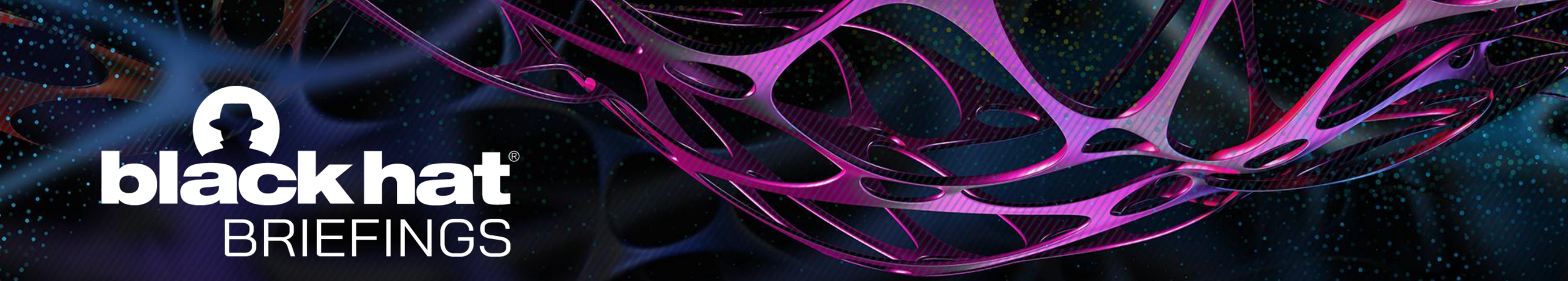


AUGUST 6-7, 2025

MANDALAY BAY / LAS VEGAS

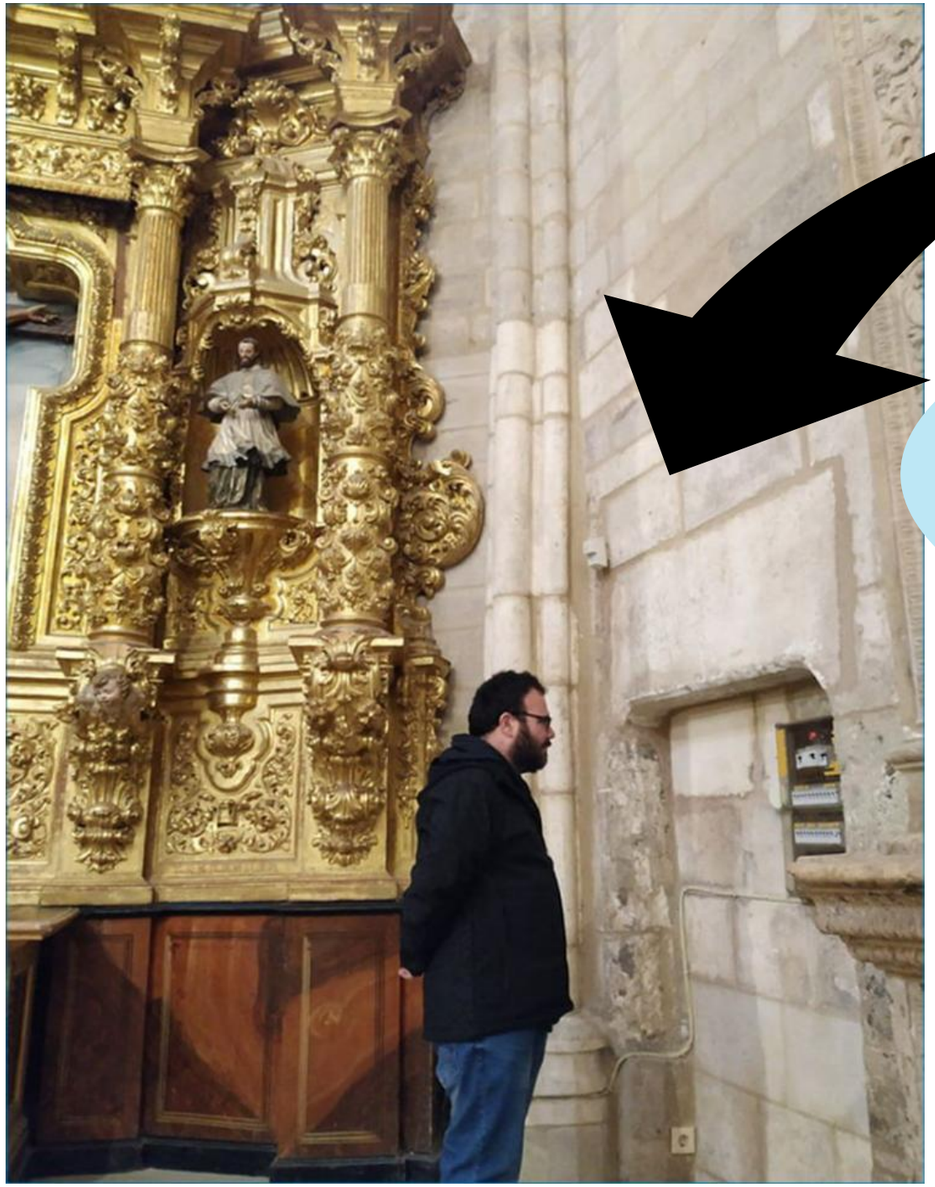
Consent & Compromise

Abusing Entra OAuth for Fun and Access to Internal Microsoft Applications

Vaisha Bernard

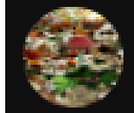
https://graph.microsoft.com/v1.0/me

```
{
  "displayName": "Vaisha Bernard",
  "jobTitle": "Chief Hacker",
  "companyName": "Eye Security",
  "country": "The Netherlands",
  "hireDate": "2020-04-01T00:00:00Z",
  "aboutMe": "15+ years offensive security, 5 years
    incident response",
  "interests": [
    "hiking",
    "camping",
    "weightlifting",
    "interior design"
  ],
  "userPrincipalName": "vaisha.bernard@eye.security"
}
```



