

# API guide

---

This guide is targeted to developers who want to access Identity Governance using the REST Application Programming Interface (API).



## **About the API**

Learn about the Identity Governance API.



## **Access Request endpoints**

Learn how to access the Access Request endpoints.



## **Access Review endpoints**

Learn how to access the Access Review endpoints.

# Access request

---

The following are Identity Governance API Access Request endpoints:

## access-request/user

Requests against the /user endpoint

### **GET Get User**

Allows end users to query against user population

Endpoint

Endpoint

```
{{idmRoot}}/access-request/user?queryString=john
```

Headers

```
X-OpenIDM-Username    {{endUserUsername}}
X-OpenIDM-Password    {{endUserPassword}}
Content-Type           application/json
```

Params

```
queryString           John
_fields
_pageSize
_pagedResultsOffser
_sortKeys
```

Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-
request/user?queryString=John' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password:
{{endUserPassword}}' \
--header 'Content-Type: application/json'
```

### **GET** *Get Visible Requestees*

Retrieves the list of user IDs that the authenticated user is allowed to see access for (themselves and their direct reports)

Endpoint

```
{{+idmRoot}}/access-request/user/requestees
```

Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Params

- \_fields**
- \_pageSize**
- \_pagedResultsOffser**
- \_sortKeys**

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-request/user/requestees' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json'
```

### **GET** *Get User BY Id*

Allow end-users to query a specific user.

#### Endpoint

```
{{idmRoot}}/access-request/user/{{targetUserId}}
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-
request/user/{{targetUserId}}' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json'
```

## access-request/item

Requests against the /item endpoint

### **GET** Get Item

Allows end users to query individual items.

#### Endpoint

```
{{idmRoot}}/access-request/item?queryString=Admin
```

#### Headers

```
X-OpenIDM-Username  {{endUserUsername}}
X-OpenIDM-Password {{endUserPassword}}
Content-Type       application/json
```

#### Params

```
queryString          Admin
_fields
_pageSize
_pagedResultsOffser
_sortKeys
```

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-
request/item?queryString=Admin' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
```

```
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json'
```

### **GET** *Get Item By Id*

Allows end users to query a specific item.

Endpoint

```
{{idmRoot}}/access-request/{{itemId}}
```

Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	<b>application/json</b>

Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-  
request/item/{{itemId}}' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json'
```

### **POST** *Get Request Fields For Item*

Given a glossary item ID, return the fields that can be submitted with a request for that item.

Endpoint

```
{{idmRoot}}/access-request/item/fields/{{itemId}}
```

Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}

**Content-Type** application/json

Body raw

```
{}
```

Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-request/item/fields/{{itemId}}' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{}'
```

### **POST** *Get Request Fields For Items*

Given a list of glossary item IDs, return the fields that can be submitted with a request for those items.

Endpoint

```
{{idmRoot}}/access-request/item/fields
```

Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

Body raw

```
{
  "itemIds": [
    "e7997f97-cd00-4f16-b566-01879185eb2e",
    "c336c6a5-da19-4078-8ba5-3a297c605564"
  ]
}
```

```
    ]  
  }  
}
```

### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-  
request/item/fields' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
    "itemIds": [  
        "e7997f97-cd00-4f16-b566-01879185eb2e",  
        "c336c6a5-da19-4078-8ba5-3a297c605564"  
    ]  
}'
```

## access-request/bundle

Requests against the /bundle endpoint.

### **GET** Get Bundle

Allows end users to query requestable bundles.

#### Endpoint

```
{{idmRoot}}/access-request/bundle?queryString=Admin
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Params

```
queryString      Admin
_fields
_pageSize
_pagedResultsOffser
_sortKeys
```

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-
request/bundle?queryString=Admin' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json'
```

### **GET** *Get Bundle By Id*

Allows end users to query a specific requestable bundle.

#### Endpoint

```
**{{idmRoot}}/access-request/bundle/{{bundleId}}
```

#### Headers

```
X-OpenIDM-Username    {{endUserUsername}}
X-OpenIDM-Password  {{endUserPassword}}
Content-Type        application/json
```

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-
request/bundle/{{bundleId}}' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json'
```

### **POST** *Create Bundle*



Allows end users to query a specific requestable bundle.

#### Endpoint

```
**{{idmRoot}}/access-request/bundle/{{bundleId}}
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Body raw

```
{
  "name": "Administrator Bundle",
  "description": "Collection of administrator roles",
  "class": "requestable-item-bundle",
  "constraints": {},
  "itemIds": [
    "{{itemId}}",
    "{{itemId2}}"
  ]
}
```

#### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/bundle' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "name": "Administrator Bundle",
  "description": "Collection of administrator roles",
  "class": "requestable-item-bundle",
  "constraints": {},
  "itemIds": [
    "{{itemId}}",
```

```
        "{{$itemId2}}"
    ]
}'
```

### **POST Update Bundle**

Update an existing bundle definition.

#### Endpoint

```
**{{$idmRoot}}/access-request/bundle/{{$bundleId}}?
_action=update
```

#### Headers

<b>X-OpenIDM-Username</b>	{{\$arAdminUsername}}
<b>X-OpenIDM-Password</b>	{{\$arAdminPassword}}
<b>Content-Type</b>	application/json

#### Params Body raw

<b>_action</b>	update
----------------	--------

#### Body raw

```
{
  "_id": "{{$bundleId}}",
  "name": "Administrator Bundle",
  "description": "Collection of administrator roles",
  "class": "requestable-item-bundle",
  "constraints": {},
  "itemIds": [
    "{{$itemId}}",
    "{{$itemId2}}"
  ]
}
```

## Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/bundle/{{bundleId}}?_action=update' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
    "_id": "{{bundleId}}",
    "name": "Administrator Bundle",
    "description": "Collection of administrator roles",
    "class": "requestable-item-bundle",
    "constraints": {},
    "itemIds": [
        "{{itemId}}",
        "{{itemId2}}"
    ]
}'
```

## **DEL Delete Bundle**

Allows end users to delete a specific requestable bundle.

### Endpoint

```
**{{idmRoot}}/access-request/bundle/{{bundleId}}
```

### Headers

<b>X-OpenIDM-Username</b>	{{arAdminUsername}}
<b>X-OpenIDM-Password</b>	{{arAdminPassword}}
<b>Content-Type</b>	application/json

### Body raw

```
{}
```

## Example Request

```
curl --location -g --request DELETE '{{idmRoot}}/access-
request/bundle/{{bundleId}}' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{}'
```

## access-request/requestFields

Requests against the /requestFields endpoint.

### **GET** *Get Request Fields*

Query for defined request fields that can be assigned to any requestable item.

#### Endpoint

```
{{idmRoot}}/access-request/requestFields?
pageSize=10&pageNumber=0
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Params

<b>pageSize</b>	10
<b>pageNumber</b>	0
<b>sortBy</b>	
<b>q</b>	(filter term)
<b>name</b>	(match name property)

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-
request/requestFields?pageSize=10&pageNumber=0' \
```

```
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \  
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \  
--header 'Content-Type: application/json'
```

### **POST** Create Request Field

Create a request field that can be assigned to any requestable item.

#### Endpoint

```
{{idmRoot}}/access-request/requestFields?_action=create
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Params

<b>_action</b>	<b>create</b>
----------------	---------------

#### Body raw

```
{  
  "name": "Justification",  
  "description": "Reason for requesting this access",  
  "inputType": "text",  
  "required": true  
}
```

#### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-  
request/requestFields?_action=create' \  
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \  
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \  

```

```
--header 'Content-Type: application/json' \  
--data-raw '{  
  "name": "Justification",  
  "description": "Reason for requesting this access",  
  "inputType": "text",  
  "required": true  
'
```

### **POST** Create Request Field - 2

Create a request field that can be assigned to any requestable item.

Endpoint

```
{{idmRoot}}/access-request/requestFields?_action=create
```

Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

Params

<b>_action</b>	<b>create</b>
----------------	---------------

Body raw

```
{  
  "name": "Location",  
  "description": "Choose the location at which you are  
working",  
  "inputType": "radio",  
  "inputOptions": [  
    "New York",  
    "Miami"  
  ],  
}
```

```
"required": true
}
```

#### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/requestFields?_action=create' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "name": "Location",
  "description": "Choose the location at which you are
working",
  "inputType": "radio",
  "inputOptions": [
    "New York",
    "Miami"
  ],
  "required": true
}'
```

#### **POST** Update Request Field

Update a request field that can be assigned to any requestable item.

#### Endpoint

```
{{idmRoot}}/access-
request/requestFields//{{requestfieldid}}?_action=update
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Params

**\_action**                      **update**

#### Body raw

```
{
  "name": "Justification",
  "description": "Reason for requesting this access",
  "inputType": "text",
  "required": true
}
```

#### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/requestFields/{{requestfieldid}}?_action=update' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "name": "Justification",
  "description": "Reason for requesting this access",
  "inputType": "text",
  "required": true
}'
```

### **POST** *Delete Request Field*

Delete a request field that can be assigned to any requestable item.

#### Endpoint

```
{{idmRoot}}/access-
request/requestFields//{{requestfieldid}}?_action=update
```

#### Headers

<b>X-OpenIDM-Username</b>	<b>{{endUserUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{endUserPassword}}</b>



**Content-Type**                    application/json

Params

**\_action**                        delete

Body raw

```
{
  "fieldIds": [
    "{{requestfieldid}}"
  ]
}
```

Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/requestFields?_action=delete' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "fieldIds": [
    "{{requestfieldid}}"
  ]
}'
```

## access-request/requestable

Requests against the /requestable endpoint.

### **GET** Get Requestable Item

Query requestable item (item or bundle) by its ID.

Endpoint

```
{{idmRoot}}/access-request/requestable/{{itemId}}
```

## Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

## Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-  
request/requestable/{{itemId}}' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json'
```

## **GET** *Get Requestable Items*

Query requestable items (item or bundle).

## Endpoint

```
{{idmRoot}}/access-request/requestable
```

## Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

## Params

<b>userId</b>	Check the requestable item's against the user to see if they are assigned to them.
---------------	--

## Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-
request/requestable' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json'
```

## access-request/approval

Requests against the /approval endpoint.

### **GET** *Get Approval*

Get an approval task its ID.

#### Endpoint

```
{{idmRoot}}/access-request/approval/{{approvalTaskId}}
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-
request/approval/{{approvalTaskId}}' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json'
```

### **GET** *Get Approvals*

Get approval tasks assigned to user.

#### Endpoint

```
{{idmRoot}}/access-request/approval?  
pageSize=10&pageNumber=0
```

#### Headers

```
X-OpenIDM-Username    {{endUserUsername}}  
X-OpenIDM-Password    {{endUserPassword}}  
Content-Type          application/json
```

#### Params

```
pageSize              10  
pageNumber            0  
_fields  
sortBy  
requesteeId  
requesterId  
itemId  
id
```

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-  
request/approval?pageSize=10&pageNumber=0' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json'
```

### **GET** *Get Approval Count*

Get current number of active approval tasks assigned to user.

#### Endpoint

```
{{idmRoot}}/access-request/approval?getResultCount=true
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Params

<b>_fields</b>	
<b>sortBy</b>	
<b>requesteeId</b>	
<b>requesterId</b>	
<b>itemId</b>	
<b>getResultCount</b>	<b>true</b>

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-request/approval?getResultCount=true' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json'
```

### **GET** *Get Approvals - Admin*

Get approval tasks, as administrator.

#### Endpoint

```
{{idmRoot}}/access-request/approval?  
pageSize=10&pageNumber=0
```

#### Headers

<b>X-OpenIDM-Username</b>	{{arAdminUsername}}
<b>X-OpenIDM-Password</b>	{{arAdminPassword}}
<b>Content-Type</b>	application/json

#### Params

```
pageSize          10
pageNumber        0
_fields
sortBy
approverId
requesterId
requesteeId
itemId
id
```

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-
request/approval/admin?pageSize=10&pageNumber=0' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json'
```

### **POST** Create Approval Task

Manually create an approval task. For use within custom workflows.

