An Overview of Cloud Identity RAPIs

—

Ross Holman
Identity and Access Management Support Professional

IBM Security

IBM

Join IBM VIP Rewards

Engage. Earn points. Get Rewards.

Learn more… ibm.biz/vip-rewards	Join IBM VIP Rewards for Security… ibm.biz/JoinIBMVIPRewards-Security

IBM

IBM VIP Rewards for Security

IBM Security Learning Academy

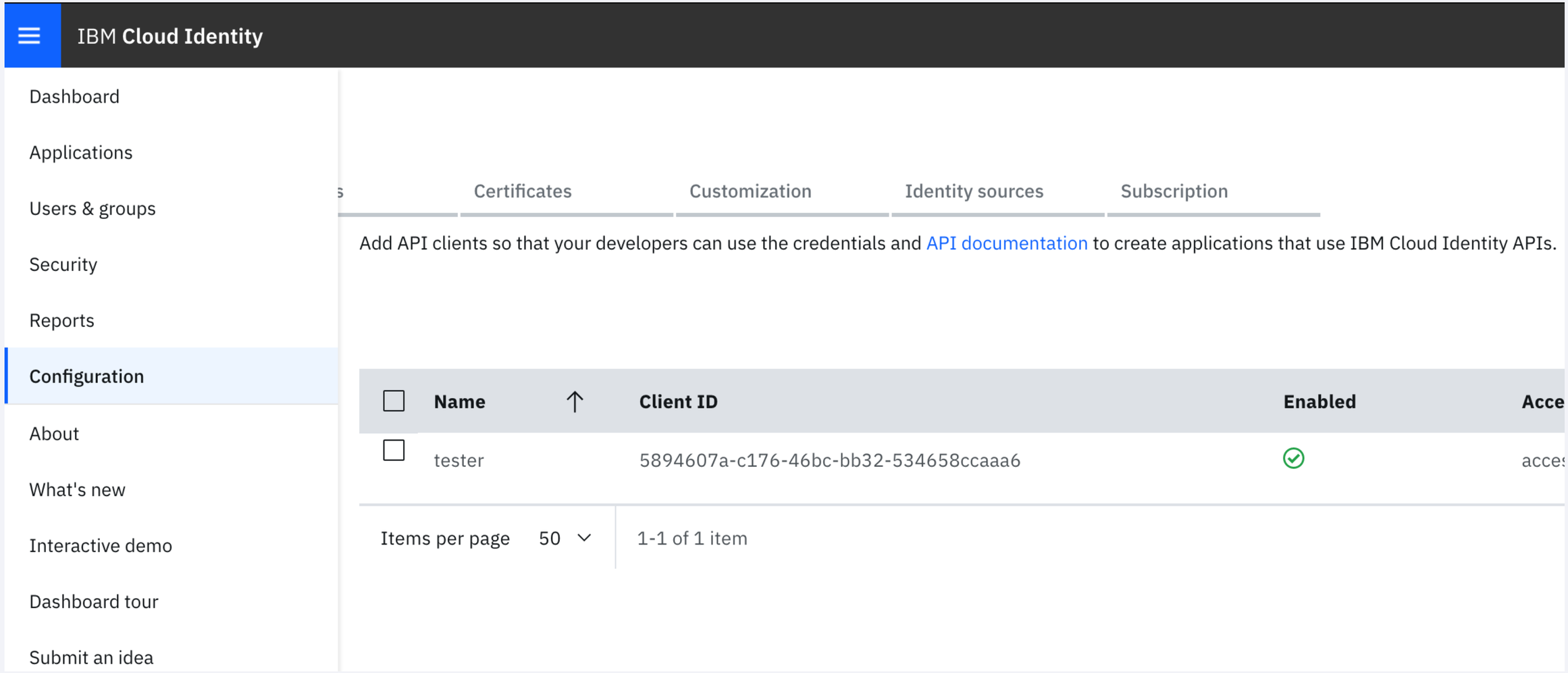
- Courses
- Videos
- Hands-on Labs
- Live Events
- Badges

Learning at no cost.

New content published daily.

