Administration guide

This guide is written for administrators who must manage and maintain ForgeRock® Identity Governance.

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

This guide is written for ForgeRock Identity Governance administrators performing actions in certification campaigns, Segregation-of-Duty (SOD) violation processes, request administration, and other general administrative configurations throughout the module.

Common Interfaces

Learn about the Identity Governance common interfaces.

Access Review

Learn about the Identity Governance access review.

Access Request

Learn about the Identity Governance access request.

System Settings

Identity Glossary

Learn about the Identity Governance system settings.

Learn about the Identity Governance identity glossary.

Global Data Privacy Regulation (GDPR)

Learn about the Identity Governance GDPR compliance.

Installation

The following chapter provides details about the Identity Governance installation.

Provided Files

The installer is provided in the `identity-governance-7.1.0.zip` archive on the ForgeRock BackStage Downloads site. 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.
- **legal-notices**: Contains the ForgeRock license agreement and any third party licensing agreements.
- **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.
- **integrations**: Files and scripts used to make adjustments to out of the box ForgeRock IDM configuration files.

Installation Instructions

1. Unzip the `identity-governance-7.1.0.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 installer prints updates to the console until successful completion.

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.

Use the following parameters when installing:

- **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.
- **identity_governance_installer_location**: Location where the installer is being run from.
- **openidm_version**: The version of IDM you are installing IGA with.

IMPORTANT

This property respects major and minor versions. For example, `7.1`. Do not use patch release versions.

- **initial_install**: If this is the first install in a cluster of installs, provide this parameter.

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.

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

Clustered Environment

The installer script can only be run once per environment. In a clustered environment, you must run manual steps to copy artifacts to subsequent nodes once the install 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. The entire `./openidm/governance` directory, copied into the openidm installation directory.
    f. The entire `./legal-notices` directory, copied into the openidm installation directoryl
2. Copy the following files from the first node's IDM installation directory:
    - `openidm/script/access.js`
    - `openidm/conf/managed.json`
    - `openidm/conf/policy.json`

Post-Installation Instructions

The UI context for Identity Governance can be found by navigating to /governance from your IDM server URL.

Additional configuration is needed on each node as described below:

- **Administrator Roles**. For a user to access the administrator functionality of Identity Governance, they must be assigned the intended internal authorization role (`governance-administrator`, `access-request-admin`, or `glossary-admin`) that was created during installation. Note that if you are assigning the role to the currently logged in user you must log out and back in again for the role to take effect, and internal users (e.g., `openidm-admin`) are not supported by Identity Governance}.

- **Enable Workflow**. If planning to use the IDM workflow functionality for certification remediation or custom request flows, Identity Governance requires workflow to be enabled in the IDM administrator configuration. To do so, navigate to Configuration > System Preferences > Workflow and toggle the `Enable` setting.
- **Setting the membershipProperties configuration**. Administrators have the ability to determine which default managed user property will be used to determine membership for group assigned approvals, either roles or authzRoles. If ‘roles’ is selected, users that are assigned a managed role to their Provisioning Roles attribute (‘roles’ in the schema) will be eligible to approve tasks assigned to that managed role. If ‘authzRoles’ is selected, users that are assigned a role to their Authorization Roles attribute (‘authzRoles’) will be eligible to approve tasks assigned to that role. In previous versions of Access Request this was always determined by the Authorization Roles property.

  To edit this configuration, open the file found at `openidm/conf/commons.json` and edit the `membershipProperties` array value. By default the configuration contains both `‘authzRoles’` and `‘roles’` as options; however, it is recommended that only one is chosen. Note that only those two properties are currently supported as options for determining group membership.
- **Event-Driven Certifications**. In order to enable event based certifications for managed users or other managed objects, the following snippet of code (in JavaScript) must be added to the `onUpdate` hook for each individual object that you want to create certifications for:

  ```
  require('script/idg/onUpdateManagedObject.js').triggerCerts(ol
  dObject,newObject, 'user');
  ```

  where ‘user’ should correspond to the managed object you are editing (e.g., ‘role’, ‘assignment’, etc.)
- **Reactive Policy Scans**. In order to enable reactive policy scans on managed users, the following snippet of code (in JavaScript) must be added to the postUpdate hook for the managed user object:

  ```
  if(request.method.equals('update') ||
  request.method.equals('patch'))
    openidm.action('governance/policyScan', 'reactive', {
  userId: object._id });
  ```

  > 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.

Installer Backups

As part of the installation process, backups of any IDM files that are changed or edited are created within the `openidm/backup` folder. The file names follow the pattern of `<original file name>.pre-accessreview-install-<timestamp>`\`, and are located within the same subdirectories of the backup folder as they would be in the original `openidm` directory.

IDM/AM Integration for 7.X

If installing Identity Governance into an IDM environment that is configured to authenticate through Access Management, you must configure an OAuth client in AM for the Governance context.

To start, refer to section 2.4.2 of the ForgeRock Platform Setup Guide.

In step 5 of the section, instructions are given to configure a client for the end-user-ui. For Identity Governance, please repeat those steps with the following adjustments:

- Client ID: `identity-governance-ui`
- Core:
  - Redirect URIs: <IDM domain>/governance/appAuthHelperRedirect.html
- Advanced:
  - Subject Type: Public

In the ForgeRock Platform admin interface, click **Applications**, and then **Add Application**. The data entered in this form should match the configurations included in the AM client.

> NOTE
>
> The compatible IDM versions are 7.X and onwards.

Patching/Updating Process

If installing a patch update to the current installation, run the following steps to ensure proper installation of the update.

For updating a major version of the product (e.g. 2.5 > 3.0), consult the release notes for any instructions on the upgrade process.

> 1. Check the patch/update zip for a README file and confirm if there are any additional actions that need to be taken for the specific patch or update. Any steps found within this file should take precedence over the steps found below.

2. Manually create a backup of the following directories with the openidm installation: `/conf`, `/script/idg`, `/script/commons`, `/governance`, and `/workflow`.
3. Unzip the provided patch/update into the `openidm` directory
4. Restart the IDM server.

IMPORTANT

In the event the update needs to be backed out or reverted, simply copy the backup directories to the [path]openidm directory to overwrite the new changes and restart the server once again.

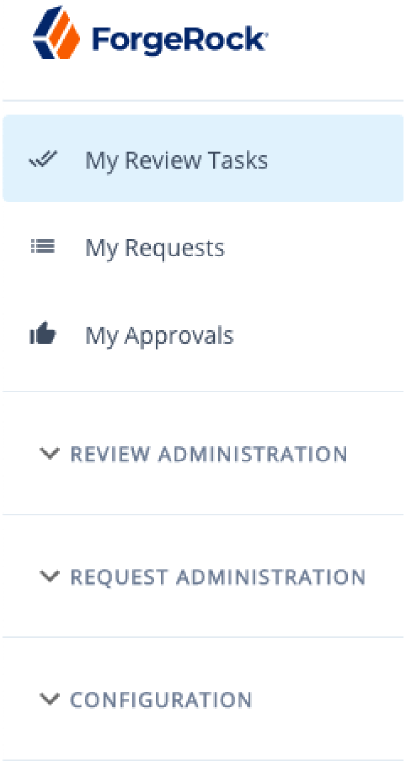
Common interfaces

The following sections detail functionality common throughout the Identity Governance Administrative Screens.

Navigation Sidebar

The navigation sidebar is the main way for users and administrators to navigate Identity Governance. The page is split into four separate sections: one for the end user functionality (My Review Tasks, My Requests, My Approvals) and one section each for the different administrator roles and capabilities: Review Administration, Request Administration, and Configuration.

All administrative screens are available from this location, and only those accessible to a given user based on their administrator privileges will be shown.


My Review Tasks

My Requests

My Approvals

REVIEW ADMINISTRATION

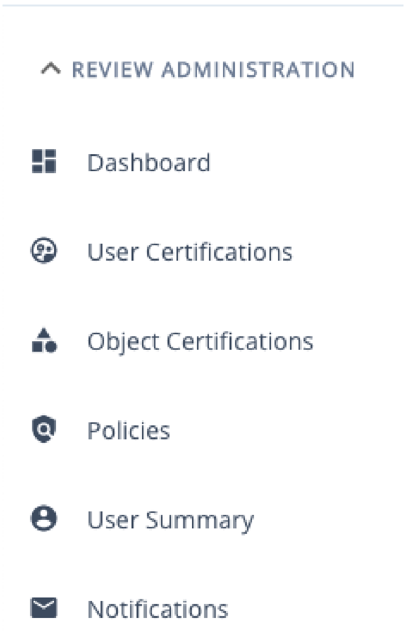
REQUEST ADMINISTRATION

CONFIGURATION

Access Review Administration

This section will be available to any user assigned the governance-administrator internal role and includes the following options:

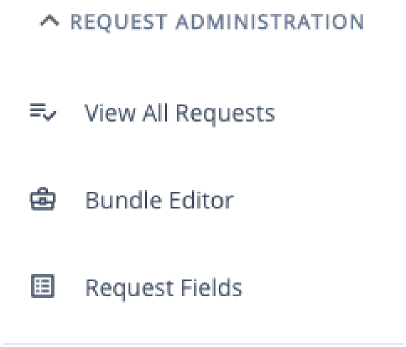
- **Dashboard**. Administrative dashboard
- **User Certifications**. Manage and create user certification campaigns
- **Object Certifications**. Manage and create object certification campaigns
- **Policies**. Manage and create policies, scans, and violations
- **User Summary**. View individual user certification history and tasks view
- **Notifications**. Manage Access Review notification templates



Access Request Administration

This section will be available to any user assigned the access-request-admin internal role and includes the following options:

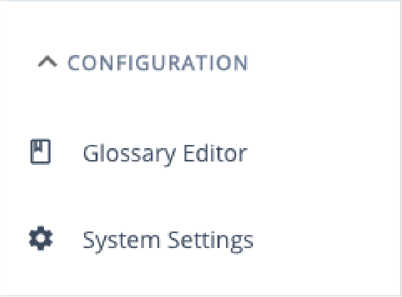
- **View All Requests**. Manage requests for access
- **Bundle Editor**. Create and manage request bundles
- **Request Fields**. Create and manage custom form fields for requests



Configuration

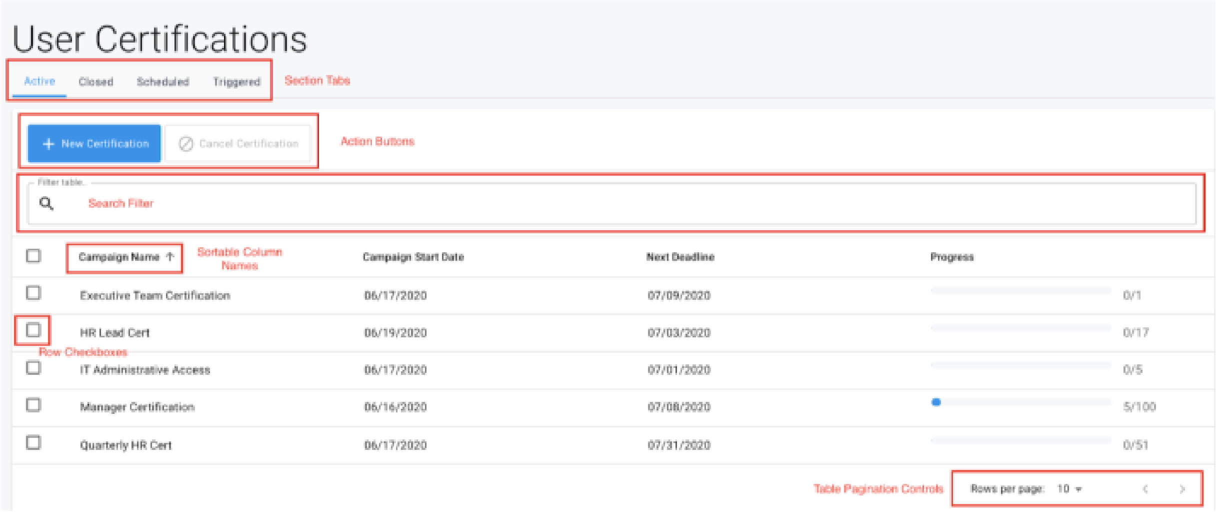
This section will be available to any user that is assigned any of the three Identity Governance internal roles and includes the following options:

- **Glossary Editor**. Create and manage glossary entries
- **System Settings**. Configuration options (available to governance-administrators and access-request-admins)



Tables

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



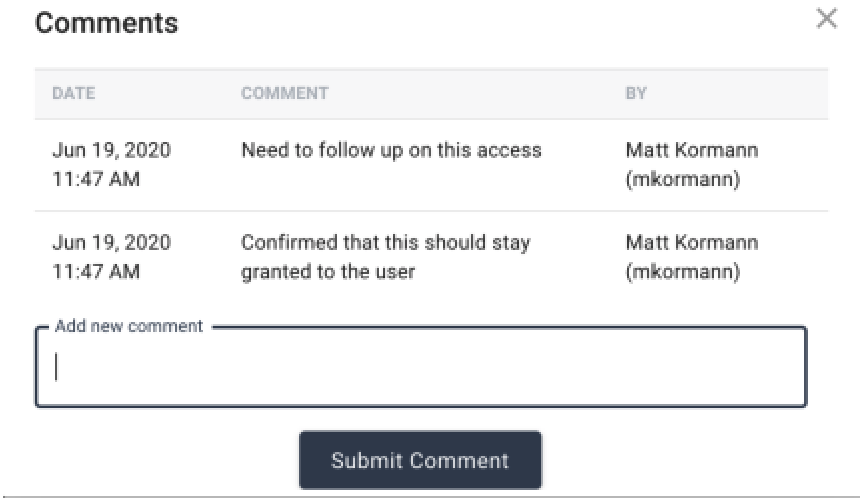
□	Campaign Name ↑	Campaign Start Date	Next Deadline	Progress
□	Executive Team Certification	06/17/2020	07/09/2020	0/1
□	HR Lead Cert	06/19/2020	07/03/2020	0/17
□	IT Administrative Access	06/17/2020	07/01/2020	0/5
□	Manager Certification	06/16/2020	07/08/2020	5/100
□	Quarterly HR Cert	06/17/2020	07/31/2020	0/51

- **Section Tabs**. Navigate through the different tabs that the current table view allows
- **Action Buttons**. Lists the available actions that can be taken on the table rows. Note that some actions require one or more rows to be selected via the row checkboxes and will remain gray if disabled.
- **Search Filter**. Will allow the user to enter in a value to search against the different columns of the table. Note that not all columns in a given table are searchable, please refer to the individual sections of documentation for more information.
- **Sortable Column Names**. Clicking the column name will sort the data by that column. Clicking again will reverse the search order.
- **Row Checkboxes**. If a table has row checkboxes available, these can be used to select one or more rows to target for the available stage actions.
- **Table Pagination Controls**. Rows per page allows you to select the number of results made visible at a specific time within the table. Values may include 10, 25, or 50. Also included are navigation arrows for moving forward and backward between pages.

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:

- **Date**. Time an action was taken
- **Comment**. The message entered by the user when performing the action or submitting a general comment
- **By**. Display name of the user who submitted the comment

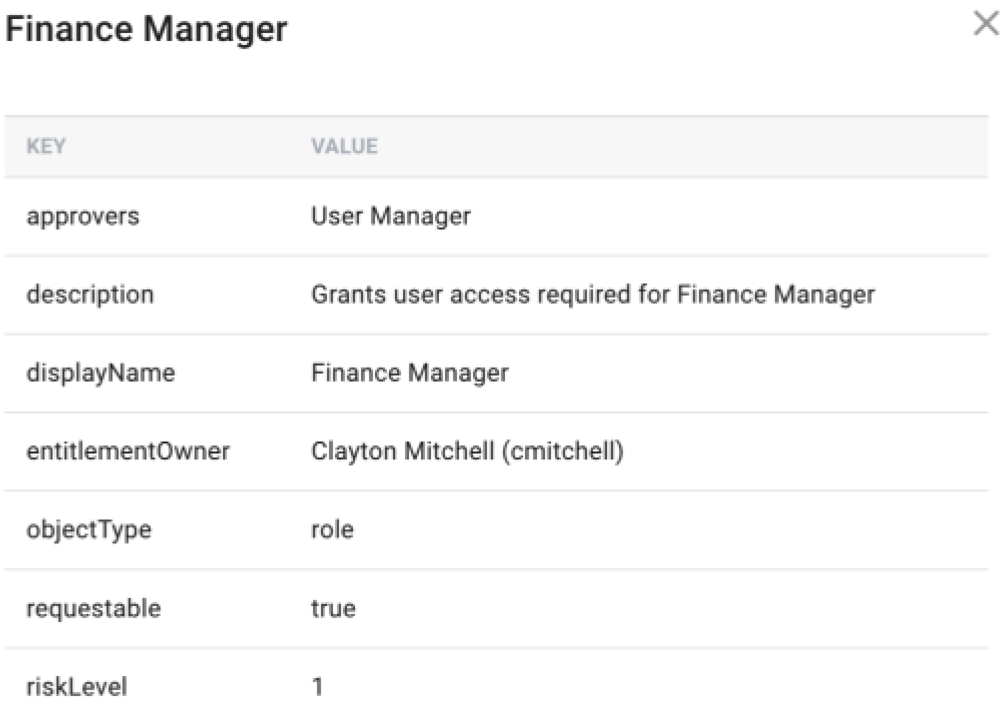


Comments

DATE	COMMENT	BY
Jun 19, 2020 11:47 AM	Need to follow up on this access	Matt Kormann (mkormann)
Jun 19, 2020 11:47 AM	Confirmed that this should stay granted to the user	Matt Kormann (mkormann)

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. In some cases, this metadata may even substitute the value that is displayed to the certifier. Pictured above is a sample metadata screen that appears when clicking on a certification entitlement. Additional information is detailed in the Identity Glossary section.



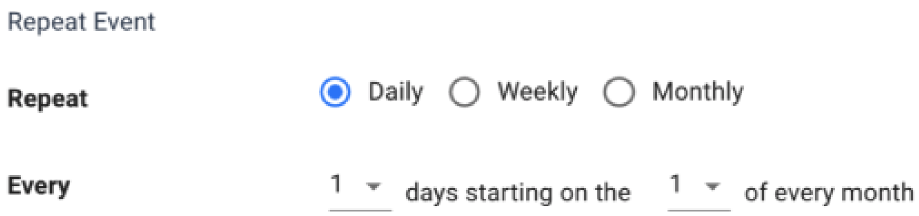
Finance Manager

KEY	VALUE
approvers	User Manager
description	Grants user access required for Finance Manager
displayName	Finance Manager
entitlementOwner	Clayton Mitchell (cmitchell)
objectType	role
requestable	true
riskLevel	1

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.

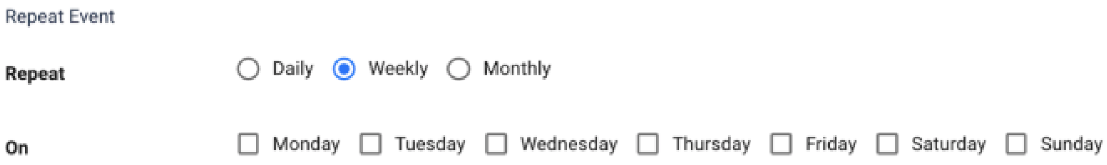


Repeat Event

Repeat ● Daily ○ Weekly ○ Monthly

Every 1 days starting on the 1 of every month

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

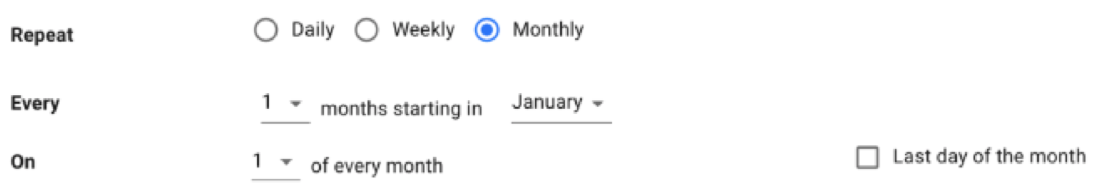


Repeat Event

Repeat ○ Daily ● Weekly ○ Monthly

On □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

- **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.



Repeat ○ Daily ○ Weekly ● Monthly

Every 1 months starting in January

On 1 of every month □ Last day of the month

Remediation Tasks

Remediation Tasks complete revocations resulting from certifications or violations via workflows defined in IDM. Identity Governance includes a single remediation workflow to handle basic remediation for both violations and certifications, 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
- **Remove Entitlements**. Will take the following actions depending on the type of task being remediated:
  - **Certifications**. For any revoked entitlement will either remove or alter the attribute depending on the type of attribute as defined in the object schema:
    - **Relationship**. Relationship between target and entitlement will be deleted
    - **Array**. Item will be removed from array
    - **Other**. Attribute will be altered to generic stage or to reflect remediation (e.g. appending "-REMEDIATED" to a string or setting a boolean to false)
  - **Violation**. For every target attribute defined within the given policy's expression, the same actions listed above for certification will be taken on the target object.

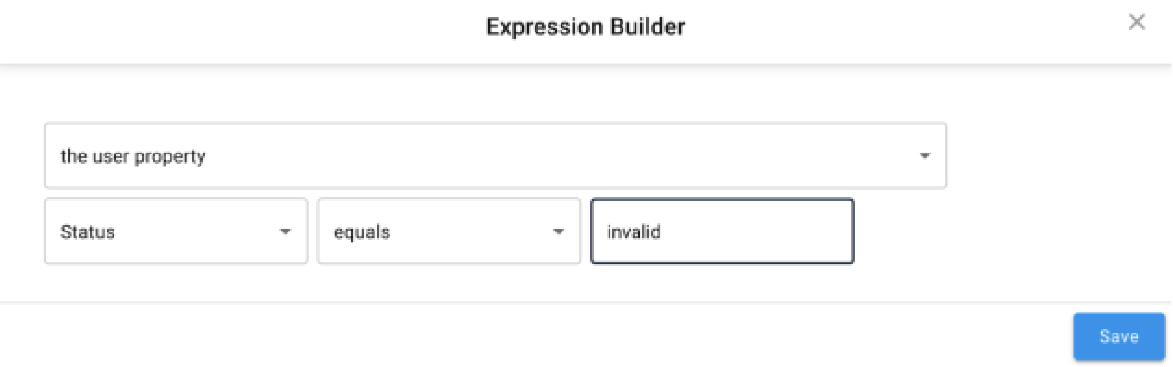
Expression Builder

Expression Builder identifies criteria for filters in certification definitions and policy rules. The criteria identify attribute constraints for target users. Depending on the exact expression builder being used (e.g. user target filter, user event based expression, policy expression) the options in the builder may differ. This section covers the basic format and use of a generic expression builder, refer to section Expression Builder for more specific details.

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.

- **Every [user/role/etc]**. Selects every matching object to the given object type. Does not require any further nested expressions.
- **The [user/role/etc] property**. Allows the administrator to specify an attribute and evaluate its value. Depending on the attribute chosen the administrator can specify whether to evaluate a direct equals comparison or a contains comparison. In the

instance of event based certifications, users can choose is, was, or changed to compare previous values, current values, or detect any change at all.


Expression Builder

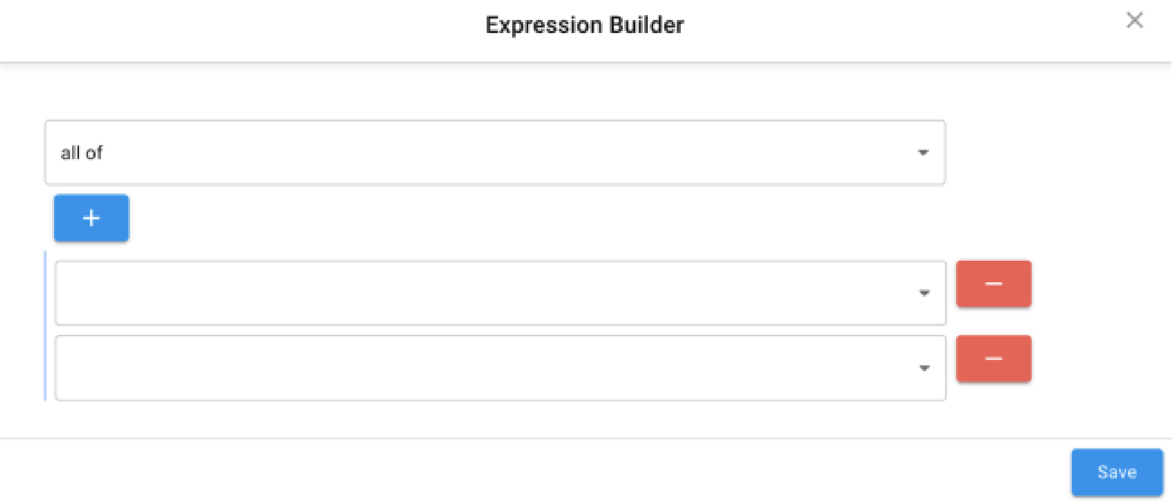
the user property

Status

equals

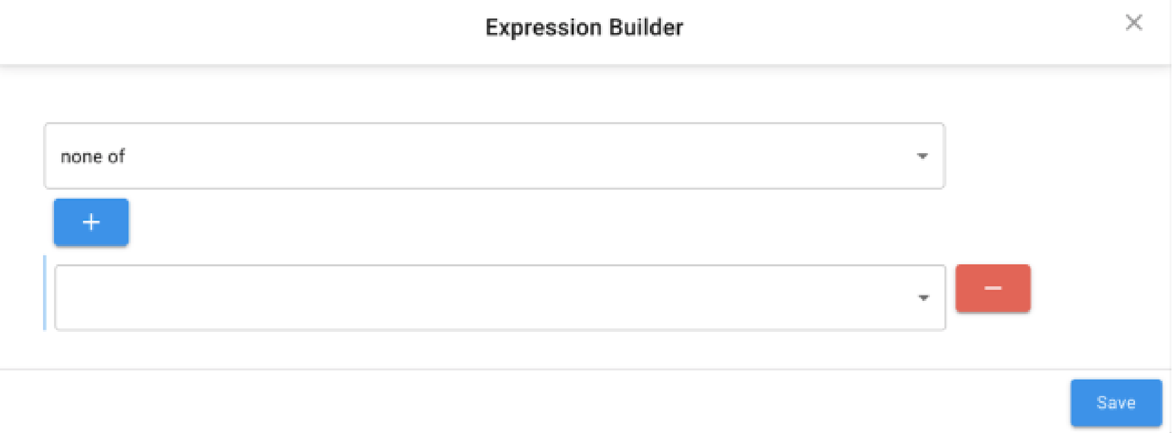
invalid

- **Any of**. Allows the administrator to specify multiple expressions concatenated by 'OR' conditions. If any of the contained expressions are true, the entire expression evaluates to true. Selecting '+' appends additional expressions while selecting '-' removes expressions from the end.
- **All of**. Allows the administrator to specify multiple expressions concatenated by 'AND' conditions. If all of the contained expressions are true the entire expression evaluates to true. Selecting '+' appends additional expressions while selecting '-' removes expressions from the end.


Expression Builder

all of

- **None of**. Allows the administrator to specify an expression and negate its value. If the contained expression is false, the expression evaluates to true.


Expression Builder

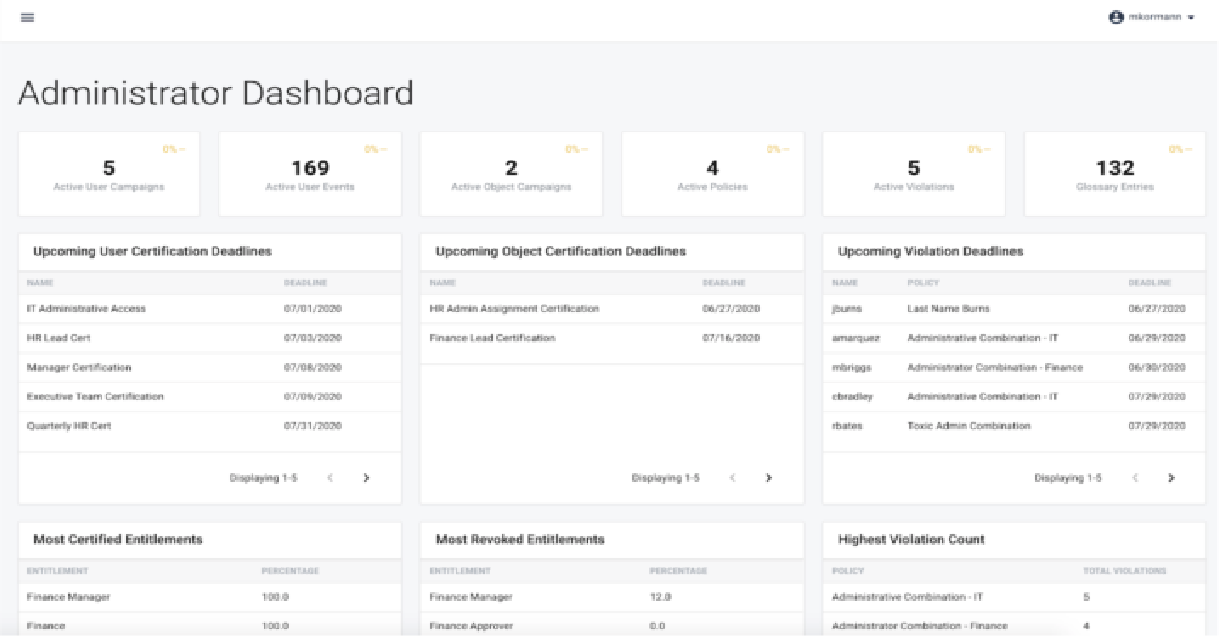
none of

- **The user has application**. In user target filters for certifications, you can filter users by whether or not they have a link to an externally connected system.

Access review

Users can find the UI context for Identity Governance by navigating to `/governance` from your IDM server URL. Once logged in, the user can find the Administrator dashboard by clicking on the Dashboard link in the Administration section of the navigation sidebar, or alternatively by navigating directly to `/governance/#/admin/dashboard`.

> NOTE
>
> Identity Governance does not support internal users for administrative or end-user tasks. To access the product functionality correctly, you must be logged in as a managed user. Internal users will be redirected to a page informing them of this policy.



Administrator Dashboard

5 Active User Campaigns 0% –

169 Active User Events 0% –

2 Active Object Campaigns 0% –

4 Active Policies 0% –

5 Active Violations 0% –

132 Glossary Entries 0% –

Upcoming User Certification Deadlines

NAME	DEADLINE
IT Administrative Access	07/01/2020
HR Lead Cert	07/03/2020
Manager Certification	07/08/2020
Executive Team Certification	07/09/2020
Quarterly HR Cert	07/31/2020

Displaying 1-5

Upcoming Object Certification Deadlines

NAME	DEADLINE
HR Admin Assignment Certification	06/27/2020
Finance Lead Certification	07/16/2020

Displaying 1-5

Upcoming Violation Deadlines

NAME	POLICY	DEADLINE
jburns	Last Name Burns	06/27/2020
amarquez	Administrative Combination - IT	06/29/2020
mbriggs	Administrator Combination - Finance	06/30/2020
cbradley	Administrative Combination - IT	07/29/2020
rbates	Toxic Admin Combination	07/29/2020

Displaying 1-5

Most Certified Entitlements

ENTITLEMENT	PERCENTAGE
Finance Manager	100.0
Finance	100.0

Most Revoked Entitlements

ENTITLEMENT	PERCENTAGE
Finance Manager	12.0
Finance Approver	0.0

Highest Violation Count

POLICY	TOTAL VIOLATIONS
Administrative Combination - IT	5
Administrator Combination - Finance	4

Dashboard Overview

To access the Administrator Dashboard, log into Identity Governance as a user with the `governance-administrator` authorization role. Select Dashboard in the navigation side bar menu under Review Administration.

The administrator dashboard offers admin users an overview of the entire state of the Review portion of Identity Governance, presenting statistics on the current count of total certifications, events, and more, as well as some analytical information to keep the administrators up to date on the decisions being made by certifiers.

The statistics shown on the dashboard are updated in one of two ways. Some, which are less intensive on the system to calculate on demand, are loaded in at the time the dashboard is accessed. Others, which look through the entire certification history of the system, are calculated via a scheduled script and are stored in the repository at a configurable interval. The script schedule is defined in the file `schedule-script_adminDashboard.json` in the `openidm/conf` directory, where the schedule can be updated to run as often as desired.

The following metrics are displayed as part of the dashboard:

- **Name**. title of the metric shown
- **Description**. Brief explanation of what the metric shows
- **Action**. hether metric is clickable or interactive in some way
- **Key**. Reference key for the metric, can be referenced in adminDashboard API call to retrieve a single metric

Dashboard Metrics

Name	Description	Action	Key
Active User Campaigns	Number of current user certification campaigns in flight	No	activeUserCampaigns
Active User Events	Number of current individual user events in flight (where event is each task within a campaign)	No	activeUserEvents
Active Object Campaigns	Number of current object certification campaigns in flight	No	activeObjectCampaigns
Active Policies	Number of active policies defined in the system	No	activePolicies
Active Violations	Number of current violation tasks with a status of 'in-progress' awaiting action	No	activeViolations
Glossary Entries	Number of entries defined in the Identity Glossary	No	glossaryEntries
Upcoming User Certification Deadlines	Table of active user certifications, ordered by most recent upcoming stage deadline	Yes	upcomingUserCertificationDeadlines

Name	Description	Action	Key
Upcoming Object Certification Deadlines	Table of active object certifications, ordered by most recent upcoming stage decline	Yes	upcomingObjectCertificationDeadlines
Upcoming Violation	Table of active violations, ordered by most recent upcoming deadline	Yes	upcomingViolation Deadlines
Most Certified Entitlements	Table of entitlements that have been certified and signed-off, sorted by the percentage of outcomes that are marked as 'certify'	Yes	mostCertifiedEntitlements
Most Revoked Entitlements	Table of entitlements that have been certified and signed-off, sorted by the percentage of outcomes that are marked as 'revoke.’	Yes	mostRevokedEntitlements
Highest Violation Count	Table of policies, sorted in descending order by the number of violations that have been found against the policy.	No	highestViolationCount
Certification Results	This chart allows the admin to see the complete breakdown of all certified entitlements within the system, grouped by the certification decision that was made against them.	Yes	certificationResults
Violation Results	This chart allows the admin to see the complete breakdown of all violations acted on within the system, grouped by the decision that was made against them.	Yes	violationResults

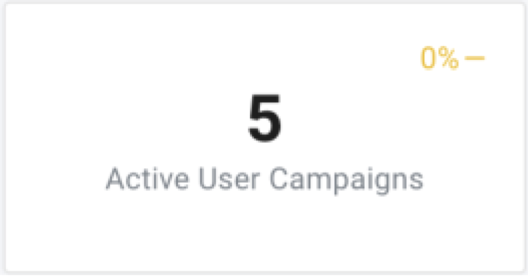
Metric Display Types

Metrics are displayed on the dashboard using one of three different display types, each of which is described below.

Stat Card

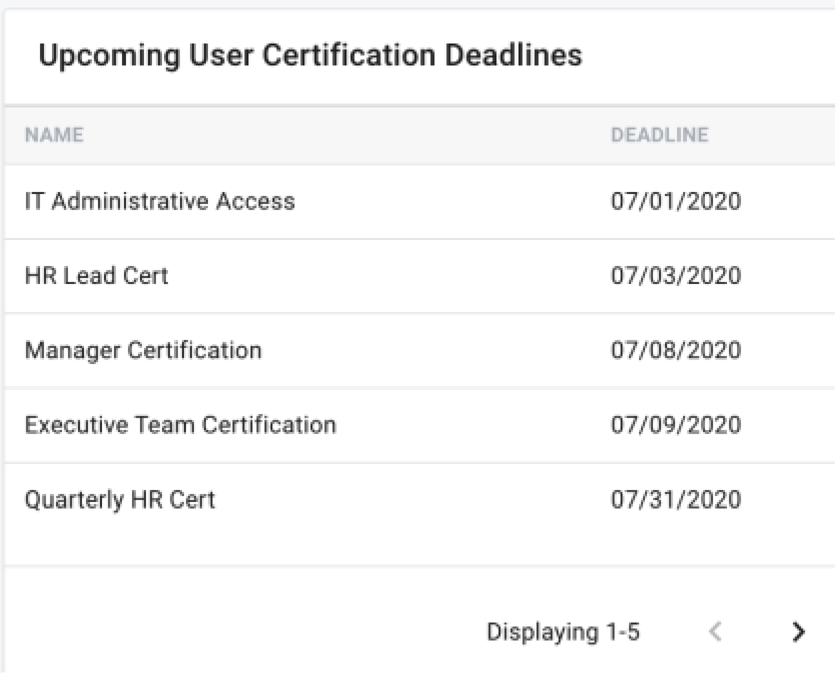
The top row of metrics on the dashboard are all displayed as stat cards. This display is used for basic counts or totals of things within the Access Review environment such as Active User Campaigns or total Glossary Entries.

A single stat card displays the metric value centered on the card, with the title displayed along the bottom. The percentage on the top right of the card shows the difference in value between the most recent scheduled run of the admin dashboard script and the current value. Note that the longer the time period between iterations of the scheduled script, the more informative these numbers tend to be.



Table

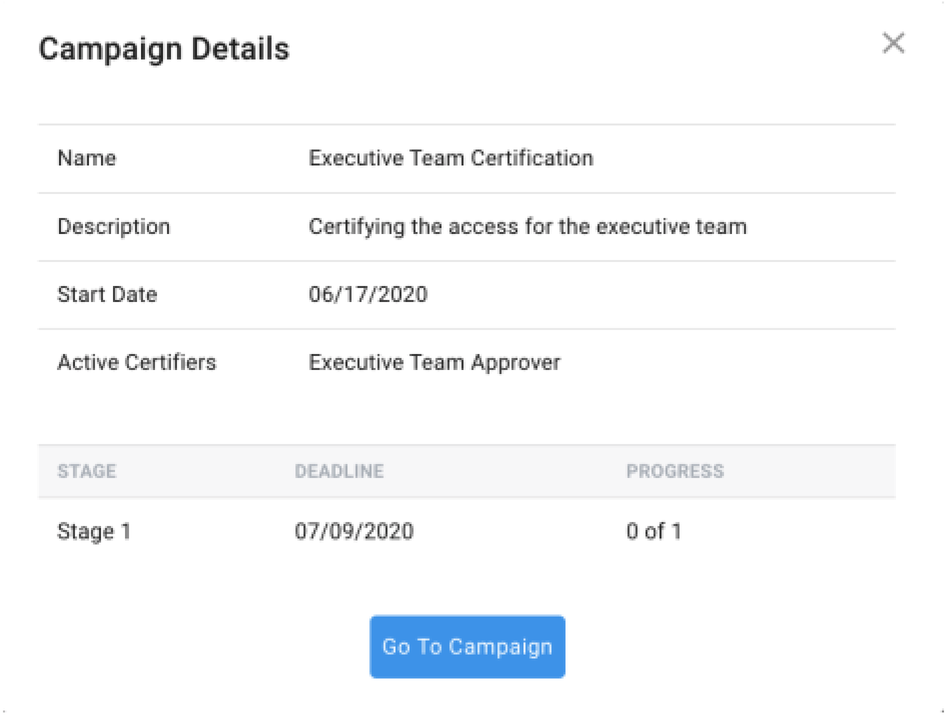
Dashboard metrics that are displayed within a table view offer a paginated and interactive view to a sorted list of campaigns, violations, or entitlements within the system. The tables are all defaulted to show five (5) rows per page, and can be individually advanced through sorted pages by using the navigation arrows found at the bottom right of the table.



Upcoming User Certification Deadlines

NAME	DEADLINE
IT Administrative Access	07/01/2020
HR Lead Cert	07/03/2020
Manager Certification	07/08/2020
Executive Team Certification	07/09/2020
Quarterly HR Cert	07/31/2020

Most of the tables within the view offer the ability to click on a given row and view more information about the item chosen. Tables of certifications offer you a brief preview of the certification campaign, as well as a button that will take the administrator directly to the administration view of the campaign.

