

Note: ComAp cloud API v 1.1 are using the ComAp Cloud Identity and OAuth2 protocol for authentication.

Please see. <https://oauth.net/2/> for OAuth2 protocol documentation.

This Guide describes how to use APIS on developer portal. You can use API by your own apps too in machine to machine mode of course.

How to refresh expired secret.

Your application is registered and secret is expired. You obtain HTTP status 401 on the “Authenticate” API endpoint. And

```
{ "error": "invalid_client", "error_description": "AADSTS7000222: The provided client secret keys for app '<---clientID of your registered app--->', are expired. Visit the Azure portal to create new keys for your app: https://aka.ms/NewClientSecret, or consider using certificate credentials for added security: https://aka.ms/certCreds. Trace ID: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX Correlation ID: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX Timestamp: \"::\"YYYY-MM-DD HH:MM:SSZ\", \"error_codes\": [7000222], \"timestamp\": \"YYYY-MM-DD HH:MM:SSZ\", \"trace_id\": \"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX\", \"correlation_id\": \"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX\", \"error_uri\": https://login.microsoftonline.com/error?code=7000222 }
```

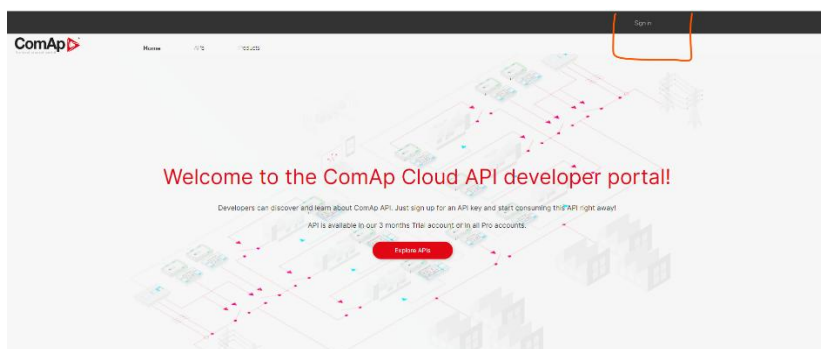
in the body.

Step 1

- Go to <https://portal.websupervisor.net> page.

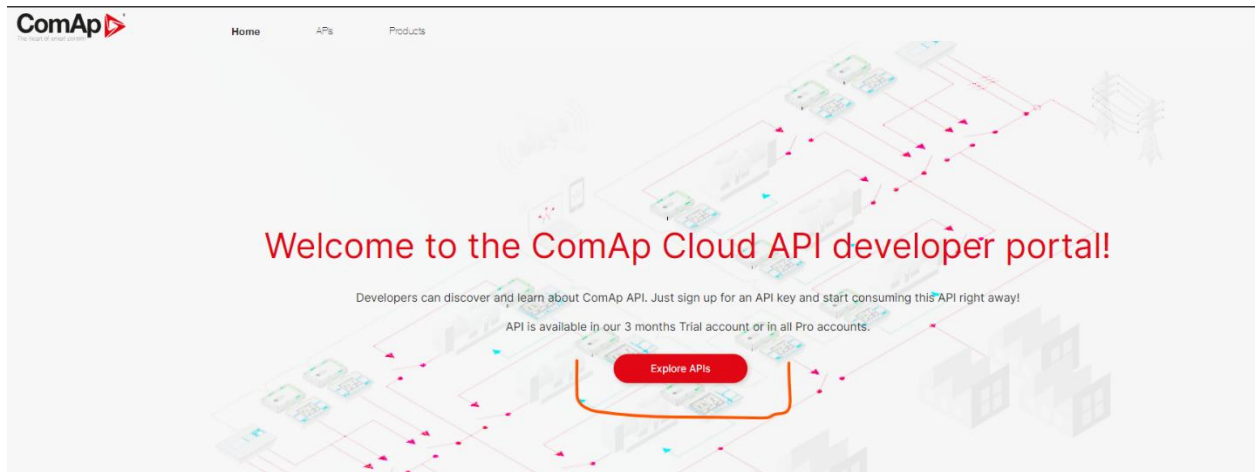
Step 2

- Sign up for a ComAp Cloud Identity (CCI).