#### Endpoint

```
{{idmRoot}}/access-
request/requestFields//{{requestFieldId}}?_action=update
```

#### Headers

```
X-OpenIDM-Username    {{arAdminUsername}}
X-OpenIDM-Password    {{arAdminPassword}}
Content-Type           application/json
```

#### Body raw

```
{
  "requestId": "{{requestId}}",
  "itemIds": [
```

```
        "{{itemId}}"
    ],
    "approverId": "{{approverId}}",
    "workflowTaskId": "{{workflowTaskId}}"
}
```

#### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/requestFields?_action=delete' \
curl --location -g --request POST '{{idmRoot}}/access-
request/approval' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "requestId": "{{requestId}}",
  "itemIds":[
    "{{itemId}}"
  ],
  "approverId": "{{approverId}}",
  "workflowTaskId": "{{workflowTaskId}}"
}'
```

### **POST** *Get Autonomous Identity Recommendations For Use*

Queries Autonomous Identity to get recommendations for entitlements for the given user.

#### Endpoint

```
{{idmRoot}}/access-request/approval?
_action=getRecommendations
```

#### Headers

<b>X-OpenIDM-Username</b>	<b>{{arAdminUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{arAdminPassword}}</b>
<b>Content-Type</b>	<b>application/json</b>

## Params

<code>_action</code>	<code>getRecommendations</code>
----------------------	---------------------------------

## Body raw

```
{
  "userId": "{{requestId}}",
  "entitlements": [
    "{{itemId}}"
  ]
}
```

## Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/approval?_action=getRecommendations' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "userId": "{{requestId}}",
  "entitlements": [
    "{{itemId}}"
  ]
}'
```

## **GET** Get Approval Repository Object

Directly read an approval task from the repository. Also, supports PUT and DELETE operations.

## Endpoint

```
{{idmRoot}}/repo/governance/approvalTask/
{{approvalTaskId}}
```

## Headers



<b>X-OpenIDM-Username</b>	{{idmAdminUsername}}
<b>X-OpenIDM-Password</b>	{{idmAdminPassword}}
<b>Content-Type</b>	application/json

#### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/repo/governance/approvalTask/{{approvalTaskId}}' \
--header 'X-OpenIDM-Username: {{idmAdminUsername}}' \
--header 'X-OpenIDM-Password: {{idmAdminPassword}}' \
--header 'Content-Type: application/json'
```

### **GET** Query Approval Repository Objects

Query the repository objects for approval tasks directly.

#### Endpoint

```
{{idmRoot}}/repo/governance/approvalTask?_queryFilter=true
```

#### Headers

<b>X-OpenIDM-Username</b>	{{idmAdminUsername}}
<b>X-OpenIDM-Password</b>	{{idmAdminPassword}}
<b>Content-Type</b>	application/json

#### Example Request

```
_queryFilter      true
```

#### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/repo/governance/approvalTask?
_queryFilter=true' \
```

```
--header 'X-OpenIDM-Username: {{idmAdminUsername}}' \  
--header 'X-OpenIDM-Password: {{idmAdminPassword}}' \  
--header 'Content-Type: application/json'
```

## access-request/request

Requests against the /request endpoint.

### **POST** Cancel Request(s)

As an access request administrator, requester, or requestee, cancel the requests provided.

#### Endpoint

```
{{idmRoot}}/access-request/request?_action=cancel
```

#### Headers

<b>X-OpenIDM-Username</b>	{{arAdminUsername}}
<b>X-OpenIDM-Password</b>	{{arAdminPassword}}
<b>Content-Type</b>	application/json

#### Params

<b>_action</b>	cancel
----------------	--------

#### Body raw

```
{  
  "requestIds": [  
    "{{requestId}}"  
  ]  
}
```

#### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request?_action=cancel' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
    "requestIds": [
        "{{requestId}}"
    ]
}'
```

### **POST** Create Request

Create a request for access.

Endpoint

```
{{idmRoot}}/access-request/request
```

Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

Body raw

```
{
  "userIds": [
    "1sasdaf97-cd00-4f16-b566-01879185eb2e"
  ],
  "items": [
    {
      "itemId": "{{itemId}}",
      "requestType": "add",
      "fields": {
      }
    }
  ],
}
```

```
"comment": "Comment"
}
```

#### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "userIds":[
    "1sasdaf97-cd00-4f16-b566-01879185eb2e"
  ],
  "items":[
    {
      "itemId":"{{itemId}}",
      "requestType":"add",
      "fields": {

      }
    }
  ],
  "comment": "Comment"
}'
```

#### **POST** Create Request Policy Check

Given a create request payload, check whether the request would result in any policy violations.

#### Endpoint

```
{{idmRoot}}/access-request/request/policy
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

### Body raw

```
{
  "userIds":[
    "222"
  ],
  "items":[
    {
      "itemId":"managed/role/2007",
      "requestType":"add"
    }
  ]
}
```

### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request/policy' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "userIds":[
    "222"
  ],
  "items":[
    {
      "itemId":"managed/role/2007",
      "requestType":"add"
    }
  ]
}'
```

### **GET** Get Requests

Get requests for the user.

### Endpoint

```
{{idmRoot}}/access-request/request?  
status=active&pageSize=10&pageNumber=0
```

#### Headers

```
X-OpenIDM-Username    {{endUserUsername}}  
X-OpenIDM-Password    {{endUserPassword}}  
Content-Type          application/json
```

#### Params

```
status                active  
pageSize              10  
pageNumber            0  
sortBy  
approverId  
requesteeId  
requesterId  
itemId  
id
```

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-  
request/request?status=active&pageSize=10&pageNumber=0' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json'
```

### **GET** *Get Requests - Admin*

Get requests as an administrator.

#### Endpoint

```
{{idmRoot}}/access-request/request/admin?  
status=active&pageSize=10&pageNumbe
```

## Headers

<b>X-OpenIDM-Username</b>	{{arAdminUsername}}
<b>X-OpenIDM-Password</b>	{{arAdminPassword}}
<b>Content-Type</b>	application/json

## Params

<b>status</b>	active
<b>pageSize</b>	10
<b>pageNumber</b>	0
<b>sortBy</b>	
<b>approverId</b>	
<b>requesteeId</b>	
<b>requesterId</b>	
<b>itemId</b>	
<b>id</b>	

## Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-request/request/admin?status=active&pageSize=10&pageNumber=' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json'
```

## **GET** Get Request

Get requests by ID..

## Endpoint

```
{{idmRoot}}/access-request/request/{{requestId}}
```

## Headers

<b>X-OpenIDM-Username</b>	{{arAdminUsername}}
<b>X-OpenIDM-Password</b>	{{arAdminPassword}}
<b>Content-Type</b>	application/json

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-  
request/request/{{requestId}}' \  
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \  
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \  
--header 'Content-Type: application/json'
```

### **GET** *Get Request Repository Object*

Read a request object directly from the repository. Also, supports PUT and DELETE operations.

#### Endpoint

```
{{idmRoot}}/repo/governance/request?_queryFilter=true
```

#### Headers

<b>X-OpenIDM-Username</b>	{{idmAdminUsername}}
<b>X-OpenIDM-Password</b>	{{idmAdminPassword}}
<b>Content-Type</b>	application/json

#### Params

<b>_queryFilter</b>	<b>true</b>
---------------------	-------------

#### Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/repo/governance/request?_queryFilter=true' \  
--header 'X-OpenIDM-Username: {{idmAdminUsername}}' \  

```



```
--header 'X-OpenIDM-Password: {{idmAdminPassword}}' \  
--header 'Content-Type: application/json'
```

### **GET** Query Request Repository Objects

Query repository for request objects directly.

Endpoint

```
{{idmRoot}}/repo/governance/request?_queryFilter=true
```

Headers

<b>X-OpenIDM-Username</b>	{{idmAdminUsername}}
<b>X-OpenIDM-Password</b>	{{idmAdminPassword}}
<b>Content-Type</b>	application/json

Params

<b>_queryFilter</b>	<b>true</b>
---------------------	-------------

Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/repo/governance/request?_queryFilter=true' \  
--header 'X-OpenIDM-Username: {{idmAdminUsername}}' \  
--header 'X-OpenIDM-Password: {{idmAdminPassword}}' \  
--header 'Content-Type: application/json'
```

### **POST** Reassign Approval Task

Reassign a task to a new user/group

Endpoint

```
{{idmRoot}}/access-request/request?_action=reassign
```

## Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

## Params

<b>_action</b>	<b>reassign</b>
----------------	-----------------

## Body raw

```
{
  "approvalIds": [
    "{{approvalTaskId}}"
  ],
  "newApproverId": "managed/user/211"
}
```

## Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request?_action=reassign' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "approvalIds": [
    "{{approvalTaskId}}"
  ],
  "newApproverId": "managed/user/211"
}'
```

### **POST** Consult Approval Task

Add a consulting user/group to the approval task

## Endpoint

```
{{idmRoot}}/access-request/request?_action=consult
```

#### Headers

```
X-OpenIDM-Username    {{endUserUsername}}
X-OpenIDM-Password    {{endUserPassword}}
Content-Type           application/json
```

#### Params

```
_action                consult
```

#### Body raw

```
{
  "approvalIds": [
    "{{approvalTaskId}}"
  ],
  "consultId": "managed/user/235"
}
```

#### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request?_action=consult' \
--header 'X-OpenIDM-Username: {{endUserPassword}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "approvalIds": [
    "{{approvalTaskId}}"
  ],
  "consultId": "managed/user/235"
}'
```

Cancel a consulting user/group to the approval task

#### Endpoint

```
{{idmRoot}}/access-request/request?_action=cancelconsult
```

#### Headers

<b>X-OpenIDM-Username</b>	<b>{{endUserUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{endUserPassword}}</b>
<b>Content-Type</b>	<b>application/json</b>

#### Params

<b>_action</b>	<b>cancelconsult</b>
----------------	----------------------

#### Body raw

```
{
  "approvalIds": [
    "{{approvalTaskId}}"
  ]
}
```

#### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request?_action=cancelconsult' \
--header 'X-OpenIDM-Username: {{endUserPassword}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "approvalIds": [
    "{{approvalTaskId}}"
  ]
}'
```

## POST Upload File To Request

Upload file to a given request. Optionally provide itemIds within the request that the file are specific to.

### Endpoint

```
{{idmRoot}}/access-request/request?_action=upload
```

### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

### Params

<b>_action</b>	<b>upload</b>
----------------	---------------

### Body raw

```
{
  "requestId": "{{requestId}}",
  "itemIds": [
    "{{itemId}}"
  ],
  "fileName": "report.pdf",
  "fileType": "text/plain",
  "content": "dGhpcyBpcyBhIGZpbGU="
}
```

### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request?_action=upload' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
```

```
--data-raw '{
  "requestId": "{{requestId}}",
  "itemIds": [
    "{{itemId}}"
  ],
  "fileName": "report.pdf",
  "fileType": "text/plain",
  "content": "dGhpcyBpcyBhIGZpbGU="
}'
```

### GET Download File From Request

Download a file from a request given a request ID and file name.

#### Endpoint

```
{{idmRoot}}/access-request/request/download?
fileName&requestId
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Params

<b>fileName</b>	Name of file
<b>requestId</b>	ID of request file is attached to

#### Example Request

```
curl --location -g --request GET '{{idmRoot}}/access-
request/request/download?fileName=&requestId=' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json'
```

## POST Download File From Request

Download a file from a given request

### Endpoint

```
{{idmRoot}}/access-request/request?_action=download
```

### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

### Params

<b>_action</b>	<b>download</b>
----------------	-----------------

### Body raw

```
{
  "requestId": "{{requestId}}",
  "fileName": "report.pdf"
}
```

### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request?_action=download' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "requestId": "{{requestId}}",
  "fileName": "report.pdf"
}'
```

## **POST** Delete File From Request

Remove a file from a given request

### Endpoint

```
{{idmRoot}}/access-request/request?_action=removeFile
```

### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

### Params

<b>_action</b>	<b>removeFile</b>
----------------	-------------------

### Body raw

```
{
  "requestId": "{{requestId}}",
  "fileName": "report.pdf"
}
```

### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request?_action=removeFile' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "requestId": "{{requestId}}",
  "fileName": "report.pdf"
}'
```



## POST Comment on Request

Comment on a request. Optionally provide the specific items within the request that this comment will apply to.

### Endpoint

```
{{idmRoot}}/access-request/request?_action=comment
```

### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

### Params

<b>_action</b>	<b>removeFile</b>
----------------	-------------------

### Body raw

```
{
  "requestId": "{{requestId}}",
  "itemIds": [
    "{{itemId}}"
  ],
  "comment": "Comment",
  "isHidden": false
}
```

### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request?_action=comment' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
```

```
"requestId": "{{requestId}}",
"itemIds": [
    "{{itemId}}"
],
"comment": "Comment",
"isHidden": false
}'
```

### **POST** Complete Approval Task

Complete an approval task as the approver. This endpoint with action 'complete' requires individual item decisions to be included in the request body.

#### Endpoint

```
{{idmRoot}}/access-request/request/approval?
_action=complete
```

#### Headers

<b>X-OpenIDM-Username</b>	{{endUserUsername}}
<b>X-OpenIDM-Password</b>	{{endUserPassword}}
<b>Content-Type</b>	application/json

#### Params

<b>_action</b>	<b>complete</b>
----------------	-----------------

#### Body raw

```
{
  "approvalId": "{{approvalTaskId}}",
  "approvalData": [
    {
      "itemId": "{{itemId}}",
      "outcome": "approved"
    }
  ]
}
```

```
    ]  
  }  
}
```

### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-  
request/request/approval?_action=complete' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
    "approvalId": "{{approvalTaskId}}",  
    "approvalData": [  
        {  
            "itemId": "{{itemId}}",  
            "outcome": "approved"  
        }  
    ]  
}'
```

### **POST** Complete Approval Task - Approval All

Complete an approval task as the approver. This endpoint with action 'complete' requires individual item decisions to be included in the request body.