Table of contents

Locating Rest APIs in the CI Environment



Reviewing the Swagger Format

IBM Cloud Identity API

Use these API definitions to develop and integrate applications with the IBM Cloud Identity services such as authentication, customization, users and groups management, and others. A new version of the API will be released if there are attributes that are removed or renamed. New resources, parameters, or attributes can be added without advance notice. When you use these APIs, ignore the unrecognized response parameters.

Access Policy Management	Show/Hide | List Operations | Expand Operations
Admin Entitlement Management	Show/Hide | List Operations | Expand Operations
API Clients	Show/Hide | List Operations | Expand Operations
Application Access	Show/Hide | List Operations | Expand Operations
Attributes	Show/Hide | List Operations | Expand Operations
Authentication Factors v1.0 (deprecated)	Show/Hide | List Operations | Expand Operations
Authentication Factors v2.0	Show/Hide | List Operations | Expand Operations
Authentication Methods	Show/Hide | List Operations | Expand Operations
Authentication Token Exchange	Show/Hide | List Operations | Expand Operations
Authenticator Clients	Show/Hide | List Operations | Expand Operations
Authenticators	Show/Hide | List Operations | Expand Operations
Certificates	Show/Hide | List Operations | Expand Operations
Certification Campaign assignments	Show/Hide | List Operations | Expand Operations
Certification Campaign configurations	Show/Hide | List Operations | Expand Operations
Certification Campaign instances	Show/Hide | List Operations | Expand Operations

Reviewing the Swagger Format

Reports

Show/Hide | List Operations | Expand Operations

POST /v1.0/reports/export/{name} — Export reports for a specified tenant into CSV file.

POST /v1.0/reports/{name} — Run a report.

Implementation Notes

This endpoint is used to run most of the reports. Provide the report name and request payload in the body section.
For example: POST /reporting/v1.0/reports/auth_audit_trail API is used to the get first batch of authentication events.
Use POST /reporting/v1.0/reports/auth_audit_trail_search_after API to get the ramaining events.
Entitlements required: readReports, or manageReports.
Some example report names to retrieve are authentication activity, application usage, admin activity and user activity. Their example request payload are also listed.
NOTE:The default values for SORT_ORDER - desc, SORT_BY- time, FROM - now-24h, TO - now, and SIZE - 10. The range for size is 1 to 10000. The TENANT ID is supplied implicitly by x-forwared-host.

Report Name	Example Payload Request
auth_audit_trail	{ "FROM":"now-24h", "TO":"now", "SIZE":"10", "SORT_BY":"time", "SORT_ORDER":"asc" }
auth_audit_trail_search_after	{ "FROM":"now-24h", "TO":"now", "SIZE":"10", "SORT_BY":"time", "SORT_ORDER":"asc", "SEARCH_AFTER":"\"1554479231870\",\"30f5a726-0e11-4066-a49f-e1e1d03a62b4\"" } The SEARCH_AFTER value is an array of the timestamp and ID of the last response entry from the auth_audit_trail report
app_audit_trail	{ "APPID":"481222907047286663", "FROM":"now-24h", "TO":"now", "SIZE":"10", "SORT_BY":"time", "SORT_ORDER":"asc" }
app_audit_trail_search_after	{ "APPID":"481222907047286663", "FROM":"now-24h", "TO":"now", "SIZE":"10", "SORT_BY":"time", "SORT_ORDER":"asc", "SEARCH_AFTER":"\"1554479231870\",\"30f5a726-0e11-4066-a49f-e1e1d03a62b4\"" } The SEARCH_AFTER value is an array of the timestamp and ID of the last response entry from the app_audit_trail report
admin_activity	{ "FROM":"now-24h", "TO":"now", "SIZE":"10", "SORT_BY":"time", "SORT_ORDER":"asc" }
admin_activity_search_after	{ "FROM":"now-24h", "TO":"now", "SIZE":"10", "SORT_BY":"time", "SORT_ORDER":"asc", "SEARCH_AFTER":"\"1554479231870\",\"30f5a726-0e11-4066-a49f-e1e1d03a62b4\"" } The SEARCH_AFTER value is an array of the timestamp and ID of the last response entry from the admin_activity report
user_activity	{ "USERID":"507W22XX4W", "USERNAME":"scott@cse-bank.net", "REALM":"cloudIdentityRealm", "FROM":"now-24h", "TO":"now", "SIZE":"10", "SORT_BY":"time", "SORT_ORDER":"asc" }
user_activity_search_after	{ "USERID":"507W22XX4W", "USERNAME":"scott@cse-bank.net", "REALM":"cloudIdentityRealm", "FROM":"now-24h", "TO":"now", "SIZE":"10", "SORT_BY":"time", "SORT_ORDER":"asc", "SEARCH_AFTER":"\"1554479231870 \",\"30f5a726-0e11-4066-a49f-e1e1d03a62b4\"" } The SEARCH_AFTER value is an array of the timestamp and ID of the last response entry from the user_activity report