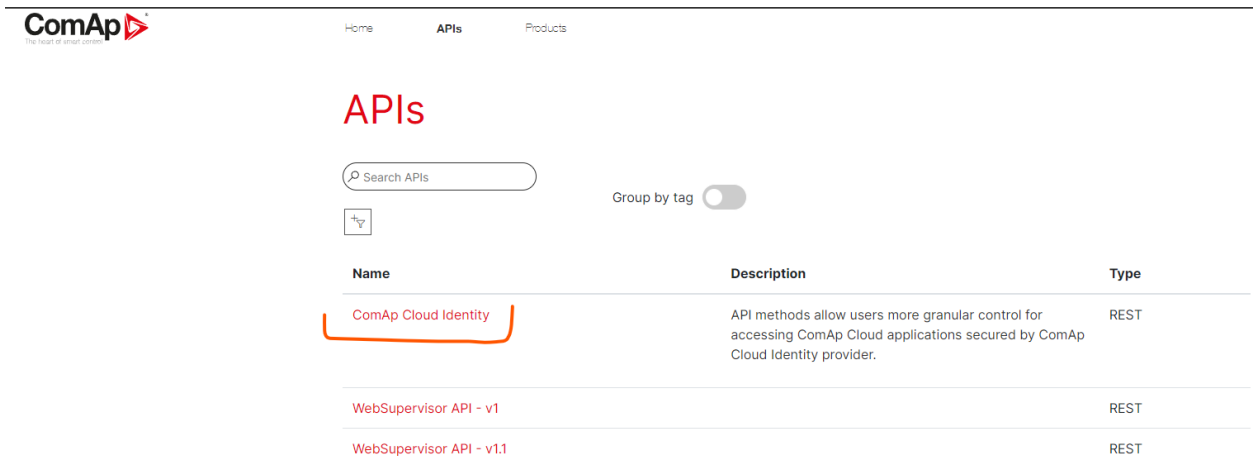


Step 3

- Navigate to the API section
- Then to ComAp Cloud Identity API

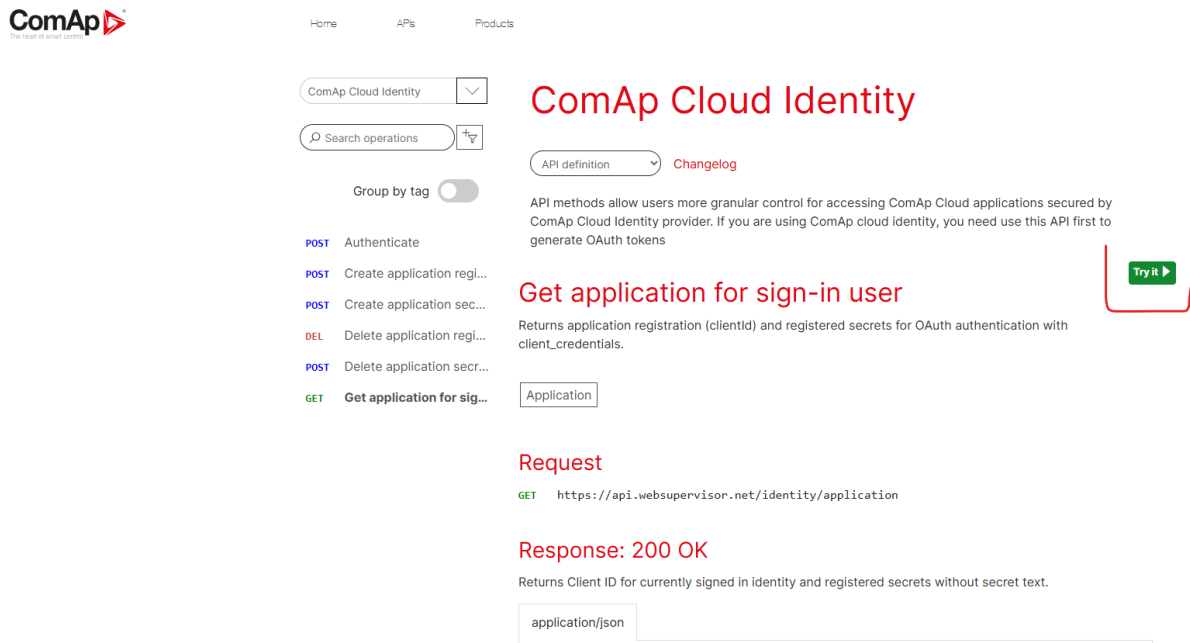


•



Step 4

- Check secrets under account
- Navigate to the “Get application for sign-in user” GET method and use “Try it” button



