FORGEROCK®

API Guide

/ Autonomous Identity 2020.10.2

Latest update: 2020.10.2

,
, ,

Abstract

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

Table of Contents

Overview iv
1. Introduction to the Autonomous Identity API 1
    Swagger 1
2. Authentication 3
3. Config 5
4. User Details 6
5. Report 10
6. Company View 17
7. Single View with Application 22
8. Role Owner with Application Oriented 25
9. Manager with Application Oriented 28
10. Entitlements 31
11. Rules 34
12. Appcentric View 39
Glossary 43

Overview

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

ForgeRock® Autonomous Identity is an entitlements analytics system that lets you fully manage your company's access to your data.

An entitlement refers to the rights or privileges assigned to a user or thing for access to specific resources. A company can have millions of entitlements without a clear picture of what they are, what they do, and who they are assigned to. Autonomous Identity solves this problem by using advanced artificial intelligence (AI) and automation technology to determine the full entitlements landscape for your company. The system also detects potential risks arising from incorrect or over-provisioned entitlements that lead to policy violations. Autonomous Identity eliminates the manual re-certification of entitlements and provides a centralized, transparent, and contextual view of all access points within your company.

Quick Start

About the API Learn about the Autonomous Identity API	Authentication Learn how to access the Authentication endpoints.	Config Learn about the config endpoint.
User Details Learn about the user details endpoint.	Reports Learn about the Reports API.	Company View Learn about the Company View API.
Single View with App Learn about the single view with app endpoints.	Role Owner with App Learn how to set the role owner with app endpoints.	Manager with App Learn how to set the manager with app endpoints.

Entitlements	Rules	Appcentric View
Learn about the entitlements endpoints.	Learn about the rules endpoints.	Learn about the appcentric view endpoints.

Chapter 1

Introduction to the Autonomous Identity API

Autonomous Identity provides a RESTful application programming interface (API) that lets you use HTTP request methods (GET, PUT, and POST) to interact with the system and its components. The API lets a developer make requests to send or receive data to an Autonomous Identity endpoint, a point where the API communicates with the system. The data that is sent or returned is in JavaScript Object Notation (JSON) format.

Autonomous Identity provides a Swagger client that you can access on the console.

Swagger

The Autonomous Identity installs with a Swagger client that lets you interact with the Autonomous Identity API and the configuration service API. Swagger is a popular software that provides design, build, test, and documentation tools for RESTful APIs.

Access the Autonomous Identity API on Swagger

1. Open a browser, and point it to `https://autoid-ui.forgerock.com/`. Log in to the Autonomous Identity console.
2. Open another browser tab, and point to `https://autoid-ui.forgerock.com/swagger/`. You should see a default Swagger API page.
3. Open another browser tab, and point to `https://autoid-ui.forgerock.com/api/swagger`. You should see a raw text version of the API.
4. Go back to the Swagger page in step 2, and enter `https://autoid-ui.forgerock.com/api/swagger` in the field, and click Explore. You will see the Autonomous Identity API service.

Authorize on Swagger

1. On the Swagger page, scroll down to the Login API.
2. In the Login API section, click POST, and then click Try it out.
3. In the request body, enter the username and password of a user. Click Execute.
4. Scroll down to Response Body, and highlight the returned Bearer Token value.

5. Scroll back to the top of the page, and click Authorize. Enter `Bearer <Token Value>` by pasting in the value of the Bearer Token. Click Authorize. You can close the panel.

   You can now access the Autonomous Identity API endpoints in Swagger.

Access the Autonomous Identity Configuration Service API on Swagger

1. Access the Swagger page as presented in "**Access the Autonomous Identity API on Swagger**".
2. Open another browser tab, and point to `https://autoid-ui.forgerock.com/conf/swagger`. You should see a raw test version of the API.
3. Go back to the Swagger page in step 1, and enter `https://autoid-ui.forgerock.com/conf/swagger` in the field, and click Explore. You will see the Configuration Service API.
4. At the top of the page, click Authorize. Enter `configadmin` and password. The password was set in the `~/autoid-config/vault.yml` during install. Click Authorize, and then close the dialog.

   You can now access the Configuration Service API endpoints in Swagger.

Chapter 2
Authentication

The following are Autonomous Identity authentication endpoints:

POST Login

Log in to the system. The endpoint accepts the `username` and `password` in the body of the request. The token provided has an expiry date that can be obtained by decoding the returned JWT and using the `exp` data inside the token.