Response Class (Status 200)

Success

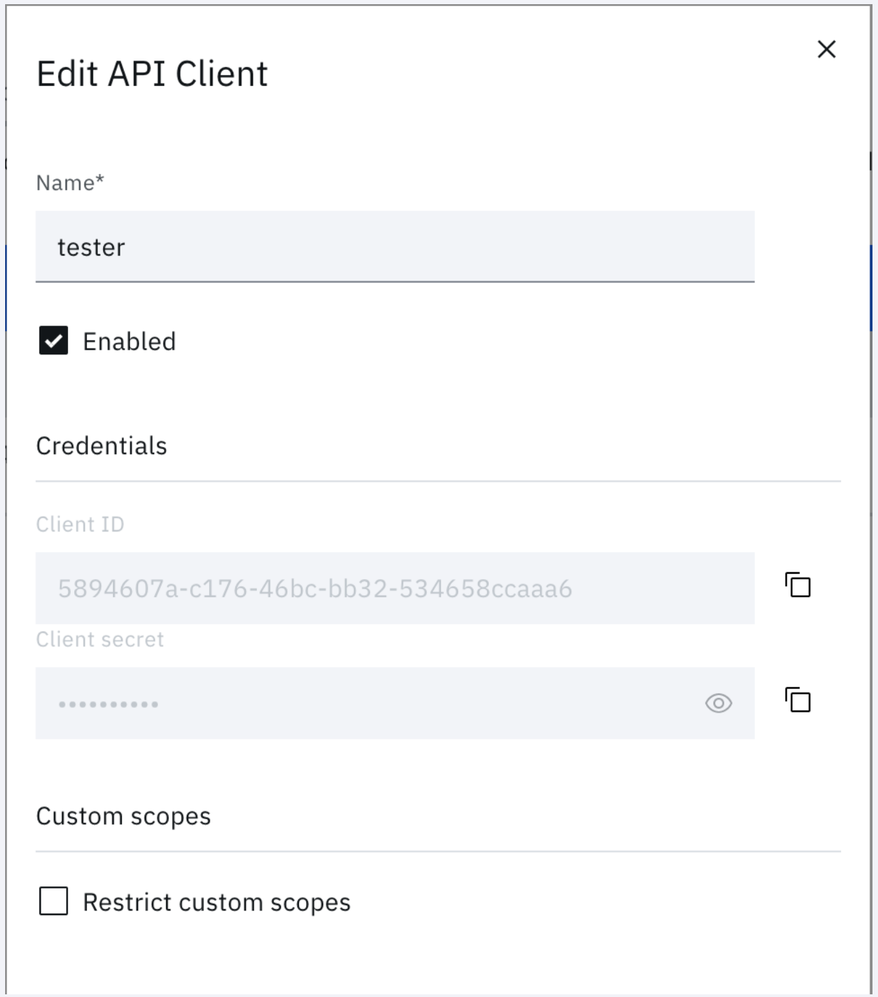
Reviewing the Swagger Format

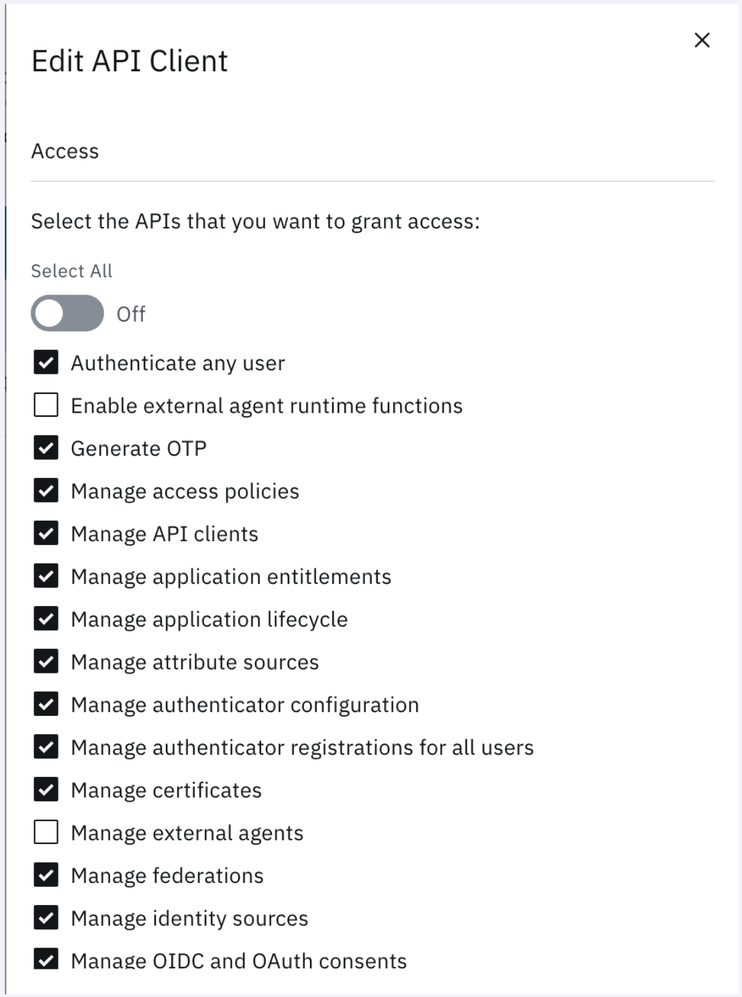
Parameter	Value	Description	Parameter Type	Data Type
name	(required)	**The name of the report.** **Some example report names are** **auth_audit_trail, auth_audit_trail_search_after, app_audit_trail, app_audit_trail_search_after, admin_activity, admin_activity_search_after, user_activity, user_activity_search_after, mfa_activity, mfa_activity_search_after, risk_adaptive_access, risk_adaptive_access_search_after**	path	string
body	`{ "FROM":"now-24h", "TO":"now", "USERID":"userid", "USERNAME":"user_name", "REALM":"realm_name", "RESULT":"\"failure\",\"success"" }` Parameter content type: application/json	**Report parameters.** Report Names / Optional Filters: auth_audit_trail, auth_audit_trail_search_after: RESULT, USERNAME, REALM, CLIENT_IP, COUNTRY_NAME, COUNTRY_CODE, SOURCE_TYPE, DEVICE_ID, MDM_COMPLIANT, MDM_MANAGED, PROVIDER_ID, SUBTYPE