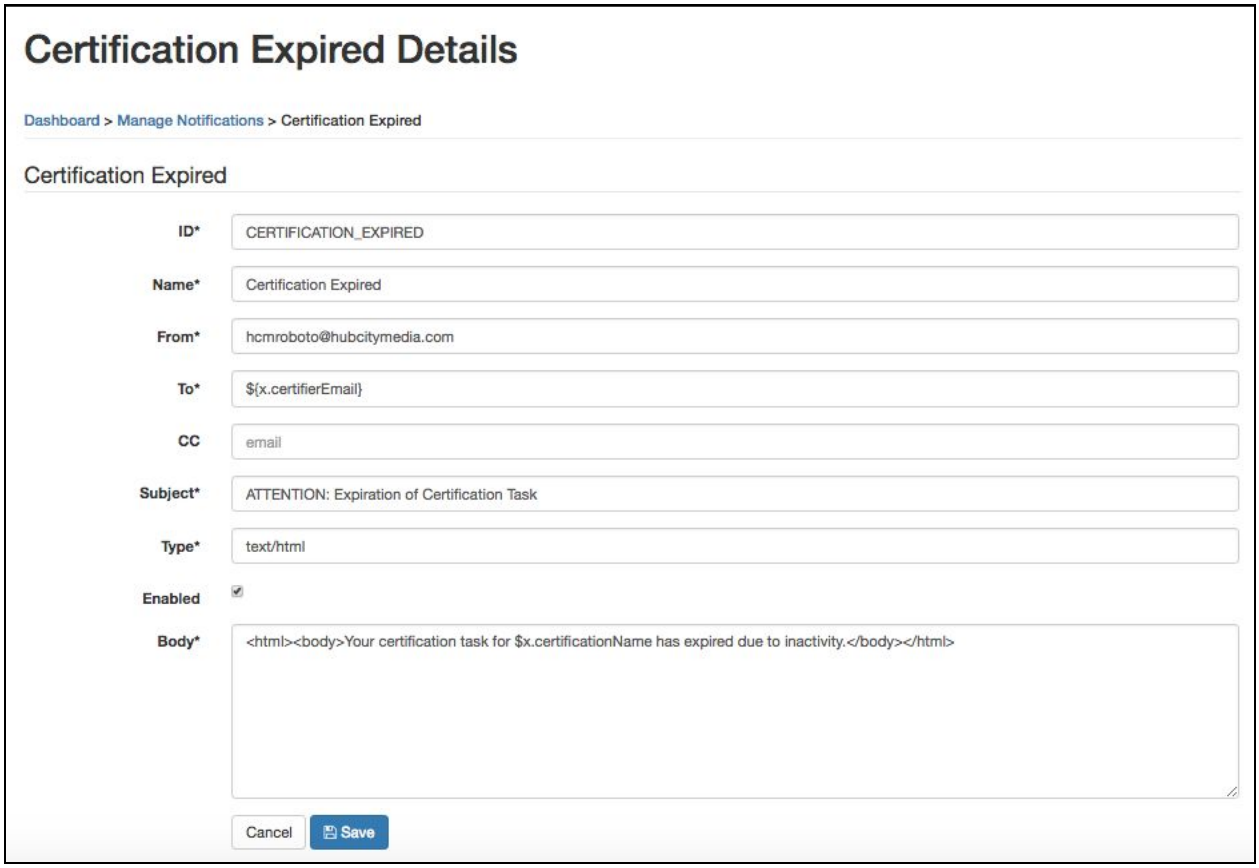
Notification templates are used to define the messages sent to administrators and end-users when a certain event occurs.

9.1 Modifying a Notification Template

1. Navigate to the Manage Notifications page, located in the Dashboard Management Dashboard under Notifications



2. View contents under Notification List
   - **Notification List:** Details predefined notification templates
     - **Notification Name:** Name of a notification template



3. To display additional information about the notification, select a notification from the Notification List. The following details are displayed:
   - ***Notification Name*:** Allows the administrator to modify the contents of a notification. The form is titled according to the Notification Name.
     - **ID:** *(Required)* Represents unique identifier for the notification template. **This field should not be modified unless otherwise specified by a Forgerock Engineer.**
     - **Name:** *(Required)* Name of a notification template
     - **From:** *(Required)* Information that appears in the From field of the notification
     - **To:** *(Required)* Address of those who will receive the notification**.** It contains a default variable that evaluates information from the certification.