Endpoint

```
/api/authentication/login
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Body

```
{
 "username": "admin@test.com",
 "password": "test"
}
```

Example Request

```
curl --location --request POST '/api/authentication/login' \
--header 'Content-Type: application/json' \
--data-raw '{
 "username": "admin@test.com",
 "password": "test"
}'
```

POST renewToken

Renew a token for the system. The endpoint accepts the JWT in the header `Authorization: Bearer $JST`. The expiry time of the token is reset and return in the new token.

Endpoint

```
/api/authentication/renewToken
```

Authorization

```
Token            {{token}}
```

Headers

```
Content-Type      application/json
```

Body

```
''
```

Example Request

```
curl --location --request POST '/api/authentication/renewToken' \
--header 'Content-Type: application/json' \
--data-raw ''
```

GET actions

Retrieve the permitted actions of the currently authenticated user.

Endpoint

```
/api/authentication/action
```

Authorization

```
Token           {{token}}
```

Headers

```
Content-Type      application/json
```

Example Request

```
curl --location --request GET '/api/authentication/actions' \
--header 'Content-Type: application/json'
```

Chapter 3
Config

The following are Autonomous Identity config endpoint:

GET /

Get the configuration. This endpoint is mainly used by the Autonomous Identity UI microservice to get values stored in Consul.

Endpoint

```
/api/config
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Example Request

```
curl --location --request GET '/api/config' \
--header 'Content-Type: application/json'
```

Example Response

```
{
  "thresholds": {
    "top": 1.01,
    "high": 0.75,
    "medium": 0.35,
    "low": 0
  },
  "volumeThresholds": {
    "high": 90,
    "low": 20
  }
}
```

Chapter 4
User Details

The following are Autonomous Identity user details endpoints:

POST /

Get user details.

Endpoint

```
/api/userDetails
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Body

```
{
 "userId": "elizabeth.saiz"
}
```

Example Request

```
curl --location --request POST '/api/userDetails' \
--header 'Content-Type: application/json' \
--data-raw '{
 "userId": "elizabeth.saiz"
}'
```

POST drivingFactor

Get driving factors

Endpoint

```
/api/userDetails/drivingFactor
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Body

```
{
 "entitlement": "Web_NAS_Share_Case Management_7HQ"
}
```

Example Request

```
curl --location --request POST '/api/userDetails/drivingFactor' \
--header 'Content-Type: application/json' \
--data-raw '{
 "entitlement": "Web_NAS_Share_Case Management_7HQ"
}'
```

POST search

Search for user details.

Endpoint

```
/api/userDetails/search
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Body

```
{
 "username": "a"
}
```

Example Request

```
curl --location --request POST '/api/userDetails/search' \
--header 'Content-Type: application/json' \
--data-raw '{
 "username": "elizabeth saiz"
}'
```

Example Response

```
{
  "values": [
    {
      "user": "elizabeth.saiz",
      "isentitlementowner": "true",
      "issupervisor": "true",
      "userdisplayname": "Elizabeth Saiz",
      "userdisplayname_lowercase": null
    }
  ]
}
```

POST Entitlements

Search for entitlements.

Endpoint

```
/api/userDetails/search/ent
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Body

```
{
 "entitlement": "test"
}
```

Example Request

```
curl --location --request POST '/api/userDetails/search/ent' \
--header 'Content-Type: application/json' \
--data-raw '{
 "entitlement": "test"
}'
```

POST Auto Provision

Get auto provision.

Endpoint

```
/api/userDetails/ent/autoprovision
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Body

```
{
 "user": "test"
}
```

Example Request

```
curl --location --request POST '/api/userDetails/ent/autoprovision' \
--header 'Content-Type: application/json' \
--data-raw '{
 "user": "test"
}'
```

GET Entitlement Decisions

Get entitlement decisions.

Endpoint

```
/api/userDetails/decision?user=james.ayache
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Params

```
user              james.ayache
```

Example Request

```
curl --location --request GET '/api/userDetails/decisions?user=james.ayache' \
--header 'Content-Type: application/json' \
--data-raw ''
```

POST Entitlement Decisions

Post entitlement decisions.

Endpoint

```
/api/userDetails/decision
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Example Request

```
curl --location --request POST '{{zoran_api}}userDetails/decision' \
--header 'Content-Type: application/json' \
--data-raw '{
 "users": [
        "james.ayache",
        "other.user"
    ],
    "entitlements": [
        "ABC",
        "DEFFF"
    ],
    "is_certified": true
}'
```

Chapter 5
Report

Autonomous Identity captures information in its log files that are useful when troubleshooting problems. You can access the reports using REST calls to the Reports API endpoint.

POST /EventBasedCertification

Get the event based certification report.

Endpoint

```
/api/report
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Params

```
fields
```

Body

```
{
 "fields": [
  "id",
  "type",
  "batch_id",
  "original",
  "update"
 ],
 "reportType": "EventBasedCertification"
}
```

Example Request

```
curl --location --request POST '/api/report' \
--header 'Content-Type: application/json' \
--data-raw '{
 "fields": [
  "id",
  "type",
  "batch_id",
  "original",
  "update"
 ],
 "reportType": "EventBasedCertification"
}'
```

POST /RoleMining

Get the role mining report.