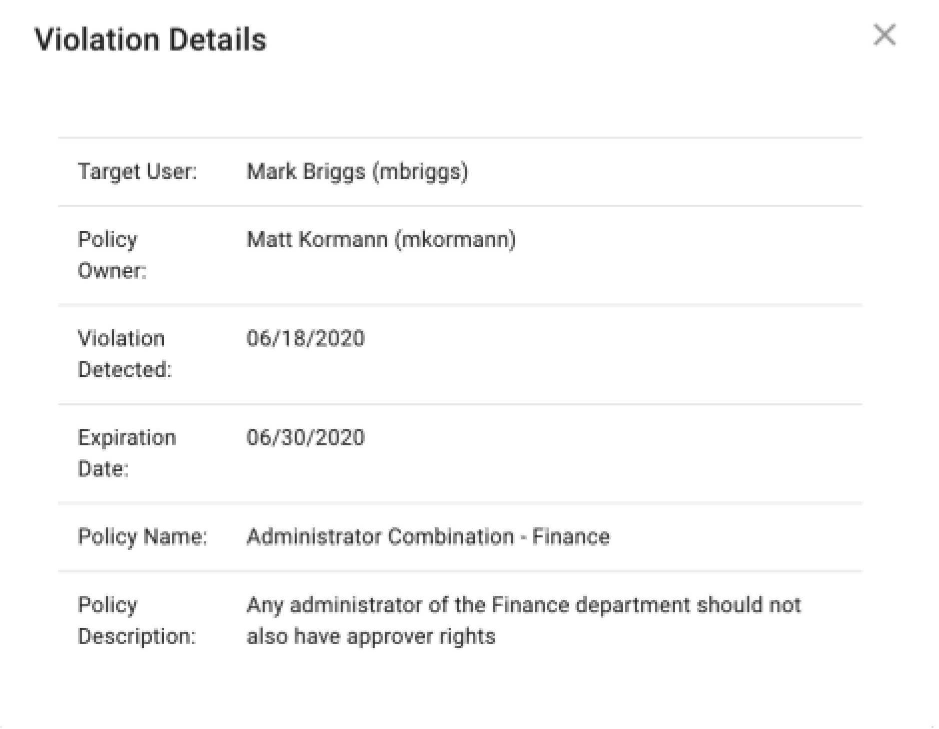


Campaign Details

Name	Executive Team Certification
Description	Certifying the access for the executive team
Start Date	06/17/2020
Active Certifiers	Executive Team Approver

STAGE	DEADLINE	PROGRESS
Stage 1	07/09/2020	0 of 1

Violation tables, when clicked, will show the administrative view of a violation that is available to admins when accessed from the Policies and Violations table.



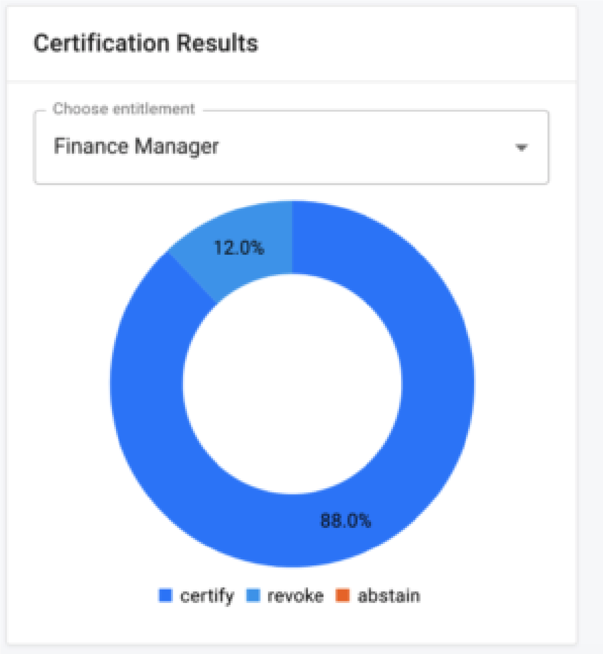
Violation Details

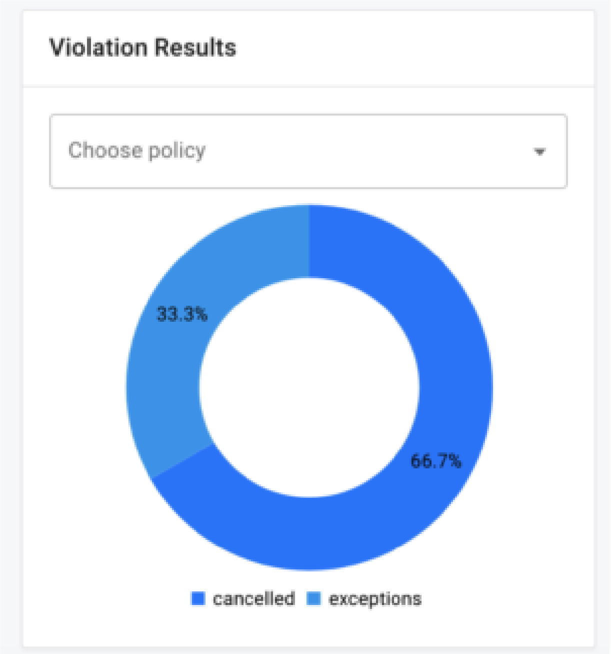
Target User:	Mark Briggs (mbriggs)
Policy Owner:	Matt Kormann (mkormann)
Violation Detected:	06/18/2020
Expiration Date:	06/30/2020
Policy Name:	Administrator Combination - Finance
Policy Description:	Any administrator of the Finance department should not also have approver rights

Finally, the entitlement tables will display the standard metadata screen view when clicked. This information is grabbed directly from the corresponding glossary entry for the certified entitlement.

Pie Chart

Metrics displayed via a pie chart show the division of entitlement certification of violation details. Upon initial installation, these charts will not appear populated until certifications and/or violations have been created and signed-off/completed and a scheduled scan of the adminDashboard script has been run. Each chart contains a select box above the chart that allows administrators to target an entitlement or policy in order to see the data that pertains only to that single object.





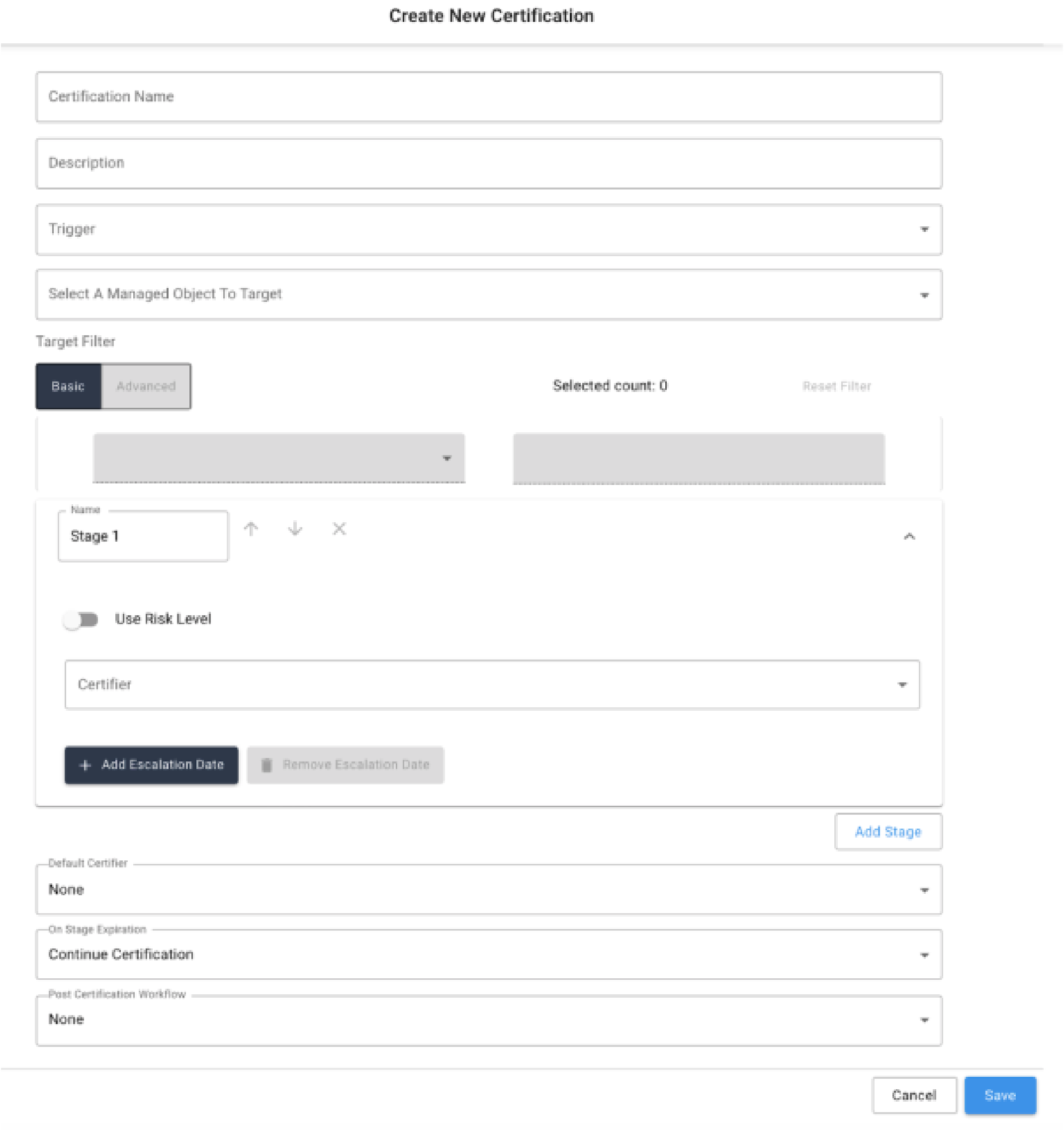
User and Object Certifications

User and object certifications target individual users or managed objects for certification. Certifications allow one or more certifiers to review a target's attributes and properties from the IDM schema. For user certifications, attributes and access defined within a linkey system may be reviewed in the applications section, and for object certifications glossary metadata as defined in the Identity Glossary can be certified. Certifiers can make a certification decision as to whether they want to certify or revoke a given entitlement, or abstain from making a choice entirely.

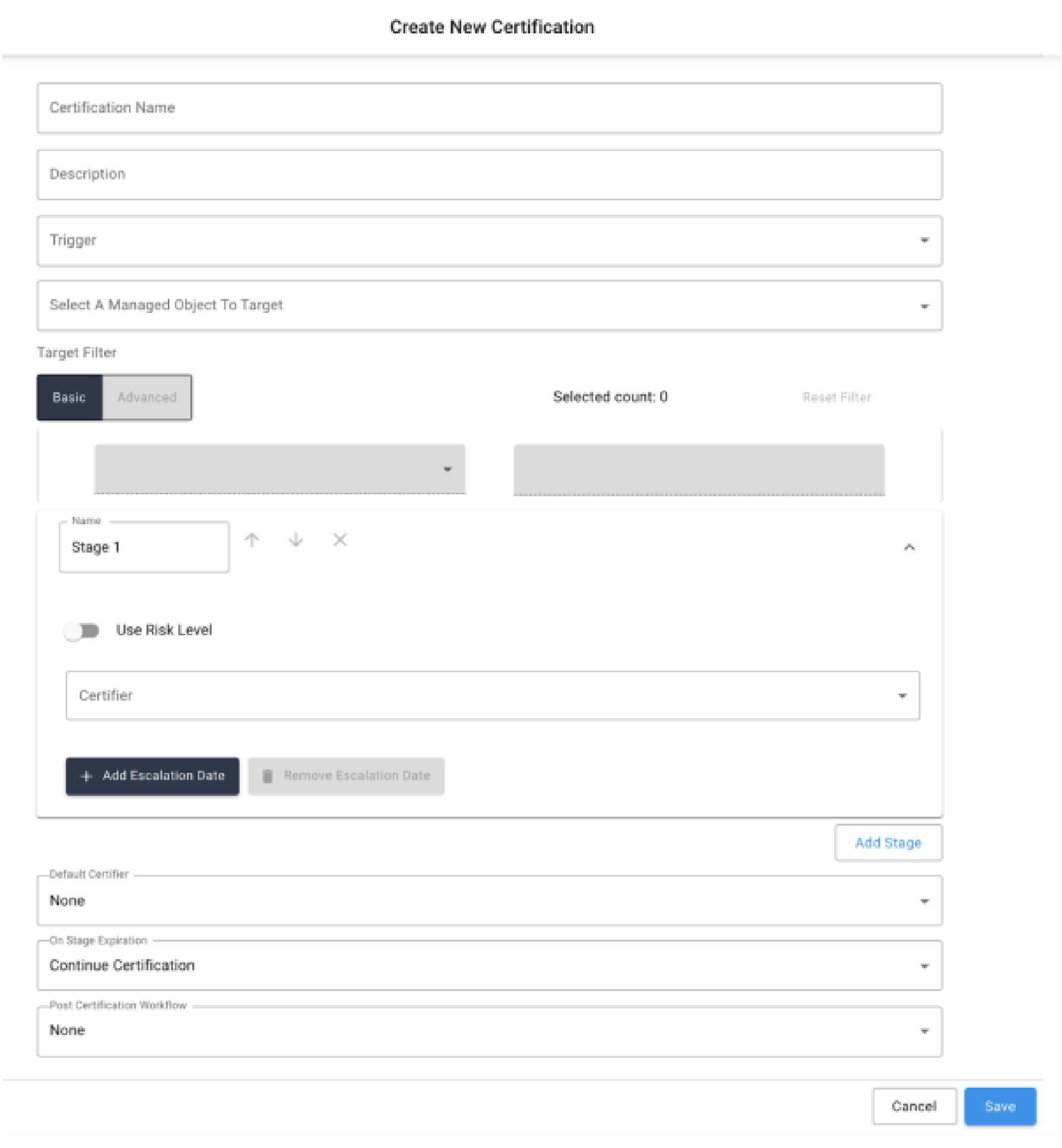
Creating New Certification Definitions

Create a user certification:

1. For User Certifications, navigate to the User Certifications screen by clicking on its link on the navigation sidebar.
2. From the User Certifications page, click the **New Certification** button in the actions row of the table.



3. On the Create New Certification screen, fill in each of the required fields. Additional details on the available fields are presented below.



Selected count: 0

Name: Stage 1

Default Certifier: None

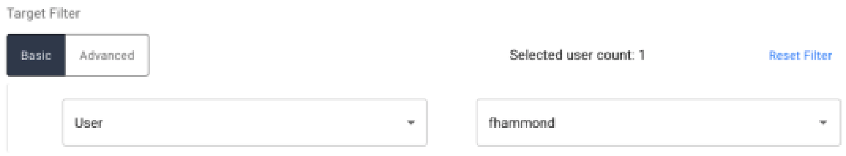
On Stage Expiration: Continue Certification

Post Certification Workflow: None

- **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 Scheduling Events.
  - **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 Expression Builder.

- **Target Object Type**. **(Object Certifications Only)**. Object certifications must specify which managed object type will be targeted in the campaign. A certification can target any number of instances of the chosen object type, but it can only target one type per campaign. All managed objects within the system are eligible to be targeted by an object certification with the exception of ‘user’ (which is handled separately.) As noted in other places within this document, it is highly recommended that any object type you wish to target in a campaign have at a minimum a name and description as part of its schema properties in order to display properly within the certification screens.
- **Target Filter**. **(Required)**. Identifies filter for targeting a specific subset of users 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 and Advanced.
    - **Basic**. Upon selecting, the left dropdown is populated with the following options:
        - **User/Single Object**. Allows certification to be filtered to target only one specific user or managed object. Upon selecting, the right input box becomes available to enter in a username or object name.

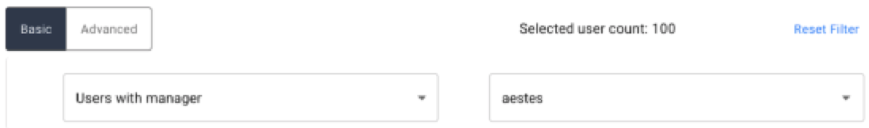


Selected user count: 1

User

fhammond

        - **Users with manager**. (User Certifications Only). 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.

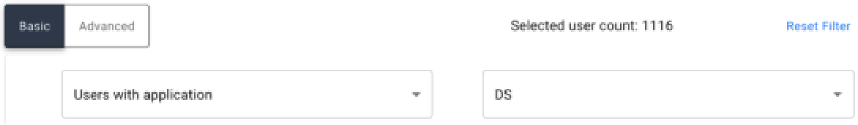


Selected user count: 100

Users with manager

aestes

        - **Users with application**. (User Certifications Only). 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.

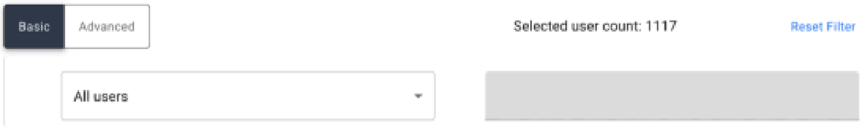


Selected user count: 1116

Users with application

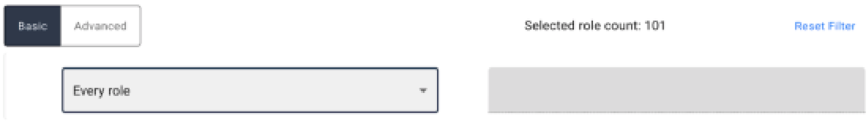
DS

    - **All Users/Every Object**. Allows certification to be run with no filter and target all users/objects of the type selected.



Selected user count: 1117

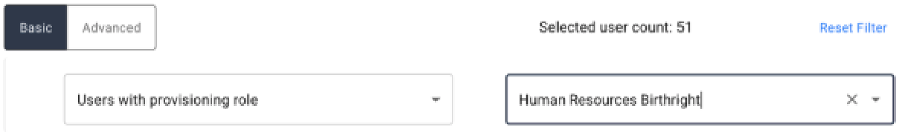
All users



Selected role count: 101

Every role

    - **Filter by provisioning/authorization role**. (User Certifications Only). 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.

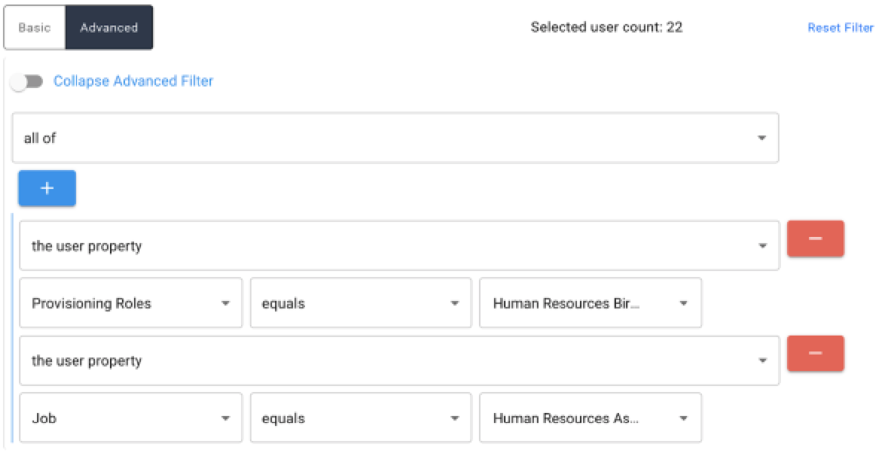


Selected user count: 51

Users with provisioning role

Human Resources Birthright

- **Advanced**. Upon selecting, the advanced expression builder is displayed. The following options for creating a custom expression are available within the certification creation advanced target filter. For a more detailed description of what the individual options determine, refer to section Expression Builder.
    - **User/Object property**. Choose from any user attribute
    - **User application**. (User Certifications Only). Allows choice of any connected application to be selected from the dropdown menu
    - **All of**. Match all of the nested rows.
    - **Any of**. Match at least one of the nested rows.
    - **None of**. Negate the expression in the nested row.
    - **All users/Every object**. Select all users.



Selected user count: 22

all of

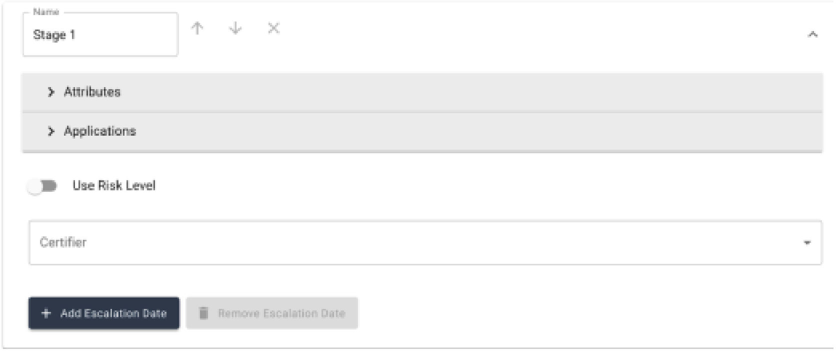
the user property

Provisioning Roles | equals | Human Resources Bir...

the user property

Job | equals | Human Resources As...

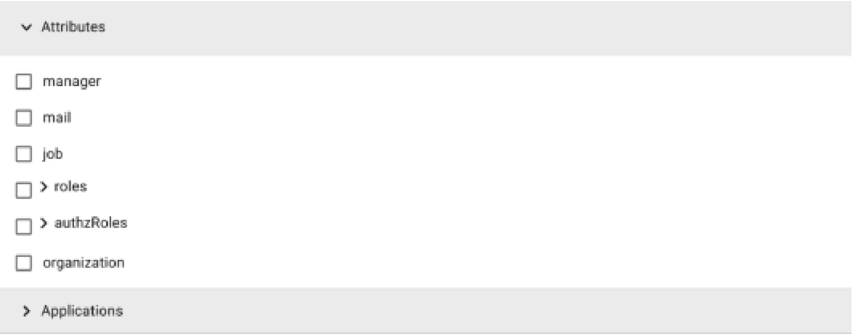
- **Certification Stages**. A certification may have one or more stages. Each selected certifier is responsible for one stage, and additional stages may be added as needed (by selecting the ‘Add Stage’ button.), while selecting. Optionally, stage names may be modified by editing the text within the Name input field.
    - **Stage icons**. Name Input: Change the stage name
        - Up/Down arrows (next to the stage name): Change the stage order
        - ‘X’ icon: remove a specific stage
        - Caret: (at the top left of each stage): collapse/expand details for a given stage



Name: Stage 1

    - **Entitlement Filter**. Specifies the entitlements/access that will appear to certifiers within the given stage. For user certifications, the attributes/applications that appear in these sections correspond to those that are defined with a key of certifiable set to true in the glossary metadata. For object certifications, the entire managed object schema for the selected type will be available to choose as certifiable in any campaign.
        - **Attributes**. The entitlements on the user or object that are tracked and stored by IDM; the managed object properties defined on the object’s schema. Basic attributes and single object relationships are included in a certification stage via a

basic checkbox. Multi-valued relationship objects are chosen and included as shown below:

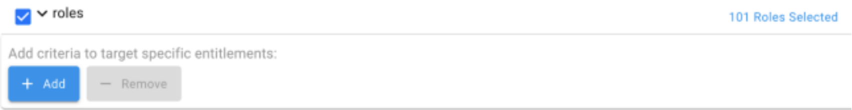


Attributes

□ manager
□ mail
□ job
□ roles
□ authzRoles
□ organization

Applications

- **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.

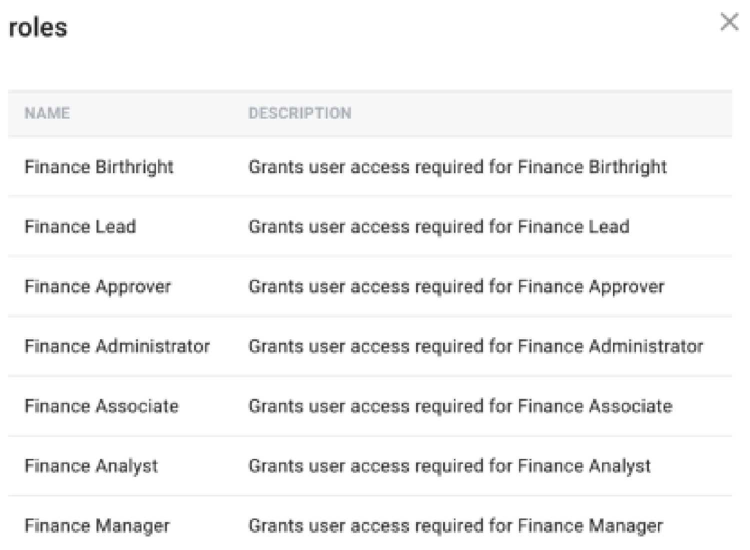


☑ roles — 101 Roles Selected

Add criteria to target specific entitlements:

When choosing to filter a multi-valued relationship, the administrator is decided which values of the managed object will be eligible for inclusion within this certification. Any objects that match this filter and belong to a target as part of the selected attribute will appear in the campaign, while those excluded by the filter won't, even if a target user has that relationship. The following operators are available:

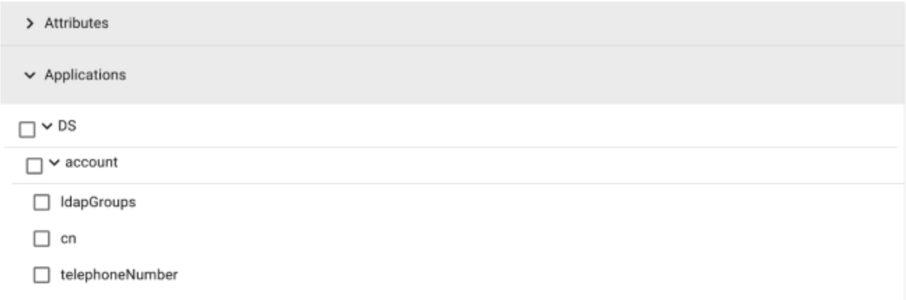
  - Equals - Exact match of property
  - Contains - Property value contains string
  - Does Not Contain - Negation of above
  - Starts With - Property value starts with string
  - Does Not Start With - Negation of above
  - Selected Roles: Clicking on the number of objects currently selected on the top right of the attribute row will display the targeted screen. This screen shows the names and descriptions of the items selected.



roles

NAME	DESCRIPTION
Finance Birthright	Grants user access required for Finance Birthright
Finance Lead	Grants user access required for Finance Lead
Finance Approver	Grants user access required for Finance Approver
Finance Administrator	Grants user access required for Finance Administrator
Finance Associate	Grants user access required for Finance Associate
Finance Analyst	Grants user access required for Finance Analyst
Finance Manager	Grants user access required for Finance Manager

- **Applications**. (User Certifications Only). The external applications and user data that are tracked by IDM through a connected system. To populate the applications list with certifiable systems, a glossary system entry must be created for the connector and assigned a key of certifiable. In addition, the attributes that can be certified must also correspond to a system-attribute entry with a key of certifiable set to true.



> Attributes

⌄ Applications

□ ⌄ DS

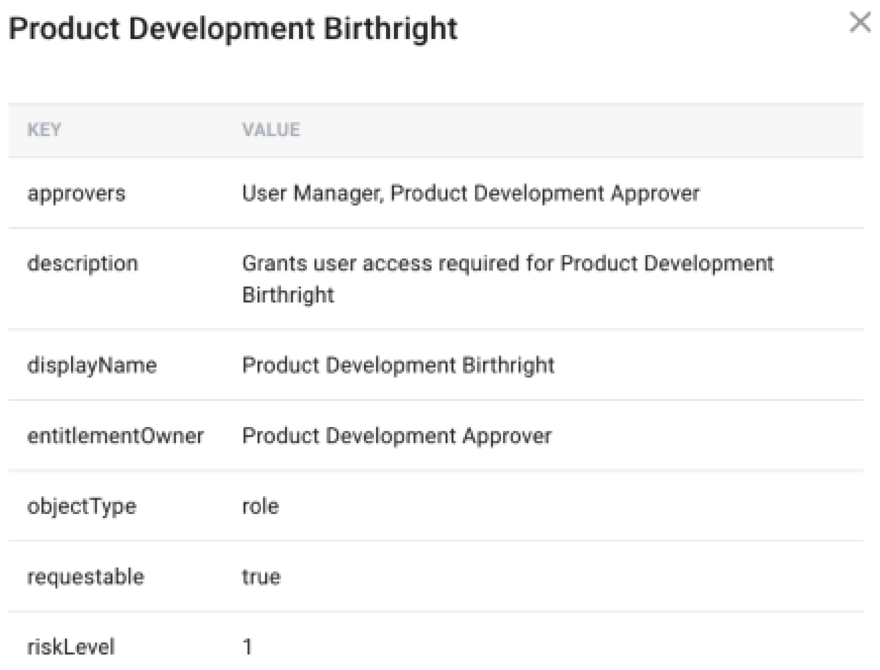
□ ⌄ account

□ ldapGroups

□ cn

□ telephoneNumber

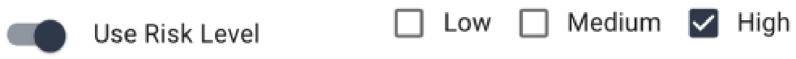
- **Metadata**. (Object Certifications Only). The entries within the Identity Glossary entry for the targeted managed object(s). Since the keys and entries that exist within the glossary are entirely arbitrary and could contain any given values across multiple instances of the same object, the administrator has the option to either not certify metadata at all, or to include all existing metadata to be certified by the certifier(s).



Product Development Birthright

KEY	VALUE
approvers	User Manager, Product Development Approver
description	Grants user access required for Product Development Birthright
displayName	Product Development Birthright
entitlementOwner	Product Development Approver
objectType	role
requestable	true
riskLevel	1

- **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. For more information on how Low, Medium and High risk levels are defined, see System Settings. Risk level on an entitlement basis is defined within the identity glossary. Relationships to managed objects will use the corresponding glossary entry of type object, while managed user properties with specific values will use glossary entries of type identity-value to define their risk.

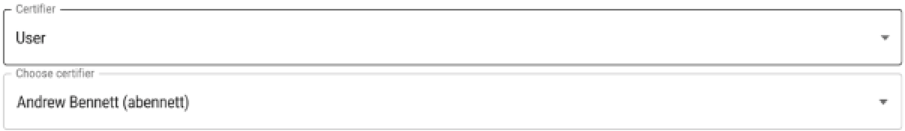
  

  Use Risk Level ☐ Low ☐ Medium ☑ High

  The following results will occur from selecting the listed filter combination:

  - **Use Risk Level off**. Risk level will not be considered when filtering entitlements in a given campaign. Entitlements with a risk level defined at any level, as well as entitlements without a risk level defined will be included.
  - **Use Risk Level on, one box selected**. Only items that match that risk level range will be included.
  - **Use Risk Level on, two boxes selected**. Only items that match either level selected will be included.
  - **Use Risk Level on, all selected**. All items that have a risk level defined will be included in certification. Entitlements without a risk level defined will be excluded.
- **Certifier**. (Required). Identifies to whom the certification stage will be assigned once generated, with the following available options:

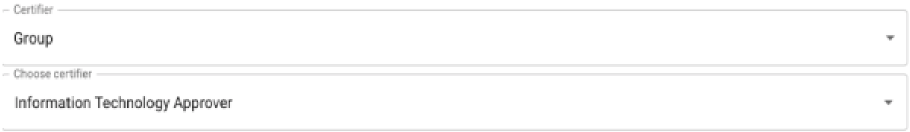
- **User**. User certifier will assign the generated certification stage to a specific user and a single user will certify all targets. When specifying a user, autocomplete will help identify the user login for the assignment.



Certifier: User

Choose certifier: Andrew Bennett (abennett)

- **Group**. Certifier assigns generated certification stage to a group of specified users. All targets will be certified by users with the given group role attribute. To specify a group, select an available role in the choose certifier drop-down menu. See the section in the post-installation steps on membership property for information on how group membership is determined.



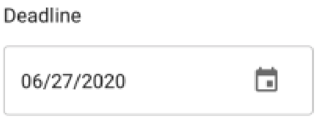
Certifier: Group

Choose certifier: Information Technology Approver

- **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 ‘Group.’
- **Entitlement Owner**. (User Certifications Only). 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 Access Review Glossary (glossary key of entitlementOwner, with a type of managed object.) This option will allow for multiple certifiers to be assigned a subset of entitlements for a given certification within a stage.
- **Glossary Key**. (Object Certifications Only). This option allows administrators to specify any glossary key of their choosing to become the certifier for the selected stage. This allows for any defined key, or multiple keys using subsequent stages, to be certifiers for entitlements in a given stage. As with entitlement owner certifications, if a given entitlement has the defined key in its glossary entry, that key is defined as type managed object, and that managed object is a user or role, then that person or role will be assigned as the certifier. If the entitlement does not have the

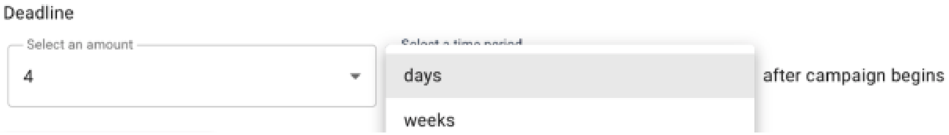
    entry defined as described above, the entitlement will not be included in the stage or will go to the default certifier if specified.

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

  Deadline

  06/27/2020

  Deadline

  Select an amount: 4

  Select a time period: days

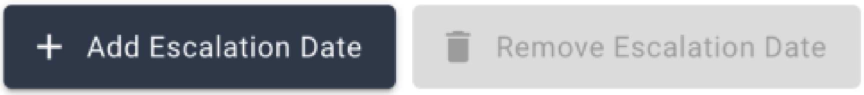
  weeks

  after campaign begins

- **Escalation Schedule**. Administrators are now able to define a configured schedule of escalation notifications that are delivered to a specific party at a specific time period before the certification expires.
  - **Add an escalation date**. To add an escalation notification to the schedule, simply click the ‘Add Escalation Date’ button located on the stage form beneath the deadline field. This will populate a single instance of the escalation form which consists of the following fields:
    - **Amount**. The numeric value that combines with the chosen time period to determine the time before the certification expires that the notification will be sent.
    - **Time period**. Days or weeks before certification expires.
    - **Escalation owner type**. Who will be notified of the escalation. Choice of either user, group, or manager. Manager in this case refers to the manager of the certifier for the given user events.
    - **Choose escalation owner**. If owner type is user or group, select the user or role that will receive the notification.

      In order to add an additional escalation date the preceding form must be completed before the add button is enabled again. Escalation dates must be added in order of furthest from the deadline to closest.
  - **Escalation Schedule**. Administrators are now able to define a configured schedule of escalation notifications that are delivered to a specific party at a specific time period before the certification expires.

    To add an escalation notification to the schedule, simply click the ‘Add Escalation Date’ button located on the stage form beneath the deadline field. This will populate a single instance of the escalation form which consists of the following fields:



        - **Amount**. The numeric value that combines with the chosen time period to determine the time before the certification expires that the notification will be sent.
        - **Time period**. Days or weeks before certification expires.
        - **Escalation owner type**. Who will be notified of the escalation. Choice of either user, group, or manager. Manager in this case refers to the manager of the certifier for the given user events.
        - **Choose escalation owner**. If owner type is user or group, select the user or role that will receive the notification.

          In order to add an additional escalation date the preceding form must be completed before the add button is enabled again. Escalation dates must be added in order of furthest from the deadline to closest.

    - **Remove escalation date**. To remove the most recent escalation date, click on the ‘Remove Escalation Date’ found next to the add button.

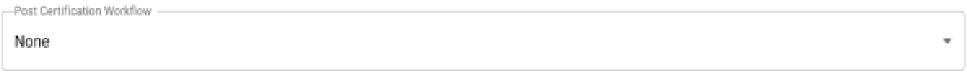
- **Default Certifier**. Specifies a default certifier for the entire campaign. If a default certifier is set, then stage events with no owner will be assigned to that certifier. If no default certifier is set, events with no owner will receive the status ‘No Certifier'. If no default certifier is set,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

On Stage Expiration
Continue Certification

    - **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

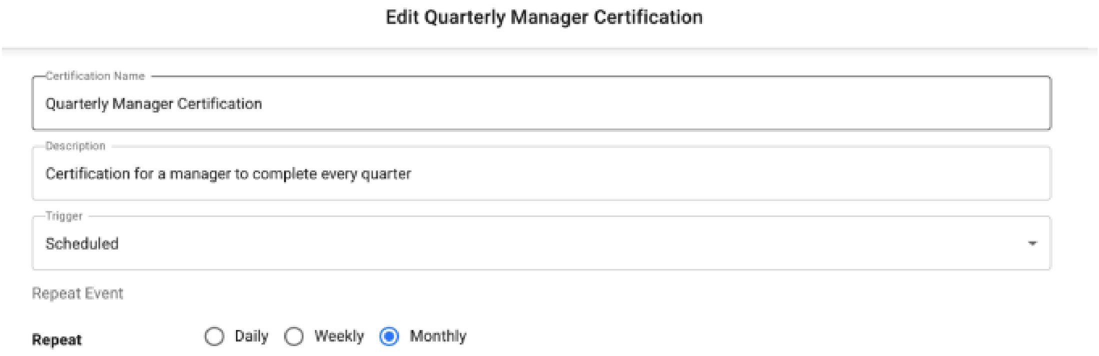
of the campaign to take action on the event.

- **Post Certification Workflow**. Identifies an automated remediation task for handling revocations from the certification. Note: For more information on remediation tasks, refer to section Remediation Tasks.


Post Certification Workflow
None

Modifying Certification Definitions

1. To modify an existing certification definition, click on the User or Object Certifications link under the administrative section of the side navigation bar.
2. Choose either the Scheduled or Triggered tabs.
3. The table will be populated with all existing scheduled or triggered certification definitions that exist within the system.
4. To modify a given certification, click on the row that contains the desired campaign to open up the edit screen. This screen will be the same as the one used for creating certifications, with the certification data from the given campaign populated.
5. Once you have finished making your adjustments to the certification, click Save at the bottom of the form to complete the update. Note: For additional information on fields to update on this form, refer to section Creating New Certification Definitions.


Edit Quarterly Manager Certification

Certification Name
Quarterly Manager Certification

Description
Certification for a manager to complete every quarter

Trigger
Scheduled

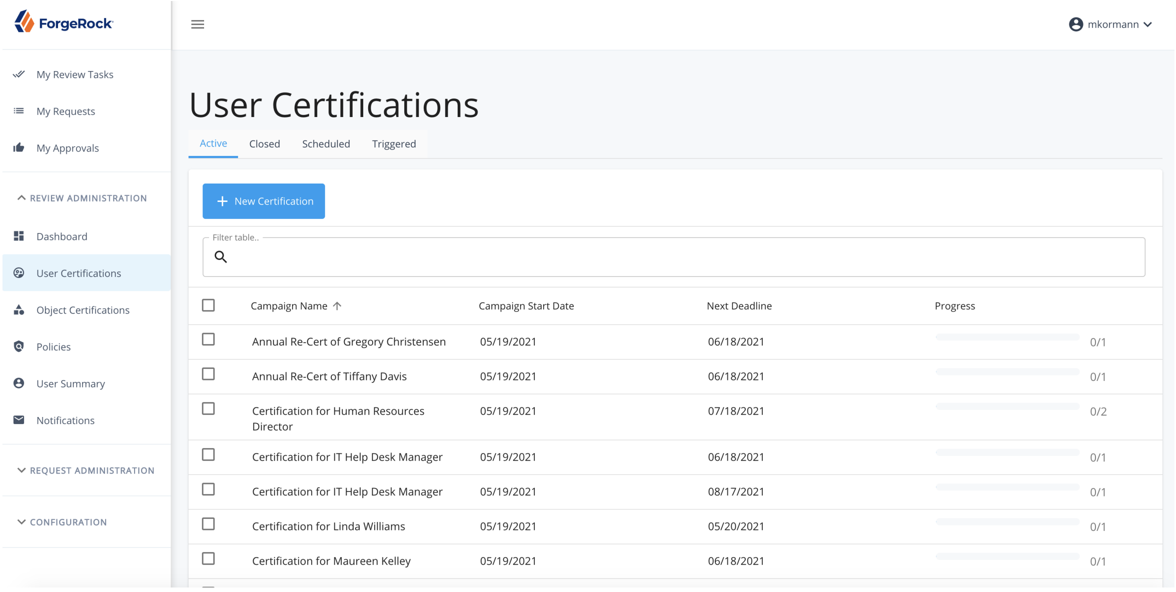
Repeat Event

Repeat ○ Daily ○ Weekly ● Monthly

Certification Tables

To review the different certifications tables, click on the User or Object Certifications link under the Administrative section of the side navigation bar. The information below will describe the columns and functionality of each of the existing tables.