also me

Most talks about cybersecurity are just someone stumbling around

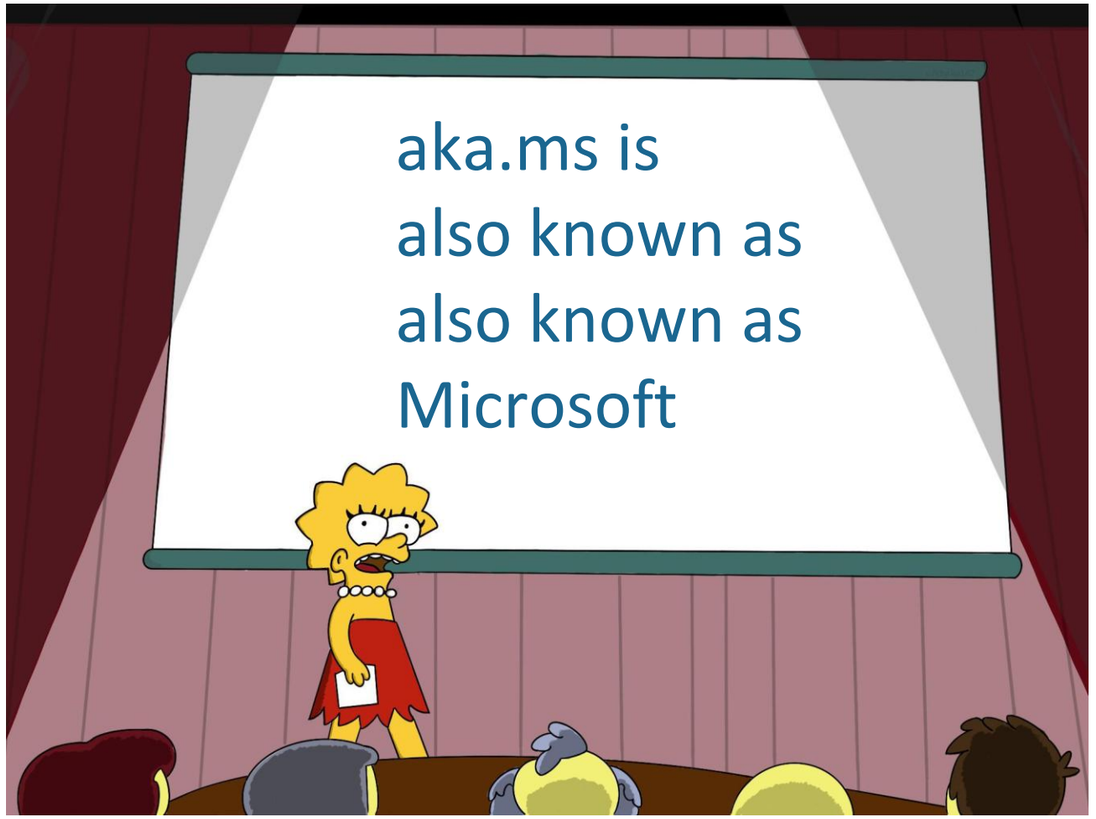


@realqxji 5 months ago

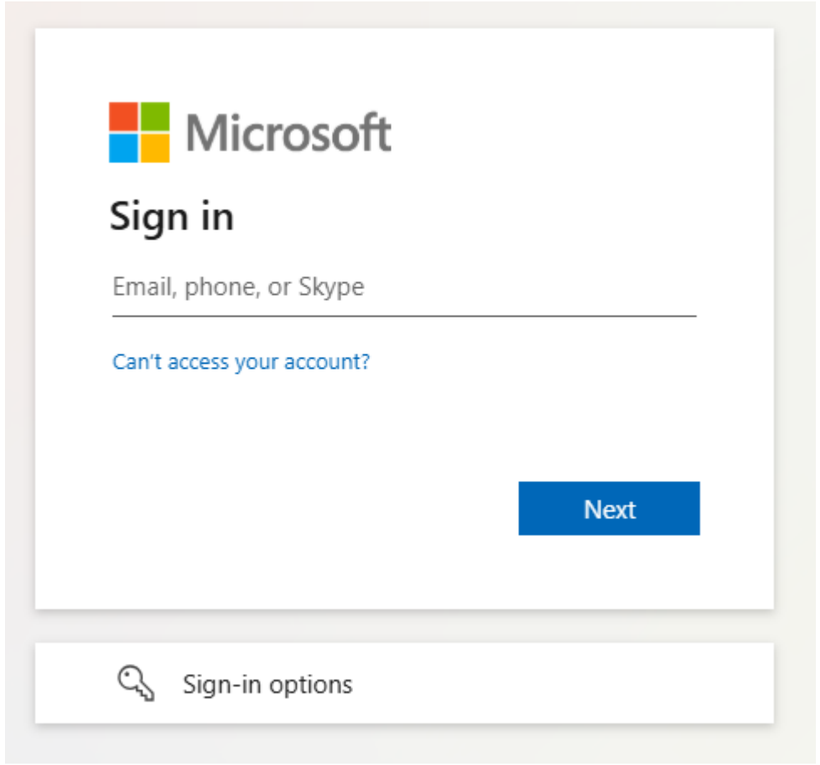
I am terrified that most of the talks about cybersecurity vulnerabilities are really just someone stumbling around having issues and then finding truly horrifying vulnerabilities