Endpoint

```
/api/report
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Params

```
fields
```

Body

```
{
 "fields": [
  "entt_id",
  "entt_name",
  "policy",
  "role",
  "total_employees",
  "total_entts"
 ],
 "reportType": "RoleMining"
}
```

Example Request

```
curl --location --request POST '/api/report' \
--header 'Content-Type: application/json' \
--data-raw '{
 "fields": [
  "user_name"
 ],
 "reportType": "RoleMining"
}'
```

POST /AnomalyReport

Get the anomaly report.

Endpoint

```
/api/report
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Params

```
fields
```

Body

```
{
 "fields": [
  "app_name",
  "avg_conf_score",
  "confidence",
  "entitlement",
  "entitlement_name",
  "freq",
  "frequnion",
  "justification",
  "last_usage",
  "manager_name",
  "median",
  "num_below_conf_threshold",
  "percent_below_threshold",
  "total_assignees",
  "user",
  "user_name"
 ],
 "reportType": "AnomalyReport"
}
```

Example Request

```
curl --location --request POST '/api/report' \
--header 'Content-Type: application/json' \
--data-raw '{
 "fields": [
  "app_name",
  "avg_conf_score",
  "confidence",
  "entitlement",
  "entitlement_name",
  "freq",
  "frequnion",
  "justification",
  "last_usage",
  "manager_name",
  "median",
  "num_below_conf_threshold",
  "percent_below_threshold",
  "total_assignees",
  "user",
  "user_name"
 ],
 "reportType": "AnomalyReport"
}'
```

POST /RecommendPredictions

Get the Recommend Predictions report.

Endpoint

```
/api/report
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Params

```
fields
```

Body

```
{
 "fields": [
  "conf",
  "ent",
  "freq",
  "frequnion",
  "rule",
  "usr_key"
 ],
 "reportType": "RecommendPredictions"
}
```

Example Request

```
curl --location --request POST '/api/report' \
--header 'Content-Type: application/json' \
--data-raw '{
 "fields": [
  "conf",
  "ent",
  "freq",
  "frequnion",
  "rule",
  "usr_key"
 ],
 "reportType": "RecommendPredictions"
}'
```

POST /AutoRecertificationFeed & FullOutputFeed

Get the Auto Recertification Feed report.

Endpoint

```
/api/report
```

Authorization

```
Bearer Token <JWT-value>
```

Headers

```
Content-Type      application/json
```

Params

```
fields
```

Body

```
{
 "fields": [
  "app_id",
  "app_name",
  "auto_recert",
  "chiefyesno",
  "city",
  "costcenter",
  "ent_size",
  "entitlement",
  "entitlement_name",
  "event_recert",
  "freq",
  "frequnion",
  "jobcodename",
  "justification",
  "lineofbusiness",
  "lineofbusinesssubgroup",
  "managername",
  "score",
  "user",
  "user_name",
  "userdepartmentname",
  "userdisplayname",
  "usremptype",
  "usrmanagerkey"
 ],
 "reportType": "AutomaticRecertificationFeed"
}
```

Example Request

```
curl --location --request POST '/api/report' \
--header 'Content-Type: application/json' \
--data-raw '{
 "fields": [
  "app_id",
  "app_name",
  "auto_recert",
  "chiefyesno",
  "city",
  "costcenter",
  "ent_size",
  "entitlement",
  "entitlement_name",
  "event_recert",
  "freq",
  "frequnion",
  "jobcodename",
  "justification",
  "lineofbusiness",
  "lineofbusinesssubgroup",
  "managername",
  "score",
  "user",
  "user_name",
  "userdepartmentname",
  "userdisplayname",
  "usremptype",
  "usrmanagerkey"
 ],
 "reportType": "AutomaticRecertificationFeed"
}'
```

Chapter 6
Company View

The following are Autonomous Identity company view endpoints:

GET /

Get the data for company view.

Endpoint

```
/api/companyview
```

Authorization

```
Bearer Token <JWT-value>
```

Example Request

```
curl --location --request GET '/api//companyview'
```

GET allEntitlementsAvgGroups

Get the company view all entitlements average groups.

Endpoint

```
/api/companyview/allEntitlementAvgGroups
```

Authorization

```
Bearer Token <JWT-value>
```

Example Request

```
curl --location --request GET '/api//companyview/allEntitlementAvgGroups'
```

GET entitlementAvgGroupDetails Start End

Get the company view entitlements average groups.

Endpoint

```
/api/companyview/entitlementAvgGroupDetails/0.1/0.15
```

Authorization

```
Bearer Token <JWT-value>
```

Example Request

```
curl --location --request GET '/api//companyview/entitlementAvgGroupDetails/0.1/0.15'
```

GET mostCriticalEntitlements

Get the company view most critical entitlements.

Endpoint

```
/api/companyview/mostCriticalEntitlements
```

Authorization

```
Bearer Token <JWT-value>
```

Example Request

```
curl --location --request GET '/api//companyview/mostCriticalEntitlements'
```

GET Assignment Stats

Get the company view assignment statistics.

Endpoint