app_audit_trail, app_audit_trail_search_after: RESULT, USERNAME, REALM, CLIENT_IP, APP_NAME, COUNTRY_NAME, COUNTRY_CODE, SOURCE_TYPE, DEVICE_ID, MDM_COMPLIANT, MDM_MANAGED, APP_TYPE, PROVIDER_ID, CLIENT_ID, REDIRECT_URL, CAUSE admin_activity, admin_activity_search_after: PERFORMED_BY_USERNAME, PERFORMED_BY_REALM, PERFORMED_BY_CLIENTNAME, PERFORMED_BY_TYPE, CLIENT_IP, COUNTRY_NAME, COUNTRY_CODE, TARGET_ID, ACTION, RESOURCE user_activity, user_activity_search_after: RESULT, PERFORMED_BY_USERNAME, CLIENT_IP, EVENT_TYPE, COUNTRY_NAME, COUNTRY_CODE mfa_activity, mfa_activity_search_after: REALM, RESULT, USERNAME, CLIENT_IP, COUNTRY_NAME, COUNTRY_CODE, MFA_METHOD, MFA_DEVICE risk_adaptive_access, risk_adaptive_access_search_after: REALM, USERNAME, CLIENT_IP, COUNTRY_NAME, COUNTRY_CODE, RISK_LEVEL **The default value these filters is "\"*\""**	body	Model | Example Value `{}`