- **Active Certifications**



User Certifications

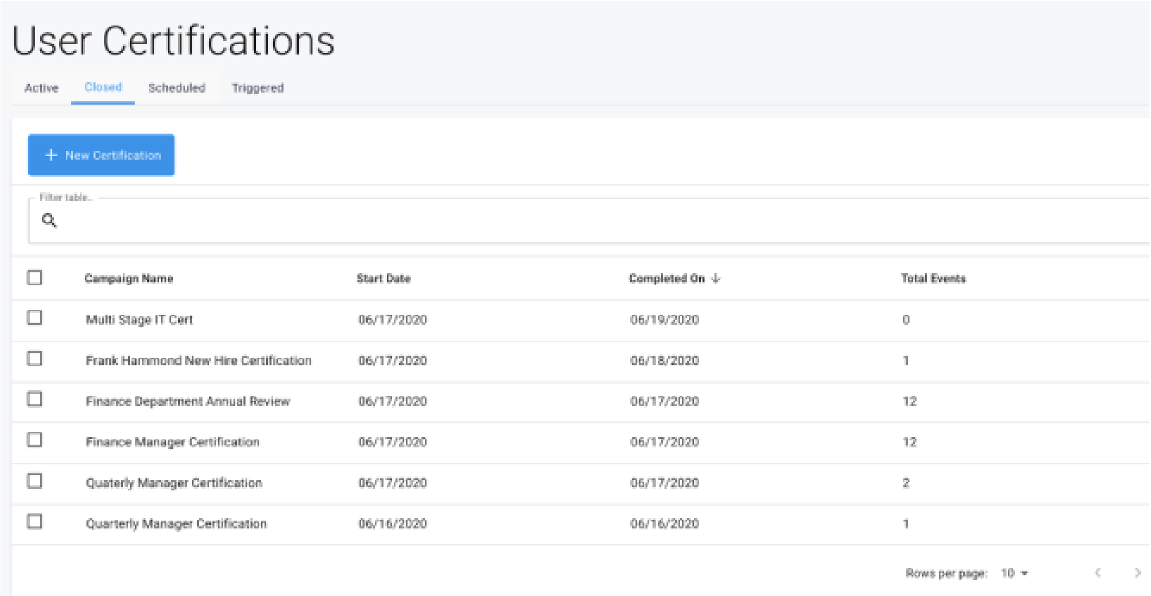
□	Campaign Name ↑	Campaign Start Date	Next Deadline	Progress
□	Annual Re-Cert of Gregory Christensen	05/19/2021	06/18/2021	0/1
□	Annual Re-Cert of Tiffany Davis	05/19/2021	06/18/2021	0/1
□	Certification for Human Resources Director	05/19/2021	07/18/2021	0/2
□	Certification for IT Help Desk Manager	05/19/2021	06/18/2021	0/1
□	Certification for IT Help Desk Manager	05/19/2021	08/17/2021	0/1
□	Certification for Linda Williams	05/19/2021	05/20/2021	0/1
□	Certification for Maureen Kelley	05/19/2021	06/18/2021	0/1

- Action Buttons
  - New Certification. Create a new certification campaign.
  - Cancel Certification. Cancel an in-progress campaign.
- Display Columns
  - Campaign Name
    - Description: Name of the active campaign
    - Searchable: Yes
    - Sortable: Yes
  - Object Type (Object certifications only).
    - Description: Type of managed object the campaign is targeting
    - Searchable: Yes
    - Sortable: Yes
  - Campaign Start Date
    - Description: Date the campaign was initially kicked off
    - Searchable: No
    - Sortable: Yes
  - Next Deadline
    - Description: Deadline of the earliest active stage (future stages may have a deadline further out than this date.)
    - Searchable: No
    - Sortable: Yes
  - Progress
    - Description: Shows the number of events completed out of the total number of events across all stages of the campaign. Note that to be

considered completed, an event must be reviewed and signed-off by the certifier.

            - Searchable: No
            - Sortable: No

- **Closed Certifications**



User Certifications

□	Campaign Name	Start Date	Completed On ↓	Total Events
□	Multi Stage IT Cert	06/17/2020	06/19/2020	0
□	Frank Hammond New Hire Certification	06/17/2020	06/18/2020	1
□	Finance Department Annual Review	06/17/2020	06/17/2020	12
□	Finance Manager Certification	06/17/2020	06/17/2020	12
□	Quaterly Manager Certification	06/17/2020	06/17/2020	2
□	Quarterly Manager Certification	06/16/2020	06/16/2020	1

    - **Action Buttons**
        - New Certification
    - **Display Columns**
        - Campaign Name
            - Description: Name of the closed campaign
            - Searchable: Yes
            - Sortable: Yes
    - **Object Type (Object certifications only)**
        - Description: Type of managed object the campaign is targeting
        - Searchable: Yes
        - Sortable: Yes
    - **Campaign Start Date**
        - Description: Date the campaign was initially kicked off
        - Searchable: No
        - Sortable: Yes
    - **Completed On**
        - Description: Date that the last stage of the campaign was completed and signed-off
        - Searchable: No

        - Sortable: Yes
    - **Total Events**
        - Description: Total events in campaign
        - Searchable: No
        - Sortable: No
- **Scheduled Certifications**
    - **Action Buttons**
        - New Certification
        - Cancel Certification
    - **Display Columns**
        - Campaign Name
            - Description: Name of the scheduled campaign
            - Searchable: Yes
            - Sortable: Yes
    - **Next Run Date**
        - Description: Date that the scheduled campaign will start based on its defined scheduler object
        - Searchable: No
        - Sortable: Yes
- **Triggered Certifications**
    - **Action Buttons**
        - New Certification
        - Cancel Certification
    - **Display Columns**
        - Campaign Name
            - Description: Name of the scheduled campaign
            - Searchable: Yes
            - Sortable: Yes

Canceling Active Campaigns

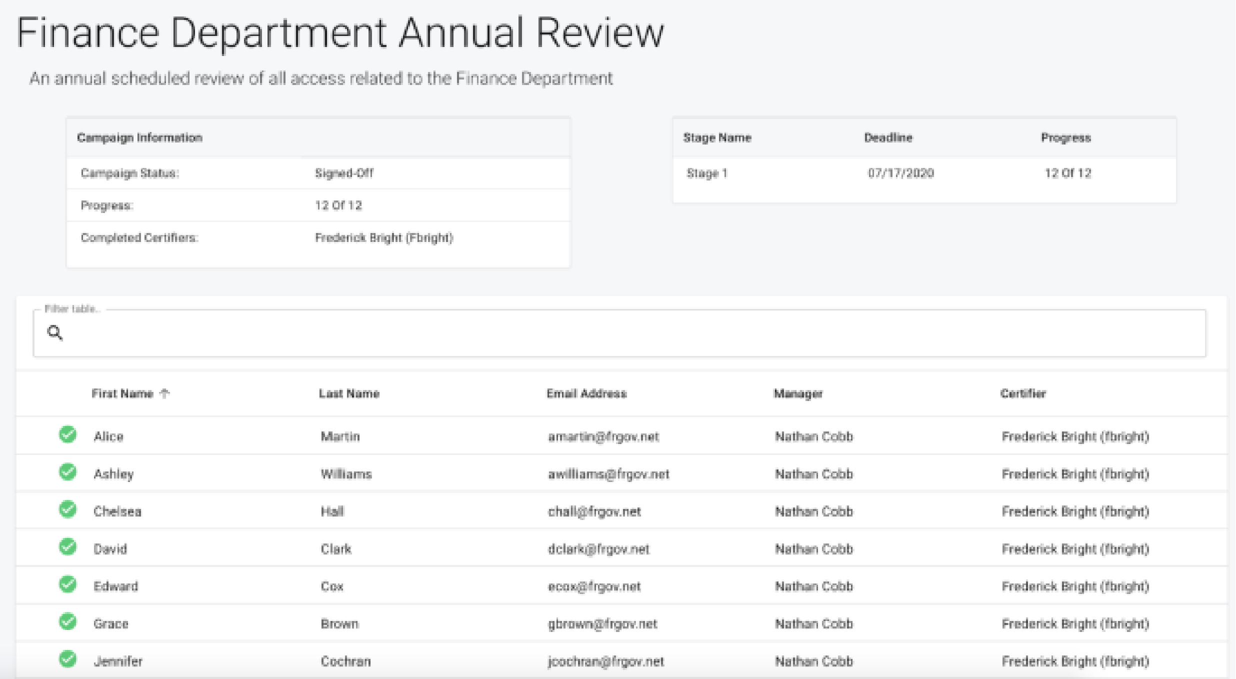
To cancel an active campaign from the “Active” tab, check the checkbox next to the row of the campaign or campaigns that you wish to cancel. Note that once at least one row selected, the cancel certification button in the table’s action row will become enabled. Once this button is clicked the administrator will be asked to confirm their choice, and if done so, the certification campaigns will be cancelled.

Deleting Certification Definitions

Deleting a certification definition from the scheduled or triggered tab of a Certifications page works exactly as described above for cancellation of active campaigns.

Reviewing Active Certifications

From the active certifications tab of the User or Object Certifications table, search or sort the table until you find the desired campaign that you wish to review. Clicking on that certifications row will take you to the administrator certification list for that campaign.



Finance Department Annual Review

An annual scheduled review of all access related to the Finance Department

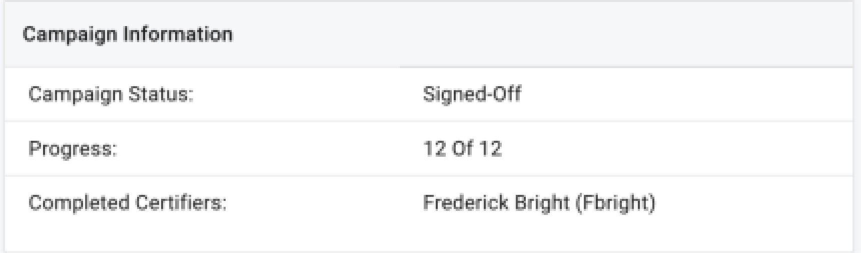
Campaign Information	
Campaign Status:	Signed-Off
Progress:	12 Of 12
Completed Certifiers:	Frederick Bright (Fbright)

Stage Name	Deadline	Progress
Stage 1	07/17/2020	12 Of 12

	First Name ↑	Last Name	Email Address	Manager	Certifier
✓	Alice	Martin	amartin@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	Ashley	Williams	awilliams@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	Chelsea	Hall	chall@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	David	Clark	dclark@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	Edward	Cox	ecox@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	Grace	Brown	gbrown@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	Jennifer	Cochran	jcochran@frgov.net	Nathan Cobb	Frederick Bright (fbright)

Select a certification from the Active Certifications list to display additional information. The following details will be displayed:

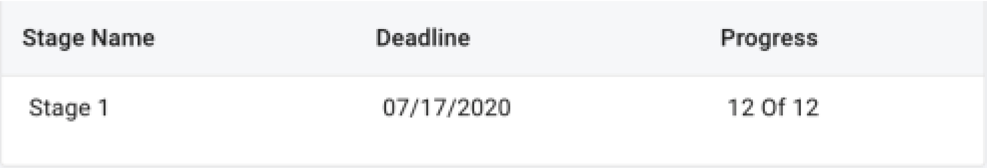
- **Campaign Name**. Name of the campaign
- **Campaign Description**. Description of the campaign
- **Campaign Information**. Displays a summary of the campaign with the following information:

Campaign Information	
Campaign Status:	Signed-Off
Progress:	12 Of 12
Completed Certifiers:	Frederick Bright (Fbright)

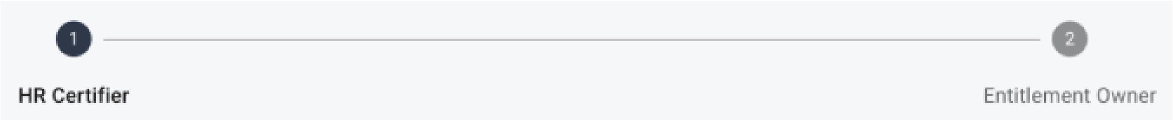
  - **Campaign Status**. Identifies the current state of the certification. Values may include In-Progress, Cancelled, Signed-off, or Expired

  - **Progress**. The number of campaign events signed-off against the total number of events in the campaign
  - **Active Certifiers**. Any certifier with an in-progress event assigned to them that is part of the given campaign. Note this does not include certifiers with a pending (future stage) event assigned to them.
  - **Completed Certifiers**. Any certifier that has completed and signed-off on an event that is part of the given campaign.
- **Stage Information**. Displays a breakdown of each stage within the certification campaign with the following information:



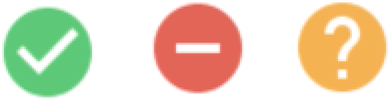
Stage Name	Deadline	Progress
Stage 1	07/17/2020	12 Of 12

  - **Stage Name**. Name assigned to the stage
  - **Deadline**. Date that stage is set to or did expire
  - **Progress**. The number of stage events signed-off against the total number of events in the stage
- **Stage Stepper**. Shows a chronological visual of the certification stages. By selecting a stage node, the page will be updated to reflect data for the selected stage.



- **Target List**. List containing all targets for the certification. Each line contains a summary of the targeted user or object with the following information:
  - **Status icon**. The status of the current target's event for the selected stage. The following statuses are possible:
    - Pending
    - Incomplete
    - Certified
    - Certified, signed off
    - Revoked
    - Revoked, signed off
    - Abstained
    - Abstained, signed off
    - Cancelled
    - No Certifier
    - Expired

Each status is displayed via a circular icon, and may have a different color or fill depending on the individual status. Certified statuses will be colored green, revoked colored red, and abstained colored yellow. The difference between when a normal value and the signed-off version of that value is displayed, the normal version will be displayed when all actions on an event have been completed, but the certifier has not yet signed off on it. After sign-off, the signed off version of the icon will be displayed. This allows the administrator to have a little more insight at this level into the progress of the campaign even before any sign offs occur.

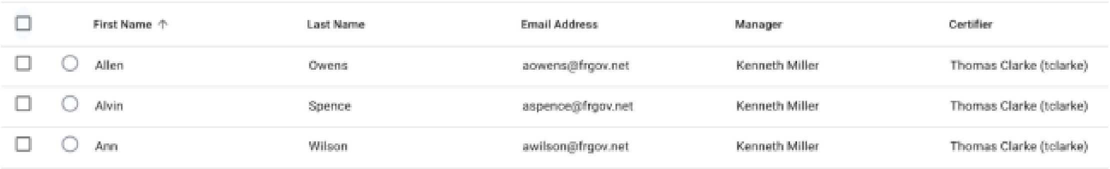


Note that each icon will display a tooltip with the display status text if the administrator hovers over the icon.

- **Displayable Target Info Columns**. The information that displays in the certification list table may vary depending on certification type and the special displayInUserInfo key in the glossary on identity objects.

  For object certifications these displayable columns will always be name and description, so it's highly recommended that these attributes exist on any custom managed object that you wish to certify

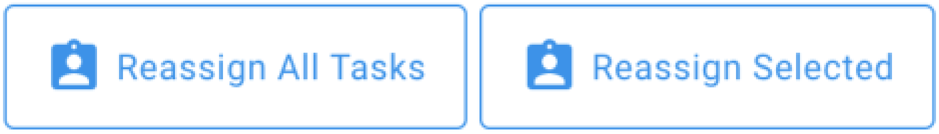
  For user certifications, the displayable columns will always include at least the user's givenName, sn, and email address, as well as any user attribute that has a glossary entry of type identity in the glossary and the displayInUserInfo boolean key set to true. Note that this key will not prevent you from displaying relationship attributes in the target list table, however with the exception of manager these attributes are not supported to display properly.
- **Claimed By**. If the certifier for the given stage is a group, this column will display to inform the administrator as to which single user, if any, has claimed the given event.
- **Certifier**. The user or role who is the certifier for the target event.



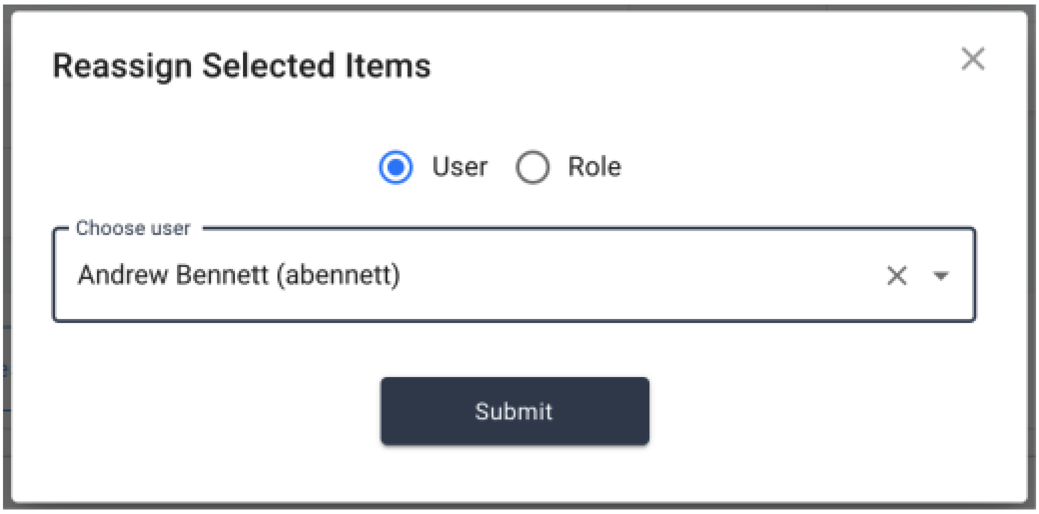
□		First Name ↑	Last Name	Email Address	Manager	Certifier
□	○	Allen	Owens	aowens@frgov.net	Kenneth Miller	Thomas Clarke (tclarke)
□	○	Alvin	Spence	aspence@frgov.net	Kenneth Miller	Thomas Clarke (tclarke)
□	○	Ann	Wilson	awilson@frgov.net	Kenneth Miller	Thomas Clarke (tclarke)

Reassigning Active Certification Events

Administrators have the ability to reassign active or pending certification events from the certification list for a given campaign. The admin has the option to either reassign all given events within a given campaign, or to select one or more rows within the target list table and reassign only those selected. The buttons to reassign the events are found in the action buttons section of the certification list table.



Once the administrator has clicked on one of the available buttons to reassign, a small dialog box will appear with a few options for selecting the new certifier. The administrator can choose to reassign to an individual user or a group. When searching for a user, the administrator can use any of the properties made available and searchable via the User Name Display Format setting, while group roles are searchable by name.

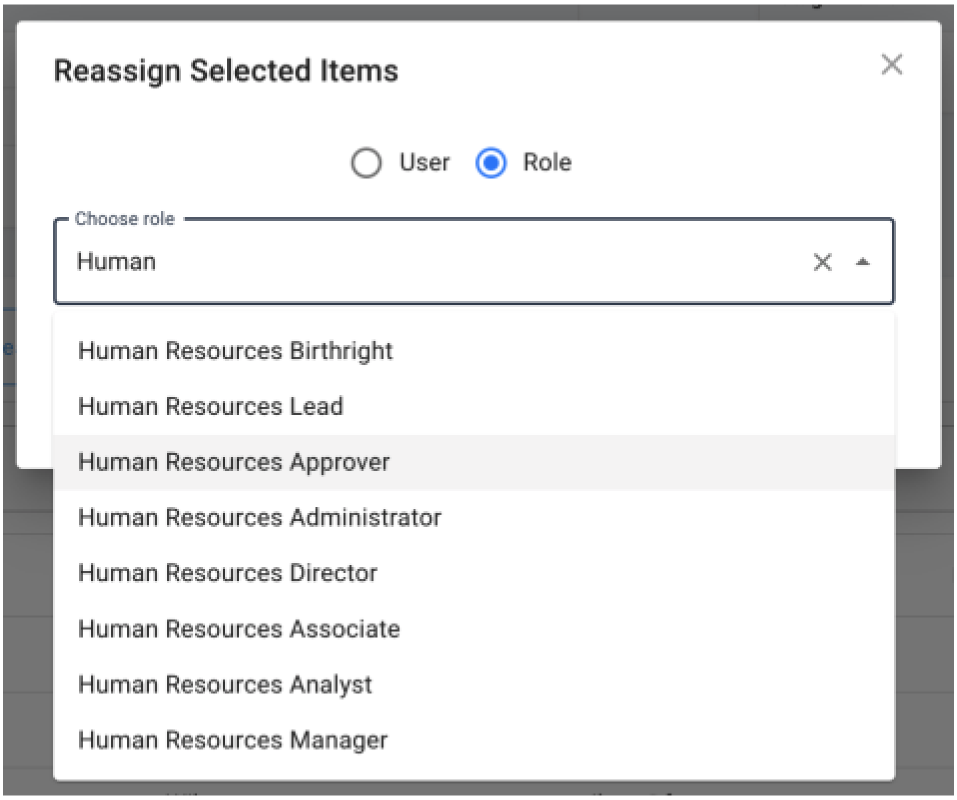

Reassign Selected Items

● User ○ Role

Choose user: Andrew Bennett (abennett)

NOTE

Reassignment of Entitlement Owner user certifications can not be done on the certification list page. For reassignment of these certifications, you can use the User Summary page reassignment function when the entitlement owner is a user. For role entitlement owners, it is recommended to add an appropriate user to the role assigned, or to reconfigure your glossary data to reflect the appropriate owner and recreate the certification to ensure integrity of the certification process.



Reassign Selected Items

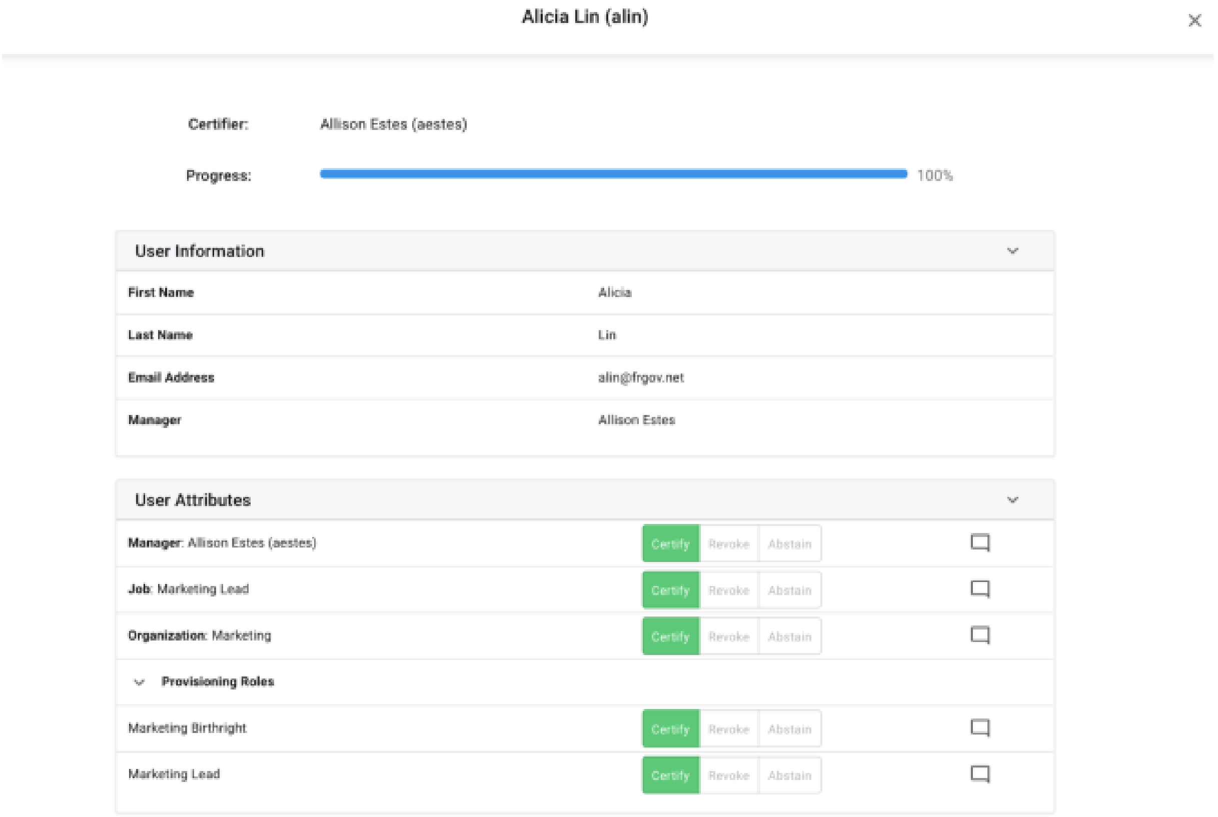
○ User ● Role

Choose role: Human

- Human Resources Birthright
- Human Resources Lead
- Human Resources Approver
- Human Resources Administrator
- Human Resources Director
- Human Resources Associate
- Human Resources Analyst
- Human Resources Manager

Reviewing Active Events

Select a target from the certification target list to display the complete event details view of the certification in a dropdown page. This is the same interface that is displayed to the end users when certifying a target, with some slight adjustments to what actions are available. The following information is displayed:



Alicia Lin (alin)

Certifier: Allison Estes (aestes)

Progress: 100%

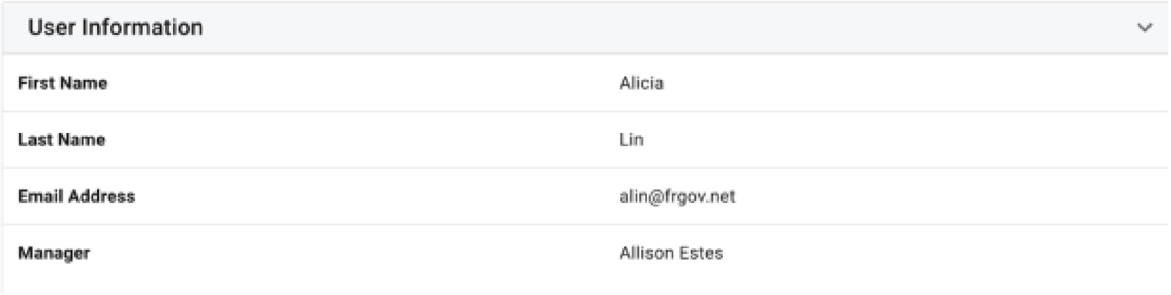
User Information

First Name	Alicia
Last Name	Lin
Email Address	alin@frgov.net
Manager	Allison Estes

User Attributes

Manager: Allison Estes (aestes)	Certify	Revoke	Abstain	□
Job: Marketing Lead	Certify	Revoke	Abstain	□
Organization: Marketing	Certify	Revoke	Abstain	□
Provisioning Roles				
Marketing Birthright	Certify	Revoke	Abstain	□
Marketing Lead	Certify	Revoke	Abstain	□

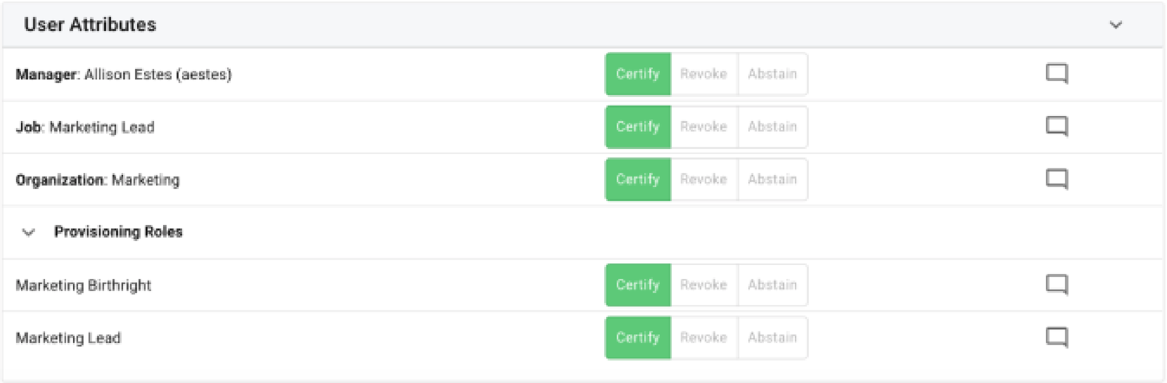
- **Event Details**. The section at the top of the page will display details about the given event's certification progress. It will include some or all of the following information:
  - **Stage Selector**. If the campaign has multiple stages, the stage stepper selection bar will be shown to allow the administrator to toggle between stages.
  - **Certifier**. The certifier for the event, if a single user or role
  - **Active Certifiers**. If an entitlement owner certification, shows the certifiers for the event that are active (have tasks to complete).
  - **Claimed By**. If the event has a role certifier and is claimed, displays the single user who has claimed it
  - **Completion Date**. Date and time that the event was signed off
  - **Progress Bar**. The progress bar for the event
- **User Information**. Details a summary of the target of the event with the following information. Note that more attributes may appear in user certifications if the displayInUserInfo boolean key is set to true on the glossary entry for the identity attributes:



User Information

First Name	Alicia
Last Name	Lin
Email Address	alin@frgov.net
Manager	Allison Estes

  - **User certifications**
    - First Name: First name of the target user
    - Last Name: Last name of the target user
    - Email Address: Contact information of the target user
    - Identity attributes set to display as described above
  - **Object certifications**
    - Name: Name of the object
    - Description: Description of the object
- **User/Object Attributes**. Contains attributes to be certified for the target of the event. 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. These attributes with parent rows can be collapsed and expanded by clicking on the expand icon to the left of the attribute name.



User Attributes

Manager: Allison Estes (aestes)

Job: Marketing Lead

Organization: Marketing

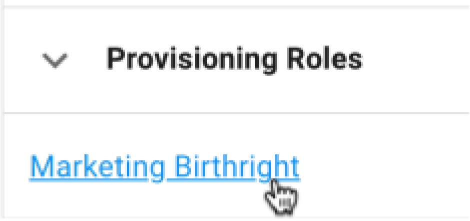
Provisioning Roles

Marketing Birthright

Marketing Lead

Each row contains the following information:

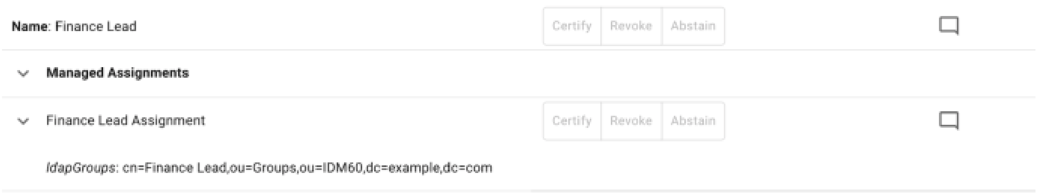
- **Attribute Name and/or Value**
    - Each attribute name and value is clickable by the administrator to see any attached metadata that belongs to the given item. Those items that do not have a corresponding glossary entry will display a page informing the administrator that no entry exists. Note that in object certifications, only the value will allow for displaying metadata as individual object schema attributes do not have direct metadata definitions.



Provisioning Roles

Marketing Birthright

> NOTE
>
> For object certifications, when certifying an object that has a relationship to an out-of-the-box ForgeRock managed assignment, the display of those entitlements within the certification table is slightly altered from any other type of entitlement. For each assignment, any entry in the attributes property of that assignment will be displayed in a readable format below the assignment name. This allows the certifiers to see exactly what access is being provisioned via this assignment, in order to make their decision easier.



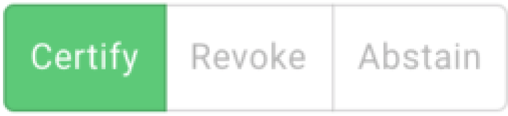
Name: Finance Lead

Managed Assignments

Finance Lead Assignment

ldapGroups: cn=Finance Lead,ou=Groups,ou=IDM60,dc=example,dc=com

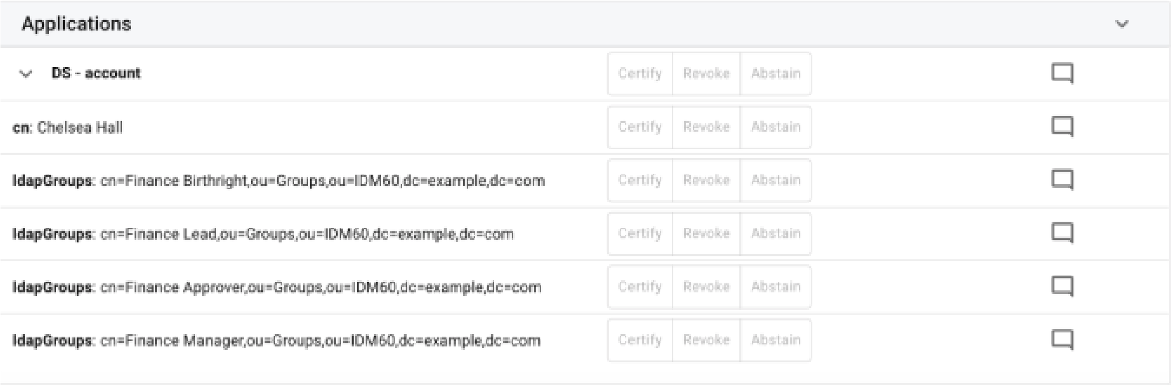
- **Certification Action Buttons**. These buttons, disabled for administrators, will show the result of the certification action taken on each item if one has been made. If no button is selected and filled, then no decision has been made for that item. The buttons included are listed below:



  - Certify
  - Revoke
  - Abstain

- **Comment Icon**. The comment icon will either be unfilled if no current comments exist, or have mini comment lines inside of the icon to indicate there are existing comments (pictured below). The administrator can click on the comment icon to display the existing comments, and also to add a new comment to that entitlement.

- **Applications (User Certifications only)**. Contains attributes within connected systems to be certified for the target user.



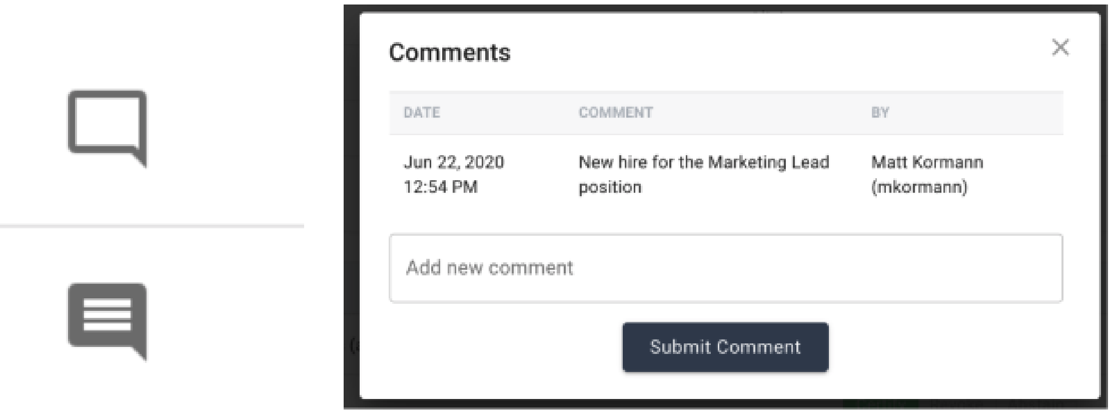
Applications

DS - account	Certify Revoke Abstain	□
cn: Chelsea Hall	Certify Revoke Abstain	□
ldapGroups: cn=Finance Birthright,ou=Groups,ou=IDM60,dc=example,dc=com	Certify Revoke Abstain	□
ldapGroups: cn=Finance Lead,ou=Groups,ou=IDM60,dc=example,dc=com	Certify Revoke Abstain	□
ldapGroups: cn=Finance Approver,ou=Groups,ou=IDM60,dc=example,dc=com	Certify Revoke Abstain	□
ldapGroups: cn=Finance Manager,ou=Groups,ou=IDM60,dc=example,dc=com	Certify Revoke Abstain	□

- **Attribute Name and/or Value**. Each attribute name and value is clickable by the administrator to see any attached metadata that belongs to the given item. Those items that do not have a corresponding glossary entry will display a page informing the administrator that no entry exists.
- **Certification Action Buttons**. These buttons, disabled for administrators, will show the result of the certification action taken on each item if one has been made. If no button is selected and filled, then no decision has been made for that item. The buttons included are listed below:
  - Certify
  - Revoke
  - Abstain
- **Comment icon**. The comment icon will either be unfilled if no current comments exist, or have mini comment lines inside of the icon to indicate there are existing comments (pictured below). The administrator can click on the

comment icon to display the existing comments, and also to add a new comment to that entitlement.

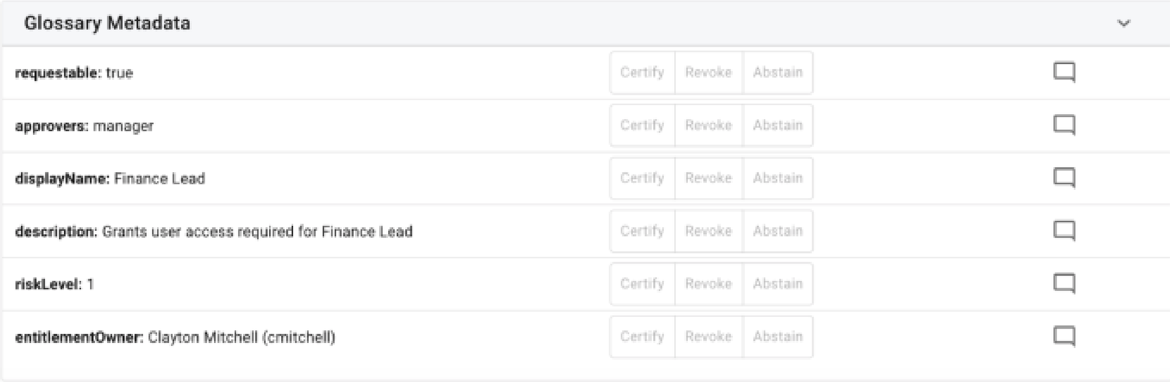
> NOTE
>
> For more information on Comments, refer to section Comments.



Comments

DATE	COMMENT	BY
Jun 22, 2020 12:54 PM	New hire for the Marketing Lead position	Matt Kormann (mkormann)

- **Metadata (Object Certifications only)**. Contains each metadata entry that exists within the glossary entry for the target object.