#### Endpoint

```
{{idmRoot}}/access-request/request/approval?  
_action=approved
```

#### Headers

<b>X-OpenIDM-Username</b>	<b>{{endUserUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{endUserPassword}}</b>
<b>Content-Type</b>	<b>application/json</b>

#### Params

**\_action**                      **approval**

Body raw

```
{
    "approvalId": "{{approvalTaskId}}",
    "comment": "Comment"
}
```

Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request/approval?_action=approved' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
    "approvalId": "{{approvalTaskId}}",
    "comment": "Comment"
}'
```

### **POST Complete Approval Task - Reject All**

Complete an approval task, rejecting all of the task's items.

Endpoint

```
{{idmRoot}}/access-request/request/approval?
_action=rejected
```

Headers

<b>X-OpenIDM-Username</b>	<b>{{endUserUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{endUserPassword}}</b>
<b>Content-Type</b>	<b>application/json</b>

Params

**\_action**                      **rejected**

Body raw

```
{
  "approvalId": "{{approvalTaskId}}",
  "comment": "Comment"
}
```

Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/request/approval?_action=rejected' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "approvalId": "{{approvalTaskId}}",
  "comment": "Comment"
}'
```

### **POST** Update Request's Items

Complete an approval task, rejecting all of the task's items.

Endpoint

```
{{idmRoot}}/access-request/request/{{requestId}}?
_action=asd
```

Headers

<b>X-OpenIDM-Username</b>	<b>{{endUserUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{endUserPassword}}</b>
<b>Content-Type</b>	<b>application/json</b>

Params

**\_action**

**asdasd**

Body raw

```
{
  "items": [
    {
      "itemId": "40b83cb6-1749-48eb-9c89-2a3b1fae71ab",
      "fields": [],
      "timesApproved": 2,
      "outcome": "provisioned"
    }
  ]
}
```

Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-request/request/{{requestId}}?_action=asdasd' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "items": [
    {
      "itemId": "40b83cb6-1749-48eb-9c89-2a3b1fae71ab",
      "fields": [],
      "timesApproved": 2,
      "outcome": "provisioned"
    }
  ]
}'
```

## access-request/notification

Requests against the /notification endpoint.

### **POST** Send Notification

As an access request administrator, send any of the defined Request notifications. To be used within custom workflows if notifications need to be sent at a certain juncture.

#### Endpoint

```
{{idmRoot}}/access-  
request/notification/APPROVAL_TASK_CREATED/{{approvalTaskId  
}}
```

#### Headers

<b>X-OpenIDM-Username</b>	{{arAdminUsername}}
<b>X-OpenIDM-Password</b>	{{arAdminPassword}}
<b>Content-Type</b>	application/json

#### Body raw

```
{}
```

#### Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-  
request/notification/APPROVAL_TASK_CREATED/{{approvalTaskId  
}}' \  
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \  
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \  
--header 'Content-Type: application/json' \  
--data-raw '{}'
```

## access-request/provision

Requests against the /provision endpoint.

### **POST Provision Access From Request**

As an access request administrator, send any of the defined Request notifications. To be used within custom workflows if notifications need to be sent at a certain juncture.

## Endpoint

```
{{idmRoot}}/access-request/provision
```

## Headers

<b>X-OpenIDM-Username</b>	{{arAdminUsername}}
<b>X-OpenIDM-Password</b>	{{arAdminPassword}}
<b>Content-Type</b>	application/json

## Body raw

```
{
  "requestId": "{{requestId}}",
  "itemId": "{{itemId}}",
  "requestType": "add"
}
```

## Example Request

```
curl --location -g --request POST '{{idmRoot}}/access-
request/provision' \
--header 'X-OpenIDM-Username: {{arAdminUsername}}' \
--header 'X-OpenIDM-Password: {{arAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "requestId": "{{requestId}}",
  "itemId": "{{itemId}}",
  "requestType": "add"
}'
```

## commons/glossary

Requests against the commons/glossary endpoint.

### **GET** *Get Workflow Definitions*

Query IDM for the available workflow definitions. Used for front-end forms.



## Endpoint

```
{{idmRoot}}/commons/workflow
```

## Headers

<b>X-OpenIDM-Username</b>	{{idmAdminUsername}}
<b>X-OpenIDM-Password</b>	{{idmAdminPassword}}
<b>Content-Type</b>	application/json

## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/commons/workflow' \
--header 'X-OpenIDM-Username: {{idmAdminUsername}}' \
--header 'X-OpenIDM-Password: {{idmAdminPassword}}' \
--header 'Content-Type: application/json'
```

## **GET** Get Glossary Entry By ID

Read a specific glossary entry.

## Endpoint

```
{{idmRoot}}/commons/glossary/{{glossaryEntryId}}
```

## Headers

<b>X-OpenIDM-Username</b>	{{glossaryAdminUsername}}
<b>X-OpenIDM-Password</b>	{{glossaryAdminPassword}}
<b>Content-Type</b>	application/json

## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/commons/glossary/{{glossaryEntryId}}' \
```

```
--header 'X-OpenIDM-Username: {{glossaryAdminUsername}}' \  
--header 'X-OpenIDM-Password: {{glossaryAdminPassword}}' \  
--header 'Content-Type: application/json'
```

### DEL Delete Glossary Entry By ID

Delete a specific glossary entry.

#### Endpoint

```
{{idmRoot}}/commons/glossary/{{glossaryEntryId}}
```

#### Headers

<b>X-OpenIDM-Username</b>	{{glossaryAdminUsername}}
<b>X-OpenIDM-Password</b>	{{glossaryAdminPassword}}
<b>Content-Type</b>	application/json

#### Body raw

```
{  
  "userId": "c336c6a5-da19-4078-8ba5-3a297c605564",  
  "attributes": [  
    {  
      "attribute": "roles",  
      "value": "managed/role/2007",  
      "action": "add"  
    }  
  ]  
}
```

#### Example Request

```
curl --location -g --request DELETE  
'{{idmRoot}}/commons/glossary/{{glossaryEntryId}}' \  
--header 'X-OpenIDM-Username: {{glossaryAdminUsername}}' \  
--header 'X-OpenIDM-Password: {{glossaryAdminPassword}}' \  
--header 'Content-Type: application/json' \  
--data-raw '{
```

```
"userId": "c336c6a5-da19-4078-8ba5-3a297c605564",
"attributes": [
  {
    "attribute": "roles",
    "value": "managed/role/2007",
    "action": "add"
  }
]
```

### **POST** Update Glossary Entry

Update a specific glossary entry.

#### Endpoint

```
{{idmRoot}}/commons/glossary/{{glossaryEntryId}}?
_action=update
```

#### Headers

<b>X-OpenIDM-Username</b>	{{glossaryAdminUsername}}
<b>X-OpenIDM-Password</b>	{{glossaryAdminPassword}}
<b>Content-Type</b>	application/json

#### Params

<b>_action</b>	<b>update</b>
----------------	---------------

#### Body raw

```
{
  "_rev": "2",
  "requestable": true,
  "approvers": [
    "manager",
    "entitlementOwner"
  ],
  "displayName": "Cloud Infrastructure Approver!",
```

```

    "description": "Grants user access required for Cloud
Infrastructure Approver",
    "objectId": "managed/role/2070",
    "riskLevel": 1,
    "constraints": {
      "riskLevel": {
        "type": "integer"
      },
      "highRiskApprover": {
        "type": "managed object id"
      },
      "description": {
        "type": "string"
      },
      "entitlementOwner": {
        "type": "managed object id"
      },
      "approvers": {
        "type": "array"
      },
      "requestable": {
        "type": "boolean"
      }
    },
    "class": "object",
    "entitlementOwner": "managed/role/2070",
    "order": []
  }
}

```

### Example Request

```

curl --location -g --request POST
'{{idmRoot}}/commons/glossary/{{glossaryEntryId}}?
_action=update' \
--header 'X-OpenIDM-Username: {{glossaryAdminUsername}}' \
--header 'X-OpenIDM-Password: {{glossaryAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "_rev": "2",
  "requestable": true,
  "approvers": [
    "manager",
    "entitlementOwner"
  ]
}'

```

```

],
  "displayName": "Cloud Infrastructure Approver!",
  "description": "Grants user access required for Cloud
Infrastructure Approver",
  "objectId": "managed/role/2070",
  "riskLevel": 1,
  "constraints": {
    "riskLevel": {
      "type": "integer"
    },
    "highRiskApprover": {
      "type": "managed object id"
    },
    "description": {
      "type": "string"
    },
    "entitlementOwner": {
      "type": "managed object id"
    },
    "approvers": {
      "type": "array"
    },
    "requestable": {
      "type": "boolean"
    }
  },
  "class": "object",
  "entitlementOwner": "managed/role/2070",
  "order": []
}'

```

### **POST** Create Glossary Entry

Create a new glossary entry.

Endpoint

```

{{idmRoot}}/commons/glossary?_action=create

```

Headers

```

X-OpenIDM-Username      {{glossaryAdminUsername}}
X-OpenIDM-Password      {{glossaryAdminPassword}}

```

Content-Type\*\*

application/json

Params

**\_action**

**create**

Body raw

```
{
  "class":"identity-value",
  "constraints":{
    "_id":{
      "type":"id"
    },
    "_rev":{

    },
    "class":{
      "type":"string"
    },
    "constraints":{
      "type":"object"
    },
    "attributeName":{
      "type":"string"
    },
    "attributeValue":{

    },
    "requestFields":{
      "type":"array"
    },
    "description":{
      "type":"string"
    }
  },
  "attributeName":"jobCode",
  "attributeValue":"B456",
  "requestFields":[

],
```

```
"description":"Marketing job code"
}
```

### Example Request

```
curl --location -g --request POST
'{{idmRoot}}/commons/glossary?_action=create' \
--header 'X-OpenIDM-Username: {{glossaryAdminUsername}}' \
--header 'X-OpenIDM-Password: {{glossaryAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "class":"identity-value",
  "constraints":{
    "_id":{
      "type":"id"
    },
    "_rev":{

    },
    "class":{
      "type":"string"
    },
    "constraints":{
      "type":"object"
    },
    "attributeName":{
      "type":"string"
    },
    "attributeValue":{

    },
    "requestFields":{
      "type":"array"
    },
    "description":{
      "type":"string"
    }
  },
  "attributeName":"jobCode",
  "attributeValue":"B456",
  "requestFields":[

],
```

```
"description": "Marketing job code"
}'
```

### GET Query Glossary Entries

Query entries in the governance glossary

Endpoint

```
{{idmRoot}}/commons/glossary
```

Headers

<b>X-OpenIDM-Username</b>	{{glossaryAdminUsername}}
<b>X-OpenIDM-Password</b>	{{glossaryAdminPassword}}
<b>Content-Type</b>	application/json

Params

```
queryFilter
```

Example Request

```
curl --location -g --request GET
'{{idmRoot}}/commons/glossary' \
--header 'X-OpenIDM-Username: {{glossaryAdminUsername}}' \
--header 'X-OpenIDM-Password: {{glossaryAdminPassword}}' \
--header 'Content-Type: application/json'
```

### POST Create Glossary Entry

Create a new glossary entry.