Response Messages

HTTP Status Code	Reason	Response Model	Headers

Creating an API Client





Configuring an Environment to use IBM Example Scripts

- https://github.com/IBM-Security/isam-support/tree/master/ci

README.md

Various RAPI for working with a CI tenant

To setup:

```
mkdir git
cd git
git clone https://github.com/IBM-Security/isam-support
Initialized empty Git repository in /home/juser/git/isam-support/.git/
remote: Enumerating objects: 64, done.
remote: Counting objects: 100% (64/64), done.
remote: Compressing objects: 100% (52/52), done.
remote: Total 545 (delta 17), reused 0 (delta 0), pack-reused 481
Receiving objects: 100% (545/545), 1.18 MiB | 1.78 MiB/s, done.
Resolving deltas: 100% (186/186), done.

cd isam-support/ci
chmod -R +x .
cd bin
./create-symlinks.sh
export PATH="`pwd`:$PATH"
```

Use:

- Generate a token. Use ci/bin/get-token.sh to get an access token

  ```
  get-token.sh tenant client_id client_secret
  {"access_token":"abcdefg","...."}
  ```

- Setting tenant and access_token environent variables makes this very easy.
  - export tenant=tenant.ice.ibmcloud.com
  - export access_token=abcdefg

Demonstrating a User Report Creation

- https://github.com/IBM-Security/isam-support/tree/master/ci/Reports

README.md

Cloud Identity Reports

Setup instructions

- Create an API client at https://tenant/ui/admin/configuration?tab=api-access&subTab=api-clients with the following access:
  - Manage reports
  - Read reports
  - Read application configuration
- Generate a token. Use ../ci/bin/get-token.sh to get an access token

```
get-token.sh tenant client_id client_secret
{"access_token":"abcdefg","...."}
```

- Setting tenant and access_token environent variables makes this very easy.
  - export tenant=tenant.ice.ibmcloud.com
  - export access_token=abcdefg

Explanation of Reports

- auth_audit_trail: Authentication failures and success.
- app_audit_trail: Application usage.
- admin_activity: Tenant Admin activity.
- user_activity: Activity for a specific user. This supports exporting to a csv file.
- auth_event_details: Details of a specific event.

Sample commands

Finding login failures and getting the details.

- reports.sh ${tenant} ${access_token} auth_audit_trail auth_audit_trail_failure.json


```
{
  "_id": "a3d0c396-0206-420f-b1a1-d4b65e30c955",
  "_index": "event-authentication-2020.3-000001",
  "_source": {
      "data": {
          "origin": "70.114.164.111",
          "realm": "cloudIdentityRealm",
          "result": "failure",
          "subject": "UNKNOWN",
          "subtype": "user_password",
          "username": "dsfadsfads"
      },
      "geoip": {
          "country_iso_code": "US",
          "country_name": "United States",
          "region_name": "Texas"
      },
      "time": 1585362232823
  }
```


- Take the event ID (_id) of a3d0c396-0206-420f-b1a1-d4b65e30c955, update auth_event_details.json, and run the report:

reports.sh ${tenant} ${access_token} auth_event_details auth_event_details.json

The output has complete details of the failure.

Use failure-events-details.sh to process an entire failure log.

- reports.sh ${tenant} ${access_token} auth_audit_trail auth_audit_trail_failure.json | python -mjson.tool > failure.log
- failure-events-details.sh ${tenant} ${access_token} failure.log > events.log

Demonstrating a User Report Creation

Branch: master ▾ **isam-support** / ci / Reports / **auth_audit_trail_failure.json**

nick-lloyd Create auth_audit_trail_failure.json

1 contributor

8 lines (8 sloc) | 134 Bytes

```
1  {
2      "FROM":"now-72h",
3      "TO":"now",
4      "SIZE":"200",
5      "SORT_BY":"time",
6      "SORT_ORDER":"DESC",
7      "RESULT":"\"failure\""
8  }
```

Demonstrating a User Report Creation

$ get-token.sh rholman.ice.ibmcloud.com 5894607a-c176-46bc-bb32-534658ccaaa6 Y2k98lXExA