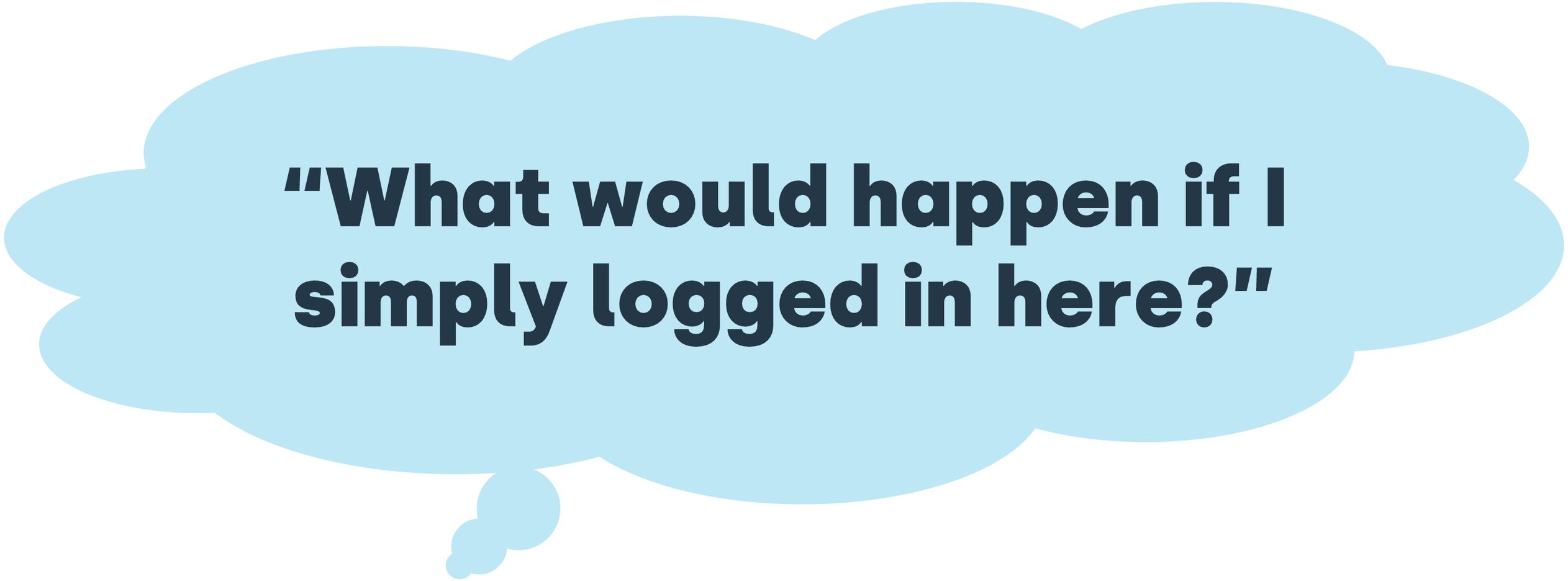
140 Reply

aka.ms

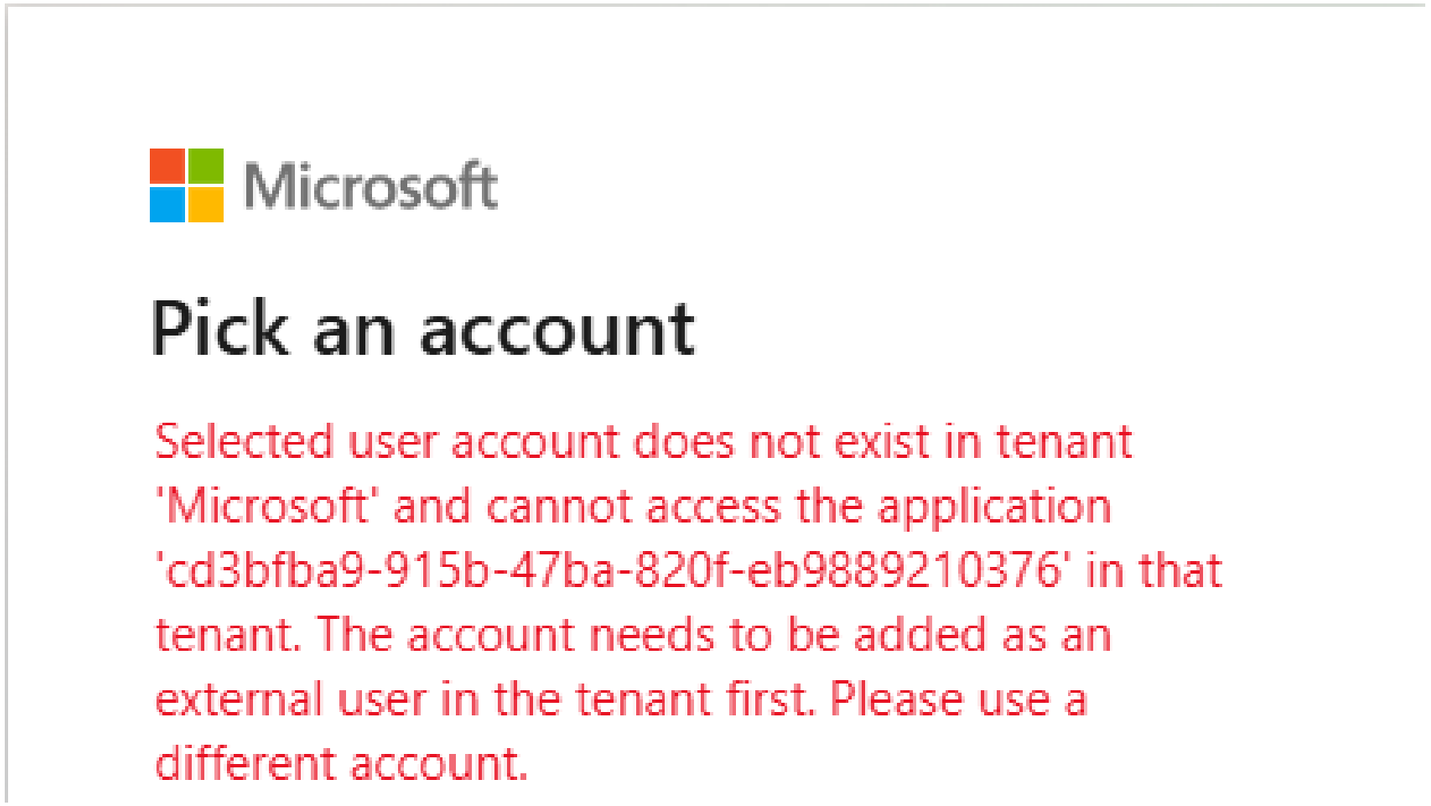


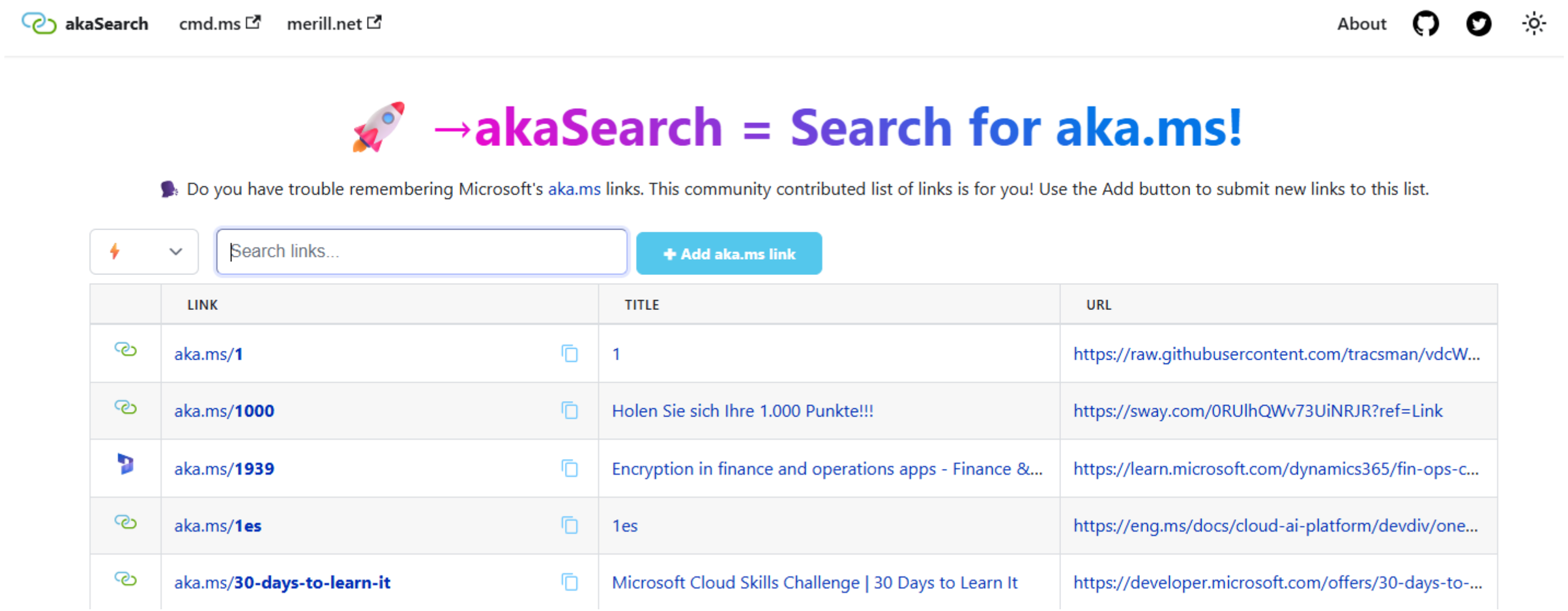
aka.ms


Microsoft
Sign in
Email, phone, or Skype
Can't access your account?
Next
Sign-in options


"What would happen if I simply logged in here?"

aka.ms


Microsoft
Pick an account
Selected user account does not exist in tenant 'Microsoft' and cannot access the application 'cd3bfba9-915b-47ba-820f-eb9889210376' in that tenant. The account needs to be added as an external user in the tenant first. Please use a different account.


akaSearch
cmd.ms
merill.net
About
→akaSearch = Search for aka.ms!
Do you have trouble remembering Microsoft's aka.ms links. This community contributed list of links is for you! Use the Add button to submit new links to this list.
Search links...
+ Add aka.ms link
LINK
TITLE
URL
aka.ms/1
1
https://raw.githubusercontent.com/tracsman/vdcW...
aka.ms/1000
Holen Sie sich Ihre 1.000 Punkte!!!
https://sway.com/0RUlhQWv73UiNRJR?ref=Link
aka.ms/1939
Encryption in finance and operations apps - Finance &...
https://learn.microsoft.com/dynamics365/fin-ops-c...
aka.ms/1es
1es
https://eng.ms/docs/cloud-ai-platform/devdiv/one...
aka.ms/30-days-to-learn-it
Microsoft Cloud Skills Challenge | 30 Days to Learn It
https://developer.microsoft.com/offers/30-days-to-...

akaSearch cmd.ms About

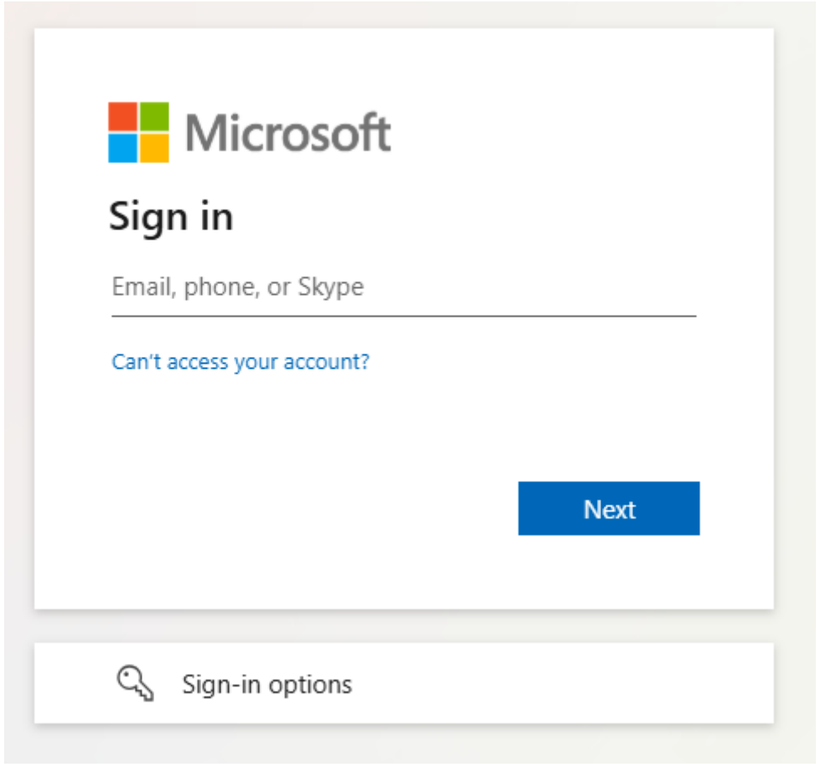
h for aka.ms!

Do you inks is for you! Use the Add button to submit new links to this list.

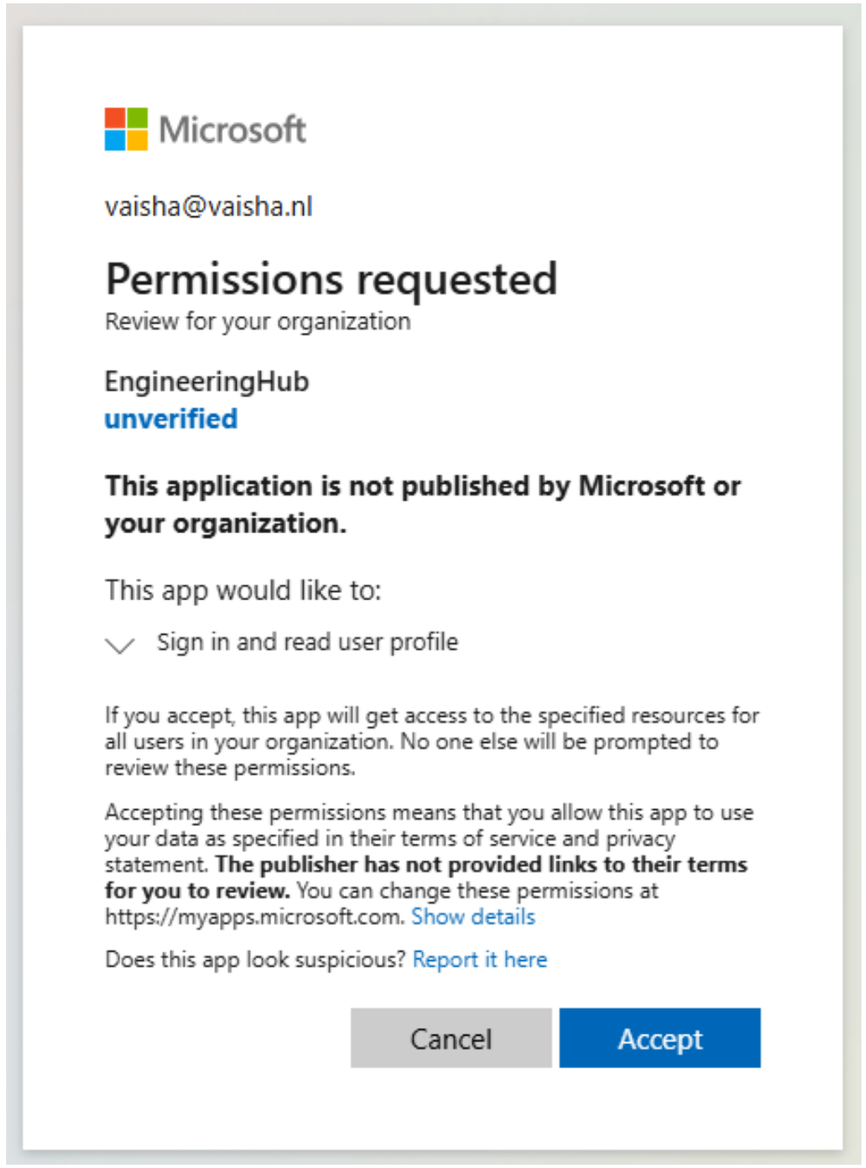
	LINK	URL
	aka.ms/	usercontent.com/tracsman/vdcW...
	aka.ms/	3UiNRJR?ref=Link
	aka.ms/	ps - Fi ics365/fin-ops-c...
	aka.ms/	https://eng.ms/d rm/devdiv/one...
	aka.ms/3	ys to Le ffers/30-days-to-...