Endpoint

```
{{idmRoot}}/commons/glossary?_action=create
```



## Headers

<b>X-OpenIDM-Username</b>	{{glossaryAdminUsername}}
<b>X-OpenIDM-Password</b>	{{glossaryAdminPassword}}
<b>Content-Type</b>	application/json

## Params

<b>_action</b>	<b>create</b>
----------------	---------------

## Body raw

```
{
  "class": "identity-value",
  "constraints": {
    "_id": {
      "type": "id"
    },
    "_rev": {
    },
    "class": {
      "type": "string"
    },
    "constraints": {
      "type": "object"
    },
    "attributeName": {
      "type": "string"
    },
    "attributeValue": {
    },
    "requestFields": {
      "type": "array"
    },
    "description": {
      "type": "string"
    }
  },
}
```

```

    "attributeName": "jobCode",
    "attributeValue": "B456",
    "requestFields": [

],
    "description": "Marketing job code"
}

```

### Example Request

```

curl --location -g --request POST
'{{idmRoot}}/commons/glossary?_action=create' \
--header 'X-OpenIDM-Username: {{glossaryAdminUsername}}' \
--header 'X-OpenIDM-Password: {{glossaryAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "class": "identity-value",
  "constraints": {
    "_id": {
      "type": "id"
    },
    "_rev": {

},
    "class": {
      "type": "string"
    },
    "constraints": {
      "type": "object"
    },
    "attributeName": {
      "type": "string"
    },
    "attributeValue": {

},
    "requestFields": {
      "type": "array"
    },
    "description": {
      "type": "string"
    }
  },
},

```

```
"attributeName": "jobCode",
"attributeValue": "B456",
"requestFields": [

],
"description": "Marketing job code"
}'
```

### GET Query Glossary Entries

Query entries in the governance glossary

Endpoint

```
{{idmRoot}}/commons/glossary
```

Headers

<b>X-OpenIDM-Username</b>	{{glossaryAdminUsername}}
<b>X-OpenIDM-Password</b>	{{glossaryAdminPassword}}
<b>Content-Type</b>	application/json

Params

```
queryFilter
```

Example Request

```
curl --location -g --request GET
'{{idmRoot}}/commons/glossary' \
--header 'X-OpenIDM-Username: {{glossaryAdminUsername}}' \
--header 'X-OpenIDM-Password: {{glossaryAdminPassword}}' \
--header 'Content-Type: application/json'
```

### POST Check User Update Against Policies

Given a userId and a list of attribute changes (in the format of attribute, value, and action), check the system's active policies against the user if their access was changed via the list of attribute changes.

NOTE

NOTE

This is an Access Review endpoint, available with the release of Access Request 2.0

+

Endpoint

```
{{idmRoot}}/governance/policyScan?_action=check
```

+

Headers

<b>X-OpenIDM-Username</b>	{{reviewAdminUsername}}
<b>X-OpenIDM-Password</b>	{{reviewAdminPassword}}
<b>Content-Type</b>	application/json

+

Params

<b>_action</b>	check
----------------	-------

+

Body raw

```
{
  "userId": "c336c6a5-da19-4078-8ba5-3a297c605564",
  "attributes": [
    {
      "attribute": "roles",
      "value": "managed/role/2007",
      "action": "add"
    }
  ]
}
```

+

## Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/policyScan?_action=check' \
--header 'X-OpenIDM-Username: {{reviewAdminUsername}}' \
--header 'X-OpenIDM-Password: {{reviewAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
    "userId": "c336c6a5-da19-4078-8ba5-3a297c605564",
    "attributes": [
        {
            "attribute": "roles",
            "value": "managed/role/2007",
            "action": "add"
        }
    ]
}'
```

## Access review

---

The following are Identity Governance API Access Review endpoints:

### Admin Certification

#### **POST** *Cancel Certification(s)*

Allows governance administrators to cancel certifications.

Endpoint

```
{{idmRoot}}/governance/adminCancelCert/{{certType}}
```

Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type        application/json
```

## Body

```
{
  "ids": [
    "{{certtocancelid}}"
  ]
}
```

## Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/adminCancelCert/{{certtype}}' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
  "ids": [
    "{{certtocancelid}}"
  ]
}'
```

### **POST** Cancel Ad-hoc User Certification

Create an ad-hoc user certification campaign.

## Endpoint

```
{{idmRoot}}/governance/certification/user
```

## Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password {{gpvernanceAdminPassword}}
Content-Type      application/json
```

## Body

```

{
  "certObjectType":"user",
  "name":"Quarterly Certification",
  "description":"Scheduled certification to run every
three months",
  "frequency":"scheduled",
  "schedule":"47 0 0 1 1/3 ?",
  "targetFilter":{
    "operator":"AND",
    "operand":[
      {
        "operator":"EQUALS",
        "operand":{
          "targetName":"roles",
          "targetValue":"managed/role/2005"
        }
      }
    ]
  },
  "stages":[
    {
      "name":"Stage 1",
      "entitlementFilter":{
        "attributes":{
          "roles":{
            "selected":true
          }
        }
      },
      "certifierName":"managed/role/2007",
      "certifierType":"authzRoles",
      "certifierKey":"",
      "deadline":"14 days",
      "escalationSchedule":[

    ],
      "riskLevelFilter":[

    ]
    }
  ],
  "onExpire":"stageOnly",
  "remediationProcess":"RemoveEntitlements"
}

```

## Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/scheduledCertification/{{certtype}}
' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
  "certObjectType":"user",
  "name":"Quarterly Certification",
  "description":"Scheduled certification to run every
three months",
  "frequency":"scheduled",
  "schedule":"47 0 0 1 1/3 ?",
  "targetFilter":{
    "operator":"AND",
    "operand":[
      {
        "operator":"EQUALS",
        "operand":{
          "targetName":"roles",
          "targetValue":"managed/role/2005"
        }
      }
    ]
  },
  "stages":[
    {
      "name":"Stage 1",
      "entitlementFilter":{
        "attributes":{
          "roles":{
            "selected":true
          }
        }
      },
      "certifierName":"managed/role/2007",
      "certifierType":"authzRoles",
      "certifierKey":"",
      "deadline":"14 days",
```



```

        "escalationSchedule":[
            ],
        "riskLevelFilter":[
            ]
        }
    ],
    "onExpire":"stageOnly",
    "remediationProcess":"RemoveEntitlements"
}'

```

### **POST** Create Ad-hoc Object Certification

Create an ad-hoc object certification campaign.

Endpoint

```

{{idmRoot}}/governance/certification/object

```

Headers

```

X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type        application/json

```

Body

```

{
  "certObjectType":"role",
  "name":"Object Certification",
  "description":"Example object cert",
  "frequency":"ad-hoc",
  "targetFilter":{
    "operator":"AND",
    "operand":[
      {
        "operator":"EQUALS",
        "operand":{
          "targetName":"name",
          "targetValue":"Finance Lead"
        }
      }
    ]
  }
}

```

```

        }
      }
    ]
  },
  "stages":[
    {
      "name":"Stage 1",
      "entitlementFilter":{
        "attributes":{
          "members":{
            "selected":true
          },
          "description":{
            "selected":true
          },
          "assignments":{
            "selected":true
          }
        },
        "certifyMetadata":true
      },
      "certifierName":"aclark",
      "certifierType":"user",
      "certifierKey":"",
      "deadline":"2020-08-06T13:30:00-04:00",
      "escalationSchedule":[

    ],
    "riskLevelFilter":[

  ]
}
],
"defaultCertifierType":"authzRoles",
"defaultCertifierName":"internal/role/governance-
administrator",
"onExpire":"stageOnly",
"remediationProcess":"RemoveEntitlements"
}

```

Example Request

```

curl --location -g --request POST
'{{idmRoot}}/governance/certification/object' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
  "certObjectType":"role",
  "name":"Object Certification",
  "description":"Example object cert",
  "frequency":"ad-hoc",
  "targetFilter":{
    "operator":"AND",
    "operand":[
      {
        "operator":"EQUALS",
        "operand":{
          "targetName":"name",
          "targetValue":"Finance Lead"
        }
      }
    ]
  },
  "stages":[
    {
      "name":"Stage 1",
      "entitlementFilter":{
        "attributes":{
          "members":{
            "selected":true
          },
          "description":{
            "selected":true
          },
          "assignments":{
            "selected":true
          }
        }
      },
      "certifyMetadata":true
    },
    "certifierName":"aclark",
    "certifierType":"user",
    "certifierKey":"",
    "deadline":"2020-08-06T13:30:00-04:00",

```

```

        "escalationSchedule":[
            ],
        "riskLevelFilter":[
            ]
        }
    ],
    "defaultCertifierType":"authzRoles",
    "defaultCertifierName":"internal/role/governance-
administrator",
    "onExpire":"stageOnly",
    "remediationProcess":"RemoveEntitlements"
}'

```

### **POST** Create Scheduled Certification

Create a scheduled certification definition.

Endpoint

```

{{idmRoot}}/governance/scheduledCertification/{{certtype}}

```

Headers

```

X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type        application/json

```

Body

```

{
  "certObjectType":"user",
  "name":"Quarterly Certification",
  "description":"Scheduled certification to run every
three months",
  "frequency":"scheduled",
  "schedule":"47 0 0 1 1/3 ?",
  "targetFilter":{
    "operator":"AND",
    "operand":[

```

```

        {
          "operator": "EQUALS",
          "operand": {
            "targetName": "roles",
            "targetValue": "managed/role/2005"
          }
        }
      ]
    },
    "stages": [
      {
        "name": "Stage 1",
        "entitlementFilter": {
          "attributes": {
            "roles": {
              "selected": true
            }
          }
        },
        "certifierName": "managed/role/2007",
        "certifierType": "authzRoles",
        "certifierKey": "",
        "deadline": "14 days",
        "escalationSchedule": [

        ],
        "riskLevelFilter": [

        ]
      }
    ],
    "onExpire": "stageOnly",
    "remediationProcess": "RemoveEntitlements"
  }

```

### Example Request

```

curl --location -g --request POST
'{{idmRoot}}/governance/scheduledCertification/{{certtype}}
' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'

```

```

\
--header 'Content-Type: application/json' \
--data-raw '{
  "certObjectType":"user",
  "name":"Quarterly Certification",
  "description":"Scheduled certification to run every
three months",
  "frequency":"scheduled",
  "schedule":"47 0 0 1 1/3 ?",
  "targetFilter":{
    "operator":"AND",
    "operand":[
      {
        "operator":"EQUALS",
        "operand":{
          "targetName":"roles",
          "targetValue":"managed/role/2005"
        }
      }
    ]
  },
  "stages":[
    {
      "name":"Stage 1",
      "entitlementFilter":{
        "attributes":{
          "roles":{
            "selected":true
          }
        }
      },
      "certifierName":"managed/role/2007",
      "certifierType":"authzRoles",
      "certifierKey":"",
      "deadline":"14 days",
      "escalationSchedule":[

    ],
      "riskLevelFilter":[

    ]
    }
  ],
  "onExpire":"stageOnly",

```

```
"remediationProcess":"RemoveEntitlements"
}'
```

### **POST** *Create Triggered Certification*

Create a triggered certification definition.

#### Endpoint

```
{{idmRoot}}/governance/triggeredCertification/user?
_action=create
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type        application/json
```

#### Params

```
_action      create
```

#### Body

```
{
  "certObjectType":"user",
  "name":"Event Based Cert",
  "description":"Test",
  "frequency":"event-based",
  "expression":"{\\"operator\\":\\"changed\\",\\"operand\\" :
{\\"field\\":\\"manager\\",\\"value\\":\\"\\\"}}",
  "targetFilter":{
    "operator":"AND",
    "operand":[
      {
        "operator":"EQUALS",
        "operand":{
          "targetName":"roles",
          "targetValue":""
        }
      }
    ]
  }
}
```

```

        }
      }
    ]
  },
  "stages":[
    {
      "name":"Stage 1",
      "entitlementFilter":{
        "attributes":{
          "roles":{
            "selected":true
          }
        }
      },
      "certifierName":"","
      "certifierType":"manager",
      "certifierKey":"","
      "deadline":"14 days",
      "escalationSchedule":[]

    ],
    "riskLevelFilter":[]
  ]
}
],
"onExpire":"stageOnly",
"remediationProcess":"RemoveEntitlements"
}'

```

### Example Request

```

curl --location -g --request POST
'{{idmRoot}}/governance/triggeredCertification/user?
_action=create' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
  "certObjectType":"user",
  "name":"Event Based Cert",

```



```

    "description": "Test",
    "frequency": "event-based",
    "expression": "{ \"operator\": \"changed\", \"operand\": { \"field\": \"manager\", \"value\": \"\" } }",
    "targetFilter": {
      "operator": "AND",
      "operand": [
        {
          "operator": "EQUALS",
          "operand": {
            "targetName": "roles",
            "targetValue": ""
          }
        }
      ]
    },
    "stages": [
      {
        "name": "Stage 1",
        "entitlementFilter": {
          "attributes": {
            "roles": {
              "selected": true
            }
          }
        },
        "certifierName": "",
        "certifierType": "manager",
        "certifierKey": "",
        "deadline": "14 days",
        "escalationSchedule": [