```
/api/companyview/assignmentsStats
```

Authorization

```
Bearer Token <JWT-value>
```

Params

```
assignmentLimit  1
highVolumeHighMinScore  0.9
highVolumentHighMinUsersCount 100
highVolumenLowMaxScore  0.2
highVolumeLowMinUsersCount 100
```

Example Request

```
curl --location --request GET '/api/companyview/assignmentsStats?
assignmentsLimit=1&highVolumeHighMinScore=0.9&highVolumeHighMinUsersCount=100&highVolumeLowMaxScore=0.2&highVol
```

GET assignmentHistConfSummary

Get the company view assignment history summary.

Endpoint

```
/api/companyview/assignmentsHistConfSummary/2020/01
```

Authorization

```
Bearer Token <JWT-value>
```

Example Request

```
curl --location --request GET '/api//companyview/assignmentsHistConfSummary/2020/01'
```

GET Assignments High Threshold

Get the company view assignment high thresholds.

Endpoint

```
/api/companyview/assignments
```

Authorization

```
Bearer Token     <JWT-value>
```

Params

```
lowThreshold   true
highThreshold  true
unscored       true
```

Example Request

```
curl --location --request GET '/api/companyview/assignments'
```

GET Entitlements Without Owner

Get the company view assignment high thresholds.

Endpoint

```
/api/companyview/entitlementsWithoutOwner
```

Authorization

```
Bearer Token <JWT-value>
```

Example Request

```
curl --location --request GET '/api/companyview/entitlementsWIthoutOwner'
```

GET Users without manager

Get the company view users without a manager.

Endpoint

```
/api/companyview/usersWithoutManager
```

Authorization

```
Bearer Token <JWT-value>
```

Params

```
lowThreshold   true
highThreshold  true
unscored       true
```

Example Request

```
curl --location --request GET '/api/companyview/usersWithoutManager'
```

GET coverage

Get the company view coverage.

Endpoint

```
/api/companyview/coverage
```

Authorization

```
Bearer Token <JWT-value>
```

Example Request

```
curl --location --request GET '/api//companyview/coverage'
```

GET companyViewEntitlementse

Get the company view entitlements.

Endpoint

```
/api/companyview/companyViewEntitlements
```

Authorization

```
Bearer Token <JWT-value>
```

Example Request

```
curl --location --request GET '/api//companyview/companyViewEntitlements'
```

GET companyViewEmployeeTypes

Get the company view employee types.

Endpoint

```
/api/companyview/companyViewEmployeeTypes
```

Authorization

```
Bearer Token <JWT-value>
```

Example Request

```
curl --location --request GET '/api//companyview/companyViewEmployeeTypes'
```

Chapter 7
Single View with Application

The following are Autonomous Identity single view with applications endpoints:

POST employees

Get an employee's entitlements and statistics.

Endpoint

```
/api/singleViewWithApp/employees
```

Authorization

```
Bearer Token <JWT-value>
```

Body

```
{
 "employeeId": "elizabeth.saiz",
 "includeLastAccessed": true,
 "pageSize": 5
}
```

Example Request

```
curl --location --request POST '/api//singleViewWithApp/employees' \
--header 'Content-Type: application/json' \
--data-raw '{
 "employeeId": "elizabeth.saiz",
 "pageSize": 2,
 "lastEntitlementId": "0ff681de-ee83-4ab1-82b5-d1cd754a7e28"
}'
```

Example Response

```
{
  "high": 0,
  "medium": 1,
  "low": 1,
  "avg_score": 0.25,
  "app_name": "",
  "app_id": "",
  "entitlement_name": "",
  "high_risk": null,
  "userEntt": [
    {
      "user": "elizabeth.saiz",
      "entitlement": "192aed21-a7d1-40c3-87a3-9dfa4a3d21f5",
      "app_id": "null",
      "app_name": "test3",
      "entitlement_name": "null",
      "freq": null,
      "frequnion": null,
      "high_risk": "null",
      "justification": [],
      "score": 0.1,
      "user_name": "alpha"
    },
    {
      "user": "elizabeth.saiz",
      "entitlement": "36bad416-d42c-47c2-991e-623aa3833028",
      "app_id": "null",
      "app_name": "test6",
      "entitlement_name": "null",
      "freq": null,
      "frequnion": null,
      "high_risk": "null",
      "justification": [],
      "score": 0.4,
      "user_name": "vce"
    }
  ],
  "user": "elizabeth.saiz",
  "entitlementsCount": 14,
  "entitlementsRemainingCount": 10,
  "lastEntitlementId": "36bad416-d42c-47c2-991e-623aa3833028"
}
```

GET entitlements/:entitlementId

Get an entitlement's statistics and list of assigned users.

Endpoint

```
/api/singleViewWithApp/entitlements/0ac4b36b-20d9-4848-a923-0084a7aa581d
```

Authorization

```
Bearer Token <JWT-value>
```

Body

```
pageSize       2
lastUserId     bgs
sortDir        desc
onlyLM         1
```

Example Request