The screenshot shows the ComAp API console interface. On the left, there is a sidebar with navigation links: Home, APIs, and Products. Below this, there is a search bar and a 'Group by tag' toggle. A list of API methods is displayed, including 'Authenticate', 'Create application regi...', 'Delete application regi...', and 'Get application for sig...'. The 'Get application for sig...' method is highlighted in green. The main content area shows the details for this method, including the title 'ComAp Cloud Identity', a description, and a 'Try it' button highlighted with a red box. Below the description, the 'Request' section shows the endpoint 'https://api.websupervisor.net/identity/application' and the 'Response' section shows a '200 OK' status and the response body 'application/json'.

- “Authorization flow:” choose “Implicit” value. In the pop up please fill your ComAp Cloud Identity e-mail and login if you are prompted
- Authorization value are filled automatically
- Then click to “Sent”
- You obtain “200” HTTP status code, you application was created.
- In the response you are able to see clientID of registered apps and secrets attributes. Keep the response saved for next steps.

HTTP response

```
HTTP/1.1 200 OK

cache-control: no-cache
content-length: 495
content-type: application/json; charset=utf-8
date: Tue, 31 Mar 2026 13:37:29 GMT
expires: -1
pragma: no-cache
strict-transport-security: max-age=31536000; includeSubDomains
vary: Origin
x-ms-client-tracking-id: 08584266426375135393051643903CU96
x-ms-correlation-id: 515e13db-63fa-43c4-80d1-9e37fd8c7449
x-ms-execution-location: westeurope
x-ms-ratelimit-burst-remaining-workflow-writes: 856
x-ms-ratelimit-remaining-workflow-download-contentsize: 61355537
x-ms-ratelimit-remaining-workflow-upload-contentsize: 61355980
x-ms-ratelimit-time-remaining-directapirequests: 2856007
x-ms-request-id: westeurope:515e13db-63fa-43c4-80d1-9e37fd8c7449
x-ms-tracking-id: 515e13db-63fa-43c4-80d1-9e37fd8c7449
x-ms-trigger-history-name: 08584266426375135393051643903CU96
x-ms-workflow-id: f6f9826e1a5845d096a5abfca739108a
x-ms-workflow-name: AADB2C_GetApplicationForIdentity_HTTP
x-ms-workflow-run-id: 08584266426375135393051643903CU96
x-ms-workflow-system-id: /locations/westeurope/scaleunits/prod-103/
workflows/f6f9826e1a5845d096a5abfca739108a
x-ms-workflow-version: 08584508530355255687

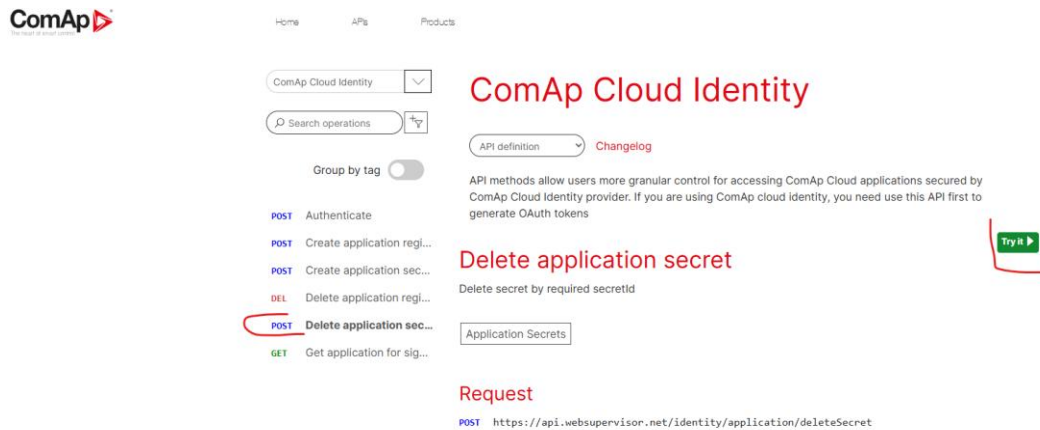
{
  "clientId": "dcb9c508-0cf2-4fe8-a238-319fc558e61d",
  "secrets": [
    {
      "customKeyIdentifier": null,
      "displayName": "new",
      "endDateTime": "2028-03-23T09:50:04.362Z",
      "hint": "2M7",
      "keyId": "5d44f4d0-150b-4825-b768-2a38fcb84645",
      "secretText": null,
      "startDateTime": "2026-03-24T09:50:04.362Z"
    },
    {
      "customKeyIdentifier": null,
      "displayName": "string",
      "endDateTime": "2028-03-02T12:19:51.9511802Z",
      "hint": "0zm",
      "keyId": "c984fa4b-7b11-4933-a798-e8ea300db32b",
      "secretText": null,
      "startDateTime": "2026-03-02T12:19:51.934638Z"
    }
  ]
}
```