        ],
        "riskLevelFilter": [

        ]
      }
    ],
    "onExpire": "stageOnly",
    "remediationProcess": "RemoveEntitlements"
  }'

```

### **POST Delete Scheduled Certification**

Delete scheduled certification definitions.

## Endpoint

```
{{idmRoot}}/governance/scheduledCertification/{{certtype}}?_action=delete
```

## Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
Content-Type        application/json
```

## Params

```
_action      delete
```

## Body

```
{
  "ids": [
    "26c64da2-a702-4cea-a79e-9879477049d4"
  ]
}
```

## Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/scheduledCertification/{{certtype}}
?_action=delete' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
  "ids": [
    "26c64da2-a702-4cea-a79e-9879477049d4"
```



```
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
    "ids": [
        "26c64da2-a702-4cea-a79e-9879477049d4"
    ]
}'
```

### **POST** *Edit Scheduled Certification*

Update a scheduled certification definition.

Endpoint

```
{{idmRoot}}/governance/scheduledCertification/{{certtype}}/
26c64da2-a702-4cea-a79e-9879477049d4?_action=update
```

Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
Content-Type        application/json
```

Params

```
_action           update
```

Body

```
{
  "certObjectType":"user",
  "name":"Quarterly Certification",
  "description":"Scheduled certification to run every
three months",
  "frequency":"scheduled",
  "schedule":"47 0 0 1 1/3 ?",
  "targetFilter":{
    "operator":"AND",
```

```

    "operand": [
      {
        "operator": "EQUALS",
        "operand": {
          "targetName": "roles",
          "targetValue": "managed/role/2005"
        }
      }
    ],
  },
  "stages": [
    {
      "name": "Stage 1",
      "entitlementFilter": {
        "attributes": {
          "roles": {
            "selected": true
          }
        }
      },
      "certifierName": "managed/role/2007",
      "certifierType": "authzRoles",
      "certifierKey": "",
      "deadline": "14 days",
      "escalationSchedule": [

      ],
      "riskLevelFilter": [

      ]
    }
  ],
  "onExpire": "stageOnly",
  "remediationProcess": "RemoveEntitlements"
}

```

### Example Request

```

curl --location -g --request POST
'{{idmRoot}}/governance/scheduledCertification/{{certtype}}
/26c64da2-a702-4cea-a79e-9879477049d4?_action=update' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\

```

```

--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
  "certObjectType":"user",
  "name":"Quarterly Certification",
  "description":"Scheduled certification to run every
three months",
  "frequency":"scheduled",
  "schedule":"47 0 0 1 1/3 ?",
  "targetFilter":{
    "operator":"AND",
    "operand":[
      {
        "operator":"EQUALS",
        "operand":{
          "targetName":"roles",
          "targetValue":"managed/role/2005"
        }
      }
    ]
  },
  "stages":[
    {
      "name":"Stage 1",
      "entitlementFilter":{
        "attributes":{
          "roles":{
            "selected":true
          }
        }
      },
      "certifierName":"managed/role/2007",
      "certifierType":"authzRoles",
      "certifierKey":"",
      "deadline":"14 days",
      "escalationSchedule":[

    ],
    "riskLevelFilter":[

  ]
}
],
"onExpire":"stageOnly",

```

```
"remediationProcess":"RemoveEntitlements"
}'
```

### **POST** Edit Triggered Certification

Update a triggered certification definition.

#### Endpoint

```
{{idmRoot}}/governance/triggeredCertification/{{certtype}}/
{{triggeredusercertificationid}}?_action=update
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type        application/json
```

#### Params

```
_action           update
```

#### Body

```
{
  "certObjectType":"user",
  "name":"Event Based Certification",
  "description":"Test",
  "frequency":"event-based",
  "expression":"{\\"operator\\":\\"changed\\",\\"operand\\":
{\\"field\\":\\"manager\\",\\"value\\":\\"\\\"}}",
  "targetFilter":{
    "operator":"AND",
    "operand":[
      {
        "operator":"EQUALS",
        "operand":{
          "targetName":"roles",
          "targetValue":""
        }
      }
    ]
  }
}
```

```

        }
      }
    ]
  },
  "stages":[
    {
      "name":"Stage 1",
      "entitlementFilter":{
        "attributes":{
          "roles":{
            "selected":true
          }
        }
      },
      "certifierName":"","
      "certifierType":"manager",
      "certifierKey":"","
      "deadline":"14 days",
      "escalationSchedule":[

      ],
      "riskLevelFilter":[

      ]
    }
  ],
  "onExpire":"stageOnly",
  "remediationProcess":"RemoveEntitlements"
}

```

### Example Request

```

curl --location -g --request POST
'{{idmRoot}}/governance/triggeredCertification/{{certtype}}
/{{triggeredusercertificationid}}?_action=update' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
  "certObjectType":"user",
  "name":"Event Based Certification",

```



```

    "description": "Test",
    "frequency": "event-based",
    "expression": "{ \"operator\": \"changed\", \"operand\": { \"field\": \"manager\", \"value\": \"\" } }",
    "targetFilter": {
      "operator": "AND",
      "operand": [
        {
          "operator": "EQUALS",
          "operand": {
            "targetName": "roles",
            "targetValue": ""
          }
        }
      ]
    },
    "stages": [
      {
        "name": "Stage 1",
        "entitlementFilter": {
          "attributes": {
            "roles": {
              "selected": true
            }
          }
        },
        "certifierName": "",
        "certifierType": "manager",
        "certifierKey": "",
        "deadline": "14 days",
        "escalationSchedule": [

        ],
        "riskLevelFilter": [

        ]
      }
    ],
    "onExpire": "stageOnly",
    "remediationProcess": "RemoveEntitlements"
  }'

```

### **GET Admin Event Details**

Allows governance administrators to get event details.

## Endpoint

```
{{idmRoot}}/governance/adminCertEventDetails/{{certtype}}/{{  
usercertificationid}}/{{stageIndex}}/{{eventIndex}}
```

## Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

## Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/governance/adminCertEventDetails/  
{{certtype}}/  
{{usercertificationid}}/{{stageIndex}}/{{eventIndex}}' \  
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'  
\  
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

## **GET** Get Scheduled Certification

Read a scheduled certification definition.

## Endpoint

```
{{idmRoot}}/governance/scheduledCertification/{{certtype}}/  
26c64da2-a702-4cea-a79e-9879477049d4
```

## Headers

```
X-OpenIDM-Username  {{endUserUsername}}  
X-OpenIDM-Password  {{endUserPassword}}  
Content-Type        application/json
```

## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/scheduledCertification/{{certtype}}
/26c64da2-a702-4cea-a79e-9879477049d4' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json'
```

## GET Get Certification

Get a specific certification.

### Endpoint

```
{{idmRoot}}/governance/adminCertification/
{{certtype}}/
{{usercertificationid}}?status=
{{certStatus}}&pageNumber=0&pageSize={{pageSize}}&sortBy&q=
{{query}}
```

### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
```

### Params

<b>status</b>	Cert status ('active' or 'closed')
<b>pageNumber</b>	0 (Pagination control)
<b>pageSize</b>	Page size (Size per page)
<b>sortBy</b>	(Property to sort by)
<b>q</b>	Query (Query for name)

### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/adminCertification/
{{certtype}}/
{{usercertificationid}}?status=
```

```
{{certStatus}}&pageNumber=0&pageSize=
{{pageSize}}&sortBy=&q={{query}}' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

### GET Get Admin Certification List

Get the certification list.

#### Endpoint

```
{{idmRoot}}/governance/adminCertList/
{{certtype}}/
{{usercertificationid}}?pageSize={{pageSize}}&pageNumber=0
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

#### Params

<b>pageSize</b>	Page size (Size per page)
<b>pageNumber</b>	0 (Pagination control)
<b>sortBy</b>	(Property to sort by)
<b>q</b>	Query (Query for name)
<b>selected</b>	0 (Selected stage)

#### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/adminCertList/
{{certtype}}/
{{usercertificationid}}?pageSize={{pageSize}}&pageNumber=0'
\
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
```

```
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

### GET Get Tasks For Specific User

Returns a list of tasks of the requested type that are assigned to the logged in user either directly or through a role.

#### Endpoint

```
{{idmRoot}}/governance/dashboard/{{userId}}?
status=active&type=user
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

#### Params

<b>status</b>	active (active or closed)
<b>type</b>	user (Type of task: user, object, violation)
<b>pageNumber</b>	0 (Pagination control)
<b>pageSize</b>	Page size (Size per page)
<b>sortBy</b>	(Property to sort by)
<b>q</b>	Query (Query for name)

#### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/dashboard/{{userId}}?
status=active&type=user' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

### GET Get Triggered Certification

Read a triggered certification definition.

Endpoint

```
{{idmRoot}}/governance/triggeredCertification/{{certtype}}/  
{{triggeredusercontentid}}
```

Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}  
Content-Type:       application/json
```

Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/governance/triggeredCertification/{{certtype}}/  
/{{triggeredusercontentid}}' \  
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'  
\  
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'  
\  
--header 'Content-Type: application/json'
```

### **GET Query Certifications**

Query certification definitions.

Endpoint

```
{{idmRoot}}/governance/adminCertification/  
{{certtype}}?  
status=active&pageNumber=0&pageSize=10&sortBy=nextDeadline
```

Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

## Params

<b>status</b>	active (active or closed)
<b>pageNumber</b>	0 (Pagination control)
<b>pageSize</b>	10 (Size per page)
<b>sortBy</b>	nextDeadline
<b>q**</b>	

## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/adminCertification/
{{certtype}}?
status=active&pageNumber=0&pageSize=10&sortBy=nextDeadline'
\
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

## **GET** Query Scheduled Certifications

Query scheduled certification definitions.

## Endpoint

```
{{idmRoot}}/governance/scheduledCertification/{{certtype}}
```

## Headers

<b>X-OpenIDM-Username</b>	{{governanceAdminUsername}}
<b>X-OpenIDM-Password</b>	{{gpvernanceAdminPassword}}
<b>Content-Type:</b>	application/json

## Params

<b>q</b>	<b>Filter</b>
<b>sortBy</b>	<b>Sort by field</b>

#### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/scheduledCertification/{{certtype}}
' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}'
\
--header 'Content-Type: application/json'
```

### **GET Query Triggered Certifications**

Query triggered certification definitions.

#### Endpoint

```
{{idmRoot}}/governance/triggeredCertification/
{{certtype}}?
pageSize=10&sortBy=name&status=triggered&pageNumber=0
```

#### Headers

<b>X-OpenIDM-Username</b>	<b>{{governanceAdminUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{governanceAdminPassword}}</b>
<b>Content-Type:</b>	<b>application/json</b>

#### Params

<b>pageSize</b>	10 (Size per page)
<b>sortBy</b>	name (Sort by field)
<b>status</b>	triggered
<b>pageNumber</b>	0



## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/triggeredCertification/
{{certtype}}?
pageSize=10&sortBy=name&status=triggered&pageNumber=0' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}' \
--header 'Content-Type: application/json'
```

## **POST** Reassign Events

Bulk reassign events. Include eventIds in body to reassign specific events, else include campaignIds in body to reassign all events for the old certifier ID in the given campaigns. If neither eventIds nor campaignIds is present, will reassign ALL tasks for oldCertifierId to newCertifierId.