Glossary Metadata

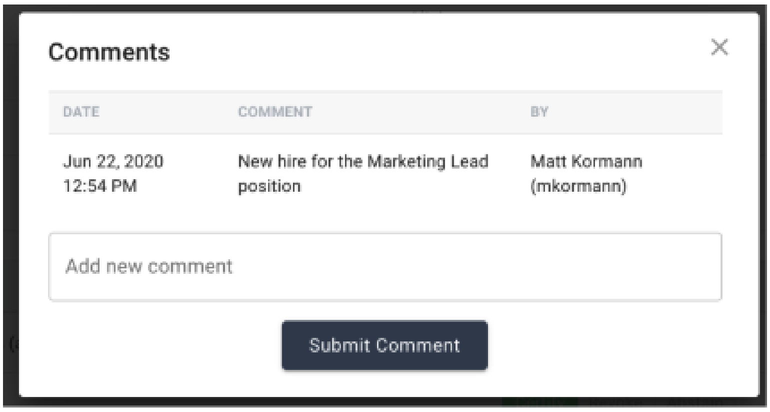
requestable: true	Certify / Revoke / Abstain	□
approvers: manager	Certify / Revoke / Abstain	□
displayName: Finance Lead	Certify / Revoke / Abstain	□
description: Grants user access required for Finance Lead	Certify / Revoke / Abstain	□
riskLevel: 1	Certify / Revoke / Abstain	□
entitlementOwner: Clayton Mitchell (cmitchell)	Certify / Revoke / Abstain	□

  - **Metadata Key and Value**. Displays the glossary entry in [Key]: [Value] format for the certifier to act on. Those entries in the glossary that are of type managed object will be converted to a displayable format if possible.
  - **Certification Action Buttons**. These buttons, disabled for administrators, will show the result of the certification action taken on each item if one has been made. If no button is selected and filled, then no decision has been made for that item. The buttons included are listed below:
    - Certify
    - Revoke
    - Abstain
  - **Comment icon**. The comment icon will either be unfilled if no current comments exist, or have mini comment lines inside of the icon to indicate there are existing comments (pictured below). The administrator can click on the comment icon to display the existing comments, and also to add a new comment to that entitlement.

NOTE

NOTE

For more information on Comments, refer to section Comments.

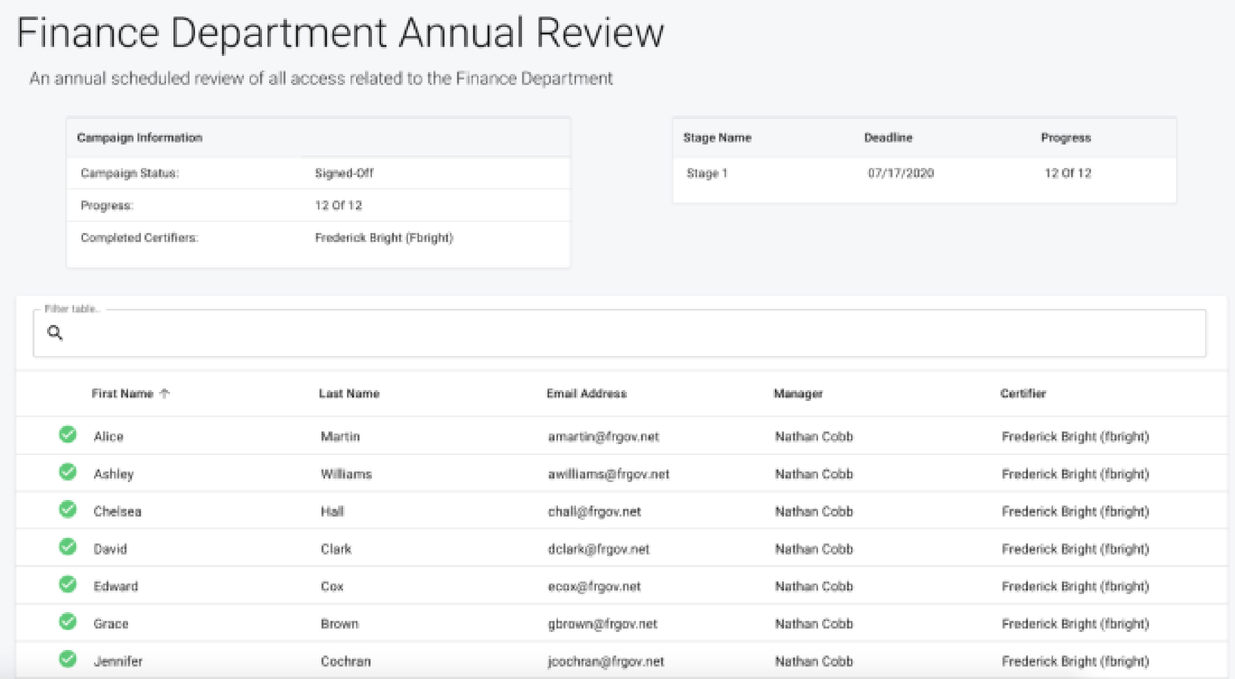


Comments

DATE	COMMENT	BY
Jun 22, 2020 12:54 PM	New hire for the Marketing Lead position	Matt Kormann (mkormann)

Reviewing Closed Certifications

From the closed certifications tab of the User or Object Certifications table, search or sort the table until you find the desired campaign that you wish to review. Clicking on that certification's row will take you to the administrator certification list for that campaign.



Finance Department Annual Review

An annual scheduled review of all access related to the Finance Department

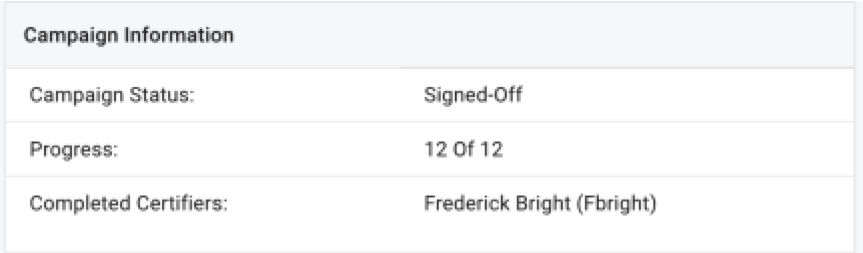
Campaign Information	
Campaign Status:	Signed-Off
Progress:	12 Of 12
Completed Certifiers:	Frederick Bright (Fbright)

Stage Name	Deadline	Progress
Stage 1	07/17/2020	12 Of 12

	First Name ↑	Last Name	Email Address	Manager	Certifier
✓	Alice	Martin	amartin@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	Ashley	Williams	awilliams@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	Chelsea	Hall	chall@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	David	Clark	dclark@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	Edward	Cox	ecox@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	Grace	Brown	gbrown@frgov.net	Nathan Cobb	Frederick Bright (fbright)
✓	Jennifer	Cochran	jcochran@frgov.net	Nathan Cobb	Frederick Bright (fbright)

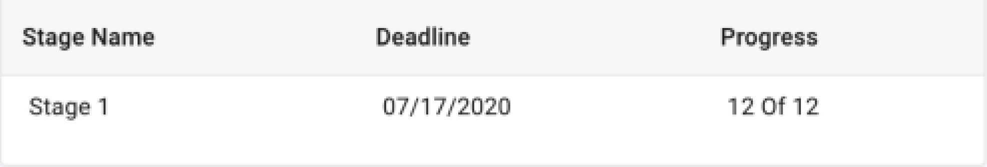
Select a certification from the Closed Certifications list to display additional information on the campaign. The following details will be displayed:

- **Campaign Name**. Name of the campaign
- **Campaign Description**. Description of the campaign
- **Campaign Information**. Displays a summary of the campaign with the following information:



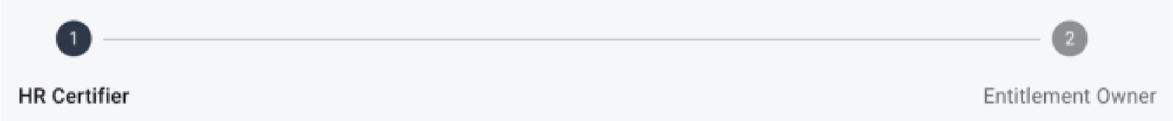
Campaign Information	
Campaign Status:	Signed-Off
Progress:	12 Of 12
Completed Certifiers:	Frederick Bright (Fbright)

  - **Campaign Status**. Identifies the current state of the certification. Values may include In-Progress, Cancelled, Signed-off, or Expired
  - **Progress**. The number of campaign events signed-off against the total number of events in the campaign
  - **Completed Certifiers**. Any certifier that has completed and signed-off on an event that is part of the given campaign.
- **Stage Information**. Displays a breakdown of each stage within the certification campaign with the following information:



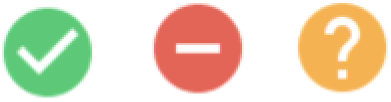
Stage Name	Deadline	Progress
Stage 1	07/17/2020	12 Of 12

  - **Stage Name**. Name assigned to the stage
  - **Deadline**. Date that stage is set to or did expire
  - **Progress**. The number of stage events signed-off against the total number of events in the stage
- **Stage Stepper**. Shows a chronological visual of the certification stages. By selecting a stage node, the page will be updated to reflect data for the selected stage.



- **Target List**. List containing all targets for the certification. Each line contains a summary of the targeted user or object with the following information:
  - **Status icon**. The status of the current target’s event for the selected stage. The following statuses are possible:
    - Pending
    - Certified, signed off
    - Revoked, signed off
    - Abstained, signed off
    - Cancelled
    - No Certifier
    - Expired

Each status is displayed via a circular icon, and may have a different color or fill depending on the individual status. Certified statuses will be colored green, revoked colored red, and abstained colored yellow. The difference between when a normal value and the signed-off version of that value is displayed, the normal version will be displayed when all actions on an event have been completed, but the certifier has not yet signed off on it. After sign-off, the signed off version of the icon will be displayed. This allows the administrator to have a little more insight at this level into the progress of the campaign even before any sign offs occur.

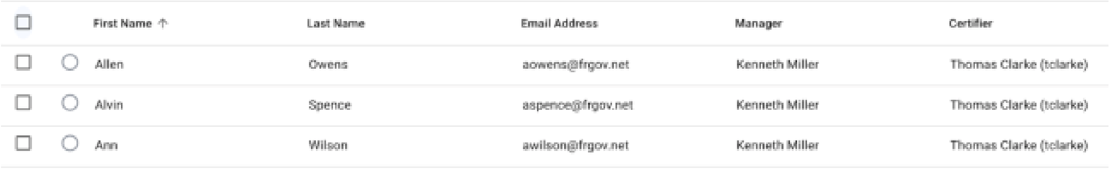


Note that each icon will display a tooltip with the display status text if the administrator hovers over the icon.

- **Displayable Target Info Columns**. The information that displays in the certification list table may vary depending on certification type and the special displayInUserInfo key in the glossary on identity objects.

  For object certifications these displayable columns will always be name and description, so it's highly recommended that these attributes exist on any custom managed object that you wish to certify

  For user certifications, the displayable columns will always include at least the user's givenName, sn, and email address, as well as any user attribute that has a glossary entry of type identity in the glossary and the displayInUserInfo boolean key set to true. Note that this key will not prevent you from displaying relationship attributes in the target list table, however with the exception of manager these attributes are not supported to display properly.
- **Claimed By**. If the certifier for the given stage is a group, this column will display to inform the administrator as to which single user, if any, has claimed the given event.
- **Certifier**. The user or role who is the certifier for the target event.

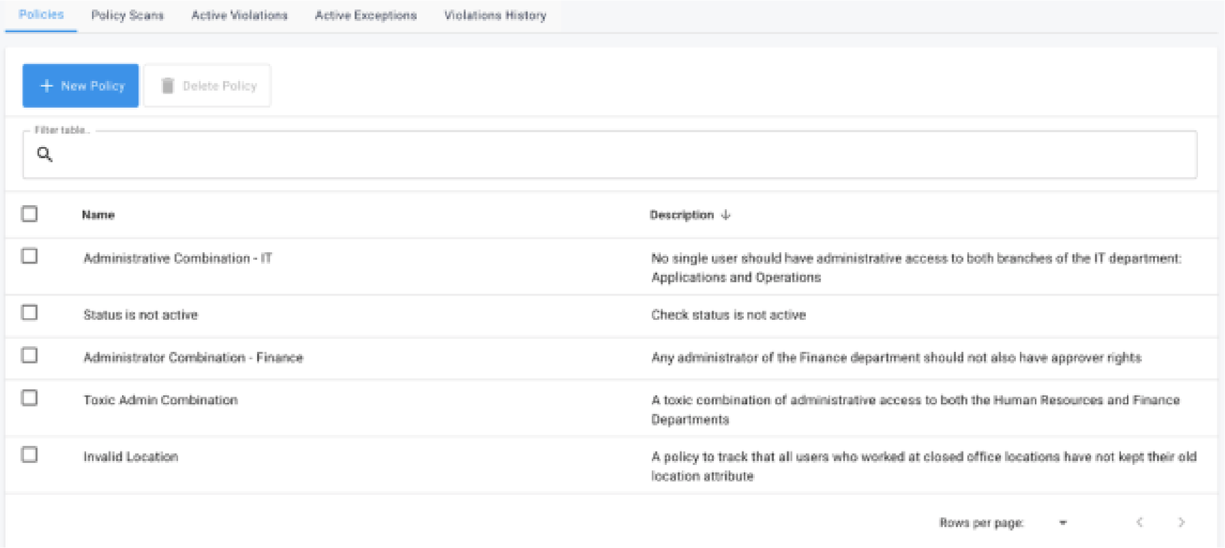


☐		First Name ↑	Last Name	Email Address	Manager	Certifier
☐	○	Allen	Owens	aowens@frgov.net	Kenneth Miller	Thomas Clarke (tclarke)
☐	○	Alvin	Spence	aspence@frgov.net	Kenneth Miller	Thomas Clarke (tclarke)
☐	○	Ann	Wilson	awilson@frgov.net	Kenneth Miller	Thomas Clarke (tclarke)

To see additional information on the individual certification events for a closed campaign, simply click on the target row in the certification list and the event details page will dropdown to view. All information contained within the event details reflects the same format and styling as described in section Reviewing Active Events.

Policies

Policies allow the administrator to define a set of criteria and schedule to determine violations within the identity system, as well as providing the ability to either grant exceptions to those violations or remediate the appropriate access. To manage violations, the administrator should create a policy with a defined expression for a given combination of access that violates a business rule, create a policy scan to generate violations from that policy 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.

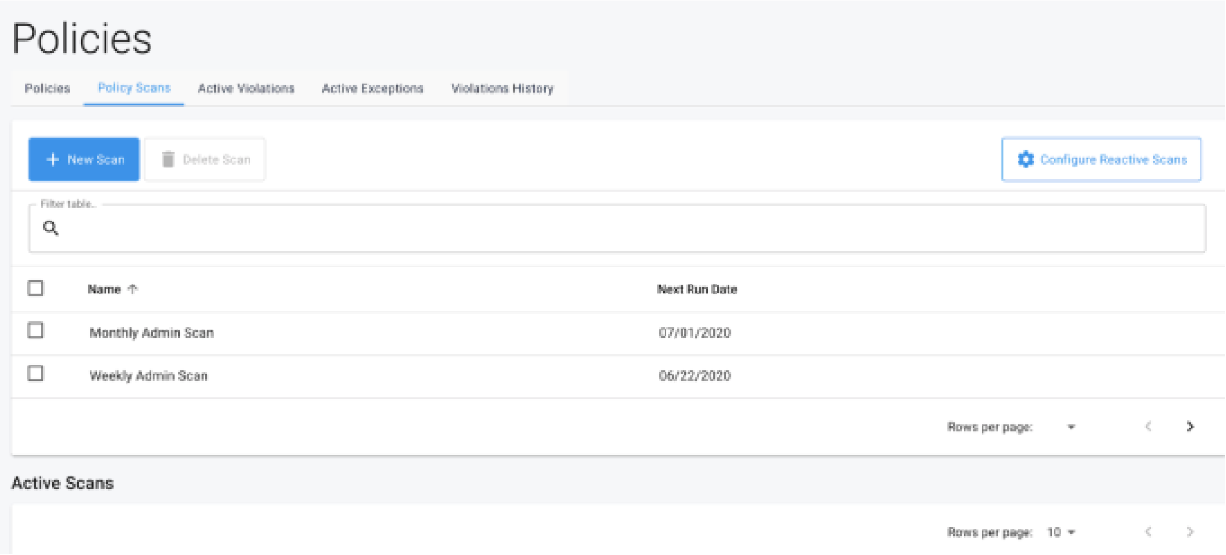


□	Name	Description ↓
□	Administrative Combination - IT	No single user should have administrative access to both branches of the IT department: Applications and Operations
□	Status is not active	Check status is not active
□	Administrator Combination - Finance	Any administrator of the Finance department should not also have approver rights
□	Toxic Admin Combination	A toxic combination of administrative access to both the Human Resources and Finance Departments
□	Invalid Location	A policy to track that all users who worked at closed office locations have not kept their old location attribute

Policy Tables

- Action Buttons
  - New Policy. Create a new policy.
  - Delete Policy. Delete an existing policy object.
- Display Columns
  - Policy Name
    - Description: Name of the policy
    - Searchable: Yes
    - Sortable: Yes
  - Description: Description of the policy
    - Searchable: Yes
    - Sortable: Yes

Policy Scans



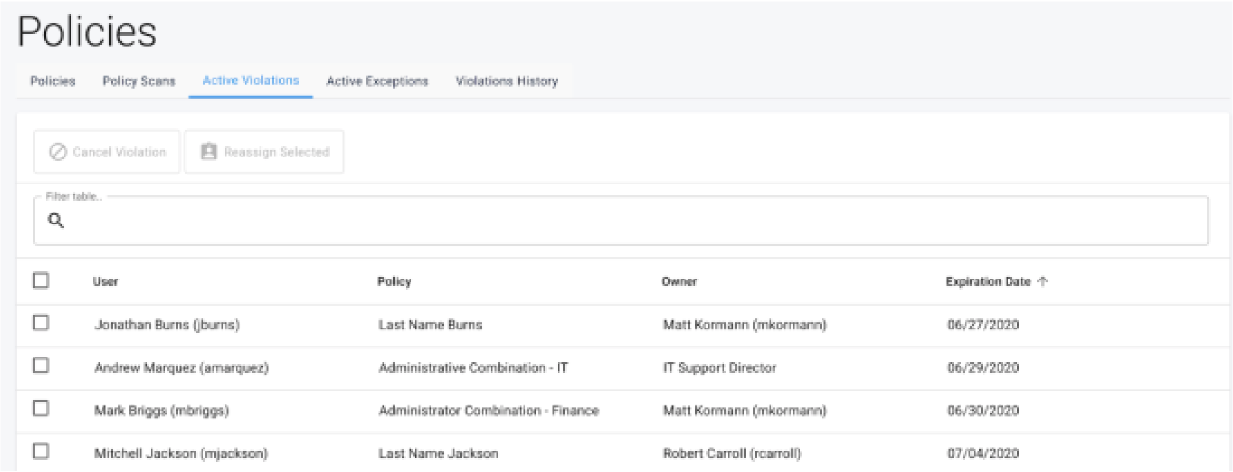
☐	Name ↑	Next Run Date
☐	Monthly Admin Scan	07/01/2020
☐	Weekly Admin Scan	06/22/2020

The policy scan and active scan tables have the following properties:

Scheduled Table:

- Action Buttons:
  - New Scan. Create a new policy scan.
  - Delete Scan. Delete an existing policy scan.
- Display Columns
  - Policy Name
    - Description: Name of the policy
    - Searchable: Yes
    - Sortable: Yes
  - Next Run Data
    - Description: Next date policy scan is scheduled to run
    - Searchable: No
    - Sortable: Yes

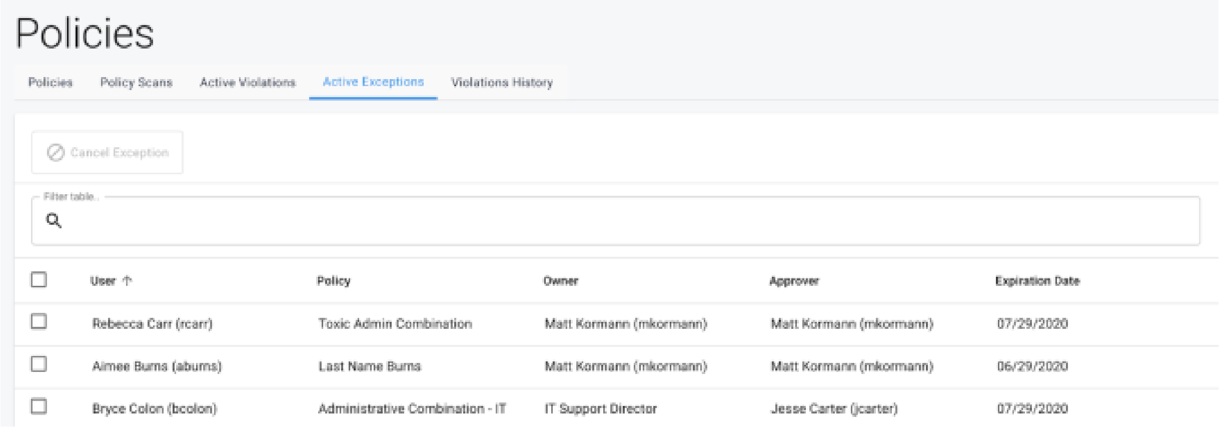
Active Violations



☐	User	Policy	Owner	Expiration Date ↑
☐	Jonathan Burns (jburns)	Last Name Burns	Matt Kormann (mkormann)	06/27/2020
☐	Andrew Marquez (amarquez)	Administrative Combination - IT	IT Support Director	06/29/2020
☐	Mark Briggs (mbriggs)	Administrator Combination - Finance	Matt Kormann (mkormann)	06/30/2020
☐	Mitchell Jackson (mjackson)	Last Name Jackson	Robert Carroll (rcarroll)	07/04/2020

- Action Buttons:
  - Cancel Violation. Cancel the selected violation(s)
  - Reassign Selected. Reassign the selected violation(s) to a different owner
  - User
    - Description: User who violated the policy
    - Searchable: Yes, by username
    - Sortable: no
  - Policy
    - Description: Name of the policy that was violated
    - Searchable: Yes
    - Sortable: Yes
  - Owner
    - Description: User or role who owns the policy violated
    - Searchable: No
    - Sortable: Yes
  - Expiration Date
    - Description: Date the violation task will expire
    - Searchable: No
    - Sortable: Yes

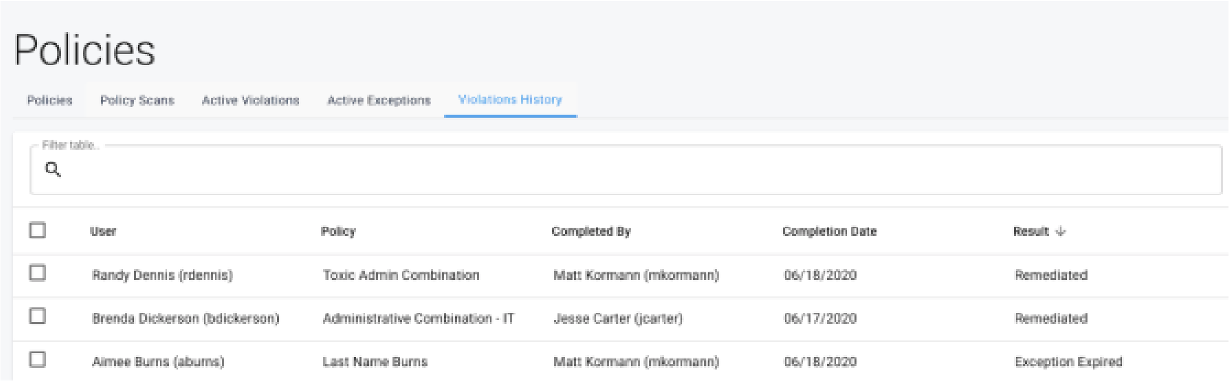
Active Exceptions



□	User ↑	Policy	Owner	Approver	Expiration Date
□	Rebecca Carr (rcarr)	Toxic Admin Combination	Matt Kormann (mkormann)	Matt Kormann (mkormann)	07/29/2020
□	Aimee Burns (aburns)	Last Name Burns	Matt Kormann (mkormann)	Matt Kormann (mkormann)	06/29/2020
□	Bryce Colon (bcolon)	Administrative Combination - IT	IT Support Director	Jesse Carter (jcarter)	07/29/2020

- Action Buttons:
    - Cancel Exception. Cancel the selected exception(s).
- Display Columns
    - User
        - Description: User who violated the policy
        - Searchable: Yes, by username
        - Sortable: no
    - Policy
        - Description: Name of the policy that was violated
        - Searchable: Yes
        - Sortable: Yes
    - Owner
        - Description: User or role who owns the violation exception
        - Searchable: No
        - Sortable: Yes
    - Expiration Date
        - Description: Date the violation exception will expire
        - Searchable: No
        - Sortable: Yes

Violation History

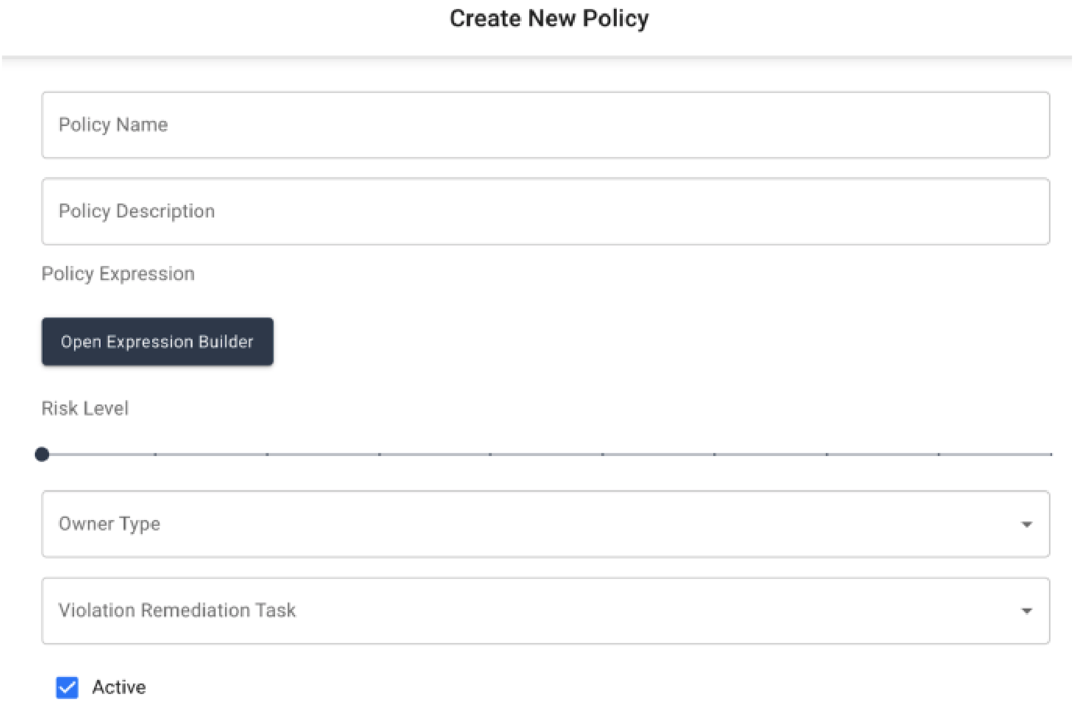


☐	User	Policy	Completed By	Completion Date	Result ↓
☐	Randy Dennis (rdennis)	Toxic Admin Combination	Matt Kormann (mkormann)	06/18/2020	Remediated
☐	Brenda Dickerson (bdickerson)	Administrative Combination - IT	Jesse Carter (jcarter)	06/17/2020	Remediated
☐	Aimee Burns (aburns)	Last Name Burns	Matt Kormann (mkormann)	06/18/2020	Exception Expired

- Action Buttons:
  - None
- Display Columns
  - User
    - Description: User who violated the policy
    - Searchable: Yes, by username
    - Sortable: no
  - Policy
    - Description: Name of the policy that was violated
    - Searchable: Yes
    - Sortable: Yes
  - Completed By
    - Description: User who completed the violation
    - Searchable: No
    - Sortable: Yes
  - Completion Date
    - Description: Date the violation was completed (date remediated, cancelled, or exception expired)
    - Searchable: No
    - Sortable: Yes
  - Result
    - Description: Final result of the violation
    - Searchable: No
    - Sortable: Yes

Creating a New Policy

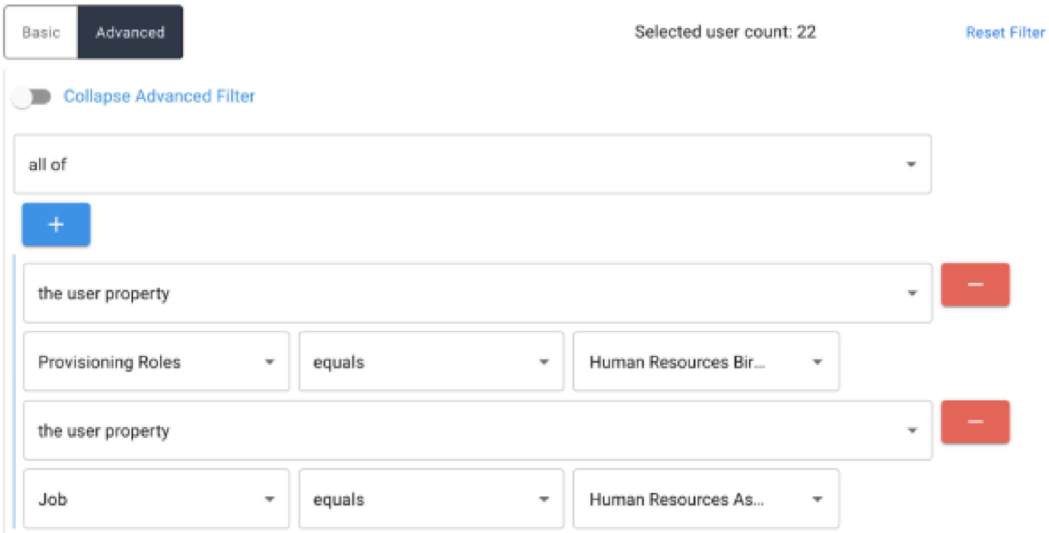
1. Navigate to the Policies page by clicking the Policies link under the Administration section of the side navigation bar.
2. From the Policies tab, select ‘New Policy’.
3. On the Create Policy page, fill in each of the required fields. Additional details on the available fields are given below:



Create New Policy

   - Policy Name: (Required) Reference name of the policy
   - Policy Description: Additional details describing the purpose of the policy. It is recommended to make this field as descriptive as possible to give the policy owner as much information as they need to make a remediation or exception decision.
   - Policy Expression: (Required) Rule for triggering a violation from the policy. If an event causing the rule to evaluate is true, a violation is created. The expression is defined using the Identity Governance expression builder.

4. Upon selecting Open Expression Builder, the advanced expression builder is displayed. The following options for creating a custom expression are available within the policy scan target filter. For a more detailed description of what the individual options determine, refer to section Expression Builder.



Basic | Advanced

Selected user count: 22

Reset Filter

Collapse Advanced Filter

all of

+

the user property −

Provisioning Roles | equals | Human Resources Bir...

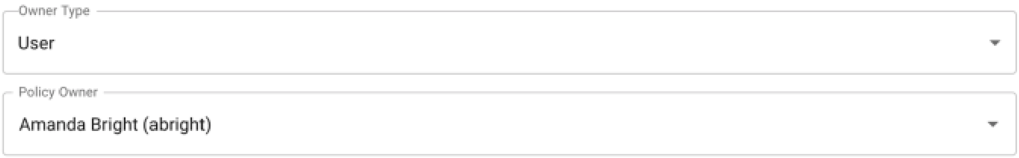
the user property −

Job | equals | Human Resources As...

- The user/object property: Choose from any user attribute
- The user application: (User Certifications Only) Allows choice of any connected application to be selected from the dropdown menu
- All of: Match all of the nested rows
- Any of: Match at least one of the nested rows
- None of: Negate the expression in the nested row
- All users

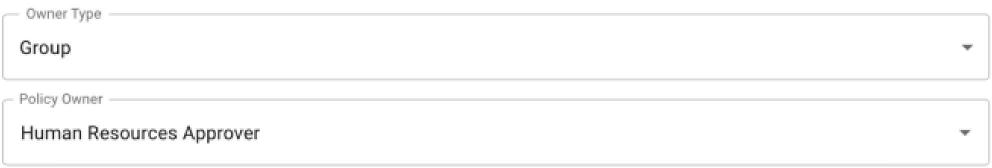
> NOTE
>
> For more information on building expressions, refer to section Expression Builder.

- Risk Level: (Required) Risk level for the policy on a 1 - 10 scale. A risk score of 1 indicates a policy that is tracking a low risk violation or combination of access, while a score of 10 is given for a policy that is tracking an access violation that is of the utmost importance. These scores can be used during a remediation workflow to determine what steps should be taken to revoke the violating access.
- Owner Type: (Required) Type of owner to assign to this policy. The options are between a single user or a group.
- Policy Owner: (Required) Specific owner being assigned to this policy. Choose the single user or role that will be the owner and responsible for decisions on all violations created by this policy.



Owner Type: User

Policy Owner: Amanda Bright (abright)



Owner Type
Group

Policy Owner
Human Resources Approver

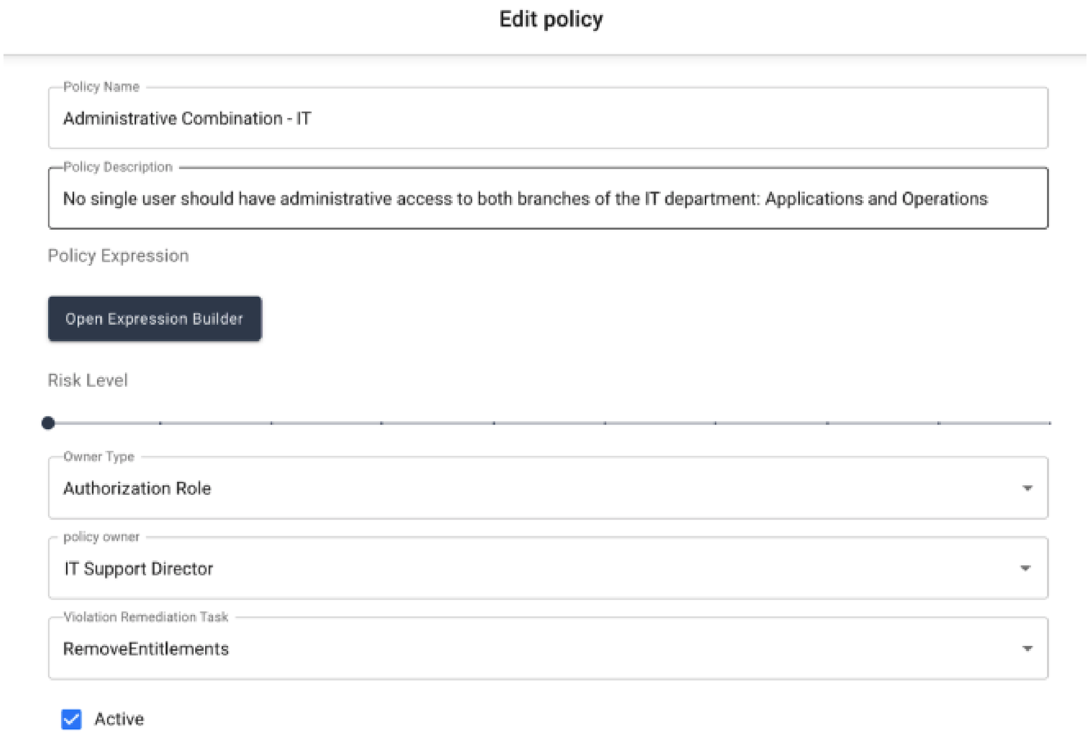
- Violation Remediation Task: An automated remediation task for handling revocations from violation acceptance .

  > NOTE
  >
  > For more information on remediation tasks, refer to section Remediation Tasks

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

Modifying Policies

1. Navigate to the Policies page by clicking the Policies link under the Administration section of the side navigation bar.
2. Ensure the Policies tab is selected.
3. The table will be populated with all existing policy definitions that exist within the system.
4. To modify a policy, click on the row that contains the desired policy definition to open up the edit page. This page will be the same as the one used for creating policies, with the policy data already populated. See section Policy Tables for descriptions of the fields found within this form.



Edit policy

Policy Name
Administrative Combination - IT

Policy Description
No single user should have administrative access to both branches of the IT department: Applications and Operations

Policy Expression

Risk Level

Owner Type
Authorization Role

policy owner
IT Support Director

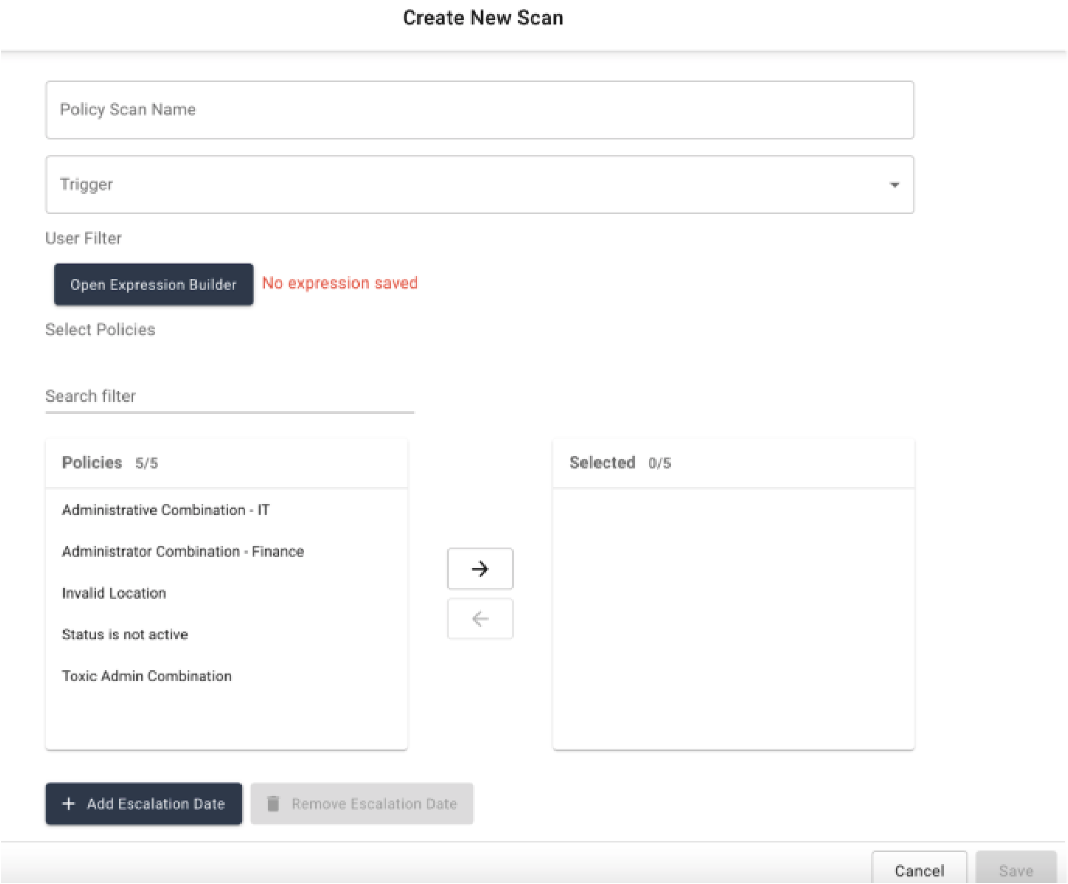
Violation Remediation Task
RemoveEntitlements

☑ Active

5. Once you have finished making your adjustments to the policy, click Save at the bottom of the form to complete the update. Note: For additional information on the fields to update on this form, refer to section Policy Tables.

Creating a New Policy Scan

1. Navigate to the Policies page by clicking the Policies link under the Administration section of the side navigation bar.
2. From the 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.