```
curl --location --request GET '/api//singleViewWithApp/entitlements/0ac4b36b-20d9-4848-
a923-0084a7aa581d?pageSize=2' \
--header 'Content-Type: application/json'
```

Example Response

```
{
  "high": 0,
  "medium": 2,
  "low": 0,
  "avg_score": 0.6,
  "app_name": "app16",
  "app_id": "null",
  "entitlement_name": "null",
  "high_risk": "null",
  "enntId": "0ac4b36b-20d9-4848-a923-0084a7aa581d",
  "users": [
    {
      "user": "elizabeth.saiz",
      "app_id": "null",
      "freq": null,
      "frequnion": null,
      "justification": [],
      "score": 0.7,
      "user_name": "eliz"
    },
    {
      "user": "fred",
      "app_id": "null",
      "freq": null,
      "frequnion": null,
      "justification": [],
      "score": 0.5,
      "user_name": "fred"
    }
  ],
  "usersCount": 12,
  "usersRemainingCount": 8,
  "lastUserId": "fred"
}
```

Chapter 8
Role Owner with Application Oriented

The following are Autonomous Identity role owner with applications endpoints:

POST unscoredEntitlements

Get unscored entitlements for role owners.

Endpoint

```
/api/roleOwnerWithAppOriented/unscoredEntitlements
```

Authorization

```
Bearer Token <JWT-value>
```

Body

```
{
 "roleOwnerId": "supervisor"
}
```

Example Request

```
curl --location --request POST '/api//roleOwnerWithAppOriented/unscoredEntitlements' \
--header 'Content-Type: application/json' \
--data-raw '{
 "roleOwnerId": "supervisor"
}'
```

POST entownuserdata

Get entitlement owner user data.

Endpoint

```
/api/roleOwnerWithAppOriented/entownuserdata
```

Authorization

```
Bearer Token <JWT-value>
```

Body

```
{
 "roleOwnerId": "elizabeth.saiz"
}
```

Example Request

```
curl --location --request POST '/api//roleOwnerWithAppOriented/entownuserdata' \
--header 'Content-Type: application/json' \
--data-raw '{
 "roleOwnerId": "26713",
 "onlyLM": "1"
}'
```

Example Response

```
{
  "roleOwner": {
    "roleOwnerId": "26713",
    "total_entitlements": 1,
    "total_subordinates": 1,
    "unscoredEntitlements": 0,
    "scoredEntitlements": 1,
    "entitlementsWithNoUser": 0,
    "entitlements": [
      {
        "app_id": "1",
        "app_name": "1",
        "entitlement": "1",
        "entitlement_name": "1",
        "high_risk": "1",
        "high": 0,
        "medium": 0,
        "low": 1,
        "avg": "0.20"
      }
    ],
    "distinctApps": [
      {
        "app_id": "1",
        "app_name": "1"
      }
    ]
  }
}
```

POST entownentdata

Get entitlement owner entitlement data.

Endpoint

```
/api/roleOwnerWithAppOriented/entownentdata
```

Authorization

```
Bearer Token <JWT-value>
```

Body

```
{
 "roleOwnerId": "elizabeth.saiz"
}
```

Example Request

```
curl --location --request POST '/api//roleOwnerWithAppOriented/entownuserdata' \
--header 'Content-Type: application/json' \
--data-raw '{
 "roleOwnerId": "26713",
 "onlyLM": "1"
}'
```

Example Response

```
{
  "roleOwner": {
    "roleOwnerId": "26713",
    "total_entitlements": 1,
    "total_subordinates": 1,
    "unscoredEntitlements": 0,
    "scoredEntitlements": 1,
    "entitlementsWithNoUser": 0,
    "entitlements": [
      {
        "app_id": "1",
        "app_name": "1",
        "entitlement": "1",
        "entitlement_name": "1",
        "high_risk": "1",
        "high": 0,
        "medium": 0,
        "low": 1,
        "avg": "0.20"
      }
    ],
    "distinctApps": [
      {
        "app_id": "1",
        "app_name": "1"
      }
    ]
  }
}
```

Chapter 9
Manager with Application Oriented

The following are Autonomous Identity manager with application oriented endpoints:

GET applications (portfolio)

Get application information.

Endpoint

```
/api/applications
```

Authorization

```
Bearer Token      <JWT-value>
```

Body

```
{
  "managerId": "Christy.Cronin",
  "pageSize": 2,
    "lastEntitlementId": "test2",
    "sortDir": "desc"
}
```

Example Request

```
curl --location --request POST '/api/managersWithAppOriented/unscoredEntitlements' \
--header 'Content-Type: application/json' \
--data-raw '{
 "managerId": "Christy.Cronin",
 "pageSize": 2,
    "lastEntitlementId": "test2",
    "sortDir": "desc"
}'
```

Example Response