{"access_token":"0DEArauZA3LS2FmmdJXMd016AFOTWWYo5zTPPe8C","scope":"openid","grant_id":"eb17cfaa-00b8-441f-b929-59d385eb5cd9","id_token":"eyJhbGciOiJub25lIn0.eyJyZWFsbU5hbWUiOiJjbG91ZElkZW50aXR5UmVhbG0iLCJhdF9oYXNoIjoidGVILXRnRVl6WmtMemhQcUxFVFdtdyIsImV4dCI6eyJ0ZW5hbnRJZCI6InJob2xtYW4uaWNlLmlibWNsb3VkLmNvbSJ9LCJpc3MiOiJodHRwczovL3Job2xtYW4uaWNlLmlibWNsb3VkLmNvbS9vaWRjL2VuZHBvaW50L2RlZmF1bHQiLCJhdWQiOiI1ODk0NjA3YS1jMTc2LTQ2YmMtYmIzMi01MzQ2NThjY2FhYTYiLCJzdWIiOiI1ODk0NjA3YS1jMTc2LTQ2YmMtYmIzMi01MzQ2NThjY2FhYTYiLCJpYXQiOjE1OTA0MzUzMjcsImV4cCI6MTU5MDQ0MjUyN30.","token_type":"Bearer","expires_in":7200}

$ export access_token=0DEArauZA3LS2FmmdJXMd016AFOTWWYo5zTPPe8C

$ export tenant=rholman.ice.ibmcloud.com

$ cd ..

$ cd Reports

$ reports.sh ${tenant} ${access_token} auth_audit_trail auth_audit_trail_failure.json

{"response":{"report":{"hits":[

{"_index":"event-authentication-2020.5-000001","_type":"_doc","_source":{"geoip":{"country_iso_code":"US","country_name":"United States","region_name":"Texas"},"data":{"result":"failure","subtype":"user_password","subject":"UNKNOWN","origin":"108.232.177.211","realm":"cloudIdentityRealm","username":"Test2"},"time":1590433146811},"_id":"5d5c0abc-8023-4e61-803d-d4ad8df95638","sort":[1590433146811,"5d5c0abc-8023-4e61-803d-d4ad8df95638"]},

{"_index":"event-authentication-2020.5-000001","_type":"_doc","_source":{"geoip":{"country_iso_code":"US","country_name":"United States”,"region_name":"Texas"},"data":

{"result":"failure","subtype":"user_password","subject":"UNKNOWN","origin":"108.232.177.211","realm":"cloudIdentityRealm","username":"Test1"},"time":1590433134222},"_id":"4e195b28-e3e6-49fc-b174-a9d64bec003b","sort":[1590433134222,"4e195b28-e3e6-49fc-b174-a9d64bec003b"]}],"total":2}},"success":true}

Summary

By utilizing this functionality provided by Cloud Identity, it will allow you to administer many aspects of your tenant without the need for engaging Cloud Identity Support.

Questions for the panel

Ask the panelists a question now

Enter your question in the Q&A area

Ask a question after this presentation

You are encouraged to ask follow-up questions in the Support forums: https://www.ibm.com/mysupport/s/forumshome

IBM Cloud Identity forum
http://ibm.biz/CloudIdentity-SupporForum

For more information

IBM Cloud Identity Forum:
https://www.ibm.com/support/pages/node/266959

Security Learning Academy:
https://www.securitylearningacademy.com/local/navigator/index.php?level=cid001

IBM Knowledge Center for IBM Cloud Identity:

https://www.ibm.com/support/knowledgecenter/SSCT62/com.ibm.iamservice.doc/kc-homepage.html

IBM Coud Identity Support:

https://www.ibm.com/mysupport/s/topic/0TO500000002XbyGAE/cloud-identity?language=en_US&productId=01t50000004Y4A8AAK

Useful links:

Get started with IBM Security Support IBM Support
Sign up for My Notifications IBM Security Community

Follow us:

utube.com/user/IBMSecuritySupport twitter.con  ty http://ibm.biz/ISCS-LinkedIn 

Thank you

Follow us:

securitylearningacademy.com

ibm.biz/JoinIBMVIPRewards-Security

youtube/user/IBMSecuritySupport

@AskIBMSecurity

ibm.biz/IBMSecurityClientSuccess-LinkedIn

securityintelligence.com

xforce.ibmcloud.com

ibm.com/security/community

All names and references for organizations and other business institutions used in this deliverable's scenarios are fictional. Any match with real organizations or institutions is coincidental. All names and associated information for people in this deliverable's scenarios are fictional. Any match with a real person is coincidental.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.