The ADHD urge to do literally anything else other than the thing you're supposed to be doing

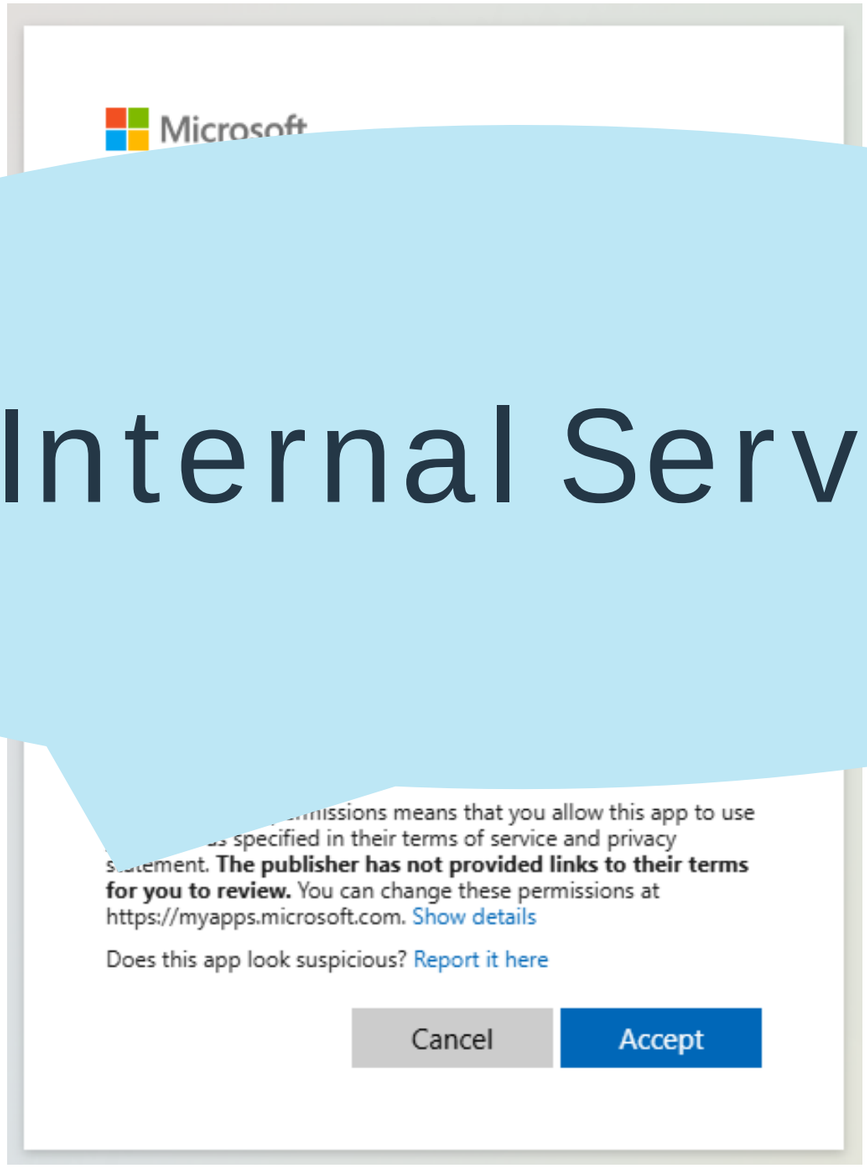
eng.ms


Microsoft
Sign in
Email, phone, or Skype
Can't access your account?
Next
Sign-in options

eng.ms

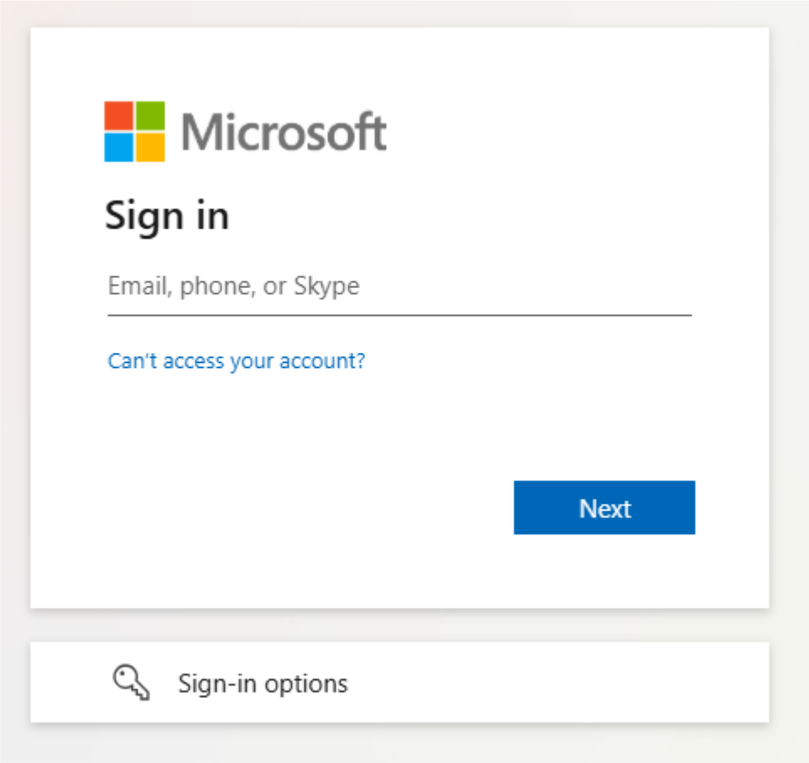

Microsoft
vaisha@vaisha.nl
Permissions requested
Review for your organization
EngineeringHub
unverified
This application is not published by Microsoft or your organization.
This app would like to:
Sign in and read user profile
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. The publisher has not provided links to their terms for you to review. You can change these permissions at https://myapps.microsoft.com. Show details
Does this app look suspicious? Report it here
Cancel
Accept

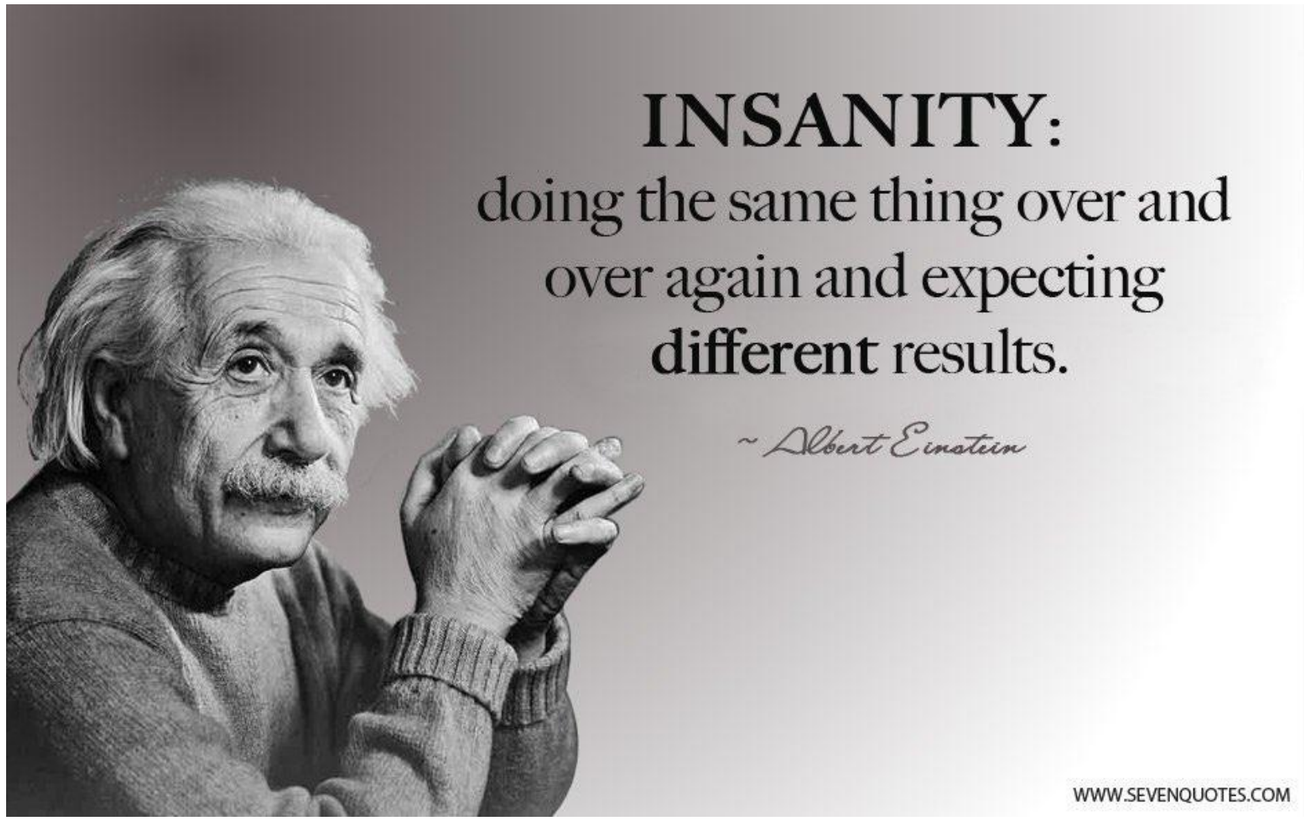
eng.ms



500 Internal Server Error

rescue.eng.ms





Engineering Hub Rescue

Search Engineering Hub Rescue

Vaisha Bernard
vaisha@vaisha.nl

This site is for disaster recovery scenarios, please use https://eng.ms if possible!