Send

- Just two secrets per application is allowed, so if have two you must delete min one.
- If you have just one secret you can jump to the step 6.

Step 5

- Delete old secrets
- Navigate to the “Delete application secret” POST method and use “Try it” button



The screenshot shows the ComAp Cloud Identity API console. The main heading is "ComAp Cloud Identity". Below it, there's a search bar and a "Group by tag" toggle. A list of API methods is shown on the left, with "Delete application secret" (POST) highlighted. The main content area shows the details for this endpoint: "Delete application secret by required secretid". There is a "Try it" button highlighted with a red box. Below the endpoint details, there is a "Request" section with the URL: `POST https://api.websupervisor.net/identity/application/deleteSecret`.

- “Authorization flow:” choose “Implicit” value. In the pop up please fill your ComAp Cloud Identity e-mail and login if you are prompted
- Authorization value are filled automatically
- Fulfill the JSON in the Request body section:

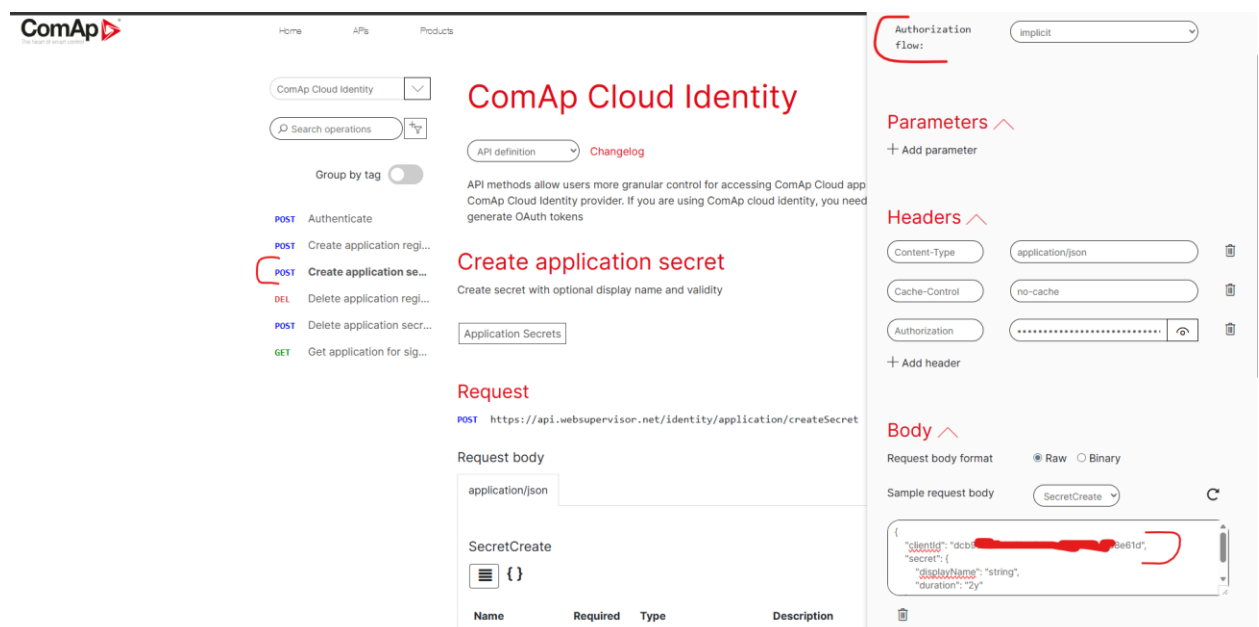
```
{
  "clientId": "< ---clientId from previous step--- >",
  "secret": {
    "secretId": "< ---keyID from previous step--- >,"
  }
}
```