## Endpoint

```
{{idmRoot}}/governance/certify/{{certtype}}/reassign
```

## Headers

```
X-OpenIDM-Username   {{governanceAdminUsername}}
X-OpenIDM-Password {{governanceAdminPassword}}
Content-Type:      application/json
```

## Params

```
queryFilter          Target a specific subset of events
within the stage
```

## Body raw

```
{
  "newCertifierId": "",
}
```

```
"oldCertifierId": "",
"campaignIds": [

    ],
"eventIds": [

    ]
}
```

#### Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/certify/{{certtype}}/reassign' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "newCertifierId": "",
  "oldCertifierId": "",
  "campaignIds": [

    ],
  "eventIds": [

    ]
}'
```

#### **POST Remediate Certification**

Call the basic remediation script on a certification event object. Content of request can be dependent on customizations to remediation script, however the example workflow will pass the entire event object to this endpoint. The OOTB script only requires the properties found in this example.

#### Endpoint

```
{{idmRoot}}/governance/remediation
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type:       application/json
```

#### Params

```
field                allowBulkCertify (Single setting ID to
return)
```

#### Body raw

```
{
  "remediationType": "revokeCertification",
  "stageIndex": 0,
  "stages": [
    {
      "eventData": {
        "metadata": [],
        "application": [],
        "managedObject": [
          {
            "riskLevel": 0,
            "comments": null,
            "attributeValue": "AB123",
            "values": [],
            "attributeName": "Job Code",
            "certifiable": 1,
            "outcome": "revoke",
            "objectType": "jobCode"
          }
        ]
      },
      "longTargetId": "managed/user/138"
    }
  ]
}
```

#### Example Request

```

curl --location -g --request POST
'{{idmRoot}}/governance/remediation' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
    "remediationType": "revokeCertification",
    "stageIndex": 0,
    "stages": [
        {
            "eventData": {
                "metadata": [],
                "application": [],
                "managedObject": [
                    {
                        "riskLevel": 0,
                        "comments": null,
                        "attributeValue": "AB123",
                        "values": [],
                        "attributeName": "Job Code",
                        "certifiable": 1,
                        "outcome": "revoke",
                        "objectType": "jobCode"
                    }
                ]
            },
            "longTargetId": "managed/user/138"
        }
    ]
}'

```

### **POST Remediate Violation**

Call the basic remediation script on a violation object. Content of request can be dependent on customizations to remediation script, however the example workflow will pass the entire violation object to this endpoint. The OOTB script only requires the targetId and the policy expression violated.

Endpoint

```
{{idmRoot}}/governance/remediation
```

## Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
Content-Type:       application/json
```

## Params

```
field                allowBulkCertify (Single setting ID to
return)
```

## Body raw

```
{
  "targetId": "managed/user/1024",
  "expression": "
{'\\''operator'\\': '\\''EQUALS'\\'', '\\''operand'\\':
{'\\''targetName'\\': '\\''jobCode'\\'', '\\''targetValue'\\': '\\''
'AB123'\\''}}",
  "remediationType": "revokeViolation"
}
```

## Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/remediation' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "targetId": "managed/user/1024",
  "expression": "
{'\\''operator'\\': '\\''EQUALS'\\'', '\\''operand'\\':
{'\\''targetName'\\': '\\''jobCode'\\'', '\\''targetValue'\\': '\\''
'AB123'\\''}}",
```

```
"remediationType": "revokeViolation"  
'
```

## Admin Policy

### **POST** *Cancel Exception*

Cancel an existing violation exception. Admin action.

#### Endpoint

```
{{idmRoot}}/governance/violation/{{violationId}}?  
_action=cancelexception
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{governanceAdminPassword}}  
Content-Type:       application/json
```

#### Params

```
_action      cancelexception
```

#### Body raw

```
{}
```

#### Example Request

```
curl --location -g --request POST  
'{{idmRoot}}/governance/violation/{{violationId}}?  
_action=cancelexception' \  
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'  
\  
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}'
```

```
\
--header 'Content-Type: application/json' \
--data-raw '{
}
}'
```

### **POST** *Cancel Exception(s)*

Bulk cancel violations.

Endpoint

```
{{idmRoot}}/governance/violation?_action=cancelexception
```

Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type:       application/json
```

Params

<b>sortBy</b>	Sort key
<b>q</b>	Query value
<b>pageSize</b>	Page size(Results per page)
<b>pageNumber</b>	0 (Page number of results)
<b>_action**</b>	cancelexception

Body raw

```
{
  "ids": [
    "{{exceptionToCancelId}}"
  ]
}
```

Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/violation?_action=cancelexception'
\
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
    "ids": [
        "{{exceptionToCancelId}}"
    ]
}'
```

### **POST** *Cancel Violation*

Cancel a violation.

#### Endpoint

```
{{idmRoot}}/governance/violation/{{violationId}}?
_action=cancel
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password {{gpvernanceAdminPassword}}
Content-Type:      application/json
```

#### Params

```
_action           cancel
```

#### Body raw

```
{}
```



## Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/violation/{{violationId}}?
_action=cancel' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
}'
```

## **POST** Cancel Violation(s)

Bulk cancel violations.

### Endpoint

```
{{idmRoot}}/governance/violation?_action=cancel
```

### Headers

<b>X-OpenIDM-Username</b>	<b>{{governanceAdminUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{governanceAdminPassword}}</b>
<b>Content-Type:</b>	<b>application/json</b>

### Params

<b>sortBy</b>	Sort key
<b>q</b>	Query value
<b>pageSize</b>	Page size (Results per page)
<b>pageNumber</b>	0 (Page number of results)
<b>_action**</b>	cancel

### Body raw

```
{
  "ids": [
    "{{violationToCancelId}}"
  ]
}
```

#### Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/violation?_action=cancel' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "ids": [
    "{{violationToCancelId}}"
  ]
}'
```

### **POST** *Comment on Violation*

Comment on a violation. Owner action.

#### Endpoint

```
{{idmRoot}}/governance/violation/{{violationId}}?
_action=comment
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password {{gpvernanceAdminPassword}}
Content-Type:      application/json
```

#### Params

<b>_action</b>	<b>comment</b>
----------------	----------------

Body raw

```
{  
    "comments": "Comments to add"  
}
```

Example Request

```
curl --location -g --request POST  
'{{idmRoot}}/governance/violation/{{violationId}}?  
_action=comment' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
    "comments": "Comments to add"  
}'
```

### **POST** *Configure a Reactive Scan*

Configure the information for reactive policy scans.

Endpoint

```
{{idmRoot}}/governance/policyScan?_action=configure
```

Headers

<b>X-OpenIDM-Username</b>	<b>{{governanceAdminUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{governanceAdminPassword}}</b>
<b>Content-Type:</b>	<b>application/json</b>

Params

**\_action**                      **configure**

Body raw

```
{
  "expirationDate": "15 days",
  "escalationSchedule": []
}
```

Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/policyScan?_action=configure' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
  "expirationDate": "15 days",
  "escalationSchedule": []
}'
```

### **POST** *Create Ad-hoc Policy Scan*

Creates and runs an ad-hoc policy scan.

Endpoint

```
{{idmRoot}}/governance/policyScan?_action=adhoc
```

Headers

```
X-OpenIDM-Username    {{governanceAdminUsername}}  
X-OpenIDM-Password   {{gpvernanceAdminPassword}}  
Content-Type:        application/json
```

## Params

<b>_action</b>	<b>adhoc</b>
----------------	--------------

## Body raw

```
{
  "name": "Adhoc Scan",
  "scanType": "ad-hoc",
  "schedule": "",
  "targetFilter": {
    "operator": "ALL",
    "operand": [

    ]
  },
  "policies": [
    "managed/policy/9b929e44-e120-4988-95b3-6306b4fa0533"
  ],
  "expirationDate": "07/31/2020",
  "escalationSchedule": [

  ]
}
```

## Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/policyScan?_action=adhoc' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
  "name": "Adhoc Scan",
  "scanType": "ad-hoc",
  "schedule": "",
  "targetFilter": {
    "operator": "ALL",
```

```
    "operand" :[
      ]
    },
    "policies" :[
      "managed/policy/9b929e44-e120-4988-95b3-6306b4fa0533"
    ],
    "expirationDate" : "07/31/2020",
    "escalationSchedule" :[
      ]
  ]
}'
```

### **POST** Create Scheduled Policy Scan

Creates a scheduled policy scan.

#### Endpoint

```
{{idmRoot}}/governance/policyScan?_action=scheduled
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type:       application/json
```

#### Params

```
_action      scheduled
```

#### Body raw

```
{
  "name" : "Scheduled scan monthly",
  "scanType" : "scheduled",
  "schedule" : "28 2 0 1 1/1 ?",
  "targetFilter" : {
    "operator" : "ALL",
```

```

    "operand" :[
      ]
    },
    "policies" :[
      "managed/policy/9b929e44-e120-4988-95b3-6306b4fa0533"
    ],
    "expirationDuration" : "7 days",
    "escalationSchedule" :[
      ]
  ]
}

```

### Example Request

```

curl --location -g --request POST
'{{idmRoot}}/governance/policyScan?_action=scheduled' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
  "name": "Scheduled scan monthly",
  "scanType": "scheduled",
  "schedule": "28 2 0 1 1/1 ?",
  "targetFilter": {
    "operator": "ALL",
    "operand": [
      ]
    },
  },
  "policies": [
    "managed/policy/9b929e44-e120-4988-95b3-6306b4fa0533"
  ],
  "expirationDuration": "7 days",
  "escalationSchedule": [
    ]
}'

```

Creates a new policy.

#### Endpoint

```
{{idmRoot}}/governance/adminPolicy?action=create
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type:        application/json
```

#### Params

```
action      create
```

#### Body raw

```
{
  "name": "Policy Name",
  "description": "Example policy",
  "expression": "{ \"operator\": \"EQUALS\", \"operand\": { \"targetName\": \"roles\", \"targetValue\": \"managed/role/2003\" } }",
  "riskLevel": "1",
  "ownerType": "user",
  "owner": {
    "_ref": "managed/user/357"
  },
  "remediationProcess": "{{violationRemediationWorkflow}}",
  "active": "true"
}
```

#### Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/adminPolicy?action=create' \
```



```
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
  "name":"Policy Name",
  "description":"Example policy",
  "expression": "{ \"operator\": \"EQUALS\", \"operand\":
{ \"targetName\": \"roles\", \"targetValue\": \"managed/role/20
03\" } }",
  "riskLevel": "1",
  "ownerType": "user",
  "owner": {
    "_ref": "managed/user/357"
  },
  "remediationProcess": "{{violationRemediationWorkflow}}",
  "active": "true"
}'
```

### **POST** Delete Policies

Delete policies from the system.

Endpoint

```
{{idmRoot}}/governance/adminPolicy?action=delete
```

Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
Content-Type:       application/json
```

Params

```
action      delete
```

Body raw

```
{
    "ids": [
        "{{policyToDeleteId}}"
    ]
}
```

#### Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/adminPolicy/policies?action=delete'
\
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
    "ids": [
        "{{policyToDeleteId}}"
    ]
}'
```

### **POST** Delete Policy Scans

Delete scheduled policy scans from the system.

#### Endpoint

```
{{idmRoot}}/governance/adminPolicy/policies?action=delete
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password {{governanceAdminPassword}}
Content-Type:      application/json
```

#### Params

**action**                      **delete**

Body raw

```
{
  "ids": [
    "{{scanToCancelId}}"
  ]
}
```

Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/adminPolicy/policies?action=delete'
\
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
\
--header 'Content-Type: application/json' \
--data-raw '{
  "ids": [
    "{{scanToCancelId}}"
  ]
}'
```

### **POST** Delete Scheduled Policy Scans

Delete policy scan definitions.

Endpoint

```
{{idmRoot}}/governance/adminPolicy/policies?action=delete
```

Headers

```
X-OpenIDM-Username    {{governanceAdminUsername}}
X-OpenIDM-Password   {{gpvernanceAdminPassword}}
```

**Content-Type:**            **application/json**

Params

**action**                    **delete**

Body raw

```
{
  "ids": [
    "{{scheduledScanId}}"
  ]
}
```

Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/policyScan?_action=delete' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "ids": [
    "{{scheduledScanId}}"
  ]
}'
```

### **POST** Edit Policy

Edit an existing policy.

Endpoint

**{{idmRoot}}/governance/adminPolicy/{{policyId}}?  
action=update**

## Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
Content-Type:       application/json
```

## Params

```
action      update
```

## Body raw

```
{
  "name": "Policy Create Test",
  "description": "Testing a created policy update",
  "expression": "{ \"operator\": \"EQUALS\", \"operand\": { \"targetName\": \"roles\", \"targetValue\": \"managed/role/2003\" } }",
  "riskLevel": "1",
  "ownerType": "user",
  "owner": {
    "_ref": "managed/user/357"
  },
  "remediationProcess": "RevokeResources",
  "active": "true"
}
```

## Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/adminPolicy/{{policyId}}?
action=update' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
```

```

    "name": "Policy Create Test",
    "description": "Testing a created policy update",
    "expression": "{ \"operator\": \"EQUALS\", \"operand\": { \"targetName\": \"roles\", \"targetValue\": \"managed/role/2003\" } }",
    "riskLevel": "1",
    "ownerType": "user",
    "owner": {
      "_ref": "managed/user/357"
    },
    "remediationProcess": "RevokeResources",
    "active": "true"
  }'

```

### **PUT** Edit Scheduled Policy Scan

Edit a scheduled policy scan definition.