```
{
  "managerId": "Christy.Cronin",
  "users": [
    {
      "userId": "bloggs",
      "entt": [
        {
          "entitlement": "test",
          "entitlement_name": null,
          "user_name": null,
          "app_name": null
        }
      ]
    },
    {
      "userId": "elizabeth.saiz",
      "entt": []
    }
  ],
  "entitlementsCount": 4,
  "entitlementsRemainingCount": 0,
  "lastEntitlementId": "test"
}
```

POST supervisor

Get supervisor info.

Endpoint

```
/api/managersWithAppOriented/supervisor
```

Authorization

```
Bearer Token <JWT-value>
```

Body

```
{
 "managerId": "Christy.Cronin"
}
```

Example Request

```
curl --location --request POST '/api/managersWithAppOriented/supervisor' \
--header 'Content-Type: application/json' \
--data-raw '{
 "managerId": "Christy.Cronin"
}'
```

POST supervisorEntitlements

Get supervisor entitlements.

Endpoint

```
/api/managersWithAppOriented/supervisorEntitlements
```

Authorization

```
Bearer Token <JWT-value>
```

Body

```
{
 "managerId": "Christy.Cronin"
}
```

Example Request

```
curl --location --request POST '/api/managersWithAppOriented/supervisorEntitlements' \
--header 'Content-Type: application/json' \
--data-raw '{
 "managerId": "Christy.Cronin"
}'
```

POST supervisorUser

Get supervisor User.

Endpoint

```
/api/managersWithAppOriented/supervisorUser
```

Authorization

```
Bearer Token <JWT-value>
```

Body

```
[../resources/rules.bash:#post-supervisorUser-body]
```

Example Request

```
curl --location --request POST '/api/managersWithAppOriented/supervisorUser' \
--header 'Content-Type: application/json' \
--data-raw '{
 "managerId": "Christy.Cronin"
}'
```

Chapter 10 Entitlements

The following are Autonomous Identity filtering by entitlements endpoints:

GET Filters by Entt Owners

Get filterable attributes and values by entitlement owner.

Endpoint

```
/api/entitlements/filters?by=entitlementOwner&ownerId=timothy.slack
```

Authorization

```
Bearer Token <JWT-value>
```

GET Filters by Supervisor

Get filterable attributes and values by supervisors.

Endpoint

```
/api/entitlements/filters?by=supervisor&ownerId=albert.pardini
```

Authorization

```
Bearer Token <JWT-value>
```

Body

```
by      supervisor
ownerId  albert.pardini
```

Example Request

```
curl --location --request GET '/api/entitlements/filters&#63;by=supervisor&amp;ownerId=albert.pardini'
 \
--header 'content-type: application/json'
```

POST Statistics by Entt Owner

Set entitlment statistics for entitlement owners with optional filters.

Endpoint

```
/api/entitlements/stats?by=entitlementOwner
```

Authorization

```
Bearer Token <JWT-value>
```

Params

```
by      entitlementOwner
```

Body

```
{
 "ownerId": "timothy.slack",
 "isHighRiskOnly": true,
 "isMediumLowRiskOnly": false,
 "isUserEntitlementsIncluded": true,
 "filters": [{
  "type": "app_id",
  "group": "criticality",
  "value": "Essential"
 }]
}
```

Example Request

```
curl --location --request POST '/api/entitlements/stats&#63;by=entitlementOwner' \
--header 'content-type: application/json' \
--data-raw '{
 "ownerId": "timothy.slack",
 "isHighRiskOnly": true,
 "isMediumLowRiskOnly": false,
 "isUserEntitlementsIncluded": true,
 "filters": [{
  "type": "app_id",
  "group": "criticality",
  "value": "Essential"
 }]
}'
```

POST Statistics by Supervisor

Set entitlement statistics for supervisors with optional filters.

Endpoint

```
/api/entitlements/stats?by=supervisor
```

Authorization

```
Bearer Token <JWT-value>
```

Params

```
by      supervisor
```

Body

```
{
 "ownerId": "albert.pardini",
 "isHighRiskOnly": true,
 "isMediumLowScoreOnly": true,
 "isUserEntitlementsIncluded": true,
 "filters": [{
  "type": "app_id",
  "group": "criticality",
  "value": "Essential"
 }]
}
```

Example Request

```
curl --location --request POST '/api/entitlements/stats&#63;by=supervisor' \
--header 'content-type: application/json' \
--data-raw '{
 "ownerId": "albert.pardini",
 "isHighRiskOnly": true,
 "isMediumLowScoreOnly": true,
 "isUserEntitlementsIncluded": true,
 "filters": [{
  "type": "app_id",
  "group": "criticality",
  "value": "Essential"
 }]
}'
```

Chapter 11
Rules

The following are Autonomous Identity rules endpoints:

GET Rule Stats

Get rules statistics.

Endpoint

```
/api/rules/info
```

Authorization

```
Bearer Token     <JWT-value>
```

Params

```
by       appOwner
user     patrick.murphy
```

Example Request

```
curl --location --request GET '{{zoran_api}}rules/info?by=appOwner&user=patrick.murphy \
  --header 'content-type: application/json'
```

Example Response