       Note: For more information on supported variables, see section 9.3

     - **CC:** Addresses of users who may receive a copy of the notification
     - **Subject:** *(Required)* Information that appears in the Subject field of the notification
     - **Type:** *(Required)* Form of the notification to be sent. The value is defaulted to 'text/html'.

- **Enabled:** *(Required)* Identifies whether the notification is enabled or disabled. If unchecked, the notification will not be sent on a triggering event.
- **Body:** *(Required)* Contents of the notification. The default format is html, according to the value in the Type field, and may contain variables.

  Note: For more information on supported variables, see section 9.3

9.2 Predefined Notification Templates

The following list describes the predefined notification templates:

Name	Description
Assignment Certification Completion	Triggered when an assignment certification is completed to inform the certifier that the certification is complete.
Assignment Certification Creation Adhoc	Triggered when an assignment certification is created from an administrator to inform the certifier that the certification is pending.
Assignment Certification Creation Scheduled	Triggered when an assignment certification is created as a scheduled event to inform the certifier that the certification is pending.
Assignment Certification Creation Triggered	Triggered when an assignment certification is created after an update to an assignment to inform the certifier that the certification is pending.
Assignment Certification Escalated	Triggered when an assignment certification is active past the escalation date set in the certification definition to inform the escalation owner that the certification is still pending.
Assignment Certification Expired	Triggered when an assignment certification was active past the expiration date set in the certification definition to inform the certifier that the certification is now inactive.
Assignment Certification Remediation Action Required	
Certification Cancelled	Triggered when an administrator cancels a certification to inform the certifier that the certification is no longer available.
Certification Completion	Triggered when a user certification is completed to inform the certifier that the certification is complete.
Certification Creation Adhoc	Triggered when a user certification is created from an administrator to inform the certifier that the certification is pending.
Certification Creation Adhoc Default Certifier	Triggered when an ad-hoc user certification event is assigned to the default certifier
Certification Creation Scheduled	Triggered when a user certification is created as a scheduled event to inform the certifier that the certification is pending.

Certification Creation Scheduled Default Certifier	Triggered when a scheduled user certification event is assigned to the default certifier
Certification Creation Triggered	Triggered when a user certification is created after an update to a user to inform the certifier that the certification is pending.
Certification Creation Triggered Default Certifier	Triggered when an event-based user certification event is assigned to the default certifier
Certification Escalated	Triggered when a user certification is active past the escalation date set in the certification definition to inform the escalation owner that the certification is still pending.
Certification Expired	Triggered when a user certification was active past the expiration date set in the certification definition to inform the certifier that the certification is now inactive.
Object Certification Completion	Triggered when an object certification is completed to inform the certifier that the certification is complete.
Object Certification Creation Adhoc	Triggered when an object certification is created from an administrator to inform the certifier that the certification is pending.
Object Certification Creation Scheduled	Triggered when an object certification is created as a scheduled event to inform the certifier that the certification is pending.
Object Certification Creation Triggered	Triggered when an object certification is created after an update to an object to inform the certifier that the certification is pending.
Object Certification Escalated	Triggered when an object certification is active past the escalation date set in the certification definition to inform the escalation owner that the certification is still pending.
Object Certification Expired	Triggered when an object certification was active past the expiration date set in the certification definition to inform the certifier that the certification is now inactive.
Policy Exception	Triggered when an exception is created for a violation to confirm the exception with the violation owner.
Policy Exception Expired	Triggered when an exception for a violation has expired to inform the violation owner of the change.
Policy remediated	Triggered when a violation is remediated by either an administrator or task to inform the violation owner.
Policy Violation Detected	Triggered when a violation is raised from a policy scan to inform the violation owner.
Policy Violation Escalated	Triggered when an escalation duration has been exceeded for a violation to inform the escalation owner of the violation.