Endpoint

```

{{idmRoot}}/governance/policyScan/{{scheduledScanId}}

```

Headers

```

X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type:       application/json

```

Body raw

```

{
  "name": "Scheduled scan monthly",
  "scanType": "scheduled",
  "schedule": "28 2 0 1 1/1 ?",
  "targetFilter": {
    "operator": "ALL",
    "operand": [

    ]
  },
  "policies": [

```

```
        "managed/policy/9b929e44-e120-4988-95b3-6306b4fa0533"
    ],
    "expirationDuration": "7 days",
    "escalationSchedule": [

]
}'
```

### Example Request

```
curl --location -g --request PUT
'{{idmRoot}}/governance/policyScan/{{scheduledScanId}}' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
    "name": "Scheduled scan monthly",
    "scanType": "scheduled",
    "schedule": "28 2 0 1 1/1 ?",
    "targetFilter": {
        "operator": "ALL",
        "operand": [

    ]
},
    "policies": [
        "managed/policy/9b929e44-e120-4988-95b3-6306b4fa0533"
    ],
    "expirationDuration": "7 days",
    "escalationSchedule": [

]
}'
```

### **GET** *get Active Policy Scans*

Query active policy scans.

Endpoint

```
{{idmRoot}}/governance/activePolicyScan}
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

#### Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/governance/activePolicyScan' \  
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'  
\  
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

### **GET** *Get Individual Policy Scan*

Query an individual policy scan.

#### Endpoint

```
{{idmRoot}}/governance/activePolicyScan}
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

#### Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/governance/activePolicyScan/{{activePolicyScan  
Id}}' \  
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'  
\  
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```



### **GET** *Get Reactive Scan Configuration*

Read reactive scan configuration.

Endpoint

```
{{idmRoot}}/governance/policyScan/reactive
```

Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
Content-Type:       application/json
```

Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/policyScan/reactive' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
--header 'Content-Type: application/json'
```

### **GET** *Get Violation*

Read a specific violation, as governance administrator.

Endpoint

```
{{idmRoot}}/governance/violation/{{violationId}}
```

Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/violation/{{violationId}}' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

### **GET** Grant Exception to Violation

Grant an exception for the violation. Owner action.

### Endpoint

```
{{idmRoot}}/governance/violation/{{violationId}}?
_action=approve
```

### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
Content-Type:       application/json
```

### Body raw

```
{
  "comments": "Exception justification",
  "exceptionEndDate": "2020-06-09T10:28:46-04:00"
}
```

### Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/violation/{{violationId}}?
_action=approve' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
```

```
--data-raw '{
    "comments": "Exception justification",
    "exceptionEndDate": "2020-06-09T10:28:46-04:00"
}'
```

### GET Query Policies

Query existing policies as a governance administrator.

#### Endpoint

```
{{idmRoot}}/governance/adminPolicy/policies?pageSize=
{{pageSize}}&pageNumber=0
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

#### Params

<b>pageSize</b>	Page size (Number of results per page)
<b>pageNumber</b>	0 (current results page)
<b>sortBy</b>	Sort key
<b>q</b>	Query value

#### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/adminPolicy/policies?pageSize=
{{pageSize}}&pageNumber=0' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
\
```

### GET Query Policy Scans

Query policy scans.

## Endpoint

```
{{idmRoot}}/governance/policyScan?  
q&pageSize=10&pageNumber=0
```

## Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}  
Content-Type:       application/json
```

## Params

<b>q</b>	Query value
<b>pageSize</b>	Page size (Number of results per page)
<b>pageNumber</b>	0 (current results page)
<b>sortBy</b>	Field to sort by

## Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/governance/policyScan?  
q=&pageSize=10&pageNumber=0' \  
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'  
\  
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'  
\  
--header 'Content-Type: application/json'
```

## GET Query Violations

Query violations as a governance administrator.

## Endpoint

```
{{idmRoot}}/governance/violation/admin?status=active
```

## Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

## Params

```
status           active (Violation status:  
active/closed/exception)  
target          Violation target user  
owner           Violation owner  
sortBy         Sort key  
q              Query value  
pageSize       Page size (Number of results per page)  
pageNumber    0 (current results page)  
fields         Fields to return
```

## Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/governance/violation/admin?status=active' \  
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \  
\   
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

## *GET Read Scheduled Policy Scan*

Read a scheduled policy scan definition.

## Endpoint

```
{{idmRoot}}/governance/policyScan/{{scheduledScanId}}
```

## Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

**Content-Type:** application/json

#### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/policyScan/{{scheduledScanId}}' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
--header 'Content-Type: application/json'
```

### **GET Reassign Violation(s)**

Bulk reassign violations. Must include a new owner id to reassign to. To reassign select violations, include an array of IDs corresponding to the intended violations. To reassign all of a given user's violations, include an oldOwnerId in lieu of the IDs array.

#### Endpoint

```
{{idmRoot}}/governance/violation?_action=reassign
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
Content-Type:       application/json
```

#### Params

<b>sortBy</b>	Sort key
<b>q</b>	Query value
<b>pageSize</b>	Page size (Number of results per page)
<b>pageNumber</b>	0 (current results page)
<b>_action</b>	reassign

#### Body raw

```
{
    "newOwnerId": "{{newOwnerId}}",
    "ids": [
        "{{violationToReassignId}}"
    ]
}'
```

#### Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/violation?_action=reassign' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
    "newOwnerId": "{{newOwnerId}}",
    "ids": [
        "{{violationToReassignId}}"
    ]
}'
```

### **POST Remediate Violation**

Kick off the remediation process for the violation. Owner action.

#### Endpoint

```
{{idmRoot}}/governance/violation/{{violationId}}?
_action=remediate
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password {{governanceAdminPassword}}
Content-Type:      application/json
```

#### Params

<b>_action</b>	<b>remediate</b>
----------------	------------------

#### Body raw

```
{}
```

#### Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/violation/{{violationId}}?
_action=remediate' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
}'
```

### **POST** Run Reactive Scan

Runs a reactive scan for all policies against a given user.

#### Endpoint

```
{{idmRoot}}/governance/policyScan?_action=reactive
```

#### Headers

<b>X-OpenIDM-Username</b>	<b>{{governanceAdminUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{governanceAdminPassword}}</b>
<b>Content-Type:</b>	<b>application/json</b>

#### Params



**\_action**                      **reactive**

Body raw

```
{
  "userId": "{{userId}}"
}
```

Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/policyScan?_action=reactive' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
  "userId": "{{userId}}"
}'
```

## Admin Dashboard

### **GET** *Get Admin Dashboard Metrics*

Get the admin dashboard statistics.

Endpoint

```
{{idmRoot}}/governance/adminDashboard
```

Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/adminDashboard' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}'
```

### **GET** *Get Individual Admin Dashboard Metric*

Query for a single admin dashboard statistic, using the stat ID.

### Endpoint

```
{{idmRoot}}/governance/adminDashboard/{{statId}}
```

### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
```

### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/adminDashboard/{{statId}}' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}'
```

### **GET** *Query Entitlements with History*

Returns a list of the available entitlements that are stored within the certification history repo object. Used by the admin dashboard to allow the user to query for a specific entitlement's history.

### Endpoint

```
{{idmRoot}}/governance/adminDashboard?
action=getStoredEntitlements&q=
```

## Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
Content-Type:       application/json
```

## Params

```
field                allowBulkCertify (Single setting ID to
return)
```

## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/adminDashboard?
action=getStoredEntitlements&q=' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

### **GET Query Policy Violation Results**

Returns the results of all policy violations, organized by policy. Can provide an optional policy id (e.g. managed/policy/{{ID}}) to get information for a specific policy.

## Endpoint

```
{{idmRoot}}/governance/adminDashboard?
action=getPolicyTotals
```

## Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

## Params

<b>action</b>	<b>getPolicyTotals</b> (Dashboard action)
<b>id</b>	<b>managed/policy/99b41c9e-de1b-447e-92b8-cc2546a8b40</b> (Policy to search for, in long id format, option)

## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/adminDashboard?
action=getPolicyTotals' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

## **GET** *Get User Certification Profile*

Get certification profile for a given user.

## Endpoint

```
{{idmRoot}}/governance/userEventData/user/{{userId}}?
system=IDM
```

## Headers

<b>X-OpenIDM-Username</b>	<b>{{endUserUsername}}</b>
<b>X-OpenIDM-Password</b>	<b>{{endUserPassword}}</b>

## Params

<b>system</b>	<b>IDM</b>
---------------	------------

## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/userEventData/user/{{userId}}?
system=IDM' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}'
```

### **GET** *Get Entitlement Certification History*

Get certification history for a single entitlement.

#### Endpoint

```
{{idmRoot}}/governance/userEventData/object?targetId=
{{entitlementId}}
```

#### Headers

```
X-OpenIDM-Username  {{endUserUsername}}
X-OpenIDM-Password {{endUserPassword}}
```

#### Params

<b>targetId</b>	entitlementId (Entitlement to get certification history for)
<b>history</b>	true (Return individual certification history of item)

#### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/userEventData/object?targetId=
{{entitlementId}}' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}'
```

## PUT Edit Notification

Update a specific governance notification.

### Endpoint

```
{{idmRoot}}/governance/notification/{{notificationId}}
```

### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
Content-Type:       application/json
```

### Body raw

```
{
  "_id": "CERTIFICATION_CREATED_ADHOC",
  "displayName": "Certification Creation Adhoc",
  "from": "governanceNotifier@ForgeRock.com",
  "to": "${x.toEmailAddress}",
  "cc": "",
  "subject": "ATTENTION: Certification Task Assigned",
  "type": "text/html",
  "body": "<html><body>A certification task for
  $x.certificationName was assigned to you from an ad hoc
  certification campaign.<br><br>Please log into <a
  href=\\\\"http://$x.hostName/governance/\\\\">FRGovernance</a
  > as soon as you are able to review and complete the
  certification Task.</body></html>",
  "enabled": true
}
```

### Example Request

```
curl --location -g --request PUT
'{{idmRoot}}/governance/notification/{{notificationId}}' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

```

\
--header 'Content-Type: application/json' \
--data-raw '{
  "_id": "CERTIFICATION_CREATED_ADHOC",
  "displayName": "Certification Creation Adhoc",
  "from": "governanceNotifier@ForgeRock.com",
  "to": "${x.toEmailAddress}",
  "cc": "",
  "subject": "ATTENTION: Certification Task Assigned",
  "type": "text/html",
  "body": "<html><body>A certification task for
  $x.certificationName was assigned to you from an ad hoc
  certification campaign.<br><br>Please log into <a
  href=\\\"http://$x.hostName/governance/\\\">FRGovernance</a
  > as soon as you are able to review and complete the
  certification Task.</body></html>",
  "enabled": true
}'

```

### GET Get Access Review System Settings

Get access review settings.

Endpoint

```

{{idmRoot}}/governance/systemSettings

```

Headers

```

X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}

```

Params

```

**field              allowBulkCertify (Single setting ID
to return)

```

Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/systemSettings' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

### **GET Query Access Review Notifications**

Query for governance notifications.

Endpoint

```
{{idmRoot}}/governance/notification?_queryId=query-all-ids
```

Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

Params

<b>_queryId</b>	<b>query-all-ids</b>
**type	role (Single managed object to
fetch)	

Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/notification?_queryId=query-all-
ids' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

### **GET Read Notification**

Read a specific governance notification.



### Endpoint

```
{{idmRoot}}/governance/notification/{{notificationId}}
```

### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}
```

### Params

```
**type                role (Single managed object to  
fetch)
```

### Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/governance/notification/{{notificationId}}' \  
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'  
\  
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

## **POST** Update Access Review System Settings

Update the governance settings.

### Endpoint

```
{{idmRoot}}/governance/systemSettings
```

### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}  
Content-Type        application/json
```

## Params

**\*\*field** allowBulkCertify (Single setting ID to return)

## Body raw

```
{
  "_id": "",
  "systemSettings": [
    {
      "section": "General",
      "fields": [
        {
          "id": "allowBulkCertify",
          "type": "boolean",
          "value": false
        }
      ]
    },
    {
      "section": "Display",
      "fields": [
        {
          "id": "userDisplayFormat",
          "type": "string",
          "value": "{{givenName}} {{sn}}
({{userName}})"
        }
      ]
    },
    {
      "section": "Delegation",
      "fields": [
        {
          "id": "delegationEnabled",
          "type": "boolean",
          "value": false
        },
        {
          "id": "userDelegate",
          "type": "dropdown",
```

```

        "value": "manager"
    }
]
},
{
    "section": "Risk Level Management",
    "fields": [
        {
            "id": "riskLevel",
            "type": "dblSlider",
            "value": {
                "lower": 5,
                "higher": 6
            }
        }
    ]
},
{
    "section": "Custom attribute mapping",
    "fields": [
        {
            "id": "userAttrMappings",
            "type": "dropdown",
            "attributes": [
                {
                    "id": "givenName",
                    "value": "givenName"
                },
                {
                    "id": "sn",
                    "value": "sn"
                },
                {
                    "id": "mail",
                    "value": "mail"
                }
            ]
        }
    ]
},
{
    "section": "Menu Management",
    "fields": [
        {
            "id": "menuManagement",

```

```

        "type": "string",
        "value": []
      }
    ]
  }
}

```

### Example Request

```

curl --location -g --request POST
'{{idmRoot}}/governance/systemSettings' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{
  "_id": "",
  "systemSettings": [
    {
      "section": "General",
      "fields": [
        {
          "id": "allowBulkCertify",
          "type": "boolean",
          "value": false
        }
      ]
    },
    {
      "section": "Display",
      "fields": [
        {
          "id": "userDisplayFormat",
          "type": "string",
          "value": "{{givenName}} {{sn}}
({{userName}})"
        }
      ]
    },
    {
      "section": "Delegation",

```

```

    "fields": [
      {
        "id": "delegationEnabled",
        "type": "boolean",
        "value": false
      },
      {
        "id": "userDelegate",
        "type": "dropdown",
        "value": "manager"
      }
    ]
  },
  {
    "section": "Risk Level Management",
    "fields": [
      {
        "id": "riskLevel",
        "type": "dblSlider",
        "value": {
          "lower": 5,
          "higher": 6
        }
      }
    ]
  },
  {
    "section": "Custom attribute mapping",
    "fields": [
      {
        "id": "userAttrMappings",
        "type": "dropdown",
        "attributes": [
          {
            "id": "givenName",
            "value": "givenName"
          },
          {
            "id": "sn",
            "value": "sn"
          },
          {
            "id": "mail",
            "value": "mail"
          }
        ]
      }
    ]
  }
]

```

```

    ]
    }
  ]
},
{
  "section": "Menu Management",
  "fields": [
    {
      "id": "menuManagement",
      "type": "string",
      "value": []
    }
  ]
}
]
}'

```

## Certifier

### **POST** Event Action - Certify

Certify an entire event.