Create New Scan

No expression saved

Policies 5/5

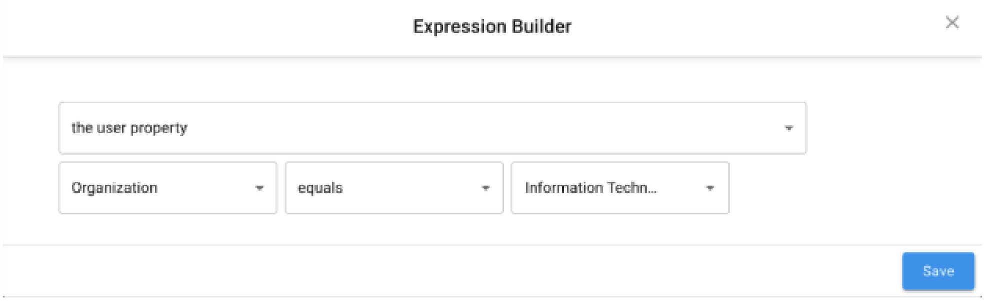
Administrative Combination - IT
Administrator Combination - Finance
Invalid Location
Status is not active
Toxic Admin Combination

Selected 0/5

Additional details on available fields are given below:

- 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 Scheduling Events

    - User Target Filter: The subset of users the created scan will search for violations
        - Upon selecting Open Expression Builder, the advanced expression builder is displayed. The following options for creating a custom expression are available within the policy scan target filter. For a more detailed description of what the individual options determine, refer to section Expression Builder.



Expression Builder

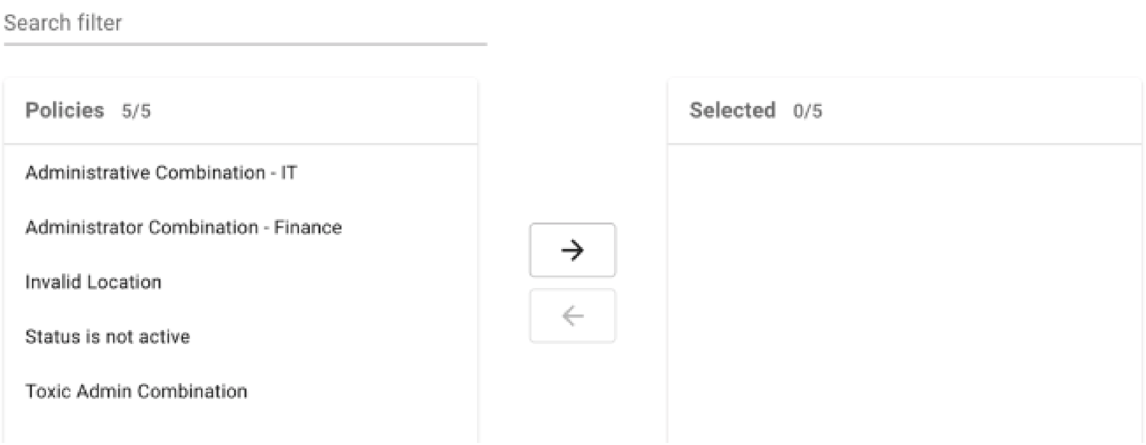
the user property

Organization

equals

Information Techn...

        - The user/object property: Choose from any user attribute
        - The user application: (User Certifications Only) Allows choice of any connected application to be selected from the dropdown menu
        - All of: Match all of the nested rows
        - Any of: Match at least one of the nested rows
        - None of: Negate the expression in the nested row
        - All users



Search filter

Policies 5/5

Administrative Combination - IT

Administrator Combination - Finance

Invalid Location

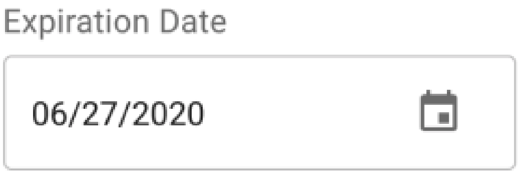
Status is not active

Toxic Admin Combination

Selected 0/5

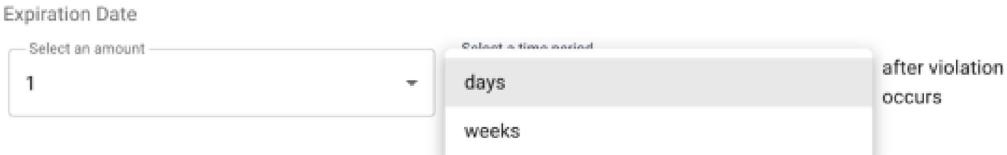
- Select Policies: (Required) Policies that will be triggered by the scan. The field consists of side-by-side lists, with the left side containing available policies and the right side containing policies to be triggered in the scan. Selecting a policy in either list will move the policy to the opposite list.
    - 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. For Ad-hoc policy scans, the expiration date is a static date in the future. For scheduled policy scans, the

expiration date is a period of time after the violation has been found and the task created.



Expiration Date

06/27/2020



Expiration Date

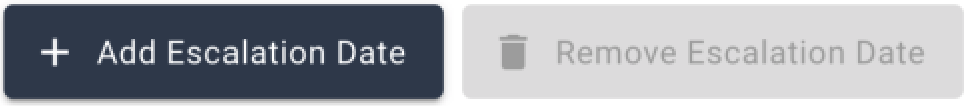
Select an amount: 1

Select a time period: days

weeks

after violation occurs

  - Escalation Schedule: Administrators are now able to define a configured schedule of escalation notifications that are delivered to a specific party at a specific time period before the violation expires.



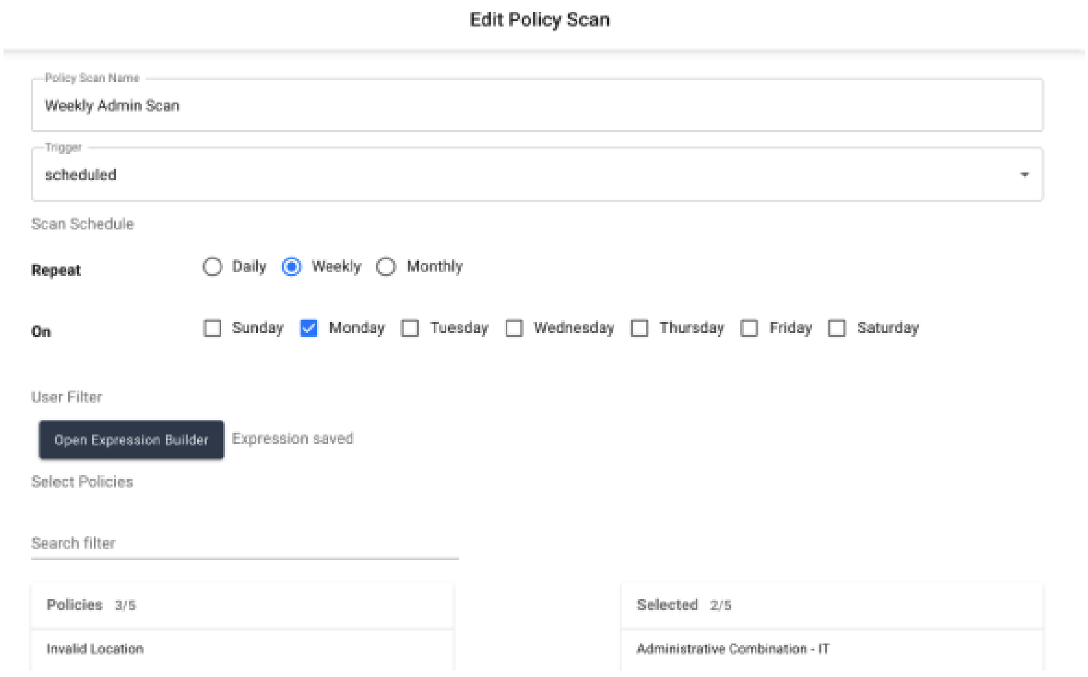
    - Add an escalation date. To add an escalation notification to the schedule, simply click the 'Add Escalation Date' button located on the stage form beneath the deadline field. This will populate a single instance of the escalation form which consists of the following fields:
        - Amount: The numeric value that combines with the chosen time period to determine the time before the certification expires that the notification will be sent
        - Time period: Days or weeks before certification expires.
        - Escalation owner type: Who will be notified of the escalation. Choice of either user, group, or manager. Manager in this case refers to the manager of the owner for the given policy.
        - Choose escalation owner: If owner type is user or group, select the user or role that will receive the notification.

          In order to add an additional escalation date the preceding form must be completed before the add button is enabled again. Escalation dates must be added in order of furthest from the deadline to closest.

- Remove escalation date. To remove the most recent escalation date, click on the 'Remove Escalation Date' found next to the add button.

Modifying Scheduled Policy Scans

1. Navigate to the Policies page by clicking the Policies link under the Administration section of the side navigation bar.
2. Click the Policy Scans tab to navigate to the scans section.
3. The top table will be populated with all existing policy scan definitions that exist within the system.
4. To modify a policy scan, click on the row that contains the desired scan definition to open up the edit page. This page will be the same as the one used for creating policy scans, with the scheduled scan data already populated. See section Creating a New Policy Scan for descriptions of the fields found within this form.



Edit Policy Scan

Policy Scan Name: Weekly Admin Scan

Trigger: scheduled

Scan Schedule

Repeat ○ Daily ● Weekly ○ Monthly

On □ Sunday ☑ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

User Filter

Open Expression Builder Expression saved

Select Policies

Search filter

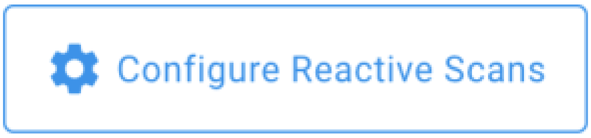
Policies 3/5	Selected 2/5
Invalid Location	Administrative Combination - IT

Reviewing Active Policy Scans

1. Navigate to the Policies page by clicking the Policies link under the Administration section of the side navigation bar.
2. Click the Policy Scans tab to navigate to the scans section.
3. If any scans are currently in progress, the bottom table will be populated with all existing active scans that exist.
4. The information within this table will constantly update as a scan is running, and once a scan is completed it will be removed from the table completely.

Configure Reactive Policy Scans

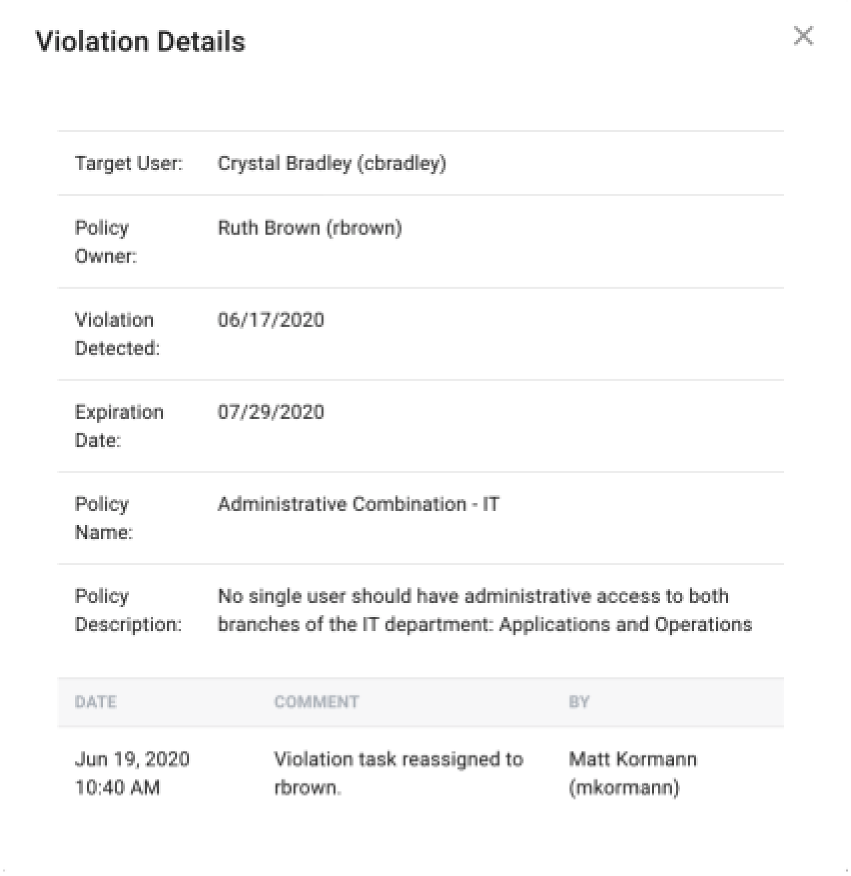
1. Navigate to the Policies page by clicking the Policies link under the Administration section of the side navigation bar.
2. Click the Policy Scans tab to navigate to the scans section.
3. On the top right of the policy scans table, there will be an action button for 'Configure Reactive Scans.' Clicking this button will display the reactive scans page.



4. The following fields are configurable for reactive scans.
   - Expiration Date: (Required) Specifies how long a violation should remain active. After the specified duration, a violation expires and becomes unavailable for modification. The expiration date is calculated from the day that the violation is found.
   - Escalation Schedule: Specifies where escalation notifications should be sent, at what day, and how many should go out overall. For more information on escalation schedules in policy scans, see section Creating a New Policy Scan.

Viewing Active Violations

1. Navigate to the Policies page by clicking the Policies link under the Administration section of the side navigation bar.
2. Click the Active Violations tab to navigate to the active violations section. The table will be populated with any active violations that are currently assigned out to users for completion. Note that this does not include violations that are currently being granted an exception, only those that are not yet acted on.



Violation Details

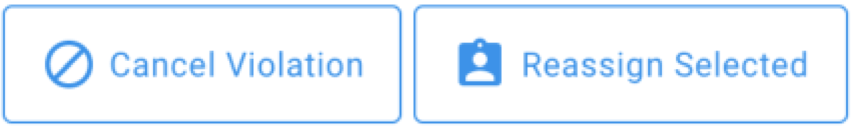
Target User:	Crystal Bradley (cbradley)
Policy Owner:	Ruth Brown (rbrown)
Violation Detected:	06/17/2020
Expiration Date:	07/29/2020
Policy Name:	Administrative Combination - IT
Policy Description:	No single user should have administrative access to both branches of the IT department: Applications and Operations

DATE	COMMENT	BY
Jun 19, 2020 10:40 AM	Violation task reassigned to rbrown.	Matt Kormann (mkormann)

3. To view a given violation, click on its row within the table to expand the violation page. This page will show the following information:
   - Target User: The user who violated the policy
   - Policy Owner: The user or role who is assigned the violation task
   - Violation Detected: Date that the violation was found
   - Expiration Date: Date that the task will expire
   - Policy Name: Policy that was violated
   - Policy Description: Description of the policy that was violated
   - Comments: Any comments on the violation will appear at the bottom of the violation view screen
     - Date: Date comment was made
     - Comment: The message that was added
     - By: The person who made the comment

Cancelling Active Violations

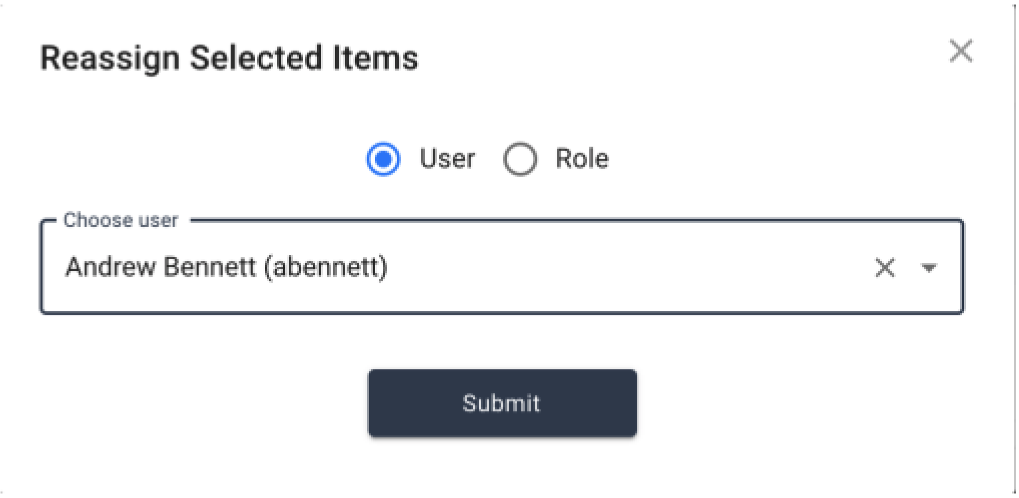
1. Navigate to the Policies page by clicking the Policies link under the Administration section of the side navigation bar.
2. Click the Active Violations tab to navigate to the active violations section.

> 3. Select the checkboxes next to the row or rows of the violations that you wish to cancel.
> 4. Click Cancel Violations.
> 5. The administrator will see a confirmation dialog to confirm that they wish to cancel the selected violations. Clicking ok will complete the cancellation action.
>
> 
>

Reassigning Active Violations

Administrators have the ability to reassign active violation tasks from the active violations tab. The button to reassign a violation is found in the action buttons section of the violation table.

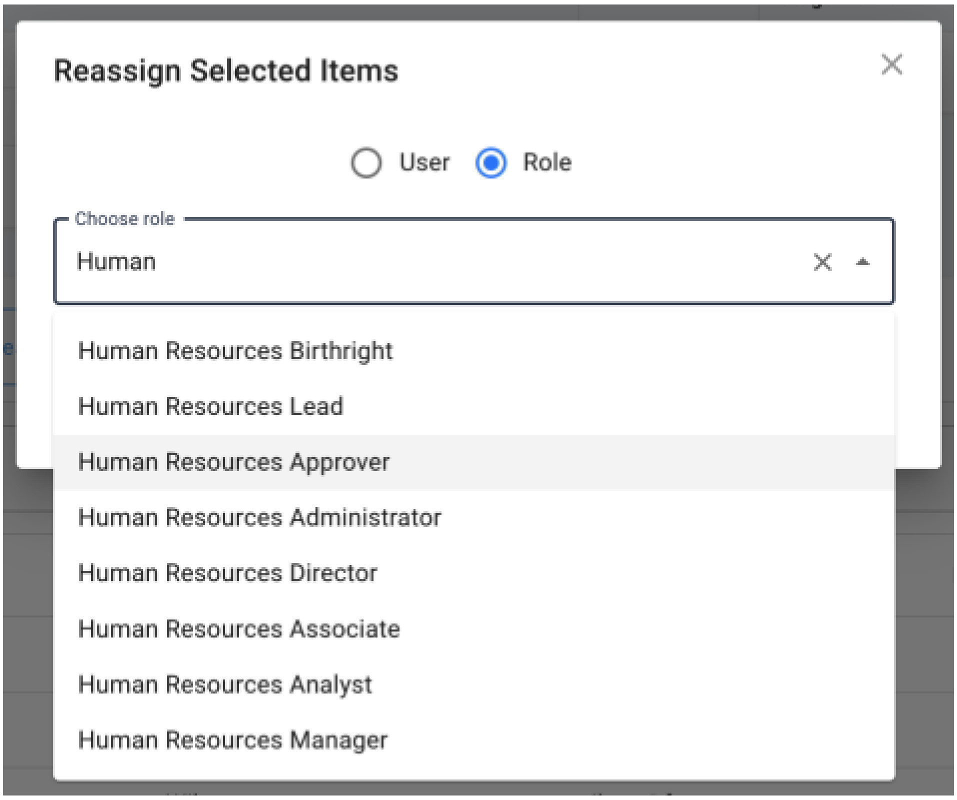
Once the administrator has selected one or more violation rows to reassign, a small dialog box will appear with a few options for selecting the new owner. The administrator can choose to reassign to an individual user or a role (group.) When searching for a user, the administrator can use any of the properties made available and searchable via the User Name Display Format setting, while roles are searchable by name.



Reassign Selected Items

● User ○ Role

Choose user: Andrew Bennett (abennett)



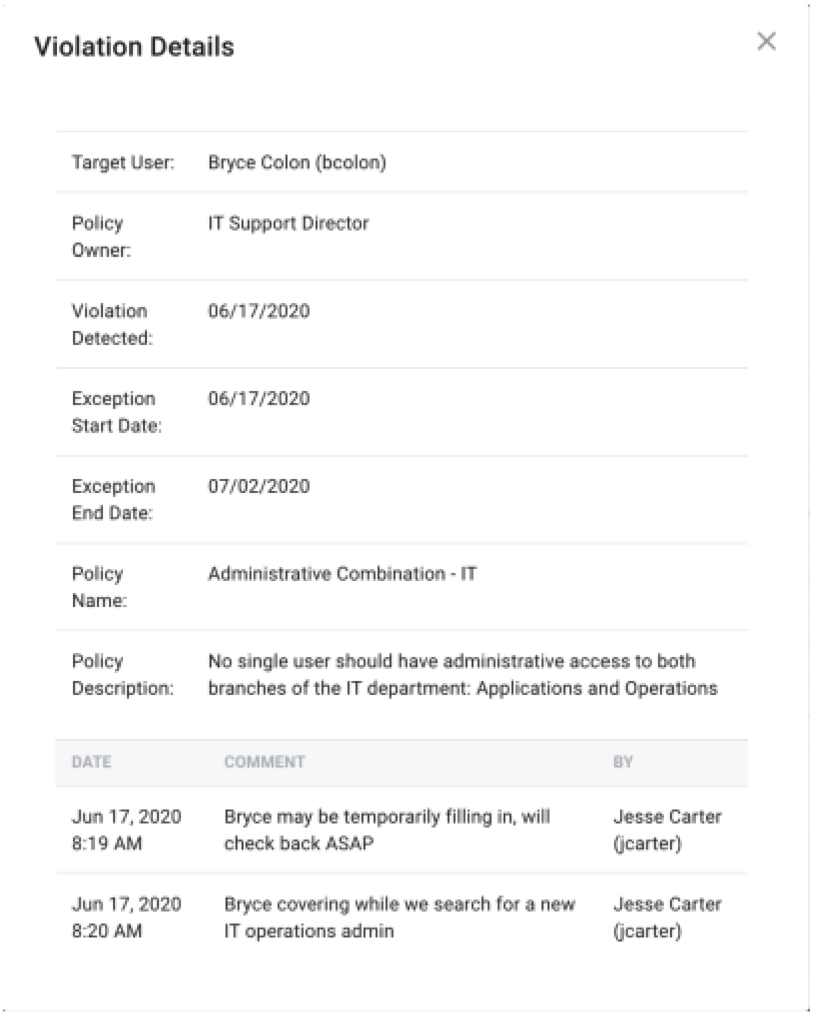
Reassign Selected Items

○ User ● Role

Choose role: Human

Viewing Active Exceptions

1. To navigate to the Policies page, click **Administration > Policies**.
2. Click the **Active Exceptions** tab to navigate to the active exceptions section. The table will be populated with any active exceptions that have currently been granted by the owner of the policy violated. A violation exception is considered `active` if it has been granted by the owner and has not yet reached its exception expiration date.



Violation Details

Target User:	Bryce Colon (bcolon)
Policy Owner:	IT Support Director
Violation Detected:	06/17/2020
Exception Start Date:	06/17/2020
Exception End Date:	07/02/2020
Policy Name:	Administrative Combination - IT
Policy Description:	No single user should have administrative access to both branches of the IT department: Applications and Operations

DATE	COMMENT	BY
Jun 17, 2020 8:19 AM	Bryce may be temporarily filling in, will check back ASAP	Jesse Carter (jcarter)
Jun 17, 2020 8:20 AM	Bryce covering while we search for a new IT operations admin	Jesse Carter (jcarter)

3. To view a given exception, click on its row within the table to expand the exception page. This page will show the following information:
   - Target User: The user who violated the policy
   - Policy Owner: The user or role who is assigned the violation task
   - Violation Detected: Date that the violation was found
   - Exception Start Date: Date that the exception was granted
   - Exception End Date: Date that the exception will expire
   - Policy Name: Policy that was violated
   - Policy Description: Description of the policy that was violated
   - Comments: Any comments on the violation will appear at the bottom of the violation view screen
     - Date: Date comment was made
     - Comment: The message that was added
     - By: The person who made the comment

Cancelling Active Exceptions

1. Navigate to the Policies page by clicking the Policies link under the Administration section of the side navigation bar.
2. Click the Active Exceptions tab to navigate to the active exceptions section.
3. Select the checkboxes next to the row(s) of exceptions that you wish to cancel.
4. Click Cancel Exception.
5. The administrator will see a confirmation dialog to confirm that they wish to cancel the selected exceptions. Clicking ok will complete the cancellation action.

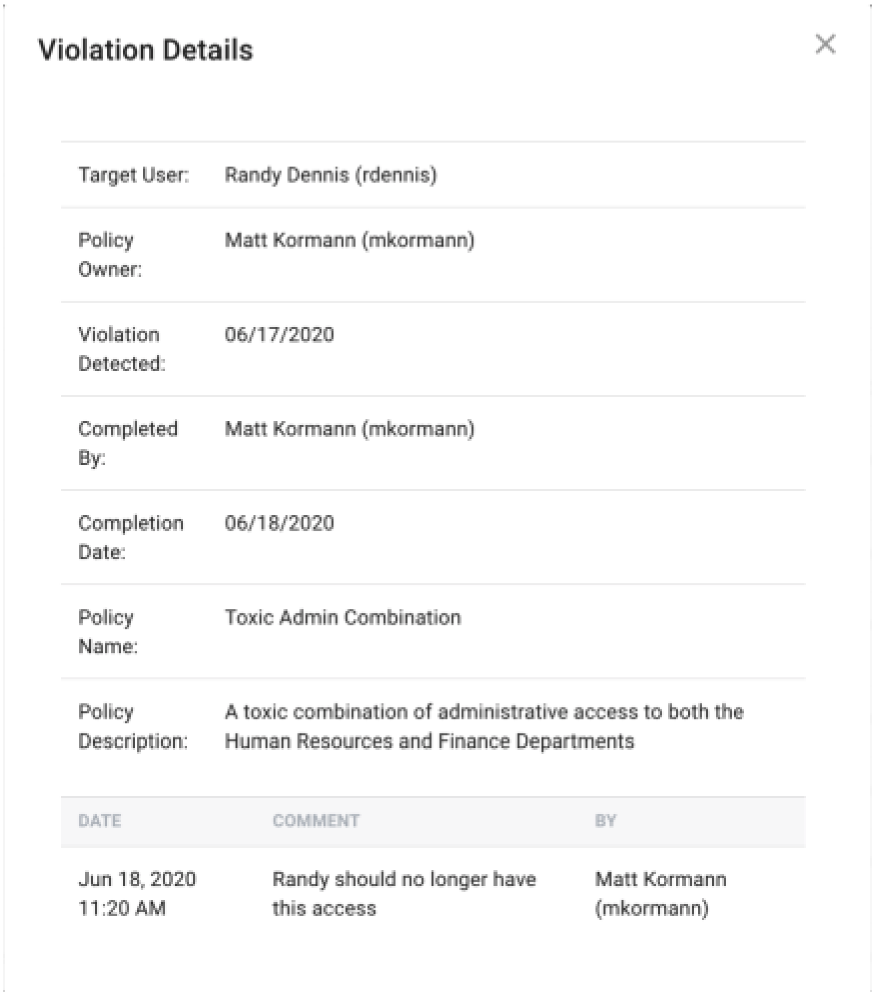
Reviewing Violation History

1. Navigate to the Policies page by clicking the Policies link under the Administration section of the side navigation bar.
2. Click the Violations History tab to navigate to the history section. The table will be populated with any past violations that have been completed. A violation is considered complete if it has any of the following statuses:
    - Remediated
    - Exception Expired
    - Cancelled

To view a completed violation, click on its row within the table to expand the violation page. This page will show the following information:

- Target User: The user who violated the policy
- Policy Owner: The user or role who is assigned the violation task
- Violation Detected: Date that the violation was found
- Exception Start Date: (if exception granted) Date that the exception was granted
- Exception End Date: (if exception granted) Date that the exception expired
- Completed By: User that completed the task
- Completion Date: Date task was completed
- Policy Name: Policy that was violated
- Policy Description: Description of the policy that was violated
- Comments: Any comments on the violation will appear at the bottom of the violation view screen
    - Date: Date comment was made
    - Comment: The message that was added

- By: The person who made the comment



Violation Details

Target User:	Randy Dennis (rdennis)
Policy Owner:	Matt Kormann (mkormann)
Violation Detected:	06/17/2020
Completed By:	Matt Kormann (mkormann)
Completion Date:	06/18/2020
Policy Name:	Toxic Admin Combination
Policy Description:	A toxic combination of administrative access to both the Human Resources and Finance Departments

DATE	COMMENT	BY
Jun 18, 2020 11:20 AM	Randy should no longer have this access	Matt Kormann (mkormann)

User Summary

The Access Review User Summary page allows governance administrators to access and view any given user's entitlement certification history in one single screen. Administrators can see the user's entire certifiable profile, the date and result of each certification of each entitlement, who made the certification decision, and view previous certifications for each entitlement as well. The user summary also allows the administrator to access any tasks that are currently assigned to that user, organized by task type (user certification, object certification, or violation). These task tables can be leveraged to easily reassign any or all tasks that belong to a given user in the event that they are no longer able to complete them as assigned.

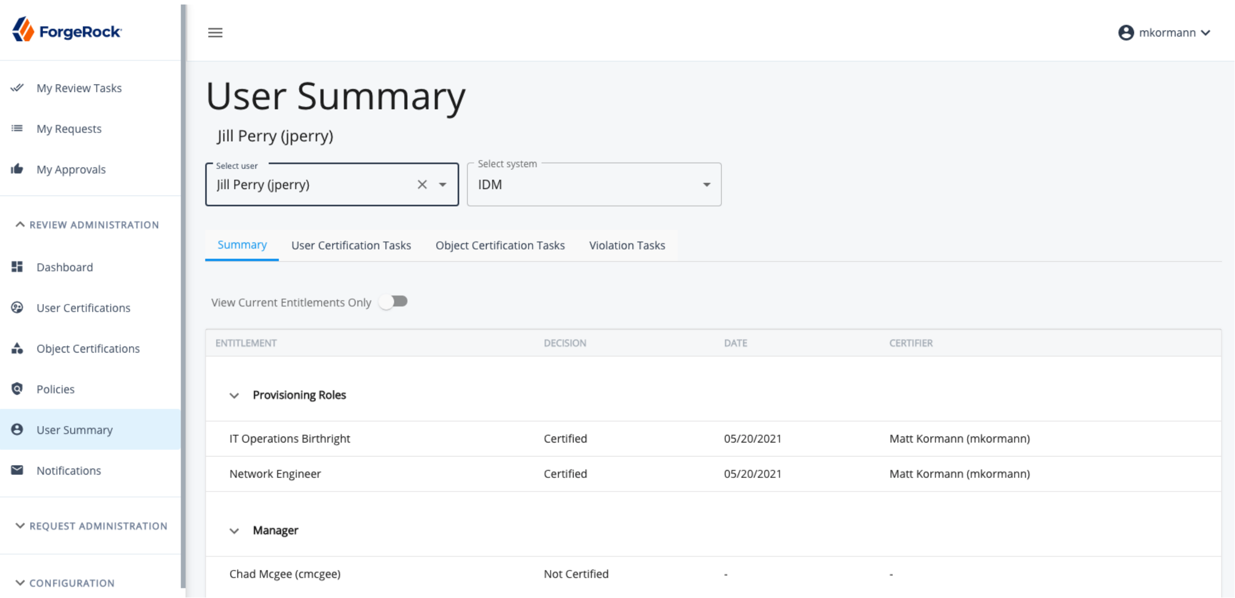
IMPORTANT

IMPORTANT

If you are using IDM 7.2 with Identity Governance, you must enable the `linkedView` endpoint to ensure the IGA User Summary UI works properly. In prior versions of IDM, the `linkedView` endpoint is enabled by default.

To enable the `linkedView` endpoint, copy the following contents into a **newly created** file at `openidm/conf/endpoint-linkedView.json`:

```
{
"context" : "endpoint/linkedView/*",
"type" : "text/javascript",
"source" : "require('linkedView').fetch(request.resourcePath);"
}
```



User Summary

Jill Perry (jperry)

Select user: Jill Perry (jperry)

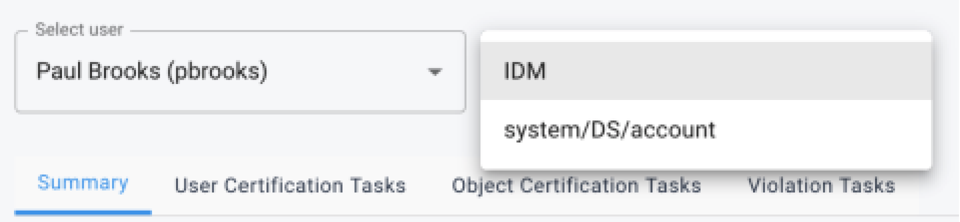
Select system: IDM

ENTITLEMENT	DECISION	DATE	CERTIFIER
Provisioning Roles			
IT Operations Birthright	Certified	05/20/2021	Matt Kormann (mkormann)
Network Engineer	Certified	05/20/2021	Matt Kormann (mkormann)
Manager			
Chad Mcgee (cmcgee)	Not Certified	-	-

User Selection

When first navigating to the User Summary section, administrators will notice a blank auto select input field labelled ‘Select User.’ This field can be used to search for any user within the IDM system using the fields found in the display name format set in the system settings. Once a user is selected, the information for the given tab selected will populate below.

Summary



Select user: Paul Brooks (pbrooks)

Select System

When the summary tab is selected, administrators will notice a second select input appears directly next to the user select input box at the top of the page, labelled ‘Select System.’ The “system” in this context refers to either the ForgeRock IDM environment or any of the linked systems that the given user has a connection to via a mapping in IDM. As ForgeRock Access Review allows attributes in both the IDM schema as well as connected systems to be certifiable, this selection will allow administrators to view certification history for the entitlements derived from any of those given sources. The default view and selection will always be ‘IDM,’ and will show the certifiable entitlements that exist on the user profile.

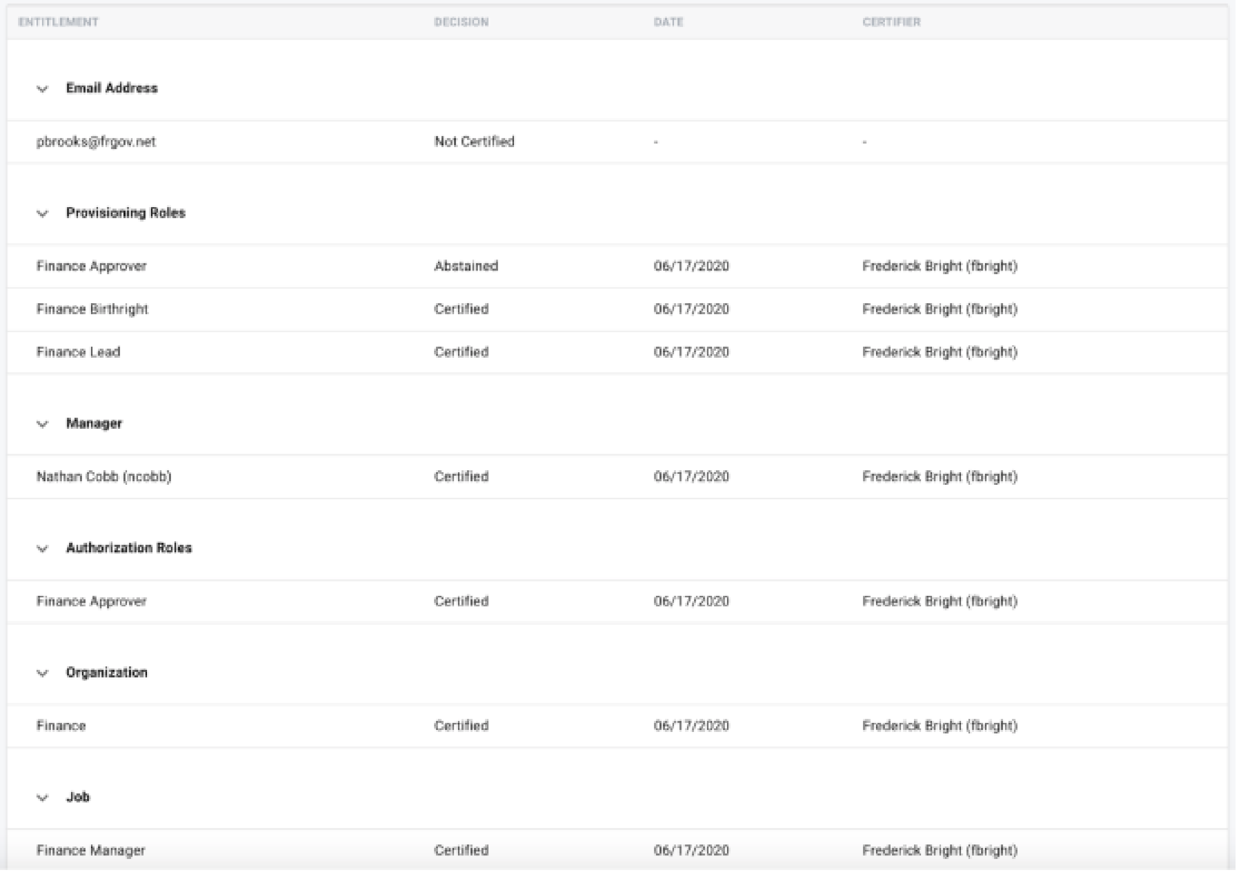
View Current Entitlements Only

Viewing Current Entitlements Only

When viewing the Summary tab, administrators have the option to toggle on or off a view of the user’s currently assigned entitlements only. If toggled on, the only items displayed in the certification history summary table will be those that exist on the current user object. This view is useful when the administrator wants to view the current certification state of the user, to gain insight into whether or not there are entitlements on the user that have not yet been certified and possibly rectify that situation. If toggled off, the administrator will see not only the user’s current entitlements, but also any other entitlement that has ever been certified for that user. This allows administrators to get an entire lifetime view of a single user, even as their access has changed, been revoked, or otherwise altered.

Entitlements Table

The entitlements table is where the individual user entitlements are displayed, displaying data in four separate columns and separated into groups by attribute name. The entry shown for any given entitlement is the most recently completed and signed-off certification of that item, or in the event that a certification is in progress for that given entry, it will show that the entitlement is currently in-progress. The four columns displayed are:



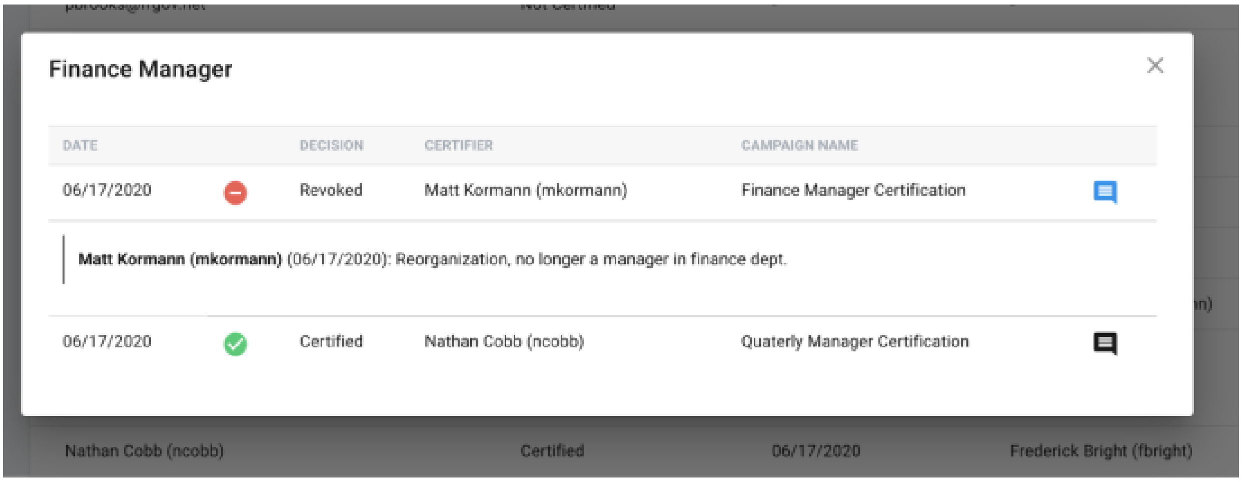
ENTITLEMENT	DECISION	DATE	CERTIFIER
Email Address			
pbrooks@frgov.net	Not Certified	-	-
Provisioning Roles			
Finance Approver	Abstained	06/17/2020	Frederick Bright (fbright)
Finance Birthright	Certified	06/17/2020	Frederick Bright (fbright)
Finance Lead	Certified	06/17/2020	Frederick Bright (fbright)
Manager			
Nathan Cobb (ncobb)	Certified	06/17/2020	Frederick Bright (fbright)
Authorization Roles			
Finance Approver	Certified	06/17/2020	Frederick Bright (fbright)
Organization			
Finance	Certified	06/17/2020	Frederick Bright (fbright)
Job			
Finance Manager	Certified	06/17/2020	Frederick Bright (fbright)

- Entitlement - Name of the given entitlement
- Decision - Most recent decision made on that entitlement. Possible values are listed below:
    - Certified
    - Revoked
    - Abstained
    - Not Certified
    - In-Progress
- Date - Most recent date of certification
- Certifier - Person who made the most recent certification decision

Each grouping of entitlements by attribute name can be collapsed or expanded by clicking on the arrow icon located to the left of the attribute name itself.