Engineering Hub is currently migrating to a new dialtone stack & hardware, authenticating with AME and other tenants with dSTS is coming soon. Please report any issues to the Engineering Hub team.

password

Cloud + AI Platform

C
p
d
a
all layers of the tech stack starting with the distributed computing fabric (cloud and edge)...

Core Services Engineer

Corporate, External &

Engineering Hub Help

Hub onboarding
entation

Onboard OpenAPI TSGs Team Docs Products

Experiences & Devices

The purpose of this team is to instill a unifying product ethos across our end-user experiences and devices. Rajeshj is the business owners. Other business owners added while adding partner develope...

Finance Group

All Apps/Systems managed by the business teams are registered in this organization.

Gaming

Connect gaming assets across PC, console, mobile and work to grow and engage the 53 million strong Xbox Live member network more deeply and frequently - from great game experiences to streaming to soc...

HR Group

Human Resources

Initiatives

Learn about the key Azure Initiatives

LinkedIn Group

LinkedIn is the world's largest professional network with more than 610 million users in more than 200 countries and territories

Marketing and Consu...

Marketing & Consumer Business Note: We have temporarily added some people from E+D as business owners and admins, to work

Microsoft Customer & ...

Microsoft Customer & Partner Solutions (MCAPS) - Core ; Formally Worldwide Commercial Business

Search Results

Search Engineering Hub Rescue

Showing 15 of 13252 results.

Search Results for *password*

CII-Service Doc • Passwords

docs/experiences-devices/opg/office-canvas/office-voice-vision/cloud-input-intelligence/cii-service-doc/incident-triage/passwords

Passwords The user name for all of the environments is the same as seen in the screenshot below In order to get the *password* each environment has this stored in a variable i

Team Documentation • passwords

docs/cloud-ai-platform/ahsi-organization/ahsi/redsa-team/cloud-readiness-criteria-labs/team-documentation/toolkit/passwords

Passwords Currently all blade and rack/chassis manager credentials (*passwords* and usernames) are stored in a keyvault [redacted]

CRMGlobal & Reporting Infrastructure • password-change

docs/microsoft-customer-partner-solutions-mcaps-core/customer-experience-and-support/customer-service-support/strategy-and-innovation-organization/crm-global-platform/crmglobal-reportin

Obtain old *password* for crmgsvc from vault Create new *password* for crmgsvc and store in vault with activation date and expiration date complying with the new policy (mini
age).

Agenda

- The Entra ID Identity Platform
- Previous Research
- Consent & Compromise
- Sound Bytes, Questions

Authentication vs. Authorization in Entra ID

AuthN

OIDC

Gatekeeper

Done first

ID Token

Authentication

Confirms users are who they say they are

Authorization

Validates users have permission to complete the attempted action

AuthZ

OAuth 2.0

Guard

Done after

Access Token

How a web app determines if the user is authenticated

Web app developers can indicate whether all or only certain pages require authentication. For example, in ASP.NET/ASP.NET Core, this is done by adding the `[Auth` ? attribute to the controller actions.

How a web app determines if the user is authenticated

Web app developers can indicate whether all or only certain pages require authentication. For example, in ASP.NET/ASP.NET Core, this is done by adding the `[Authorize]` attribute to the controller actions.

How a web app determines if the user is authenticated

Web app developers can indicate whether all or only certain pages require authentication. For example, in ASP.NET/ASP.NET Core, this is done by adding the `[Authorize]` attribute to the controller actions.

Simple authorization in ASP.NET Core

05/02/2024

In this article

Authorization in ASP.NET Core is controlled with the ? attribute and its various parameters. In its most basic form, applying the ? attribute to a controller, action, or Razor Page, limits access to that component to authenticated users.

How a web app determines if the user is authenticated

Web app developers can indicate whether all or only certain pages require authentication. For example, in ASP.NET/ASP.NET Core, this is done by adding the `[Authorize]` attribute to the controller actions.

Simple authorization in ASP.NET Core

05/02/2024

In this article

- Prerequisites
- Use the [Authorize] attribute
- Authorize attribute and Razor Pages

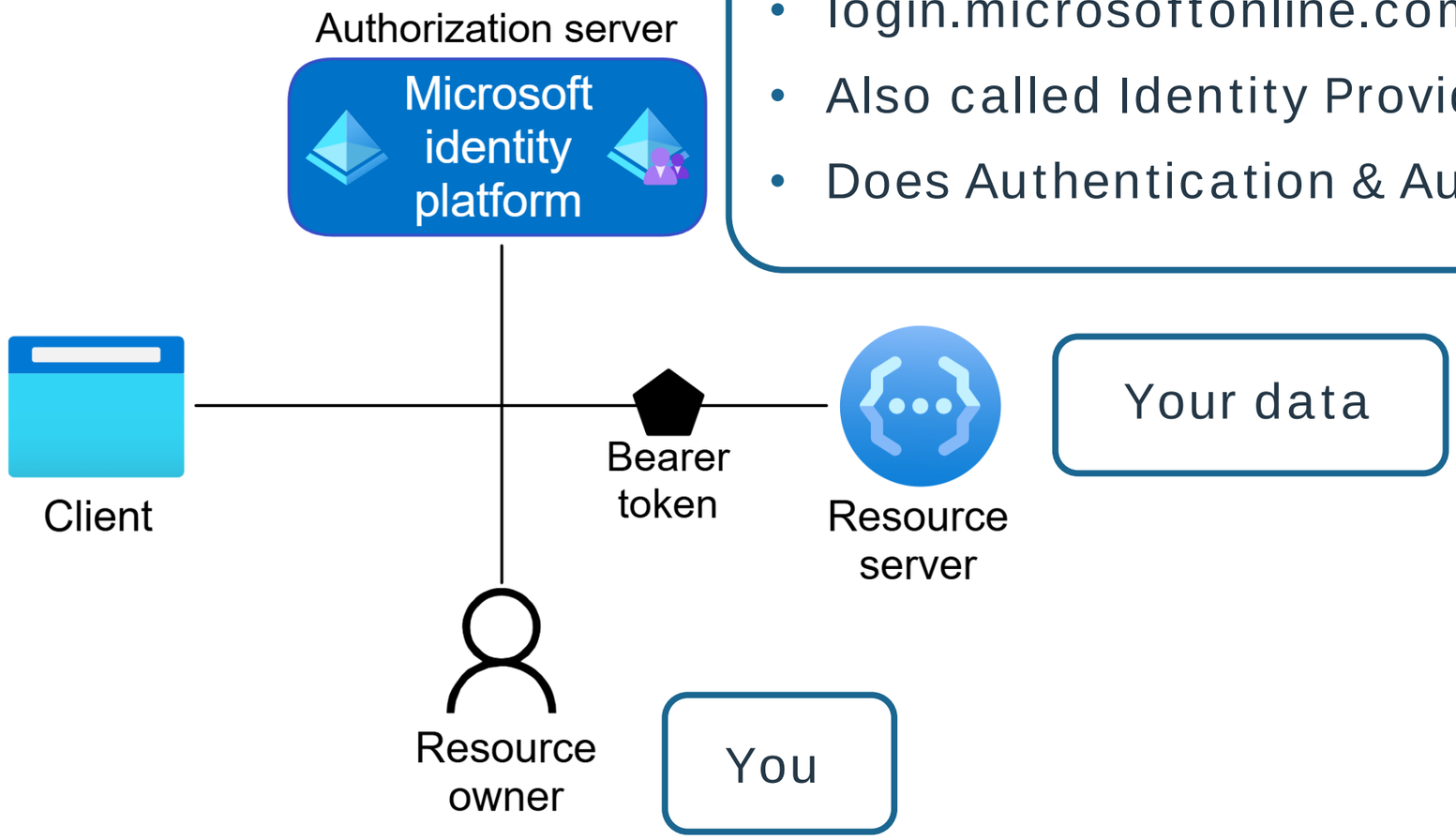
Authorization in ASP.NET Core is controlled with the [Authorize] attribute and its various parameters. In its most basic form, applying `[Authorize]` ribute to a controller, action, or Razor Page, limits access to that component to authenticated users.