Policy Violation Expired	Triggered when an expiration duration has been exceeded for a violation to inform the violation owner of the change.

9.3 Predefined Notifications Variables

The following describes the predefined variables that may be used within notifications:

Variable	Description
${x.email}	
${x.certifierEmail}	
${x.escalatorEmail}	
$x.user	
$x.certifier	
$x.owner	
$x.certificationName	

10 Customizing the UI

ForgeRock AccessReview makes it simple to add company branding and other User Interface (UI) changes to the application. This can be done by modifying the CSS styles via the **custom.css** file. Any changes added to the **custom.css** file will override the 'out of the box' styles.

1. Access the server with a user who has Read / Write capabilities to the governance directory
2. Navigate to the governance styles directory:

   cd /path/to/openidm/governance/styles/

3. Open the custom.css file in any text editor
4. Add changes to the custom.css file

   Example of replacing the logo:

```
.idg-top-navbar-logo {
  background-image: url('../images/custom/forgerock_idg_logo.svg');
  background-repeat: no-repeat;
  background-size: contain;
}
```

   Note: Any changes made must follow CSS standards

5. Save the custom.css file
6. Refresh browser to see changes

Note: If changes are not appearing make sure to clear the browser cache and try refreshing the browser again

11 Uninstalling AccessReview

IDM must be started prior to running the uninstaller

ForgeRock AccessReview can be removed from the IDM server via the uninstall scripts. This needs to be done on each individual node. Please note that there will be some components and artifacts of ForgeRock AccessReview that will remain in the system.

1. Navigate to the openidm/tools/idg directory of the IDM installation
2. Run the following command to initiate the uninstaller:

For Windows:
uninstall.bat [--properties filename | -p filename]

For Linux:
./uninstall.sh [--properties filename | -p filename]

The command can be run with the following optional argument:

- **--properties or –p <location/of/properties/file>:** Provides a properties file for script input. If no properties file is specified, user must input the following properties at run time.

The following input is used for the uninstaller:

- **openidm_location**: File location of IDM home directory
- **project_location**: File location of IDM project directory, if used. This is an optional property that will default to the openidm_location if left blank.
- **openidm_url**: URL where IDM can be reached. *This will often be localhost.*
- **openidm_version**: The version of IDM. *This will either be 5.0, 5.5, or 6.0*
- **openidm_admin**: User ID for user with the openidm-admin role
- **openidm_admin_password**: Password for IDM administrator
- **openidm_database_type**: Must be ‘mssql’ or ‘mysql’ for AccessReview 2.0.3.

Note: Names are those found in the properties file. If a properties file is not used, equivalent input will be gathered directly from the uninstaller.

The uninstaller will print updates to the console until it successfully completes

12 GDPR Compliance

Due to the GDPR regulations Forgerock has identified the following critical areas that would assist in implementing a compliant system. The below identifies what personal data is captured, where that data is stored, when it is stored and who can potentially access the data. It is the implementer's responsibility to scrub the personal data as necessary to be considered compliant with GDPR regulations.

12.1 What personal data is being stored?

Since ForgeRock IDM allows the user schema to be customized and linked to outside resources; it is not feasible to identify all the potential Personal Identification Information (PII) that ForgeRock AccessReview can access. It is important to know that any application data that contains PII linked to an IDM user is exposed to the ForgeRock AccessReview application. If the attributes that contain sensitive data are set to displayable, or certifiable, it will be stored at the time of creating the user certification.

Examples:

- User Attributes:
  - username
  - givenName
  - sn
  - email
- OpenDJ
  - member_address
  - member_ssn

12.2 Where the personal data is being stored?

- auditactivity
- genericobjects
- genericobjectproperties

12.3 When is the data being stored?

- During the creation of a user certification campaign
- When a user certification campaign is acted upon

12.4 Who can access the data?

- ForgeRock AccessReview administrators
- ForgeRock AccessReview certifiers
- IDM Admins