```
{
  "countRules": 4970,
  "countAssignments": 13085,
  "countApplications": 2,
  "countHighConfidence": 2351,
  "countMediumConfidence": 836,
  "countLowConfidence": 956,
  "applications": [
    {
      "app_id": "Ensuite Oracle DB",
      "app_name": "Ensuite Oracle DB",
      "countAssignments": 8678,
      "low": 1213,
      "medium": 1103,
      "high": 4905
    },
    {
      "app_id": "SAP Finance",
      "app_name": "SAP Finance",
      "countAssignments": 6816,
      "low": 1308,
      "medium": 1041,
      "high": 3515
    }
  ]
}
```

GET Rule Stats by Entt Owner

Get rules statistics by entitlement owners.

Endpoint

```
/api/rules/info
```

Authorization

```
Bearer Token     <JWT-value>
```

Params

```
by       enttOwner
user     david.elliott
```

Example Request

```
curl --location --request GET '{{zoran_api}}rules/info?by=enttOwner&user=david.elliott \
  --header 'content-type: application/json'
```

GET Rule Stats by App Owner

Get rules statistics by application owner.

Endpoint

```
/api/rules/info
```

Authorization

```
Bearer Token     <JWT-value>
```

Params

```
by       enttOwner
user     derick.hui
```

Example Request

```
curl --location --request GET '{{zoran_api}}rules/info?by=appOwner&user=derick.hui \
  --header 'content-type: application/json'
```

GET Rule Search

Get detailed rule information with optional filtering.

Endpoint

```
/api/rules
```

Authorization

```
Bearer Token    <JWT-value>
```

Example Request

```
curl --location --request GET '{{zoran_api}}rules?
by=appOwner&user=patrick.murphy&filter[highConfidence]=true&filter[medConfidence]=true&filter[app_id]
[]=Gateway \
--header 'content-type: application/json'
```

GET Rule Search by Entt Owner

Get detailed rule information with optional filtering by entitlement owner.

Endpoint

```
/api/rules
```

Authorization

```
Bearer Token    <JWT-value>
```

Example Request

```
curl --location --request GET '{{zoran_api}}rules?
by=enttOwner&user=david.elliott&filter[highConfidence]=true&filter[medConfidence]=true&filter[app_id]
[]=Gateway \
--header 'content-type: application/json'
```

GET Rule Search by App Owner

Get detailed rule information with optional filtering by application owner.

Endpoint

```
/api/rules
```

Authorization

```
Bearer Token    <JWT-value>
```

Example Request

```
curl --location --request GET '{{zoran_api}}rules?
by=appOwner&user=derick.hui&filter[highConfidence]=true&filter[medConfidence]=true&filter[app_id]
[]=Gateway \
--header 'content-type: application/json'
```

POST Rule Decision

Get rule decisions.

Endpoint

```
/api/rules/decision
```

Authorization

```
Bearer Token        <JWT-value>
```

Body

```
{
    "rules": [
        {
            "entitlement": "AccessType : XMLP_ADMIN_II_NYC",
            "justification": [
                "0C_CHIEF_YES_NO_Yes",
                "0C_JOBCODE_NAME_Service Representitive II",
                "0C_MANAGER_NAME_Jonathan Baxter",
                "0C_USR_EMP_TYPE_Non-Employee"
            ]
        }
    ],
    "is_autocertify": false,
    "is_autorequest": false,
    "reason": "Goodbye, world."
}
```

Example Request

```
curl --location --request POST '{{zoran_api}}rules/decision' \
--header 'content-type: application/json' \
--data-raw '{
    "rules": [
        {
            "entitlement": "AccessType : XMLP_ADMIN_II_NYC",
            "justification": [
                "0C_CHIEF_YES_NO_Yes",
                "0C_JOBCODE_NAME_Service Representitive II",
                "0C_MANAGER_NAME_Jonathan Baxter",
                "0C_USR_EMP_TYPE_Non-Employee"
            ]
        }
    ],
    "is_autocertify": false,
    "is_autorequest": false,
    "reason": "Goodbye, world."
}'
```

Chapter 12
Appcentric View

The following are Autonomous Identity appcentric view endpoints:

GET Application Statistics

Get application statistics.

Endpoint

```
/api/applications
```

Authorization

```
Bearer Token     <JWT-value>
```

Params

```
ownerId (optional)   derick.hui
cursor (optional)    eyJjb25mIjoxLCJlbnQiOiJDUlVzZXJzUHJvZCIsImp1c3RpZmljY
```

Example Request

```
curl --location --request GET '{{zoran_api}}/applications'
```

Example Response