Microsoft Identity Platform

Authorization server

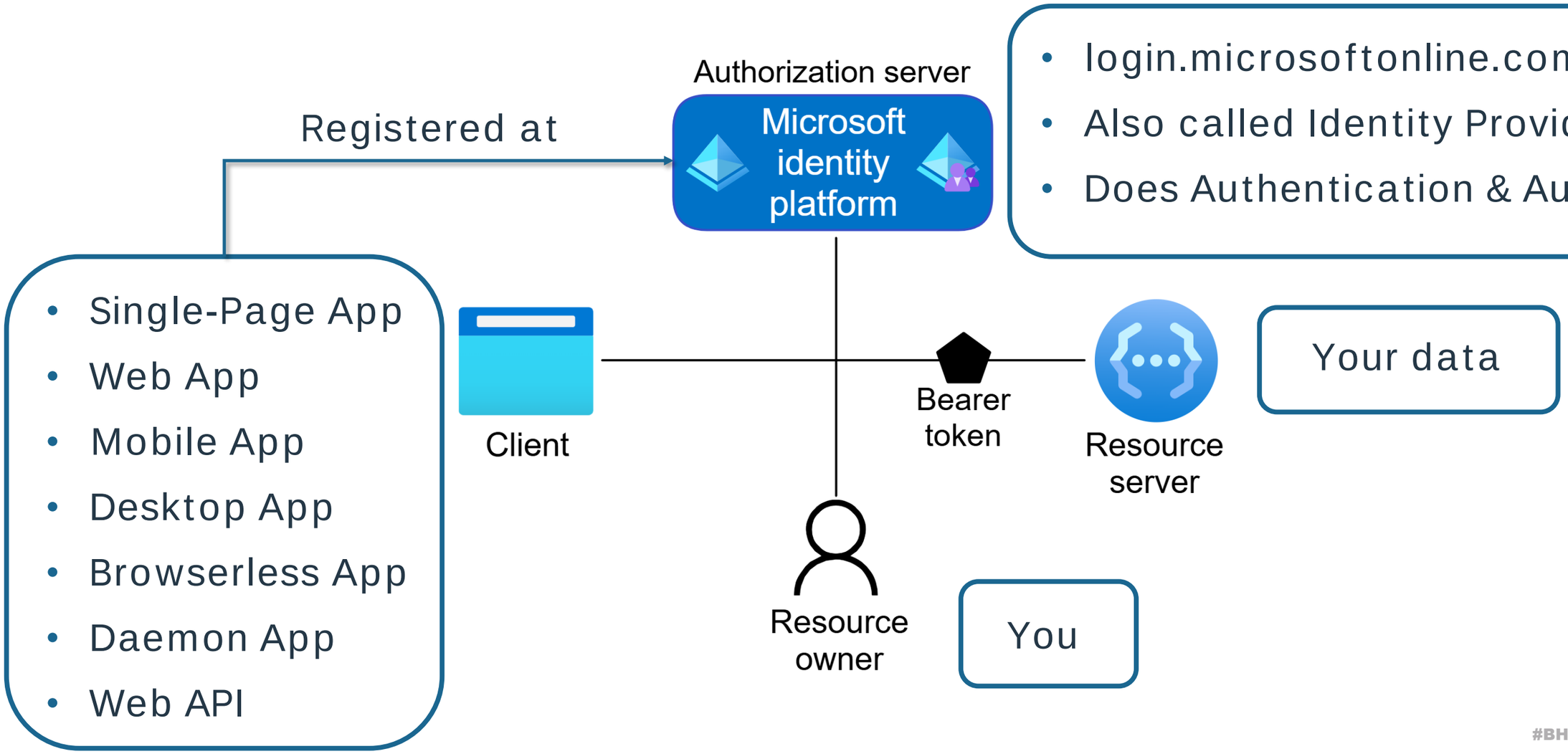
- login.microsoftonline.com
- Also called Identity Provider (IdP)
- Does Authentication & Authorization

Microsoft Identity Platform



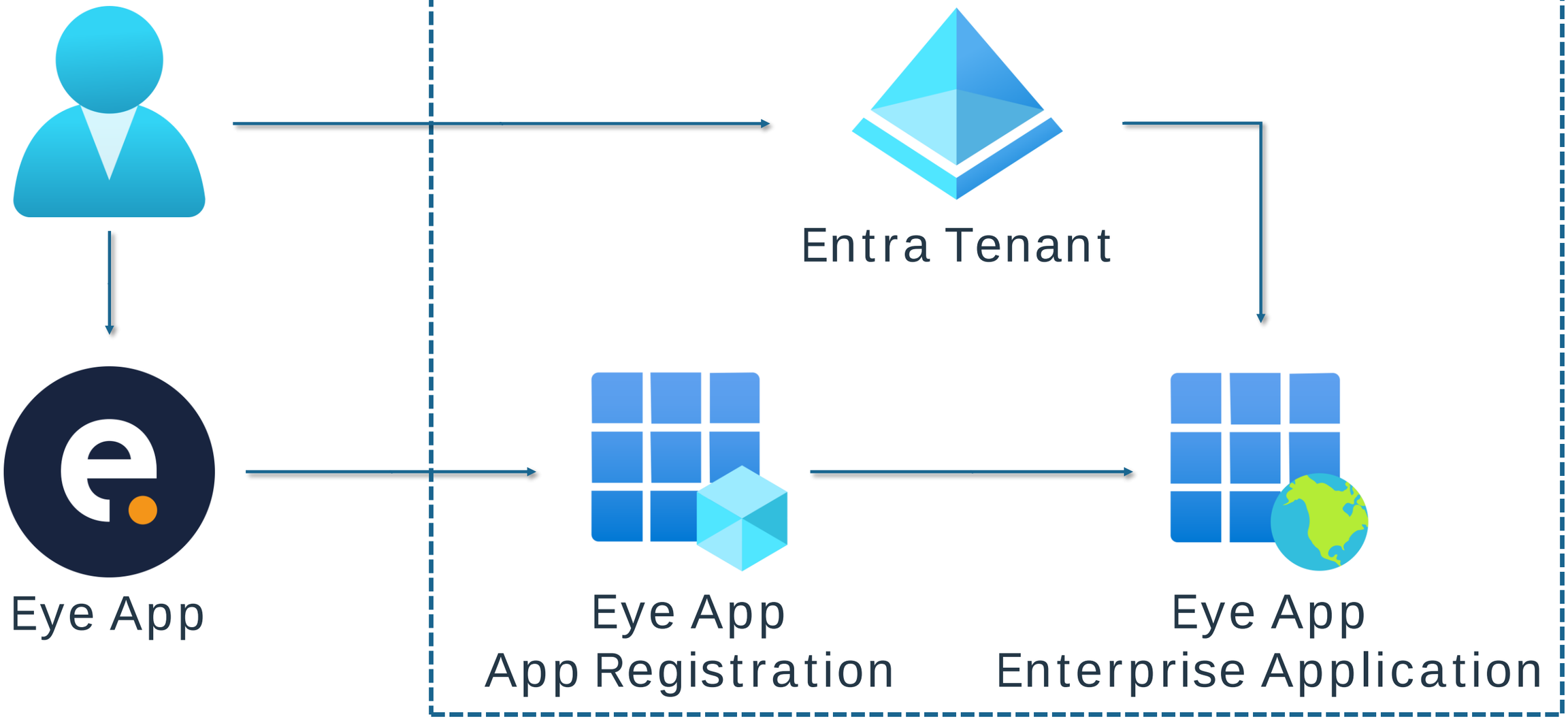
- login.microsoftonline.com
- Also called Identity Provider (IdP)
- Does Authentication & Authorization

Microsoft Identity Platform



- login.microsoftonline.com
- Also called Identity Provider (IdP)
- Does Authentication & Authorization

- Single-Page App
- Web App
- Mobile App
- Desktop App
- Browserless App
- Daemon App
- Web API


Entra Tenant
Eye App
Eye App
App Registration
Eye App
Enterprise Application

Application Types & Token Grant Flows

- Single-Page App
- Web App
- Mobile App
- Desktop App
- Browserless App
- Daemon App
- Web API