Single Entitlement History View

For any entitlement that is not listed as 'Not Certified,' the administrator can click on that entitlement row and expand the historical certification view for that item. The page that appears will show every time that the given entitlement has been certified for the target user in a table, organized by most recent data first, with the following columns:



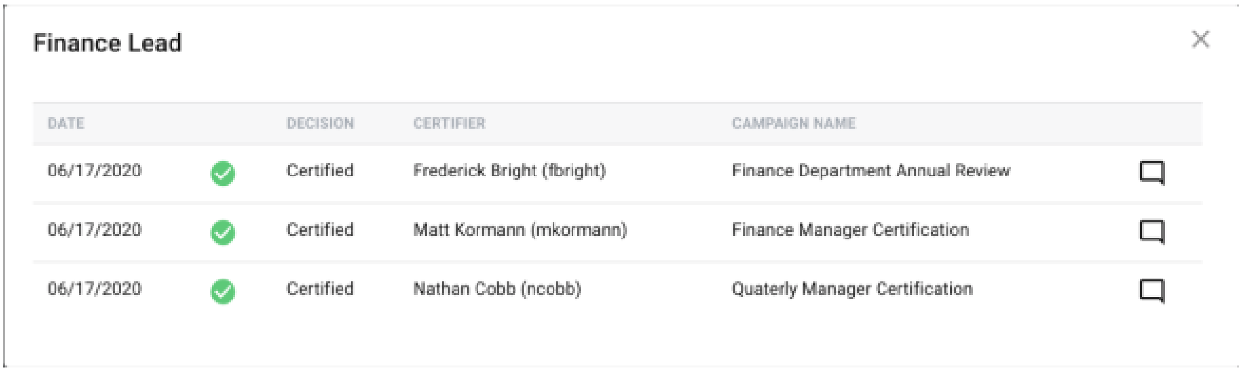
Finance Manager

DATE		DECISION	CERTIFIER	CAMPAIGN NAME
06/17/2020	⊖	Revoked	Matt Kormann (mkormann)	Finance Manager Certification
06/17/2020	✓	Certified	Nathan Cobb (ncobb)	Quaterly Manager Certification

Matt Kormann (mkormann) (06/17/2020): Reorganization, no longer a manager in finance dept.

Nathan Cobb (ncobb) Certified 06/17/2020 Frederick Bright (fbright)

- Date - Date the certification was signed off
- Decision - Decision made for that certification
- Certifier - User who completed and signed-off the listed event
- Campaign Name - The campaign which the listed event was a part of
- Comments - If comments were made on the specific object during the certification, the comment icon will be clickable, and will display the comments made in chronological order.

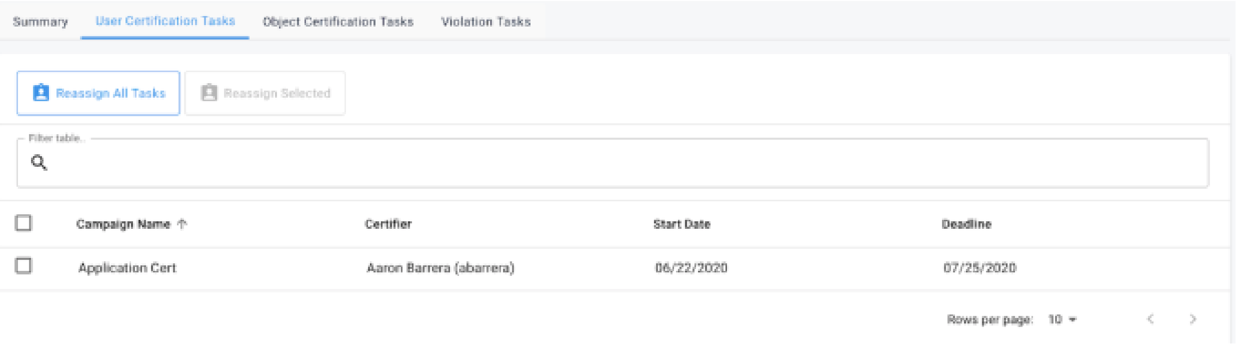


Finance Lead

DATE		DECISION	CERTIFIER	CAMPAIGN NAME
06/17/2020	✓	Certified	Frederick Bright (fbright)	Finance Department Annual Review
06/17/2020	✓	Certified	Matt Kormann (mkormann)	Finance Manager Certification
06/17/2020	✓	Certified	Nathan Cobb (ncobb)	Quaterly Manager Certification

User Certification Tasks

The User Certification Tasks tab will display any certification campaign that currently has the selected user as a certifier for any of its events. This table will not display any certification tasks that the user is eligible to certify due to their membership of a role. This table, when populated, will mirror the table found on the end-user My Tasks dashboard page. For a further description on all of the columns and information found within the table, please refer to the Identity Governance 3.0 User Guide.



☐	Campaign Name ↑	Certifier	Start Date	Deadline
☐	Application Cert	Aaron Barrera (abarrera)	06/22/2020	07/25/2020

Viewing a User Certification

To get more details on any given campaign that's assigned to the current user, the administrator can simply click on the certification row to navigate directly to the certification list. This is the same landing page that an admin ends up on when clicking a campaign from the User Certifications page.

Reassigning User Certification Tasks

Administrators have two options for reassignment of tasks from the User Certification Tasks table: reassign selected campaigns or reassign all tasks.

Reassigning Selected Campaigns

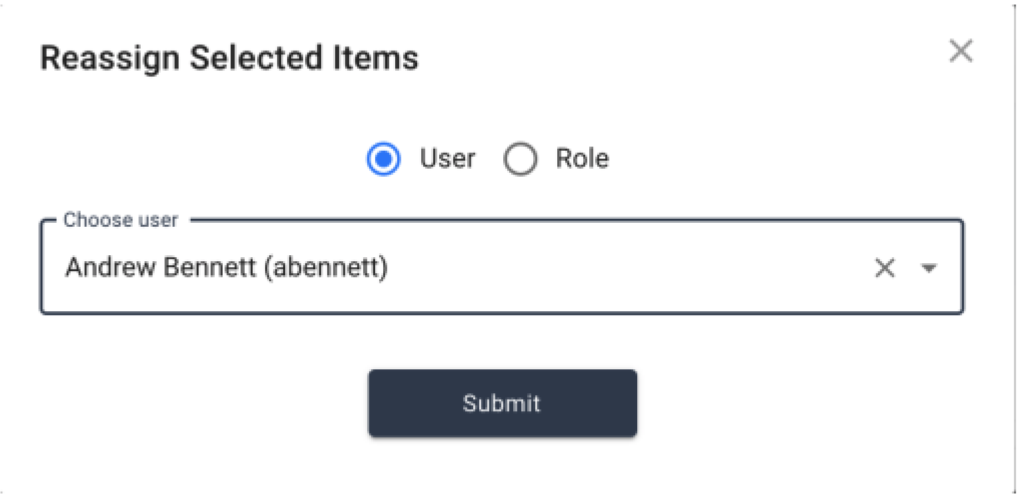
To reassign only those tasks that belong to select campaigns, the administrator can select the checkbox(es) next to any campaign that they wish to reassign. Once selected, clicking on Reassign Selected Tasks will display the reassign page where the admin can choose the user or role to reassign to. After the process has been completed any event that belonged directly to the chosen user will be assigned to the new certifier.

Reassigning All Tasks

Alternatively, admins can choose to reassign all User Certification Tasks that belong to a given user. This functionality can be used when a certifier is on an extended leave or no longer an active user within the system to transfer all of open the reassign page where the admin will choose the new certifier.

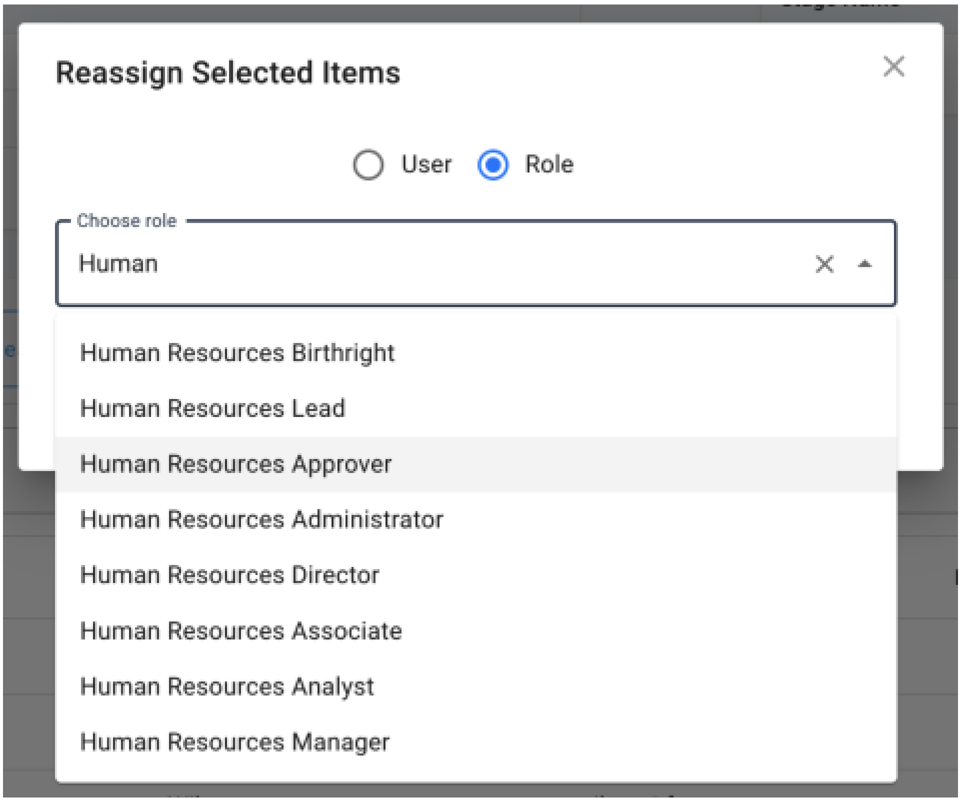
Reassigning Modal

Once the administrator has selected one of the reassign actions, a small dialog box appears with a few options for selecting the new owner. The administrator can choose to reassign to an individual user or a group (role.) When searching for a user, the administrator can use any of the properties made available and searchable using the **User Name Display Format** setting, while roles are searchable by name.


Reassign Selected Items

● User ○ Role

Choose user: Andrew Bennett (abennett)


Reassign Selected Items

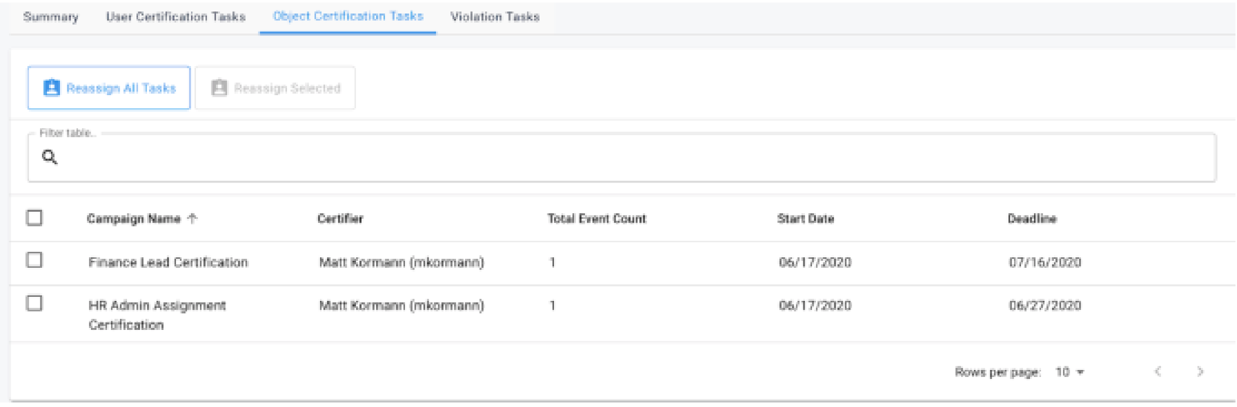
○ User ● Role

Choose role: Human

- Human Resources Birthright
- Human Resources Lead
- Human Resources Approver
- Human Resources Administrator
- Human Resources Director
- Human Resources Associate
- Human Resources Analyst
- Human Resources Manager

Object Certification Tasks

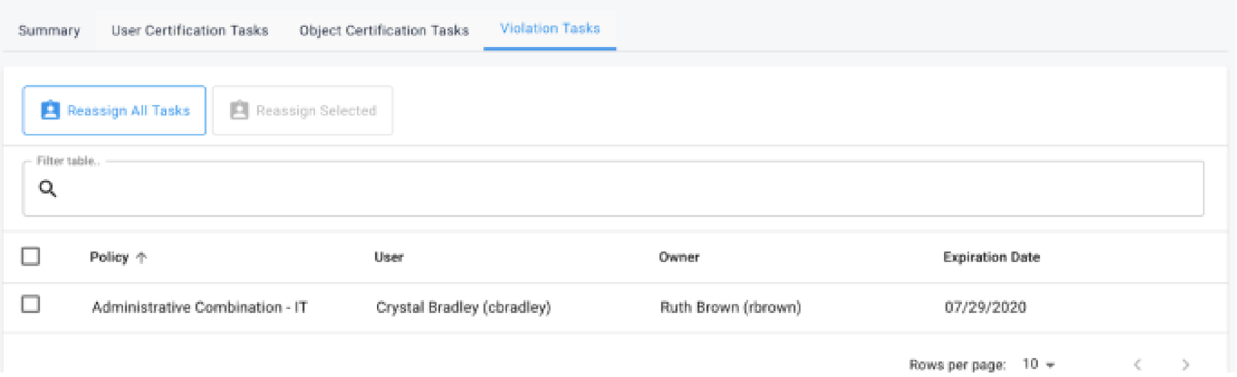
The object certification tasks table will mirror the exact functionality of the user certification tasks table but for object certification tasks. Administrators will be able to view all of the selected users' object tasks, navigate directly to the tasks' campaigns, or reassign any or all tasks from this table. For further information on the table's functionality, refer to Section Selecting a Glossary Object Class.



□	Campaign Name ↑	Certifier	Total Event Count	Start Date	Deadline
□	Finance Lead Certification	Matt Kormann (mkormann)	1	06/17/2020	07/16/2020
□	HR Admin Assignment Certification	Matt Kormann (mkormann)	1	06/17/2020	06/27/2020

Violation Tasks

Like the certification tables described above, the violation tasks table will show all of the violation tasks directly assigned to the selected user. Administrators have the ability to reassign selected violation tasks or all violations tasks to another user or role. In addition, admins can view the current status of the violation by clicking on the violation row in the displayed table.



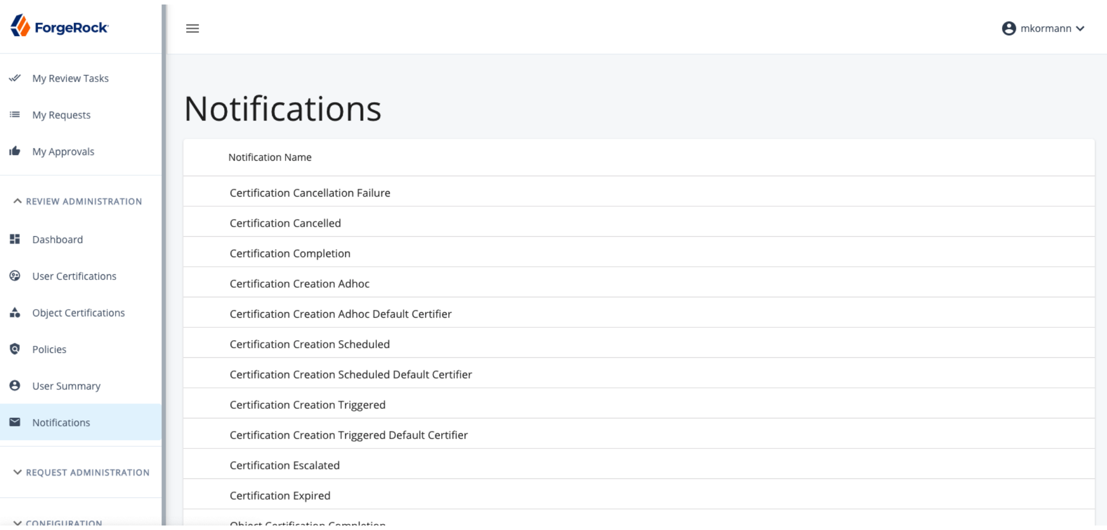
□	Policy ↑	User	Owner	Expiration Date
□	Administrative Combination - IT	Crystal Bradley (cbradley)	Ruth Brown (rbrown)	07/29/2020

Review Notifications

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

Modifying a Notification Template

1. Navigate to the Manage Notifications page, located in the Administrative section of the Navigation Bar.

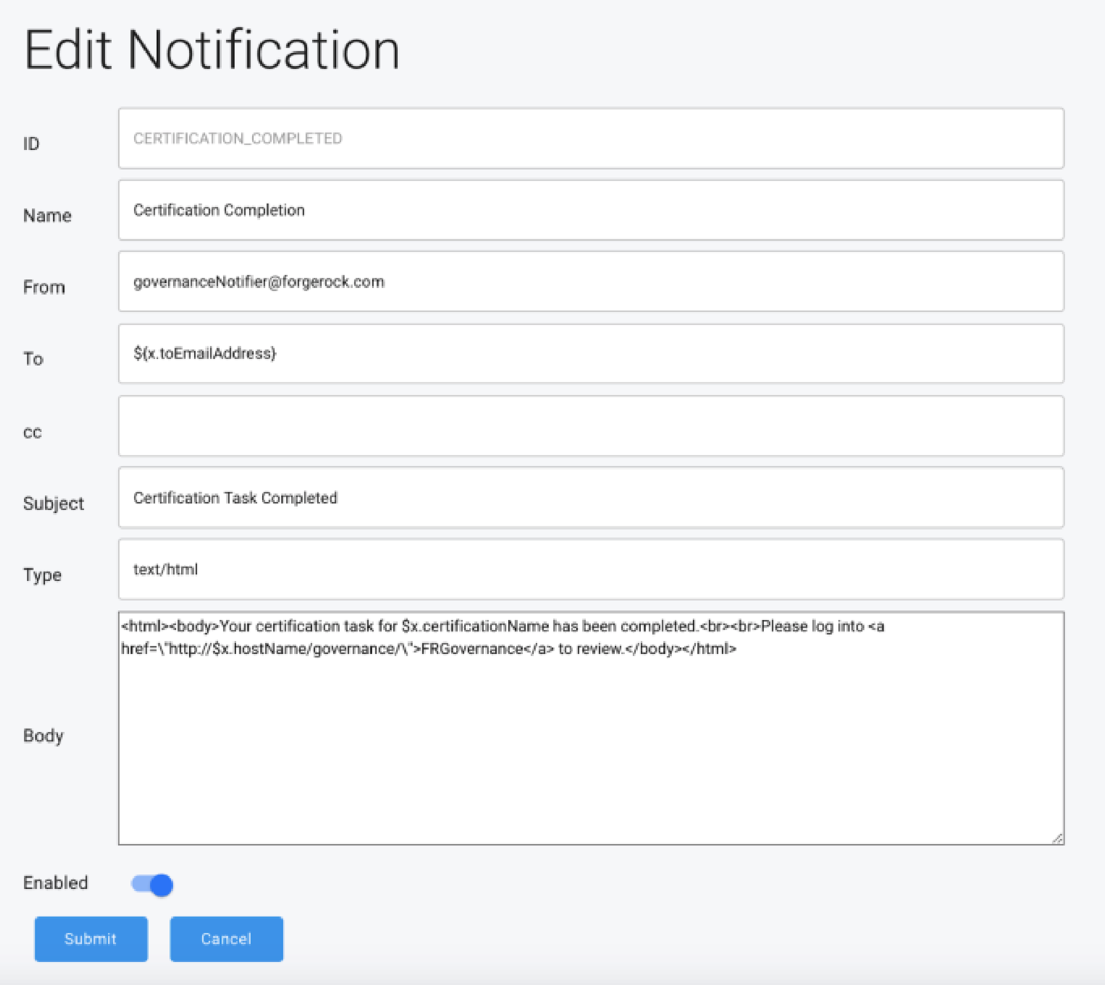


Notifications

Notification Name
Certification Cancellation Failure
Certification Cancelled
Certification Completion
Certification Creation Adhoc
Certification Creation Adhoc Default Certifier
Certification Creation Scheduled
Certification Creation Scheduled Default Certifier
Certification Creation Triggered
Certification Creation Triggered Default Certifier
Certification Escalated
Certification Expired
Object Certification Completion

2. View contents under Notification List.

3. To display additional information about the notification, select a notification from the Notification List.



Edit Notification

ID: CERTIFICATION_COMPLETED

Name: Certification Completion

From: governanceNotifier@forgerock.com

To: ${x.toEmailAddress}

cc:

Subject: Certification Task Completed

Type: text/html

Body:

```
<html><body>Your certification task for $x.certificationName has been completed.<br><br>Please log into <a
href=\"http://$x.hostName/governance/\">FRGovernance</a> to review.</body></html>
```

Enabled: ●

The following details are displayed:

- ID: Represents unique identifier for the notification template. This field is not editable.
- Name: (Required) Name of the 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 Predefined Notification Variables.
- 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’.
- Body: (Required) Contents of the notification. The default format is html, according to the value in the Type field, and may contain variables.
- Enabled: (Required) Identifies whether the notification is enabled or disabled. If unchecked, the notification will not be sent on a triggering event. Note: For more information on supported variables, see section Predefined Notification Variables.

Predefined Notification Templates

The following list describes the predefined notification templates:

Predefined Notification Templates

Name	Description
Certification Cancellation Failure	Sent when a certification cancel fails during the cancellation process.
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.

Name	Description
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.

Name	Description
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.

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

Predefined Notification Variables

The following describes the predefined variables that are used within notifications:

Predefined Notification Variables

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

Access Review Integration with the Glossary

There are a few major areas of functionality within Access Review that are handled by Glossary entries for certain identity objects. The following is the full list of keys, and what they control within the application:

Access Review Keys

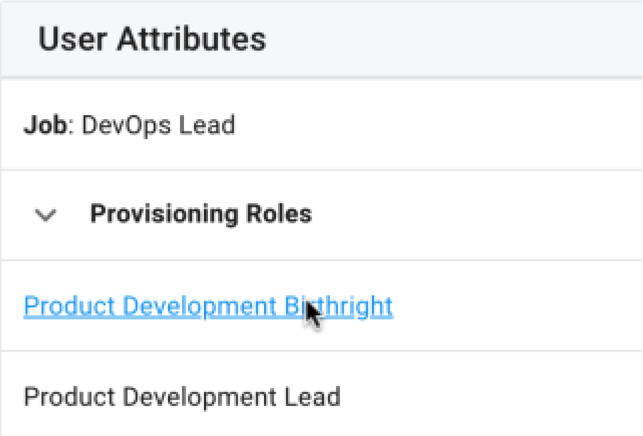
Class	Key	Type	Function
Identity	certifiable	boolean	Allows the attribute to appear within the user certification creation screen as an option for ‘Access to Certify’. If not present or set to false the attribute will not appear.

Class	Key	Type	Function
Identity	displayInUserInfo	boolean	Displays this attribute in the user certification list and event details tables. If not present or set to false the attribute will not appear. Note as of v3.0 this setting does not properly display relationship attributes within the above tables, with the exception of ‘manager’, which displays correctly.
Identity-Value	displayName	String	Displays the value defined here in lieu of the actual value on the user event details page, if the displayed attribute matches this entry.
Object	riskLevel	Integer	When risk level is enabled in system settings, certifications for user, object, and assignment will use this value to match against the provided certification filter for each object.
Object	entitlementOwner	managed object	The entitlement owner key is used to determine the user or role that should be assigned a certification task for the given object. This is used in user certifications when the certifier is set to “Entitlement Owner’, as well as when the glossary key certifier is chosen for object certifications. The value here should reference only a managed/user or a managed/role.
Object	displayName	String	Displays the value defined here in lieu of the actual value on the user event details page, if the object is included within a certification.

Class	Key	Type	Function
System	certifiable	boolean	Allows the system to appear within the user certification creation screen as an option for ‘Access to Certify’. If not present or set to false the system will not appear.
System	riskLevel	Integer	When risk level is enabled in system settings, certifications for users will use this value to match against the provided certification filter for each system. Note risk level for connected systems is global to that entire system and all its attributes.
System	entitlementOwner	managed object	The entitlement owner is used to determine the user or role that should be assigned a certification task for the given system. It’s used in user certifications when the certifier is set to 'Entitlement Owner’. The value here should reference only a managed/user or a managed/role, and is global to the system and all its attributes.
System-Attribute	certifiable	boolean	Allows the system attribute to appear within the user certification creation screen as an option for ‘Access to Certify’. If not present or set to false the attribute will not appear.
System-Attribute	displayable	boolean	Allows the system attribute to appear within the user event details page as a non-certifiable attribute. It can be used to provide the certifier more insight to the user’s account, for entitlements that may be helpful to see not certify (e.g. cn, uid, etc.)

Viewing Glossary Metadata within a Certification

When viewing the event details display of a single event within a certification, users will notice that the entitlements, and in user certifications the attribute names, of each certifiable row are clickable links. If clicked, a glossary page will appear that corresponds to the identity attribute or value chosen. If that entry exists, the metadata for that item will be displayed in a key-value table. If that entry does not exist, the user will be informed that there is no current glossary entry for that item. This view allows the certifier or admin to gain more information and perspective on the things included in that particular certification.



User Attributes

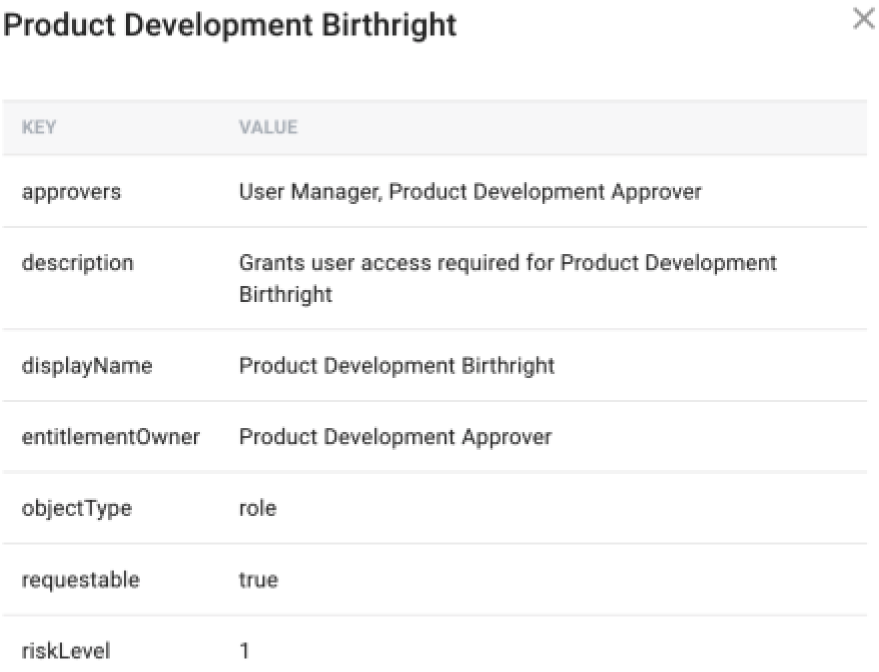
Job: DevOps Lead

Provisioning Roles

Product Development Birthright

Product Development Lead

There is often metadata in glossary entries that administrators would either not want the end user to see, whether that be for privacy reasons or simply because the information would be more confusing than helpful. Access Review leverages a configuration file within the openidm/conf directory called displayableMetadata.json to restrict the keys that will display in these pages for each of the different glossary object classes. Only keys that appear for each class type will be shown to end users, and they are global for each class type.



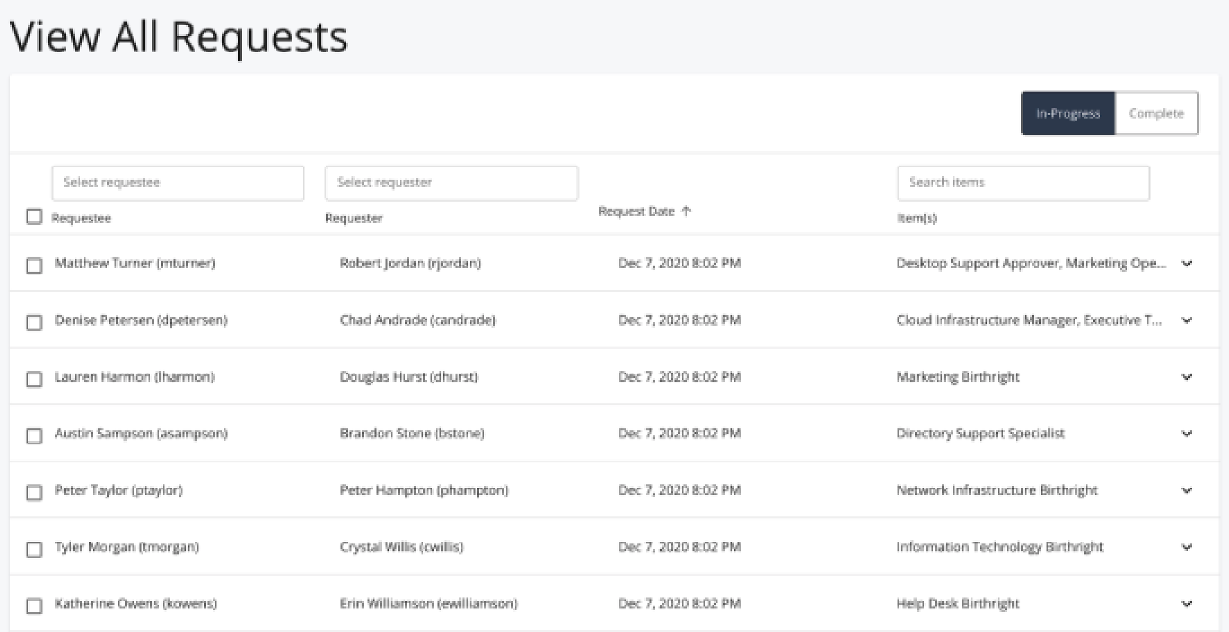
Product Development Birthright

KEY	VALUE
approvers	User Manager, Product Development Approver
description	Grants user access required for Product Development Birthright
displayName	Product Development Birthright
entitlementOwner	Product Development Approver
objectType	role
requestable	true
riskLevel	1

Access request

View all requests

The View All Requests page allows administrators to view all requests across the entire application, either in progress or completed.



View All Requests

☐	Requestee	Requester	Request Date ↑	Item(s)	
☐	Matthew Turner (mturner)	Robert Jordan (rjordan)	Dec 7, 2020 8:02 PM	Desktop Support Approver, Marketing Ope...	⌄
☐	Denise Petersen (dpetersen)	Chad Andrade (candrade)	Dec 7, 2020 8:02 PM	Cloud Infrastructure Manager, Executive T...	⌄
☐	Lauren Harmon (lharmon)	Douglas Hurst (dhurst)	Dec 7, 2020 8:02 PM	Marketing Birthright	⌄
☐	Austin Sampson (asampson)	Brandon Stone (bstone)	Dec 7, 2020 8:02 PM	Directory Support Specialist	⌄
☐	Peter Taylor (ptaylor)	Peter Hampton (phampton)	Dec 7, 2020 8:02 PM	Network Infrastructure Birthright	⌄
☐	Tyler Morgan (tmorgan)	Crystal Willis (cwillis)	Dec 7, 2020 8:02 PM	Information Technology Birthright	⌄
☐	Katherine Owens (kowens)	Erin Williamson (ewilliamson)	Dec 7, 2020 8:02 PM	Help Desk Birthright	⌄

Requests table

The table includes the following columns:

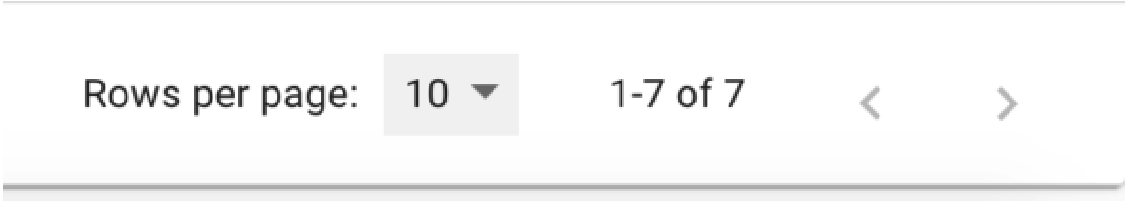
- Requestee - user for whom the access is requested
- Requester - user who submitted the request
- Request Date - date the request was submitted
- Item(s) - items that are included as part of the request

Table filters

The requests table can be filtered using any of the following options:

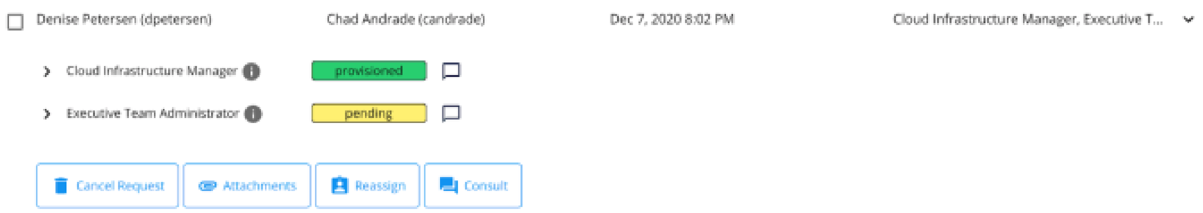
- Status:
    - In Progress - Shows all in-flight request that are still waiting on one or more user approvals to be processed
    - Complete - All previously completed requests that have either been completed by all necessary approvers or cancelled by the requester or an administrator.

- Requester: Select a user using the typeahead input box above the column label to display only requests where they are the requester.
- Requestee: Select a user using the typeahead input box above the column label to display only requests where they are the requestee.
- Item: Select a requestable item using the typeahead input box above the column label to display only requests targeting a specific item.
- Request Date: Not specifically a filter, however the current list of results within the table can be sorted by request date, either ascending or descending, by clicking on the column label “Request Date.”
- Table Pagination: The requests table allows the user to choose the amount of rows they would like to see within the page of results (10, 20, or 30.) The user has the ability to scroll through subsequent pages of request results by clicking the navigation arrows to move forward or backward.


Rows per page: 10 ▾ 1-7 of 7 ‹ ›

Request information

Clicking on an individual request will open an extended panel showing the entire request process, grouped by each individual approval task.

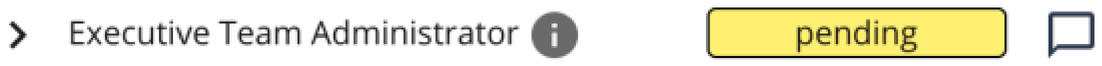

☐ Denise Petersen (dpetersen) Chad Andrade (candrade) Dec 7, 2020 8:02 PM Cloud Infrastructure Manager, Executive T... ⌄

› Cloud Infrastructure Manager ⓘ provisioned

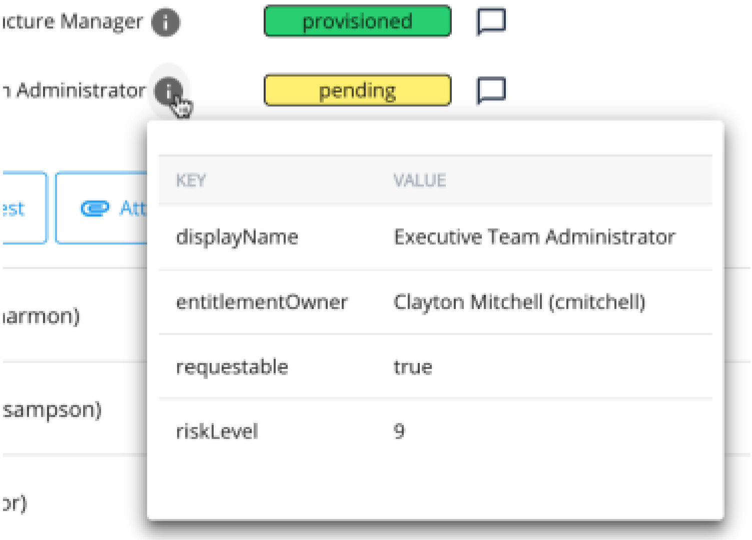
› Executive Team Administrator ⓘ pending

The expanded view of a request shows a list of all of the items that are included as part of a request. Each line includes the following information:

- Item - The display name of the item


› Executive Team Administrator ⓘ pending

- Info Icon - Get more information on the requested item. Hovering over this icon will expand a page containing all displayable metadata for the item.

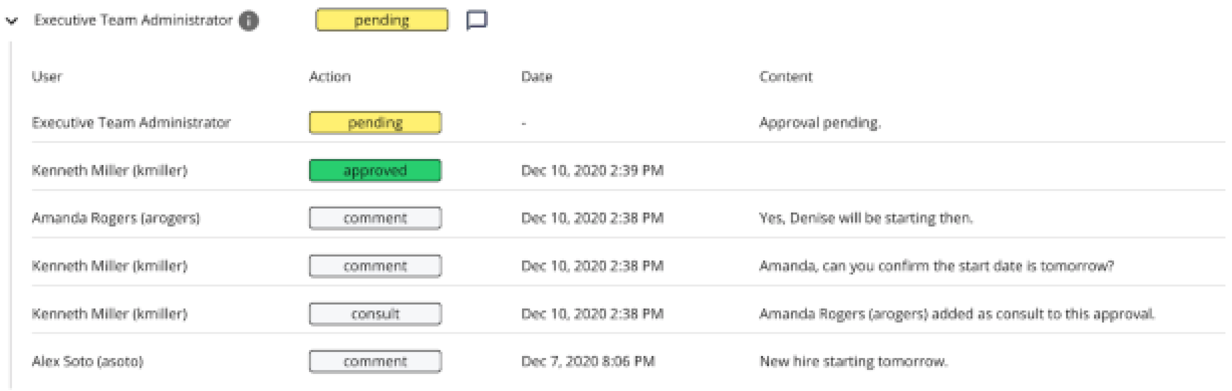


KEY	VALUE
displayName	Executive Team Administrator
entitlementOwner	Clayton Mitchell (cmitchell)
requestable	true
riskLevel	9

- Remove Icon - Any requested item that was requested to be removed will have a small, red minus icon next to its info icon.
- Status - The current approval outcome of each item
  - Pending - Item request is in-progress and still awaiting action by one or more approvers.
  - Denied - Item has been rejected during one of its approval tasks.
  - Provisioned - Item has completed its approval chain, and has been successfully provisioned to the user.
  - Not Provisioned - Item has completed its approval chain, but has not been provisioned to the user. This means one of the following has occurred:
    - An error during provisioning
    - The user already had the specific access requested
    - The item has a manual provisioning task, which the provisioner completed as “Not Provisioned”
  - Cancelled - Request has been cancelled before this item has completed its approval process.
- Comment Icon - Clicking this icon allows the user to add a comment to the given item’s history.