```
{
  "cursor": null,
  "total_applications": 7,
  "total_entitlements": 2591,
  "total_assignments": 50955,
  "applications": [
    {
      "app_id": "Active Directory",
      "app_name": "Active Directory",
      "high": 3994,
      "medium": 832,
      "low": 632,
      "avg": 0.785633931961286
    },
    {
      "app_id": "Care ",
      "app_name": "Care ",
      "high": 4215,
      "medium": 923,
      "low": 649,
      "avg": 0.7880940041207878
    }
  ]
}
```

POST Assignments Search

Make assignments search.

Endpoint

```
/api/applications/{appID}/assignments
```

Authorization

```
Bearer Token    <JWT-value>
```

Params

```
cursor (optional)     eyJjb25mIjoxLCJlbnQiOiJDUlVzZXJzUHJvZCIsImp1c3RpZmljY
```

Body

```
{
  "filters": [
    {
      "type": "user",
      "attribute": "city",
      "value": ["Seattle", "Denver"]
    },
    {
      "type": "user",
      "attribute": "line_of_business",
      "value": ["Distribution Operations"]
    }
  ]
}
```

Request

```
curl --location --request POST '{{zoran_api}}/applications/{appID}/assignments?user=jay.dowke' \
--data-raw '{
  "filters": [
    {
      "type": "user",
      "attribute": "city",
      "value": ["Seattle", "Denver"]
    },
    {
      "type": "user",
      "attribute": "line_of_business",
      "value": ["Distribution Operations"]
    }
  ]
}'
```

POST Application Search

Get detailed information for a single application with optional filtering.

Endpoint

```
/api/applications/${appID}
```

Authorization

```
Bearer Token        <JWT-value>
```

Params

```
cursor         eyJjb25mIjoxLCJlbnQiOiJDUlVzZXJzUHJvZCIsImp1c3RpZmljY
```

Body

```
{
    "filters":[
        {
            "type": "user",
            "attribute": "city",
            "value": ["Seattle", "Denver"]
        }
    ]
}
```

Example Request

```
curl --location --request POST '{{zoran_api}}/applications/{appID}}' \
--data-raw '{
    "filters":[
        {
            "type": "user",
            "attribute": "city",
            "value": ["Seattle", "Denver"]
        }
    ]
}'
```

GET filters

Get filterable attributes and values for the AppCentric view.

Endpoint

```
/api/applications/{appID}/filters
```

Authorization

```
Bearer Token        <JWT-value>
```

Example Request

```
curl --location --request GET '{{zoran_api}}/applications/{appID}/filters'
```

Glossary

anomaly report

A report that identifies potential anomalous assignments.

as-is predictions

A process where confidence scores are assigned to the entitlements that users have.

auto-certify

An action that an entitlement owner can do to approve a justification. Auto-certify indicates that anyone who has the justification is automatically approved for the entitlement.

auto-request

An action that an entitlement owner can do to approve a justification. Auto-request indicates that anyone who matches these justification attributes but may not already have access should automatically get provisioned for this entitlement.

confidence score

A score from a scale from 0 to 100% that indicates the strength of correlation between an assigned entitlement and a user's data profile.

data audit

A pre-analytics process that audits the seven data files to ensure data validity with the client.

data ingestion

A pre-analytics process that pushes the seven .csv files into the Cassandra database. This allows the entire training process to be performed from the database.

data sparsity

A reference to data that has null values. Autonomous Identity requires dense, high quality data with very few null values in the user attributes to get accurate analysis scores.

data validation

A pre-analytics process that tests the data to ensure that the content is correct and complete prior to the training process.

driving factor

An association rule that is a key factor in a high entitlement confidence score. Any rule that exceeds a confidence threshold level (e.g., 75%) is considered a driving factor.

entitlement

An entitlement is a specialized type of `assignment`. A user or device with an entitlement gets access rights to specified resources.

insight report

A report that provides metrics on the rules and predictions generated in the analytics run.

recommendation

A process run after the as-is predictions that assigns confidence scores to all entitlements and recommends entitlements that users do not currently have. If the confidence score meets a threshold, set by the `conf_thresh` property in the configuration file, the entitlement will be recommended to the user in the UI console.

resource

An external system, database, directory server, or other source of identity data to be managed and audited by an identity management system.

REST

Representational State Transfer. A software architecture style for exposing resources, using the technologies and protocols of the World Wide Web. REST describes how distributed data objects, or resources, can be defined and addressed.

stemming

A process that occurs after training that removes similar association rules that exist in a parent-child relationship. If the child meets three criteria, then it will be removed by the system. The criteria are: 1) the child must match the parent; 2) the child (e.g., [San Jose, Finance]) is a superset of the parent rule. (e.g., [Finance]); 3) the child and parent's confidence scores are within a +/- range of each other. The range is set in the configuration file.

training

A multi-step process that generates the association rules with confidence scores for each entitlement. First, Autonomous Identity models the frequent itemsets that appear in the user attributes for each user. Next, Autonomous Identity merges the user attributes with the entitlements that were assigned to the user. It then applies association rules to model the sets of user attributes that result in an entitlement access and calculates confidence scores, based on their frequency of appearances in the dataset.