- Then click on „Sent“ button
- You obtain HTTP response 204 „No Content“ – it means that the secret was deleted.

Step 6

- Create new secret
- Navigate to “Create application secret” POST method, and click on “Try it” button
- If you are logged in your Comap-Key Value are prefilled
- “ComAp Cloud Identity” value choose “Implicit” value. In the pop up please fill your ComAp Cloud Identity e-mail and log in if you are prompted
- Authorization value are filled automatically
- Fulfill the JSON in the Request body section:

```
{
  "clientId": < ---clientId from step 4.--- >,
  "secret": {
    "displayName": "< ---your name of secret --- >",
    "duration": "2y"
  }
}
```



The screenshot shows the ComAp API console interface. The main heading is "ComAp Cloud Identity". Below it, there are search and filter options. The "Create application secret" endpoint is selected, showing its details: "POST https://api.websupervisor.net/identity/application/createSecret". The "Request body" section is expanded, showing the JSON payload: `{ "secret": { "displayName": "SecretCreate", "duration": "2y" } }`. The "Authorization flow" is set to "Implicit".

- Then click on „Sent“ button

- In the API response you obtain your secret. Maximum secret age period is 2 years

```

Send
Response status
200 OK
Response latency
1'935 ms
Response content

Pragma: no-cache
<ms-workflow-run-id: 09581251565688080312425080990C095
<ms-correlation-id: 9422254-c19a-4029-9770-c0822a5c7d1
<ms-claim-tracking-id: 0858125156568808031241508060C095
<ms-trigger-history-name: 0858125156568808031241308698C095
<ms-execution-location: westeurope
<ms-workflow-system-id: /locations/westeurope/california/prod-56/workflow/1b04f6c6d7454c1797f97d64d5656
<ms-workflow-id: 1b04f6c6d7454c1797f97d64d5656
<ms-workflow-version: 0858125156568808031241308698C095
<ms-workflow-name: AAD02C_CreateSecretForApplication_HTTP
<ms-tracking-id: 04122f54-caba-403f-9770-3022a957c1
<ms-ratelimit-burst-remaining-workflow-writes: 1109
<ms-ratelimit-remaining-workflow-download-content-size: 39767876
<ms-ratelimit-remaining-workflow-upload-content-size: 39767874
<ms-ratelimit-time-remaining-directapi-requests: 3592123
<ms-request-id: westeurope:04122f54-caba-403f-9770-c0822a5c7d1
Strict-Transport-Security: max-age=31536000; includeSubdomains
Request-Context: appId=cid-v1:f2b819da-12d1-4b85-b046-0c3b4a6ddaaf
Cache-Control: no-cache
Date: Mon, 06 Feb 2023 13:47:19 GMT
Content-Length: 188
Content-Type: application/json
Expires: -1

{
  "displayName": "TestSecret",
  "endDateTime": "2023-02-06T13:47:17.851210Z",
  "hint": "20c",
  "secret": "10680[REDACTED]-Rg",
  "secretId": "55a3271-c59e-481e-b0d5-564172b6e6a1"
}

```

- Keep “secret” value for later usage.

Step 7

- Using the new secret
- Just replace old secret by one in your application.
- Then you will be able to generate tokens as usual.