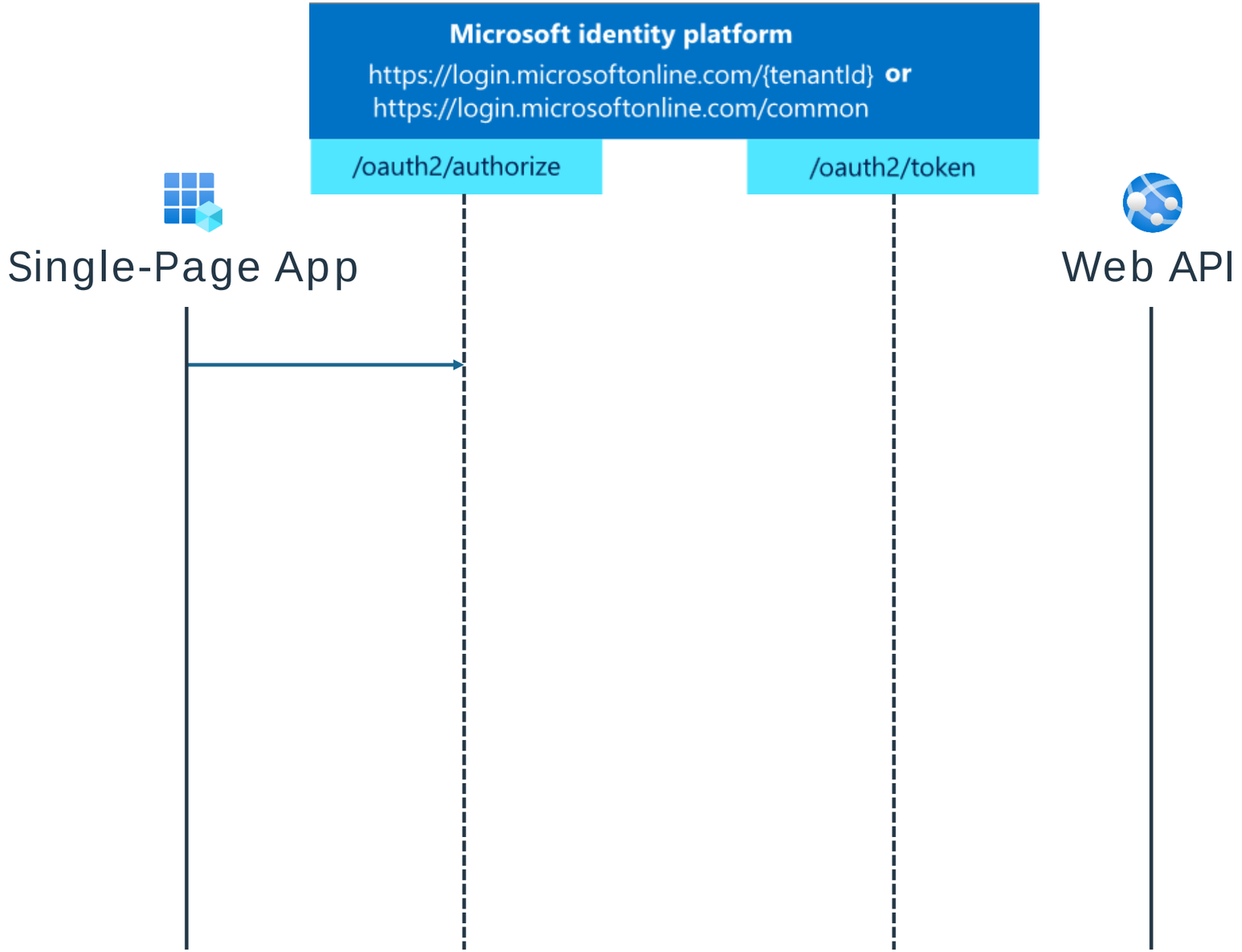
- Implicit flow
- Authorization code flow
- Resource Owner Password (ROPC)
- Device code flow
- Client credentials
- On-behalf-of flow

Application Types & Token Grant Flows

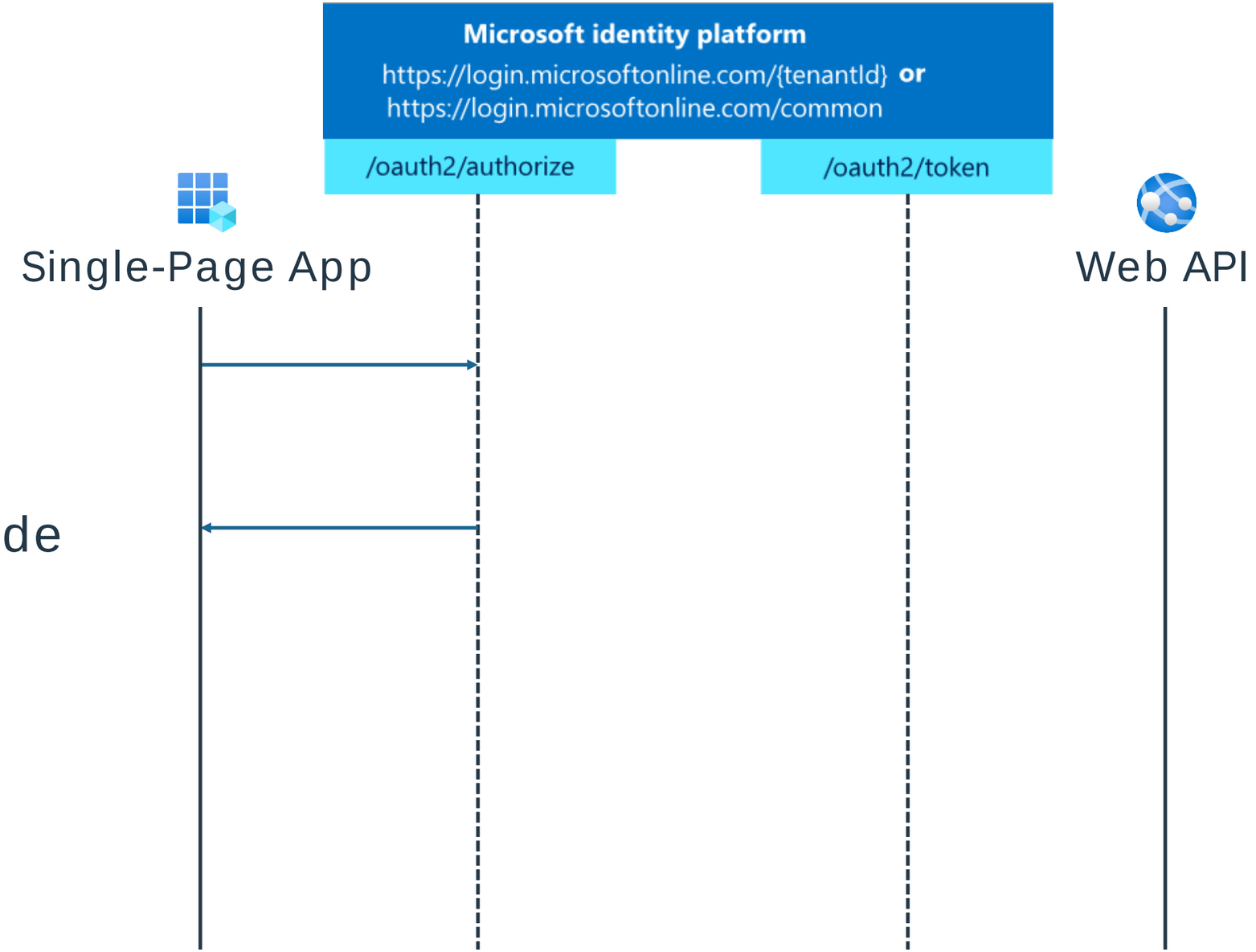
- Single-Page App
- Web App
- Mobile App
- Desktop App
- Browserless App
- Daemon App
- Web API

- Implicit flow
- Authorization code flow
- Resource Owner Password (ROPC)
- Device code flow
- Client credentials
- On-behalf-of flow