Request item history

In addition to the information presented initially, each individual line item can be clicked and expanded to reveal a chronological history of the actions taken as part of that item’s approval process. This includes comments made, approval task information, reassign or consult actions, file uploads, and more.



Executive Team Administrator pending

User	Action	Date	Content
Executive Team Administrator	pending	-	Approval pending.
Kenneth Miller (kmiller)	approved	Dec 10, 2020 2:39 PM	
Amanda Rogers (arogers)	comment	Dec 10, 2020 2:38 PM	Yes, Denise will be starting then.
Kenneth Miller (kmiller)	comment	Dec 10, 2020 2:38 PM	Amanda, can you confirm the start date is tomorrow?
Kenneth Miller (kmiller)	consult	Dec 10, 2020 2:38 PM	Amanda Rogers (arogers) added as consult to this approval.
Alex Soto (asoto)	comment	Dec 7, 2020 8:06 PM	New hire starting tomorrow.

The history view is organized as a table that includes the following columns:

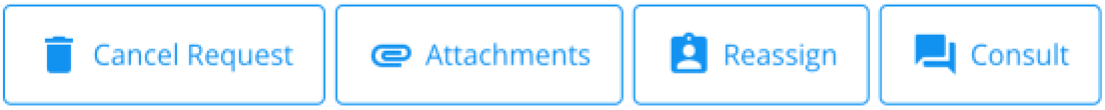
- User - The user who took the specified action on the item. In the event that the system acts directly on the request, for example during a task expiration, this column will read “SYSTEM.”
- Action - The action taken on the request. Possible values are listed below
  - Pending - An in progress approval task awaiting action
  - Approved - A completed approval task that was manually approved
  - Rejected - A completed approval task that was manually rejected
  - Auto-approved - A completed approval task that was auto-approved
  - Auto-provisioned - Indicator that item required no approval
  - Cancelled - A completed approval task that was cancelled in-progress
  - Comment - A generic comment referencing the item
  - Consult - Indicator that a consult was added to an approval task
  - Upload - Information on an uploaded file
  - Reassign - Information on a reassigned task
- Date - The date and time the action took place
- Content - The content of the action, which will vary depending on the specific action, but will always provide additional details as to what took place. Note that entries into this table for approval task completion may or may not have additional content to display.

NOTE

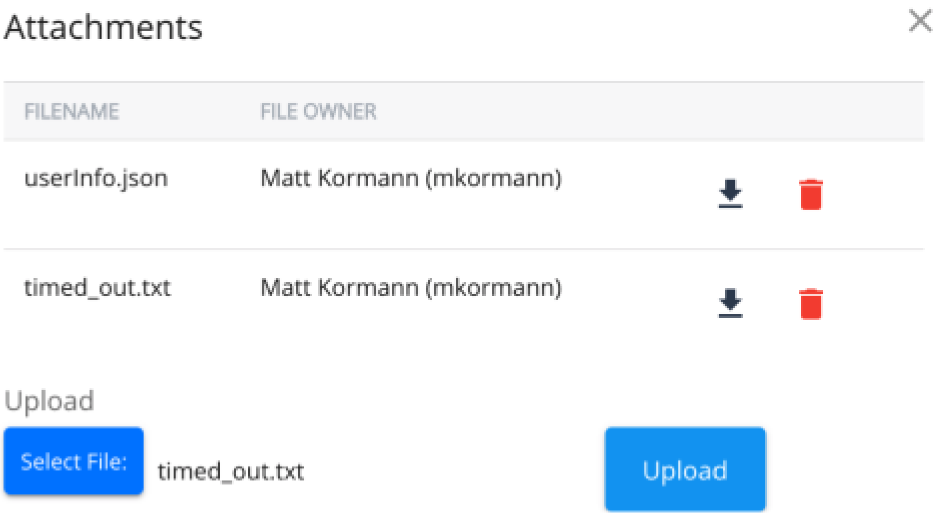
Any approval task that is currently pending/in-progress for the given item will always appear at the top of the item’s history and will be listed as pending.

Action buttons

Administrators also have access to take certain actions on individual requests via the row of action buttons found at the bottom of the expanded view. Each action is detailed below:



- Cancel Request - Cancel the request, including all currently in-progress tasks. The administrator will be asked to confirm the action before it is completed. Note that any item in a given request that already has a finalized outcome (Provisioned, Not Provisioned, Denied, etc.) will not be affected by a cancellation. Once an item is complete, the provisioning action can not be reversed.
- Attachments - Allows the user to view the current list of attachments assigned to this request, download any of those files, or upload a new file.



Attachments

FILENAME	FILE OWNER		
userInfo.json	Matt Kormann (mkormann)	⬇	🗑
timed_out.txt	Matt Kormann (mkormann)	⬇	🗑

Upload

Select File: timed_out.txt

If there are any files attached to the request, the files table will appear at the top of the page. This table consists of three columns:

- Filename - Name of the uploaded file
- File Owner - User who uploaded the file to the request
- Action Buttons
    - Download Icon - Click to download the file to your local machine
    - Delete Icon - Click to remove the file from the request

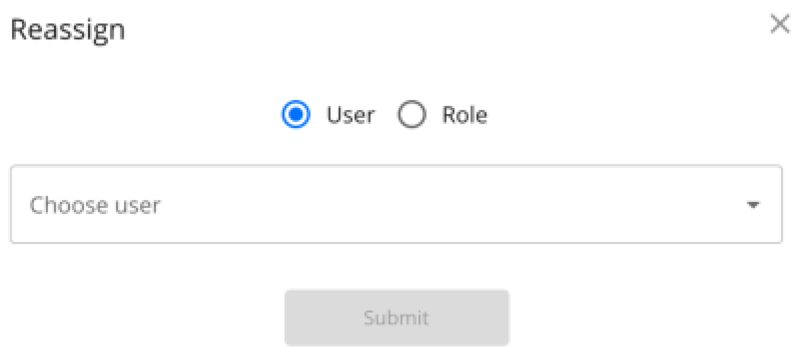
At the bottom of the page will be the upload file form for adding files to the request. To choose the file you want to upload, click on the Select File button to open up a file picker screen. Once you've selected the file, the name of the file chosen will appear next to the Select File button in the form. Finally, clicking on the Upload button to the right will complete the action and save the file to the request.

NOTE

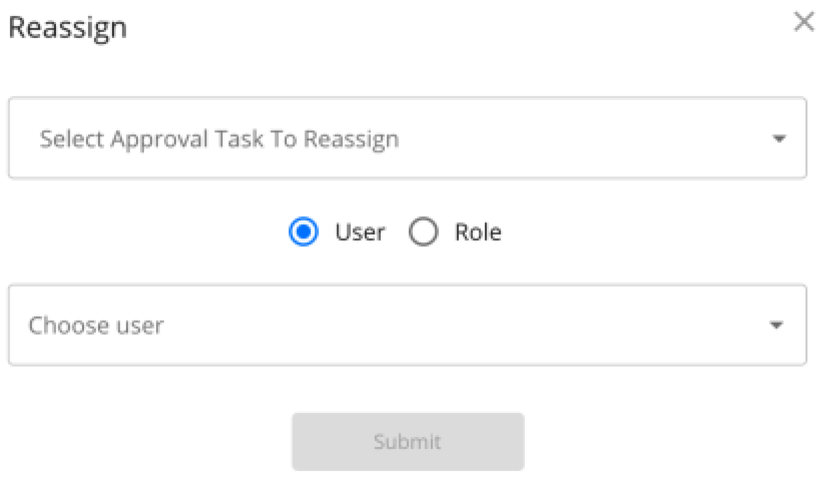
NOTE

For requests with multiple items, it is possible to “attach” a file to only certain items within the request, so that the file is only visible to those approvers who need to see its contents, and not available to approvers who may not be responsible for that specific item. In these cases there will be an extra input as part of the upload form, that allows the uploader to select the items that the file is relevant to.

- Reassign - Administrators have the ability to reassign any task that is currently awaiting approval as part of a request. Clicking on the reassign button will pop up a page form for reassigning tasks. Users can choose between reassigning a task to a user or a role/group. Once chosen, the typeahead box below will allow for searching the system for the desired assignee. When the option has been selected, clicking Submit will start the reassignment process.



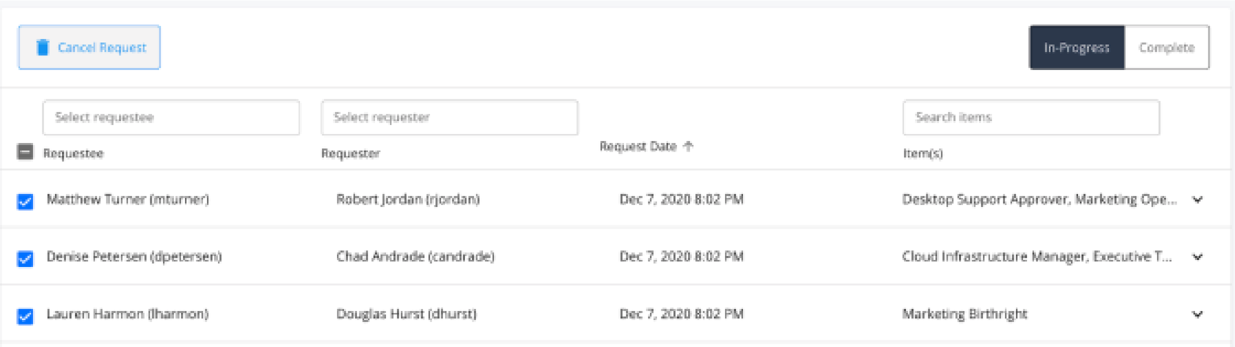
Some requests may have more than one active approval task that is eligible to be reassigned. In this case, there will be an additional selection to be made at the top of the request form for determining which approver’s task should be reassigned with this action.



- Consult - Administrators have the ability to add a consult to any task that is currently awaiting approval as part of a request. The interface for adding a consult mirrors the reassign functionality shown above.

Bulk cancelling requests

When viewing in-progress requests, you have the ability to select one (or more) requests and cancel them in bulk. To do so, simply click the checkbox next to the request(s) you wish to cancel and click the ‘Cancel Request’ button at the top left of the requests page. You will be asked to confirm your decision and then will receive a confirmation message when the request cancellation process is complete.



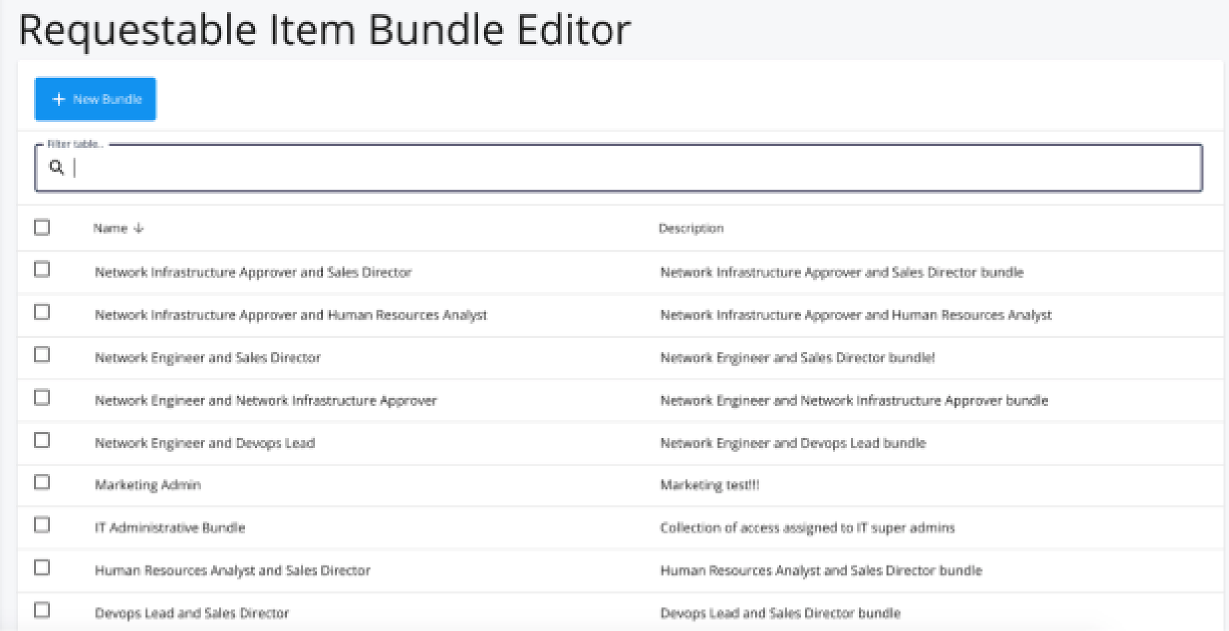
	Requestee	Requester	Request Date ↑	Item(s)
☑	Matthew Turner (mturner)	Robert Jordan (rjordan)	Dec 7, 2020 8:02 PM	Desktop Support Approver, Marketing Ope...
☑	Denise Petersen (dpetersen)	Chad Andrade (candrade)	Dec 7, 2020 8:02 PM	Cloud Infrastructure Manager, Executive T...
☑	Lauren Harmon (lharmon)	Douglas Hurst (dhurst)	Dec 7, 2020 8:02 PM	Marketing Birthright

NOTE

As mentioned above, if you cancel a request in which one or more of the items have already been provisioned, those items will remain provisioned. Items are provisioned as their individual approval chains are completed, and at that point are considered final. Any items that were still awaiting any further approvals will not be provisioned.

Bundle editor

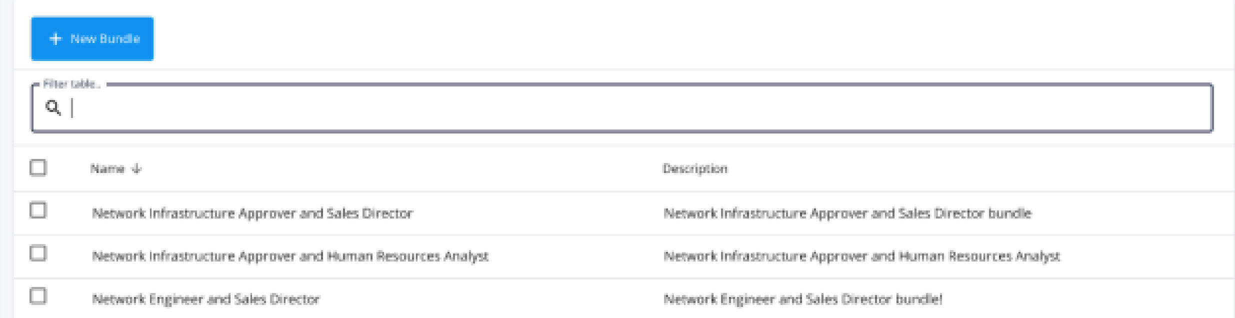
Administrators are granted the ability to create a requestable bundle of individual items, that can be submitted as part of a new request as a single package. Each individual item that is contained within a bundle still retains all of its original requirements for approval, notably its individual approval chain, however it allows for the end user to submit multiple related items simultaneously, without the need for locating and adding each individually.


Requestable Item Bundle Editor

□	Name ↓	Description
□	Network Infrastructure Approver and Sales Director	Network Infrastructure Approver and Sales Director bundle
□	Network Infrastructure Approver and Human Resources Analyst	Network Infrastructure Approver and Human Resources Analyst
□	Network Engineer and Sales Director	Network Engineer and Sales Director bundle!
□	Network Engineer and Network Infrastructure Approver	Network Engineer and Network Infrastructure Approver bundle
□	Network Engineer and Devops Lead	Network Engineer and Devops Lead bundle
□	Marketing Admin	Marketing test!!!
□	IT Administrative Bundle	Collection of access assigned to IT super admins
□	Human Resources Analyst and Sales Director	Human Resources Analyst and Sales Director bundle
□	Devops Lead and Sales Director	Devops Lead and Sales Director bundle

Requestable bundle table

After navigating to the Bundle Editor interface, the administrator will be presented with a table that displays all of the existing bundles within the system. The table includes two columns for each bundle:



☐	Name ↓	Description
☐	Network Infrastructure Approver and Sales Director	Network Infrastructure Approver and Sales Director bundle
☐	Network Infrastructure Approver and Human Resources Analyst	Network Infrastructure Approver and Human Resources Analyst
☐	Network Engineer and Sales Director	Network Engineer and Sales Director bundle!

- Name: The name given to the bundle of items
- Description: The description and/or purpose of the bundle

Bundle search

The table also allows the user to search the list of bundles by using the table’s filter box. This search feature works against both the Name and Description fields of the requestable bundle and returns all matches.

NOTE

The bundle table is not currently searchable based off of the items that are included within the bundle, therefore when creating a new bundle it is highly recommended that you leverage the description to provide sufficient information on which to search for the bundle.

Deleting bundles

The Bundle table allows the administrator to select one or more bundles at a time and delete them from the system. Simply check off any of the bundles that you wish to remove, and select the delete button on the top right of the table. Bundle deletion is permanent, and the only way to recover a deleted bundle is to recreate it manually.

NOTE

Deleting a bundle will not affect any current in-progress requests that were created using that bundle. Those requests will maintain their state, and will continue without any issue.

Create bundle

By clicking on the new button on the bundle editor page, the administrator will be able to enter information into the Edit Bundle form on the right side of the page to create a new bundle. There are three fields available:

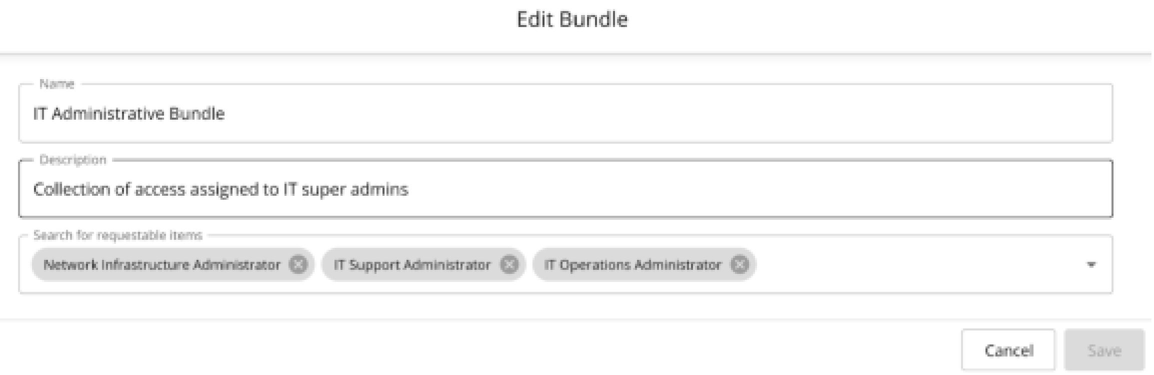
- Name: The name given to the bundle of items
- Description: The description and/or purpose of the bundle
- Items: The requestable items that will be included in any request that contains this bundle

Both the name and description fields are simple text boxes. To search for items to add to the bundle, begin by typing the desired item's name within the items input box. As you type, you will see a dropdown menu appear with selectable options that match the input that you've entered. Click on any of the available requestable items to add them to the current bundle form. Once added, clicking on the item display name in the input box will display further information about the item in a pop-up page.

Once all of the desired information is set within the form, clicking Save at the bottom of the form will save the bundle to the database and will make it available for viewing within the bundle table on the left.

Editing a bundle

To edit an existing bundle, search and find the desired bundle within the bundle table. Once found, clicking the bundle's row within the table will populate the Edit Bundle form page. The information can then be edited as needed, including the addition or removal of individual items.



Edit Bundle

Name: IT Administrative Bundle

Description: Collection of access assigned to IT super admins

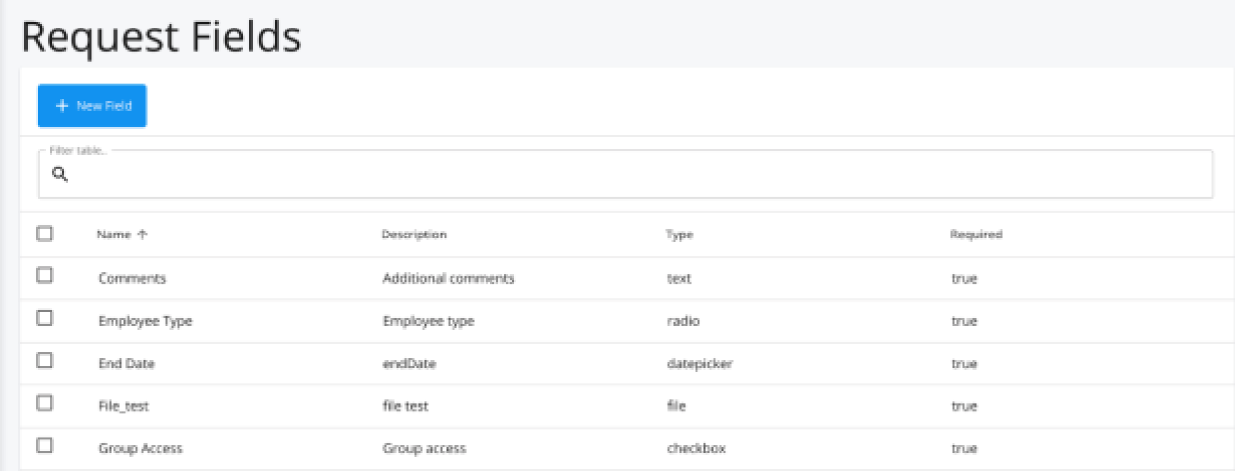
Search for requestable items: Network Infrastructure Administrator, IT Support Administrator, IT Operations Administrator

Request fields

Request fields are the building blocks that allow administrators to define custom request forms for individual requestable items. This screen allows administrators to create, manage, and delete fields from the application.

Request fields table

The table allows the admin to search the list of request fields by using the table's filter box. This search feature works against both the Name and Description fields of the request field items and returns all matches, paginated.



Request Fields

□	Name ↑	Description	Type	Required
□	Comments	Additional comments	text	true
□	Employee Type	Employee type	radio	true
□	End Date	endDate	datepicker	true
□	File_test	file test	file	true
□	Group Access	Group access	checkbox	true

Deleting request fields

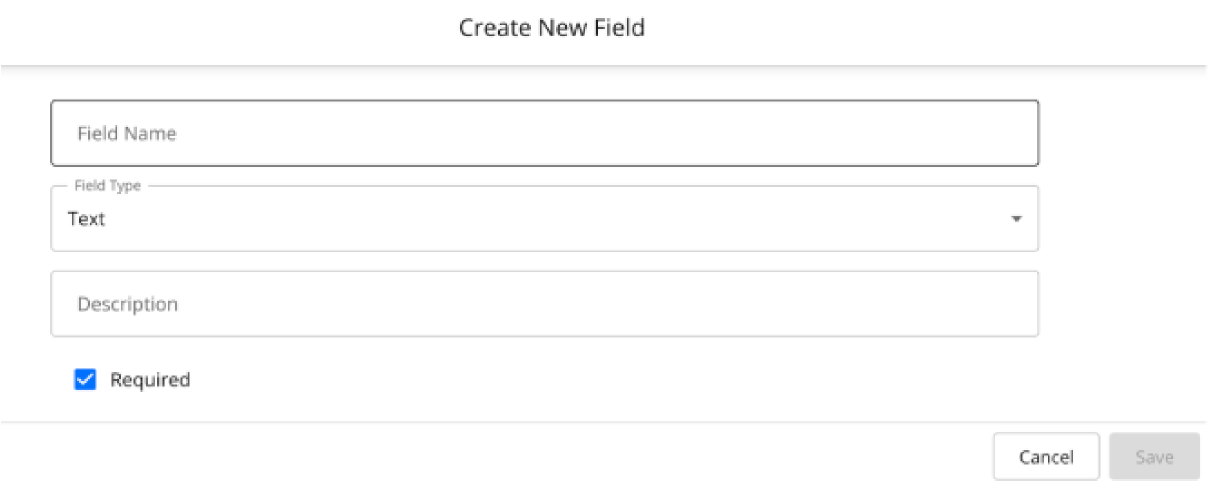
The Request Field table allows the administrator to select one or more fields at a time and delete them from the system. Simply check off any of the fields that you wish to remove, and select the delete button on the top right of the table. Request field deletion is permanent, and the only way to recover a deleted field is to recreate it manually.

NOTE

Deleting a request field will not affect any current in-progress requests that were created using that field. Those requests will maintain their state, and will continue without any issue. Furthermore, any item that is leveraging a request field that has been deleted will simply ignore that field for any new requests, and will automatically reference that field again if it is recreated with the same name.

Create request field form

By clicking on the new button on the editor page, the administrator will be able to enter information into the Request Field form on the right side of the page to create a new entry.



Create New Field

Field Name

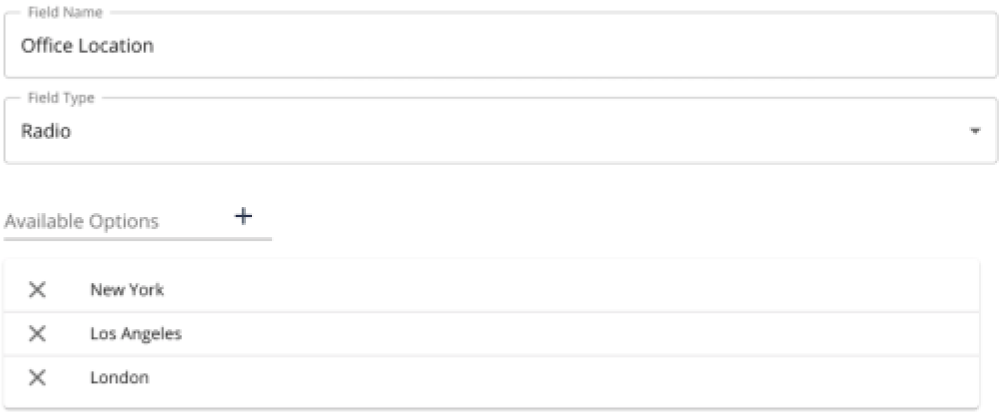
Field Type
Text

Description

☑ Required

The following fields are available:

- Field Name: The name given to the request field (this is the key referenced on each requestable item’s requestFields key.)
- Field Type: The type of input used for this field. Choose from the following options:
    - Text
    - Select
    - Typeahead
    - Radio
    - Checkbox
    - Datepicker
    - File
- Description: The description and/or purpose of the request field.
- Required: Whether or not this field is required for any requestable item that includes it. For those fields that may be required for some forms and not for others, it is recommended to create two distinct fields.
- Available Options (for Field Types of radio, select, and checkbox): Used to define the items to choose from for those input types with distinct options. Enter in the value of the option in the underlined text field, and click the ‘+’ icon to add the option to the list. To remove an entry, click the ‘x’ icon next the the field value within the list.



Field Name: Office Location

Field Type: Radio

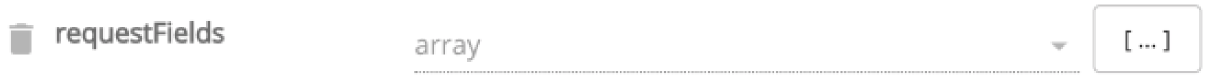
Available Options

- New York
- Los Angeles
- London

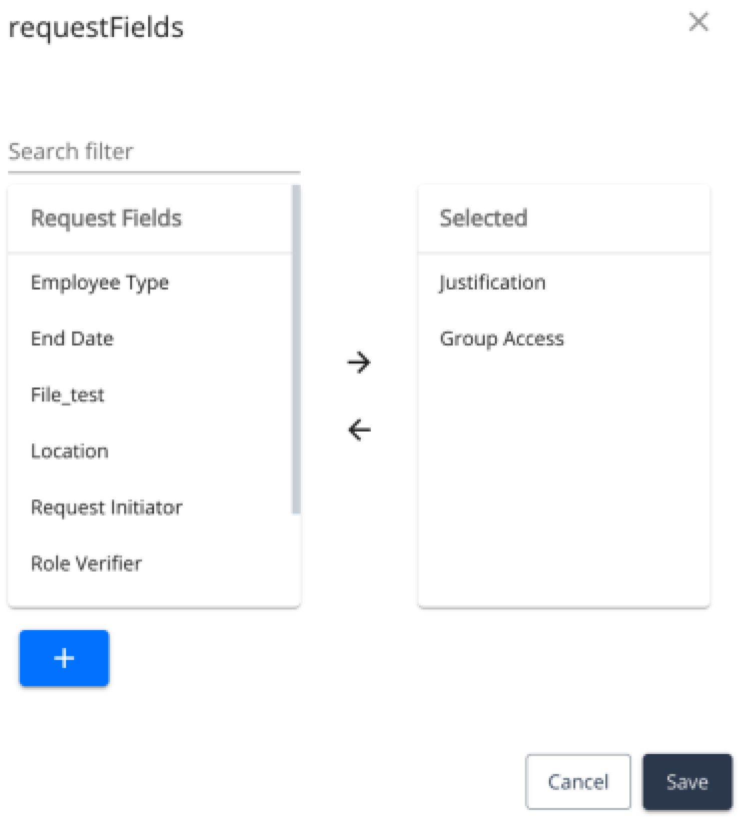
Once all of the desired information is set within the form, clicking Save at the bottom of the form will save the Request Field to the database and will appear within the main table.

Assigning request fields to items

To assign Request Fields to a requestable item, the requestFields key must be added to the glossary entry for that item. This is a reserved key on any entry, and will always be of type array. Once created, the requestFields uses a custom interface to assign the available fields to that item.



requestFields: array

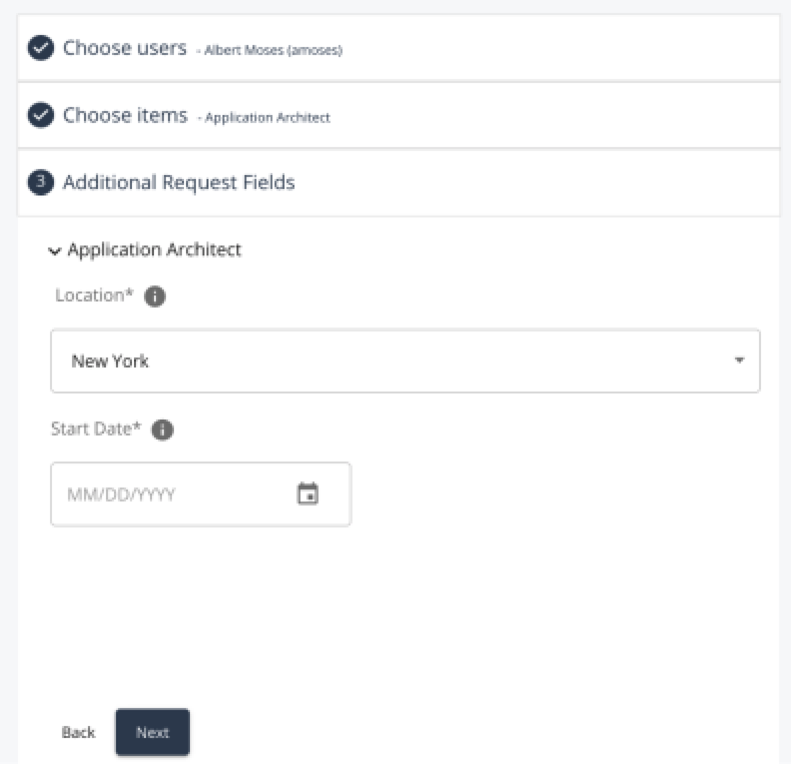


requestFields

Search filter

Request Fields	Selected
Employee Type	Justification
End Date	Group Access
File_test	
Location	
Request Initiator	
Role Verifier	

To assign existing Request Fields to the open entry, simply select (or optionally filter the options first) an entry on the left side of the form, which will move it to the selected section on the right. Once all the desired fields are attached to the requestable item, click Save to close the page and keep your changes. Note: The order of the fields added to this array key will be respected in the Create New Request interface.



Choose users - Albert Moses (amoses)

Choose items - Application Architect

3 Additional Request Fields

Application Architect

Location*

New York

Start Date*

MM/DD/YYYY

Defining requestable items

The Identity Glossary is where glossary administrators are responsible for creating and defining what items are eligible to be requested within the application, what approval process they follow, and any additional data that may or may not affect the request. To make an object requestable within the IDM environment, it must have a glossary entry that meets ALL of the following requirements:

For entries of type:

- Object
  - Must be an existing managed object within IDM
  - The managed user schema must include a relationship property between itself and the managed object type of the item (default property used is roles)
  - If using a managed user property other than the defined default (roles), the glossary item must specify the desired user property name with the userProvisionProperty key.
- Identity-Value
  - The key attributeName must be an existing non-relationship property on the managed user schema.

- System-Value
  - Must have either a provisioner key or a provisionScript key on the item. As these entries do not reference a direct IDM user property, they must have a manual provisioning step. The provisioner user/group runs as a manual provisioning task, while a provision script runs automatically on approval completion.
  - A boolean key of requestable set to true
  - A string key of displayName

If all the above criteria is met, the item will appear within the Create Request form in the Access Request application and be available for use within request.

Access request glossary keys

There are several reserved keys for glossary items that are leveraged by the Access Request application. Any key marked with an asterisk (*) is for use within the default approval flow and will not be enforced when using a custom approval flow.

> IMPORTANT
>
> Glossary keys are *case_sensitive*. For example, make sure to put `requestable` and *not* `Requestable`.

The following is a list ofo the reserved glossary keys for Access Request:

- `requestable` (boolean). Is the item available to be requested.
- `approvers` * (array). The approval chain for granting access to the requested item. The entries within this approver list will be evaluated against both the managed/user object of the requestee, as well as the keys of the glossary item itself. In order for an approver key to be evaluated correctly it must refer to a managed object of either type user or role. For managed/user properties, the specified property must be a single relationship to the user/role.

  Some examples:

  - An entry of ‘manager’ in the approvers array will evaluate to the requestee user’s manager, as the property manager exists on the user schema and is a single relationship to a managed/user.
  - An entry of ‘entitlementOwner’ in the approvers array of an item with an entitlementOwner key of type managed object id that is set to a role, will use that role as the approver.
  - If the approvers list contains a key that is not able to resolve to a single user or role ID, the Access Request workflow will default to the group defined in the Access Request settings as the Default Approver Group to handle that task

  NOTE

NOTE

> The value of 'self' is also reserved as an approver option for any approval chain that wants to use the requestee themselves as an approver. This can be useful when defining a separate approver chain for removal of access. If an item is intended to be auto-provisioned, i.e. requires no approval steps, an approvers key should be created and left as a blank list. If an item is defined as requestable but has no approvers key, it will leverage the Access Request setting for Default Approvers.

- `removalApprovers` (array). The approval chain for the item when the request type is 'remove.' If this key is not used, the approvers key will be used in its place. All the same functionality for defining approvers applies here as well.
- `parallelApproval` (boolean). If true, all approval tasks will be created concurrently. If false, or not set, approval flow will be executed sequentially. Note that provisioning tasks will always be created after all approval tasks are completed, not in parallel.
- `userProvisionProperty` (string). The managed user property for which the requestable item will be assigned to upon approval when using the default approval flow or the provision endpoint. This is used for requested items with a glossary class of object only, and has a default value of roles.
- `preRequestScript` (string). Script hook that is run immediately after creation of the request object for any pre-processing of the request, notifications, etc. This will be called before any approval task creation or custom workflows are kicked off. The value should be set to the relative path of the javascript file to be run from the openidm script directory.
- `provisionScript` (string). Script hook for handling the provisioning of an approved item. Supersedes the default provisioning of items within IDM and is called once the item's approval chain is fully approved.
- provisionScript (string). Script hook for handling the provisioning of an approved item. Supersedes the default provisioning of items within IDM and is called once the item's approval chain is fully approved.
- `provisioner` * (managed object id). If defined on an item and referencing a managed/user or managed/role, a manual provisioning task will be created when the item's approval chain is completed, and be assigned to that provisioner. Note this should only be used in instances when manual intervention is required, as it supersedes the automated provisioning that normally occurs when a request is approved.
- `requestWorkflow` (string). Identifies the custom workflow to use for the requestable item. Defining a custom request workflow on a requestable item will supersede the default approval process and control the entire approval flow. See section Standard Request Workflow for details.
  - For BPMN workflows, it is the name of the workflow definition in IDM.

    - For custom scripts, it is the relative path to the script file within the scripts directory (e.g. access-request/roleApproval.js)
  - `requestWorkflowType` (string). Identifies the type of workflow defined by the requestWorkflow key, either ‘workflow’ or ‘script.’ Any item with a requestWorkflow defined but without a requestWorkflowType will default to ‘workflow.’

Standard request workflow

ForgeRock Access Request uses an internal workflow in order to control and manage the approval process for all requestable items that do not explicitly specify their own process. All customizations and controls for the request process are available within the Access Request user interface.

The following section describes in detail the process of the out of the box workflow so that admins can better understand what actions are being taken at what stage.

Approval process

An item that is submitted within the Create Request form will follow the approval process that is explicitly defined within that item’s glossary entry. Each item has a list of approvers that the Access Request system will use to determine which users are assigned a given task and how many levels of approval are needed to provision an item. At each level of approval, the user who is assigned the task will have the ability to either approve or reject each item that belongs to their task and submit their decision. Based on those decisions, items can either be provisioned, rejected outright, or continue down the chain of approval.

Request flow

Approval flow

> 1. When a request is submitted, the following steps are taken, in order, to determine the flow of a request.
> 2. If a request contains multiple requestees, each requestee is split into their own individual request, so that each requestee’s access can be provisioned independently of the other users.
> 3. If the request contains a requestable bundle as one of the requested items, that bundle is unpacked and each item within the request is then treated as an individual item within the request. This allows each item in the bundle to maintain its defined approval process independently of the items bundled with it.

4. If there are items within the request that have a preRequestScript key in their definition, it will be executed at this point for any pre-request logic that needs to occur.
5. If an item has an explicitly defined approvers list that is empty (i.e. an approvers key within their glossary entry that is a list with no entries), then that item will be auto-provisioned at this point. This is for any items that do not require any level of approval to be granted.
6. The items within the request will then be grouped, if possible, by the assigned approver. An approval task will then be created for each individual user and group that is calculated as an approver for those items. As an example:

   A request that contains: - “Role 1”, with approver “A” - “Role 2”, with approver “A” - “Role 3”, with approver “B”

   + will result in two separate approval tasks:

   - Approver A will receive a task with “Role 1” and “Role 2”
   - Approver B will receive a task with “Role 3”
7. Depending on the system settings, auto approval may be enabled for certain approval tasks. There is an option for tasks where the requester is the direct approver and also an option for tasks where the requester belongs to the group assigned as the approver. Any items that meet the criteria of the enabled settings will be immediately sent to their next level of approval, or if none exists, will be provisioned. This feature allows end users to avoid duplication of effort, for example when a manager is requesting access for his/her reports and the initial approver for the items is defined as manager.
8. Once each approval task is created, the tasks can be completed independently of any other task that is part of the same request. This potentially allows for a single item to continue along its entire approval process and be completed without depending on a separate approval task to be decided on. Important to note here is that any item that completes its approval process will have that item provisioned to the user as soon as that final decision is made. Further, any item that has already been completed and provisioned as part of a request that is cancelled at a later date will remain provisioned. Any item that is rejected during a given approval task will be immediately removed from any further approvals, and a notification will be sent to inform users that that item was not successfully approved.
9. Approval task deadlines are calculated using the global setting defined in the access request configuration. When an approval task hits its defined deadline it does not expire or get cancelled. Instead, the task at that point is reassigned to the group defined as the Default Approver for further review. The group can decide to reassign the task elsewhere for another user to complete, if enabled.
10. After an item included in the request has either been approved by all listed approvers, its definition will be checked for a provisionScript or provisioner key.