#### Endpoint

```

{{idmRoot}}/governance/certify/
{{certtype}}/
{{usercertificationid}}/{{stageIndex}}/{{eventIndex}}?
action=certify&actingId={{certifierId}}

```

#### Headers

```

X-OpenIDM-Username  {{endUserUsername}}
X-OpenIDM-Password  {{endUserPassword}}
Content-Type:       application/json

```

#### Params

```

_action          certify (Action to take: certify,
revoke, abstain, certify-remaining, reset, comment, claim,

```

reassign)

**actingId**                    **{{certifierId}}** (ID of acting certifier (user or role)

**queryFilter**                **Target a specific subset of events within the stage**

Body raw

```
{}
```

Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/certify/
{{certtype}}/
{{usercertificationid}}/{{stageIndex}}/{{eventIndex}}?
action=certify&actingId={{certifierId}}' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{}'
```

### **GET** *Get Certification List*

Get the certifier view of the events in a campaign.

Endpoint

```
{{idmRoot}}/governance/certificationList/
{{certtype}}/
{{usercertificationid}}?pageSize={{pageSize}}&pageNumber=0
```

Headers

```
X-OpenIDM-Username    {{endUserUsername}}
X-OpenIDM-Password   {{endUserPassword}}
```

## Params

<b>pageSize</b>	Page size
<b>pageNumber</b>	0
<b>sortBy</b>	
<b>q</b>	
<b>selected</b>	0 (selected stage)

## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/certificationList/
{{certtype}}/
{{usercertificationid}}?pageSize={{pageSize}}&pageNumber=0'
\
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}'
```

## **GET** *Get Certifier Event Details*

Get the certifier view of an event.

## Endpoint

```
{{idmRoot}}/governance/certificationEventDetails/
{{certtype}}/
{{usercertificationid}}/{{stageIndex}}/{{eventIndex}}
```

## Headers

```
X-OpenIDM-Username  {{endUserUsername}}
X-OpenIDM-Password  {{endUserPassword}}
```

## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/certificationEventDetails/
{{certtype}}/
```



```
{{usercertificationid}}/{{stageIndex}}/{{eventIndex}}' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}'
```

### GET Get User Tasks

Returns a list of tasks of the requested type that are assigned to the logged in user either directly or through a role.

#### Endpoint

```
{{idmRoot}}/governance/dashboard?status=active&type=user
```

#### Headers

```
X-OpenIDM-Username  {{endUserUsername}}  
X-OpenIDM-Password  {{endUserPassword}}
```

#### Params

<b>status</b>	active (Active or closed)
<b>type</b>	user (Type of task: user, object, violation)
<b>pageNumber</b>	0 (Page number)
<b>pageSize</b>	Page size (Number of results per page)
<b>sortBy</b>	Property to sort by
<b>q</b>	String to sort by

#### Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/governance/dashboard?status=active&type=user'  
\  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}'
```

### POST Stage Action - Certify Remaining

Certify remaining events in a stage.

#### Endpoint

```
{{idmRoot}}/governance/certify/  
{{certtype}}/  
{{usercertificationid}}/{{stageIndex}}?action=certify-  
remaining&actingId={{certifierId}}
```

#### Headers

```
X-OpenIDM-Username  {{endUserUsername}}  
X-OpenIDM-Password  {{endUserPassword}}  
Content-Type        application/json
```

#### Params

```
action              certify-remaining (action to take:  
certify-remaining, reset, sign-off)  
actingId            {{certifierId}} (ID of acting  
certifier: user or role)  
queryFilter         Target a specific subset of events  
within the stage
```

#### Body raw

```
{}
```

#### Example Request

```
curl --location -g --request POST  
'{{idmRoot}}/governance/certify/  
{{certtype}}/  
{{usercertificationid}}/{{stageIndex}}?action=certify-  
remaining&actingId={{certifierId}}' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json'
```

```
--header 'Content-Type: application/json' \  
--data-raw '{}'
```

### **POST** Stage Action - Reset

Reset events in a stage.

#### Endpoint

```
{{idmRoot}}/governance/certify/  
{{certtype}}/  
{{usercertificationid}}/{{stageIndex}}?  
action=reset&actingId={{certifierId}}
```

#### Headers

```
X-OpenIDM-Username  {{endUserUsername}}  
X-OpenIDM-Password  {{endUserPassword}}  
Content-Type        application/json
```

#### Params

```
action              reset (action to take: certify-  
remaining, reset, sign-off)  
actingId            {{certifierId}} (ID of acting  
certifier: user or role)  
queryFilter         Target a specific subset of events  
within the stage
```

#### Body raw

```
{}
```

#### Example Request

```
curl --location -g --request POST  
'{{idmRoot}}/governance/certify/'
```

```
{{certtype}}/  
{{usercertificationid}}/{{stageIndex}}?  
action=reset&actingId={{certifierId}}' \  
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}' \  
--header 'Content-Type: application/json' \  
--data-raw '{}'
```

### **POST** Stage Action - Sign-off

Sign-off completed events in a stage.

#### Endpoint

```
{{idmRoot}}/governance/certify/  
{{certtype}}/  
{{usercertificationid}}/{{stageIndex}}?action=sign-  
off&actingId={{certifierId}}
```

#### Headers

```
X-OpenIDM-Username  {{endUserUsername}}  
X-OpenIDM-Password  {{endUserPassword}}  
Content-Type        application/json
```

#### Params

```
action              sign-off (action to take: certify-  
remaining, reset, sign-off)  
actingId            {{certifierId}} (ID of acting  
certifier: user or role)  
queryFilter         Target a specific subset of events  
within the stage
```

#### Body raw

```
{}
```

## Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/certify/
{{certtype}}/
{{usercertificationid}}/{{stageIndex}}?action=sign-
off&actingId={{certifierId}}' \
--header 'X-OpenIDM-Username: {{endUserUsername}}' \
--header 'X-OpenIDM-Password: {{endUserPassword}}' \
--header 'Content-Type: application/json' \
--data-raw '{}'
```

## GET Get User Violation Tasks

Get the violations that belong to the logged in user.

### Endpoint

```
{{idmRoot}}/governance/violation?status=active
```

### Headers

```
X-OpenIDM-Username  {{endUserUsername}}
X-OpenIDM-Password  {{endUserPassword}}
```

### Params

<b>status</b>	active (Violation status: active, closed, exception)
<b>sortBy</b>	Sort key
<b>q</b>	Query value
<b>pageSize</b>	Page size (Results per page)
<b>pageNumber</b>	0 (page number of results)

## Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/violation?status=active' \
```

```
--header 'X-OpenIDM-Username: {{endUserUsername}}' \  
--header 'X-OpenIDM-Password: {{endUserPassword}}'
```

## Utility

### **GET** *Get Candidates For Object Attribute*

Get possible values for the given attribute on the given managed object type.

#### Endpoint

```
{{idmRoot}}/governance/getRelationshipObjects?  
managedObject=user&attribute=authzRoles
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{gpvernanceAdminPassword}}  
Content-Type        application/json
```

#### Params

<b>managedObject</b>	user
<b>attribute</b>	authzRoles
<b>pageNumber</b>	0 (page number of results)
<b>pageSize</b>	Page size (Results per page)
<b>sortKey</b>	
<b>ascOrder</b>	

#### Example Request

```
curl --location -g --request GET  
'{{idmRoot}}/governance/getRelationshipObjects?  
managedObject=user&attribute=authzRoles' \  
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'  
\  
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}'
```

```
\
--header 'Content-Type: application/json'
```

### **POST** *Get Candidates For Object Attribute With Filter*

Get possible values for the given attribute on the given managed object type, filtered by provided query.

#### Endpoint

```
{{idmRoot}}/governance/getRelationshipObjects?
managedObject=user&attribute=authzRoles
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type        application/json
```

#### Params

<b>managedObject</b>	user
<b>attribute</b>	authzRoles
<b>pageNumber</b>	0 (page number of results)
<b>pageSize</b>	Page size (Results per page)
<b>sortKey</b>	
<b>ascOrder</b>	

#### Body raw

```
{
  "query": [
    {
      "attribute": "name",
      "operator": "co",
      "path": "managed/role",
      "value": "Admin"
    }
  ]
}
```

```
]
}
```

### Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/getRelationshipObjects?
managedObject=user&attribute=authzRoles' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
  "query": [
    {
      "attribute": "name",
      "operator": "co",
      "path": "managed/role",
      "value": "Admin"
    }
  ]
}'
```

### **GET** *Get Managed Object and System Information*

Get the schema and configuration for managed objects and configured systems.

#### Endpoint

```
{{idmRoot}}/governance/managedObjectConfig
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password {{gpvernanceAdminPassword}}
```

#### Params



<b>type</b>	<b>role (Single managed object to fetch)</b>
-------------	--

#### Example Request

```
curl --location -g --request GET
'{{idmRoot}}/governance/managedObjectConfig' \
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}'
```

### **POST** Parse Target Filter

Run expression parser on given managed object type.

#### Endpoint

```
{{idmRoot}}/governance/expressionParser/user?_action=parse
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}
X-OpenIDM-Password  {{governanceAdminPassword}}
Content-Type        application/json
```

#### Params

<b>_action</b>	<b>parse</b>
----------------	--------------

#### Body raw

```
{
  "operator": "EQUALS",
  "operand": {
    "targetName": "accountStatus",
    "targetValue": "active"
  }
}
```

```
}  
}
```

### Example Request

```
curl --location -g --request POST  
'{{idmRoot}}/governance/expressionParser/user?  
_action=parse' \  
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}'  
\  
--header 'X-OpenIDM-Password: {{governanceAdminPassword}}'  
\  
--header 'Content-Type: application/json' \  
--data-raw '{  
    "operator": "EQUALS",  
    "operand": {  
        "targetName": "accountStatus",  
        "targetValue": "active"  
    }  
}'
```

### **POST** Send Access Review Notification

Get possible values for the given attribute on the given managed object type, filtered by provided query.

#### Endpoint

```
{{idmRoot}}/governance/sendNotification/{{notificationId}}
```

#### Headers

```
X-OpenIDM-Username  {{governanceAdminUsername}}  
X-OpenIDM-Password  {{governanceAdminPassword}}  
Content-Type        application/json
```

#### Params

<b>pageNumber</b>	0 (page number of results)
<b>pageSize</b>	Page size (Results per page)
<b>sortKey</b>	
<b>ascOrder</b>	

#### Body raw

```
{
  "toEmailAddress": "managed/user/1024",
  "certificationName": "Example Certification"
}
```

#### Example Request

```
curl --location -g --request POST
'{{idmRoot}}/governance/sendNotification/{{notificationId}}' \
\
--header 'X-OpenIDM-Username: {{governanceAdminUsername}}' \
\
--header 'X-OpenIDM-Password: {{gpvernanceAdminPassword}}' \
\
--header 'Content-Type: application/json' \
--data-raw '{
  "toEmailAddress": "managed/user/1024",
  "certificationName": "Example Certification"
}'
```