Any item with a provision script will have that script executed in lieu of the default IDM provisioning and then will be marked as complete. Any item with a provisioner listed will have a manual provisioning task created on the request and assigned to that provisioner to be completed. Once that user takes the manual steps to provision the item, they can complete the task as either ‘provisioned’ or ‘not provisioned.’

11. After an item in the request has been approved by all listed approvers, its definition is checked for a provision script or provisioner key. Any item with a provision script will have that script executed in lieu of the default IDM provisioning and then will be marked as complete. Any item with a provisioner listed will have a manual provisioning task created on the request and assigned to that provisioner to be completed. Once that user takes the manual steps to provision the item, they can complete the task as either ‘provisioned’ or ‘not provisioned.’

    > NOTE
    >
    > Any disconnected application item that is being requested must include one of the above keys for provisioning, as it is not a direct IDM managed resource and cannot be automatically assigned to the user. NOTE: Any disconnected application item that is being requested must include one of the above keys for provisioning, as it is not a direct IDM managed resource and cannot be automatically assigned to the user.

12. If no further provisioning or approval tasks are required for any items within the request,, the request will be complete. All approved access will have already been provisioned and the request will move to the completed table for reference.

Custom workflows

For any item with an approval process that requires additional steps that are not covered by the out-of-the-box functionality, a custom workflow may be used to define the steps necessary for approval. There are two different options available for a custom workflow: a BPMN workflow (activiti in IDM 6.5, flowable in 7.0) or a javascript script.

Either choice will use the Access Request API to interact with the request, create approval tasks, provision access, and complete the request. The process for doing so for each method is outlined below.

When a requestable item uses a custom workflow, every step of the approval process will be controlled by that flow, immediately following the creation of the request object. Once a call is made to the create request API, the request object is saved to the repository with all of the necessary submitted request information, but no other steps are taken to advance the approval of the given item. Other items in the request will follow their own processes, if defined, and will not expect another item’s custom workflow to interact with their approval. However those other items, as part of the request object, will be available within the workflows if they need to be leveraged for any custom logic.

Defining a custom workflow on a glossary entry

There are two keys on a glossary entry that determine what custom workflow will be used to drive the request lifecycle:

- `requestWorkflow` - This defines the specific workflow definition or script that will be used to drive the request.
  - For workflows it is the name of the workflow definition within IDM. Refer to the IDM documentation for any questions on adding workflows to your environment.
  - For scripts it is the path to the javascript file, starting from within the openidm/script directory, (e.g., “basicRequest.js” for a file located directly in that directory).
- `requestWorkflowType` - Value can be either ‘workflow’ or ‘script’. Entries that have a requestWorkflow key but not a requestWorkflowType key will be assumed to be of type workflow. However, it is recommended best practice to store the proper type with this key.
- requestWorkflow - This defines the specific workflow definition or script that will be used to drive the request.
  - For workflows, it is the name of the workflow definition within IDM. Refer to the IDM documentation for any questions on adding workflows to your environment.
  - For scripts it is the path to the javascript file, starting from within the `openidm/script` directory, (e.g., “basicRequest.js” for a file located directly in that directory).
- requestWorkflowType - Value can be either ‘workflow’ or ‘script’. Entries that have a requestWorkflow key but not a requestWorkflowType key will be assumed to be of type workflow. However, it is recommended best practice to store the proper type with this key.

NOTE

There are some key differences between the two different types of custom workflow definitions because of the way each method operates. The details of each are described in the following two sections.

Creating a custom approval process with BPMN workflow

A request including an item that has a custom approval process via BPMN workflow (activiti/flowable) will have a process instance of that request created upon creation of the request. As mentioned above, a request with multiple items that each have their own custom flow defined will create a workflow instance for each individual item, rather than one process for the entire request contents.

The following information is passed into the workflow process and can be used to drive the approval process:

- `requestId` - ID of the request object this item belongs to.
- `requesterId` - ID of the user who submitted the request.
- `requesteeId` - ID of the user who is targeted by this request.
- `item` - ID of the requestable item glossary entry.
- `requestType` - Type of request submitted for this item, either add or remove.

A custom BPMN workflow must be responsible for the following functionality in the request process:

- Creating necessary approval tasks. To create an approval task via the API within a workflow, first create a user task node within the BPMN definition. Within that node's 'create' listener, make a call to 'openidm/access-request/approval' and send the following body.
    - `requestId` - ID of the request.
    - `itemIds` - List of item IDs to include in approval task (normally just the single item).
    - `approverId` - ID of approver user or group.
    - `workflowTaskId` - The user task ID that corresponds to this approval. This is used within BPMN workflows to complete the task upon approval submission and continue the workflow process.
- Sending request notifications. To send an Access Request notification via API, use the 'openidm/notification/[NOTIFICATION_ID]' endpoint with the notification template of your choosing. Templates can be found with the accessRequestNotificationTemplates.json file in the conf directory, and any POST body to the endpoint must include any of the variables described in the template definition.
- Provisioning approved access. Access Request provides a provisioning endpoint, `openidm/access-request/provision`, for IDM attribute/role assignment during simple request provisioning. Alternatively, you can create a provisioning task for any required manual operation.
- Setting the final outcome of the item on the request object. When an item's approval process is complete, the workflow must set the request item's outcome via a POST call to openidm/access-request/request?_action=update). When an item's outcome is set to a final outcome (e.g. provisioned, denied, etc.), no other action is required on

the request, and it will be closed if and when any other items on the request have been completed.

Creating a custom approval process via script

A request including an item that has a custom approval process via script will execute that script upon creation of the request, and following the completion of every approval task containing that item.

The following information is passed into the script as variables to be used to drive the approval process:

- `request` - The request object.
- `approval` - The approval task object that triggered the script; this will be null when the script is run on creation
- `glossaryItem` - The glossary entry for the requested item.

A custom script must be responsible for the following functionality in the request process:

- Creating necessary approval tasks. To create an approval task via the API within a workflow, first create a user task node within the BPMN definition. Within that node's 'create' listener, make a call to 'openidm/access-request/approval' and send the following body.
  - `requestId` - ID of request.
  - `itemIds` - List of item IDs to include in approval task (normally just the single item).
  - `approverId` - ID of approver user or group.
- Sending request notifications. To send an Access Request notification via API, use the 'openidm/notification/[NOTIFICATION_ID]' endpoint with the notification template of your choosing. Templates can be found with the accessRequestNotificationTemplates.json file in the conf directory, and any POST body to the endpoint must include any of the variables described in the template definition. For a more detailed example, refer to the Access Request Postman collection.
- Provisioning approved access. Access Request provides a provisioning endpoint (openidm/access-request/provision) for basic IDM attribute/role assignment which can be used for simple request provisioning, or a workflow can provision in another way if more appropriate. Alternatively, a provisioning approval task can be created for any required manual task.
- Sending request notifications. To send an Access Request notification via API, use the 'openidm/notification/[NOTIFICATION_ID]' endpoint with the notification template of your choosing. Templates can be found with the

accessRequestNotificationTemplates.json file in the conf directory, and any POST body to the endpoint must include any of the variables described in the template definition. For a more detailed example, please see the Access Request Postman collection.

- Provisioning approved access. Access Request provides a provisioning endpoint, `openidm/access-request/provision`, for IDM attribute/role assignment during simple request provisioning. Alternatively, you can create a provisioning task for any required manual operation.
- Setting the final outcome of the item on the request object. A request object is returned and saved with every iteration of the script, and so can be used to make any adjustments to the item's outcome within the request when a final outcome has been reached.

Every iteration of the script that is executed expects an object to be returned with two keys:

- `success` - A boolean value determining whether or not the script execution was successfully completed
- `request` - The request object, including any updates made during the script execution, which will be saved to the request.

When an item's outcome is set to a final outcome (e.g. provisioned, denied, etc.), no other action is required on the request, and it will be closed if and when any other items on the request have been completed.

Access request notifications

User notifications are sent for certain events that take place within the application.

Modifying notification templates

Notifications sent by the Access Request application are stored within the `openidm/conf/accessRequestNotificationTemplates.json` file. This file can be modified to display whatever custom message is desired for each individual notification. Modifying these templates directly will require someone with administrative privileges to edit the file within the IDM directory itself.

Templates

The following templates are used within the application:

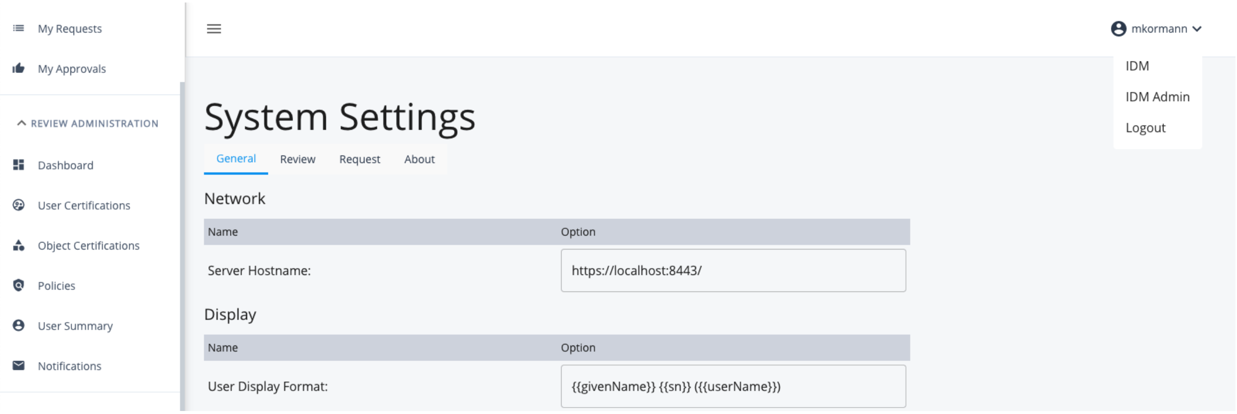
Templates

Field	Description

Field	Description
OUTCOME_UPDATE	Sent when an item or items have reached a final request decision.
APPROVAL_TASK_CREATED	Sent to approver(s) when an approval task is assigned to them.
APPROVAL_TASK_EXPIRED	Sent to the default approver group when an approval task expires and is assigned to them for review.
CONSULT_TASK_CREATED	Sent to consult(s) when added to an approval task for additional information.
CONSULT_TASK_CANCELLED	Sent to consult(s) when a consult task is cancelled.
PROVISIONING_TASK_CREATED	Sent to provisioner(s) when a manual provisioning task is assigned to them
CREATE_REQUEST_FAILED	Sent to the requester when creation of a request fails for an unknown reason.
REQUEST_CANCELLED	Sent to requester/requestee when a request has been cancelled.
APPROVAL_TASK_CANCELLED	Sent to approver(s) when an approval task has been cancelled.

System settings

Users who are assigned to either the governance-administrator or access-request-admin internal authorization role will see the System Settings tab under the Configuration subsection on the side taskbar. Navigating to this screen will allow the user to adjust any of the configuration options within the system.



System Settings

Network

Name	Option
Server Hostname:	https://localhost:8443/

Display

Name	Option
User Display Format:	{{givenName}} {{sn}} ({{userName}})

Network

Server Hostname: This field is used to define the alias for the IDM environment that is running the Identity Governance application. This setting is used in email notifications. For example, to directly link users to a request or an approval task.

User display format

User Display Format: This field is used to define the custom display format for a user within the Identity Governance module. The value set in this field is used to display usernames dynamically. Once saved, any field that leverages this property automatically updates to show the defined format.

To define a display format, simply enter the desired string into the input, using double curly braces to define a user attribute on the managed user object that you want to display. A few examples are defined below:

```
{{userName}}                            -       jsmith
{{givenName}} {{sn} {{userName}}        -       John Smith
(jsmith)
{{givenName}} {{sn}} - {{jobCode}}      -       John Smith -
AB123
{{sn}}, {{givenName}}                   -       Smith, John
```

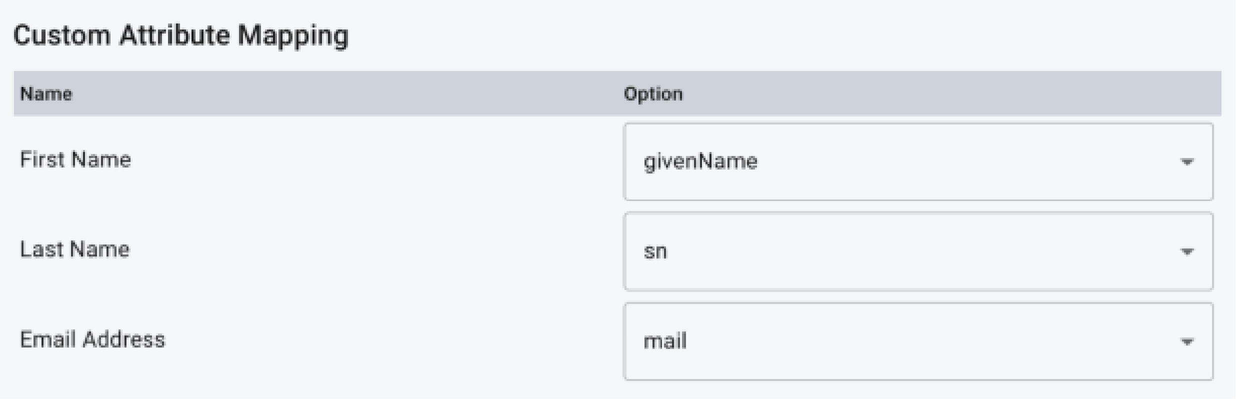
Delegation

Identity Governance allows administrators to enable a property within IDM that will be used to delegate all of a user’s tasks for certifications, violations, and approvals. If delegation is enabled and the user has a relationship to another managed user through the defined property, then delegation will occur for that user when a task is set to be assigned to them. In the event that the defined property is not a relationship property, is not a relationship property to a managed user, or is not defined for a given user, then delegation will be ignored and the user will be assigned tasks as they normally would be. When delegation does occur, it is assigned directly to the new user during task creation and will not be visible to the original intended recipient.

- **Allow User Delegation**: If enabled, the system attempts to leverage the defined User Delegation property to assign tasks.
- **User Delegation Property**: Select any property from the managed user schema that should be used to determine a user’s delegate.

Custom attribute mapping

In order to display user information throughout the user interface, ForgeRock Access Review 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.



Custom Attribute Mapping

Name	Option
First Name	givenName
Last Name	sn
Email Address	mail

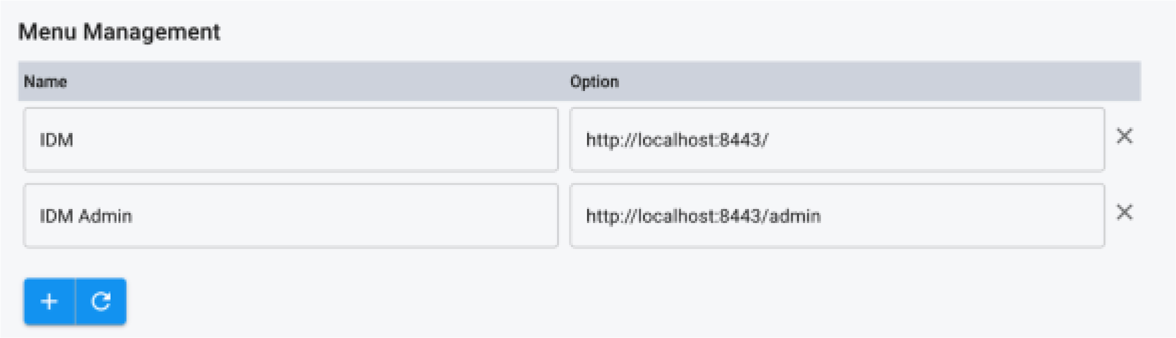
Autonomous Identity integration

For those implementations that are running Identity Governance in parallel with ForgeRock Autonomous Identity, these settings will be used to allow the application to communicate with AutoID and enable some advanced recommendations that it provides.

- **AutoID Enabled**: Whether to enable the AutoID integration.
- **AutoID URL**: Hostname of the AutoID server.
- **AutoID User**: Username of the user admin or service account to make API calls with.
- **AutoID Password**: Password of the above user/account.

Menu management

Menu management allows an administrator to add or remove links to the top-right user dropdown menu for easier navigation to other applications that would be beneficial to the end user.

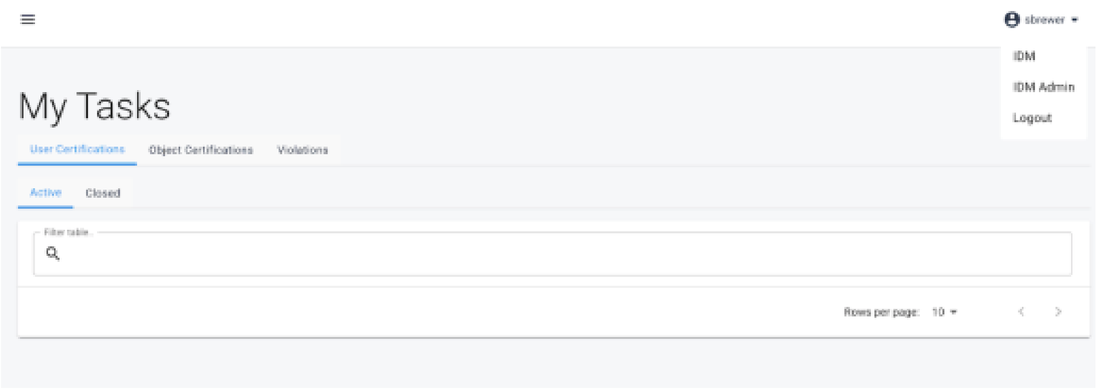


Menu Management

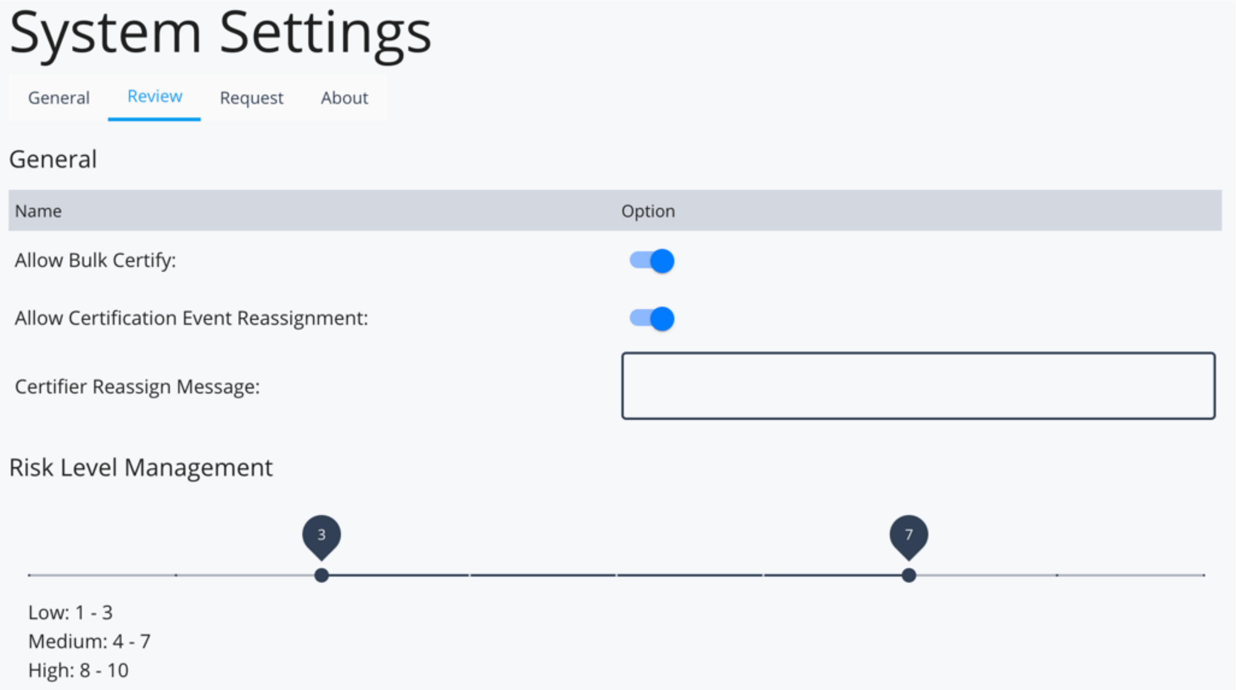
Name	Option
IDM	http://localhost:8443/
IDM Admin	http://localhost:8443/admin

> 1. To add links to the menu, select the [.label]#+" button. A new row displays for you to fill in.

2. Enter the name of the link in the name field and the URL next to it.
3. You can add multiple links at once by continuing to click the add button to show more blank rows.
4. To reset the links back to their saved value, click the reset button.
5. Once the settings have been saved, users will be able to see the navigation links in the dropdown menu at the top of the page.



Review



System Settings

General | Review | Request | About

General

Name	Option
Allow Bulk Certify:	●
Allow Certification Event Reassignment:	●
Certifier Reassign Message:	

Risk Level Management

Low: 1 - 3
Medium: 4 - 7
High: 8 - 10

- **Allow Bulk Certify**: If enabled, certifiers certify all users at once for a specific campaign. If set to False, certifiers certifies each user individually.

> NOTE
>
> It is best practice setting the **Allow Bulk Certify** option to **FALSE** to prevent certifiers from approving automatically without proper consideration.

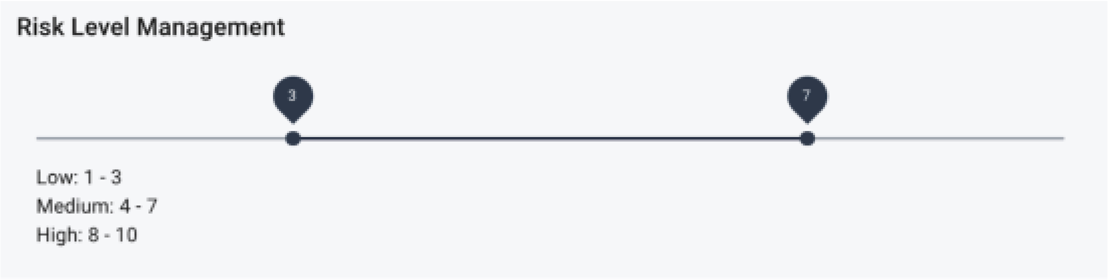
- **Allow Certification Event Reassignment**: Allow certifiers to reassign items to another user or role.

  > NOTE
  >
  > This setting is at a global level and cannot be configured on a certification basis. Administrator reassign functionality is always enabled, regardless of the value set here.

  - **Certifier Reassign Message**: When you enable **Allow Certification Event Reassignment**, configure a message for the UI to display to the certifier on the modal. The modal displays when the user attempts to reassign an item to another user or role.

Risk level management

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

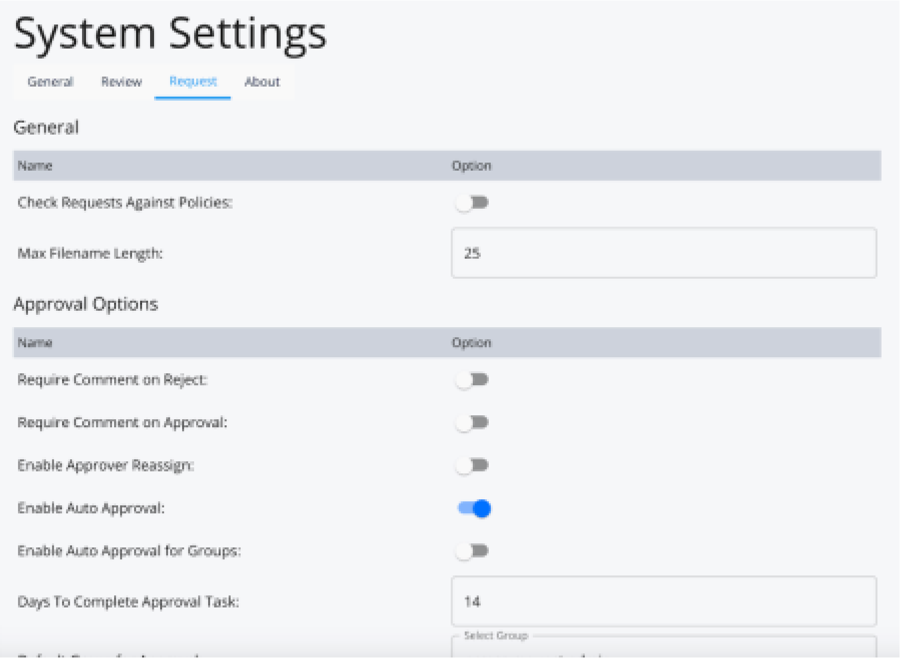


Risk Level Management

Low: 1 - 3
Medium: 4 - 7
High: 8 - 10

Drag tabs to adjust the levels of risk. As tabs move, the adjustment is reflected in the table below the bar. The leftmost tab will set the delimiter between Low risk and Medium risk, where the tab value is the inclusive upper boundary of the Low level of risk. Similarly, the rightmost tab will set the delimiter between Medium and High risk, where the tab value is the inclusive upper boundary of the Medium level of risk.

Request



System Settings

General

Name	Option
Check Requests Against Policies:	○
Max Filename Length:	25

Approval Options

Name	Option
Require Comment on Reject:	○
Require Comment on Approval:	○
Enable Approver Reassign:	○
Enable Auto Approval:	●
Enable Auto Approval for Groups:	○
Days To Complete Approval Task:	14

General

- **Check Requests Against Policies**: Enables the application to leverage policies defined in Access Review when a user attempts to submit a request. If set to true, and a user attempts to submit a request that would violate an existing policy, they will be presented an error message in the Review section of their request explaining what policy is being violated. This will block the user from submitting the request unless it is altered to meet policy conditions.
- **Max Filename Length**: Sets the max allowable size of a submitted filename in characters. Access Request saves submitted files to the IDM repository within the files table of the database. In order to increase this setting, the size of the column for filename within that table must first be increased to store longer strings of text. The default value of 25 allows Access Request to save files properly using the default value for that column as installed.

Approval options

Item	Description
Require Comment on Reject	Requires an approver to add a comment to their approval task submission for any item that they choose to reject.
Require Comment on Approval	Requires an approver to add a comment to their approval task submission for any item that they choose to approve.

Item	Description
Enable Approver Reassign	Allows approvers the ability to reassign their own tasks to another user or group.
Enable Auto Approval	If set to true, any time an approver for a task is calculated to be the same user as the one who submitted the request (e.g. a manager submits a request for their requestee, and the item requires manager approval,) that task will be auto-approved and will not require manual approval by the requester. The item will automatically advance to the next approver within its approval chain.
Enable Auto Approval for Group	If set to true, functions the same as the above setting, but applies to any approval tasks that are assigned to a group that the requester belongs to. As an example, there is a requestable item requiring approval from a manager and an admin group, and a member of that admin group submits a request for the item. The approval will go to the manager, and if approved, will then be auto-approved by the admin group that the requester belongs to.`
Days to Complete Approval Task	The number of days allowed for an approval user or group to act on an approval request before the task “expires.” Note that task expiration does not mean that the request is removed or the approval is rejected. In the event that a task is not completed by the ‘Due Date’, it will be automatically reassigned to the group defined below it with the Default Group for Approval setting. That team will then be responsible for determining which user should be given the task for completion, or alternatively cancel it.
Default Group for Approval	The group that will be assigned to handle approval tasks in the following situations: • When an approver key is set on a requestable item but can not be found during task creation (e.g. manager is not set on user, entitlementOwner that is not set on object). • When a task reaches its expiration date.
Default Approvers	This list is applied as standard approval chain for any item that is set as requestable but does not have an approvers key defined. It functions the same as the list would if it were defined the exact same way on the requestable item itself.

NOTE

NOTE

The options for enabling auto-approval and default approvers do not automatically apply to any requestable item using a custom workflow. They follow their own logic and approval process. However, they can be leveraged within those flows, if desired, by using the API to read the setting values.

Display

Item	Description
Displayable User Properties	The properties on the managed user schema that will be displayed within the popup page in requests and approval tasks when the user hovers over a user’s userName.
Displayable Item Properties	The keys on the requestable item glossary entry that will be displayed within the popup page in requests and approval tasks when the user hovers over the item’s info icon.
User Search Properties	The properties on the managed user schema that will be used to search against when a user queries for users during request creation or reassignment.
Requestable Item Search Properties	The keys on the requestable item glossary entry that will be used to search against when a user queries for items to add to request.
Requestable Item Display Format	Format used to display requestable items within the user interface. See the user display format in section User Display Format above for information on syntax.
Requestable Item Bundle Display Format	Format used to display requestable item bundles within the user interface. See the user display format in section User Display Format above for information on syntax.

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 through ForgeRock support.

Identity glossary

Users who are assigned to the glossary-admin internal authorization role will see the Glossary subsection available on the side taskbar. Navigating to this screen will allow the user to directly edit, create, or delete glossary objects within the system. This role is imperative in defining the properties on items with the IDM system that will be used as a part of Access Request. = Identity glossary

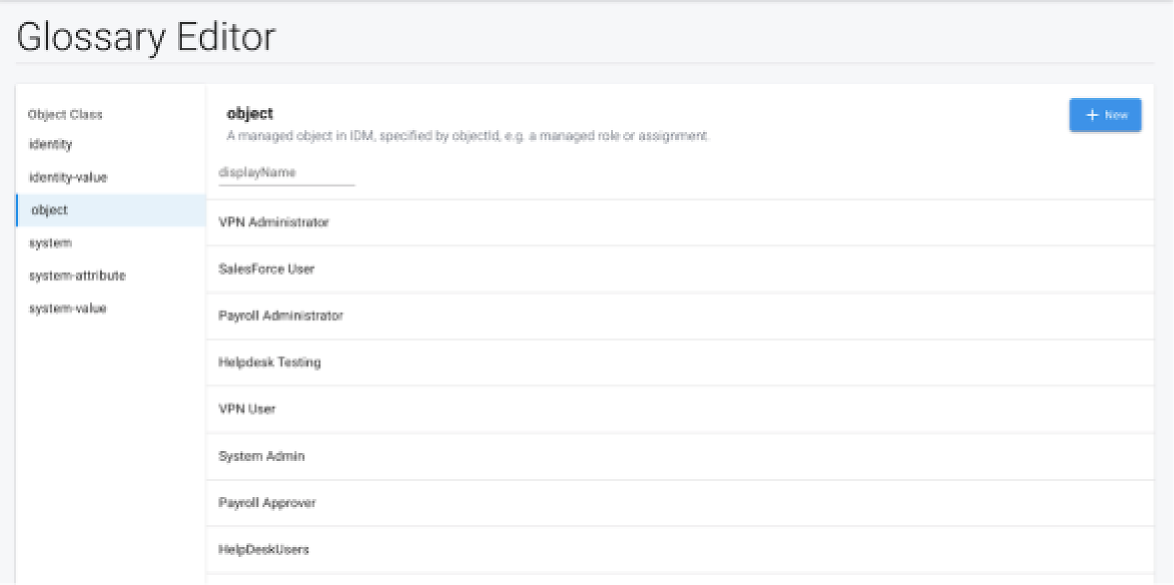
Users who are assigned to the *glossary-admin* internal authorization role will see the Glossary subsection available on the side taskbar. Navigating to this screen will allow the user to directly edit, create, or delete glossary objects within the system. This role is imperative in defining the properties on items with the IDM system that will be used as a part of Access Request. Items within the glossary are known as keys.

IMPORTANT

Glossary keys are *case_sensitive*. For example, make sure to put `requestable` and *not* `Requestable`.

Glossary Introduction

The glossary is an extensive collection of metadata that refers to any and all the identity information that is compiled and tracked by IDM. It allows administrators to store as much information as desired about any of the components described below. The data stored can directly affect some of the product functionality, or it can be as simple as arbitrary information that allows for easier maintainability and categorization of the system on a whole.



Glossary Editor

object

A managed object in IDM, specified by objectId, e.g. a managed role or assignment.

VPN Administrator

SalesForce User

Payroll Administrator

Helpdesk Testing

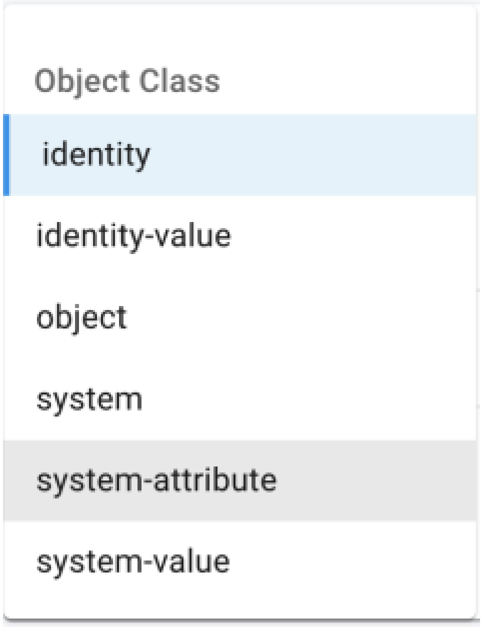
VPN User

System Admin

Payroll Approver

HelpDeskUsers

Glossary Object Classes



Object Class

identity

identity-value

object

system

system-attribute

system-value

- Identity: The user properties that exist on a managed user within IDM.
  - Examples: jobCode, department, location
  - Required Keys:
    - attributeName (string): the attribute property on the user
- Identity-Value: Specific values that are assigned to any of properties that exist on a managed user within IDM.
  - Examples: a jobCode of AT152, a status of T
  - Required Keys:
    - attributeName (string): the attribute property on the user
    - attributeValue (string): the value assigned to that property
- Object: A specific instance of a managed object within IDM. Can refer to a managed object of any type, as long as it currently exists within the system.
  - Examples: Database Administrator Role, LDAP Group Assignment
  - Required Keys:
    - objectId (managed object id): the _id of the object in IDM
    - displayName (string): the readable name of the object
    - order (array): the displayable order of the object's properties
- System: A connected external system managed by IDM
  - Examples: Active Directory, PeopleSoft
  - Required Keys:
    - name (string): the name of the connected system
- System-Attribute: A user property within the external connected system.
  - Examples: ldapGroups, cn

    - Required Keys:
        - system (string): the name of the connected system that tracks this attribute
        - objectType (string): the object type of the attribute (e.g. account or group)
        - attributeName (string): the name of the attribute
        - order (integer): numeric ranking used to determine display order
- System-Value: Specific values that are assigned to any of properties that exist on an external connected system.
    - Examples: a jobCode of AT152, a status of T
    - Required Keys:
        - system (string): the name of the connected system that tracks this attribute
        - objectType (string): the object type of the attribute (e.g. account or group)
        - attributeName (string): the name of the attribute
        - attributeValue (string): the value assigned to that attribute

Selecting a Glossary Object Class

Using the available select list, administrators will be able to view a single glossary object class at a time within the glossary editor interface. Once a class is chosen, the table will display existing glossary entries that pertain to that class in a searchable and paginated fashion. The table includes text inputs that allow you to further filter the results by properties such as name, attributeValue, system, and more. There are also pagination controls available near the bottom of the table, that allow admins to control how many entries they see at a given time.

Creating a New Glossary Entry

Once a glossary object class is selected, clicking the “New” button will display a blank form to the administrator, with all of the required keys pre-populated and awaiting entry. Note that next to each required key, the type of metadata is also pre-populated, and is locked to the required type for that entry. These fields must all be completed before a glossary entry will be allowed to be saved.

In order to add a new metadata key to the glossary object, simply add the key name to the empty input box below the existing keys marked ‘New key’ and then click on the ‘+’ icon. Doing so will add the new key to the list of entries, which will then make it editable. Each entry row has multiple inputs, the number of which may vary depending on the type selected. Firstly, the delete icon next to non-required keys will allow admins to remove the corresponding key from the object. Next to that icon is the key itself, which is followed by the entry type selector, which allows the admin to define the type of data being entered. The choices for this selector are as follows:

- String
- Boolean
- Integer
- Managed Object
- Object
- Array
- Date

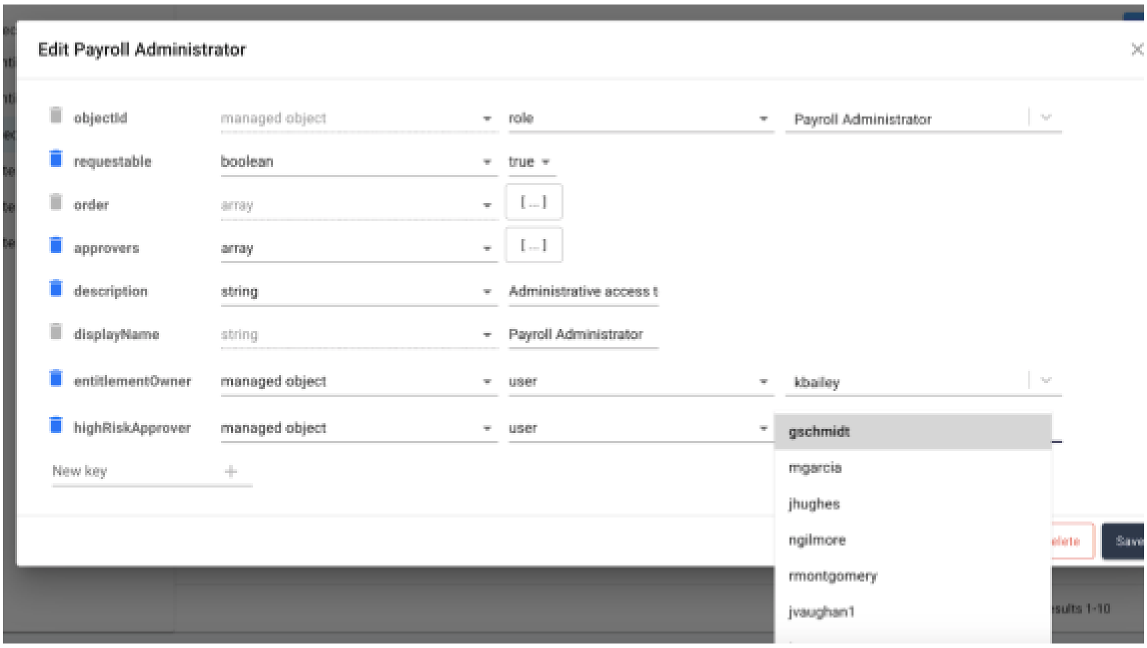
NOTE

Entries of type Managed Object will allow the admin to further choose the type of object being entered, and once the type is selected will actually query the IDM system for objects of that type. The fields for which this input box queries against per managed object is defined in the commons.json file located in the openidm/conf directory. The initial configuration of commons.json contains the IDM OOTB attributes for user, role, and assignment only. In order to add entries for different custom managed objects, each object must be added to commons.json in order for it to be an available choice for a new glossary entry.

Once all entries have been added and the entry is complete, clicking on the Save button will save the entry to the glossary.

Editing an Existing Glossary Entry

In order to edit an existing entry, simply locate the entry desired within the search table of the editor, and click on its row. Doing so will display the editor form, much like when creating a new entry, but with the current metadata populated within the form.



Edit Payroll Administrator

objectId	managed object	role	Payroll Administrator
requestable	boolean	true	
order	array	[...]	
approvers	array	[...]	
description	string	Administrative access t	
displayName	string	Payroll Administrator	
entitlementOwner	managed object	user	kbailey
highRiskApprover	managed object	user	

Deleting a Glossary Entry

In order to delete an existing glossary entry, click on the entry in question in order to display the edit glossary entry form for the object. Once populated, clicking delete will allow the entry to be removed.

Reserved Keys

While the glossary editor will allow the user to enter in nearly any value as a key within the glossary object, the admin should take note that there are certain keys that are leveraged across different products to provide different levels of functionality. Examples of these include the key approvers for Access Request and riskLevel for Access Review. Glossary admins should be aware of any keys used throughout other applications before creating new key entries to avoid potential conflicts. The full list of reserved keys used by Identity Governance can be found within the respective Access Review and Access Request sections.