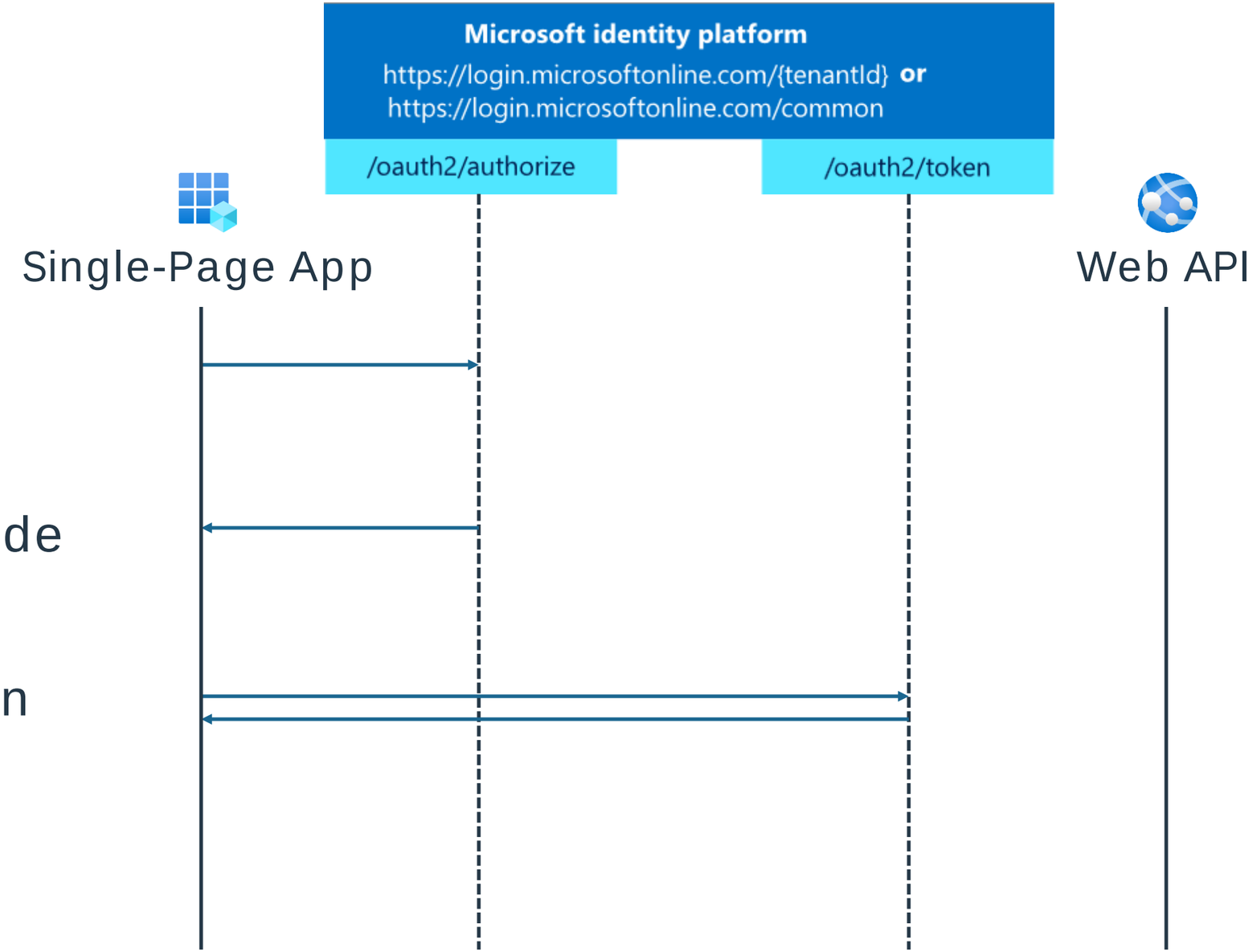
1. Sign-in & Consent



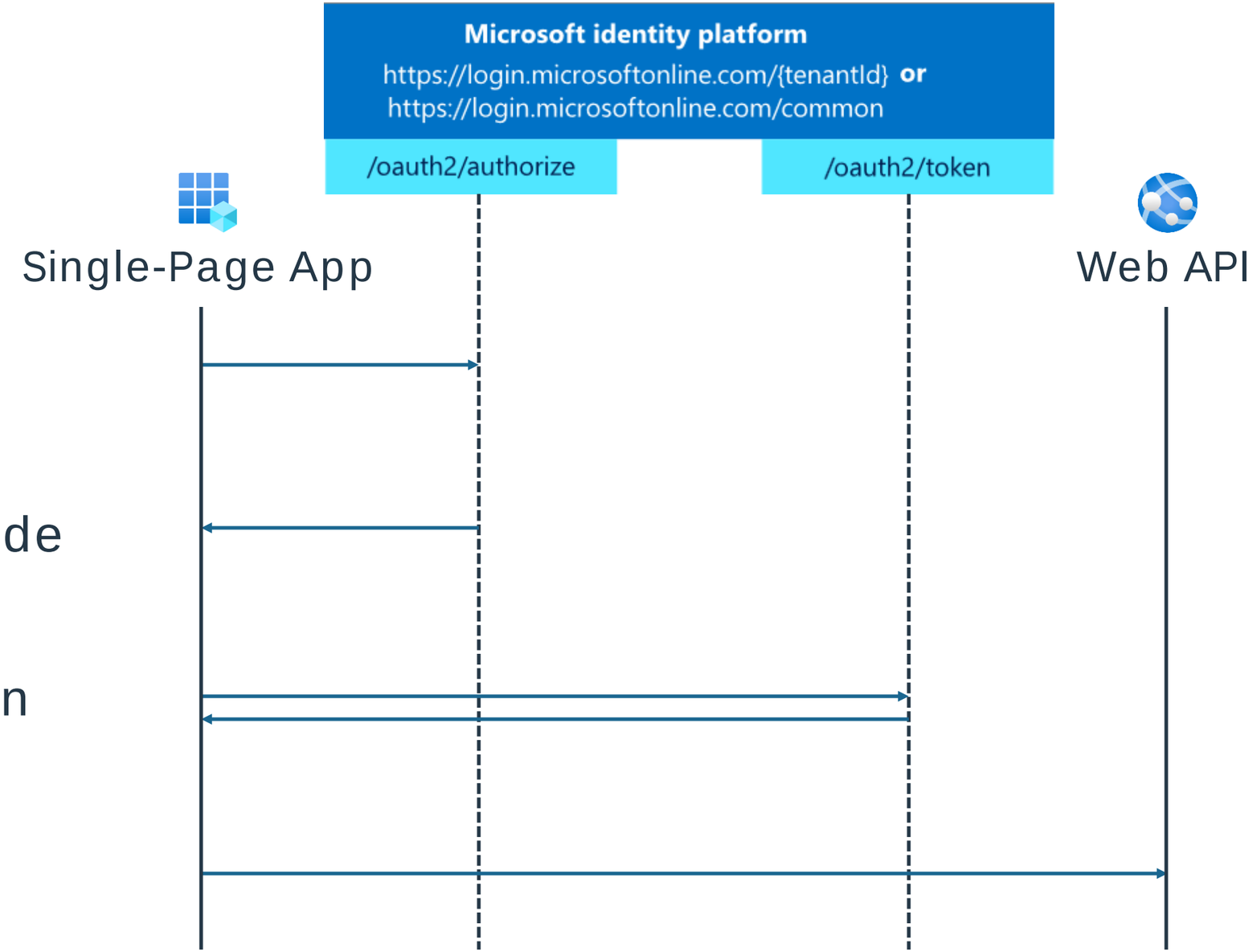
1. Sign-in & Consent
2. Get Authorization Code



1. Sign-in & Consent
2. Get Authorization Code
3. Request Access Token



1. Sign-in & Consent
2. Get Authorization Code
3. Request Access Token
4. Call Web API



Consent Flow

- User consent vs Admin consent 'On Behalf of All'
- Instantiates **Application Objects** (App registrations) into **Service Principals** (Enterprise Applications)

Consent Flow

- User consent vs Admin consent 'On Behalf of All'
- Instantiates **Application Objects** (App registrations) into **Service Principals** (Enterprise Applications)

- https://login.microsoftonline.com/common/adminconsent?client_id=<APP_ID>

Consent Flow

- User consent vs Admin consent 'On Behalf of All'
- Instantiates **Application Objects** (App registrations) into **Service Principals** (Enterprise Applications)

- https://login.microsoftonline.com/common/adminconsent?client_id=<APP_ID>

```
$token = (Get-AzAccessToken -TenantId $tenant_id -ResourceUrl 74658136-14ec-4630-ad9b-26e160ff0fc6).Token

$headers = @{'Authorization' = 'Bearer ' + $token
             'X-Requested-With'= 'XMLHttpRequest'
             'x-ms-client-request-id'= [guid]::NewGuid()
             'x-ms-correlation-id' = [guid]::NewGuid()}

$url = "https://main.iam.ad.ext.azure.com/api/RegisteredApplications/$($app_id)/Consent?onBehalfOfAll=true"
Invoke-RestMethod -Uri $url -Headers $headers -Method POST -ErrorAction Stop
```

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",
  "kid": "_jNwjeSnvTTK8XEdr5QUPkBRLLo"
}.{
  "aud": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
  "iss": "https://sts.windows.net/4c1a1e11-a052-4346-9091-807fc856e66e/",
  "iat": 1751972163,
  "nbf": 1751972163,
  "exp": 1751976928,
  "acr": "1",
  "aio":
"AdQAK/8ZAAAAESlm9/8g9kwF9BwPonmkwIwphyBtghOYvLFRM0qLZ/+eWmvnr2fT9z/U7tS0gTL2VBuqMpel2zAC+
zLV6IGHZN9lvP/8OstyxYZYTHjnKJSu12pcVB2EUHxRnb170NbKf3Rdca/y2jh/V/9XfIUjCXqURxXoEk99Yvqrng
pJXNKGhLedxN//TxWRinOfg==",
  "amr": [
    "rsa",
    "mfa"
  ],
  "appid": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
  "appidacr": "2",
  "deviceid": "f72f9e63-f51c-4b61-af85-49b6dfc6a079",
  "family_name": "Bernard",
  "given_name": "Vaisha",
  "idtyp": "user",
  "ipaddr":
  "name": "Vaisha Bernard | Eye Security",
  "oid": "38708b91-6c68-4152-9aaf-f41f1ca95e65",
  "puid": "100320009C1A777E",
  "rh": "1.AXQAER4aTFKgRkOQkYB_yFbmboNAS8SwO8FJtH2XTlPL3zytAe90AA.",
  "scp": "Organization.Read.All Policy.ReadWrite.ApplicationConfiguration User.Read",
  "sid": "006b73e9-c32f-efb6-5064-6a11fe2bddf4",
  "sub": "JYp1vkaXg8uSzNB_n2RlVspZX8dOxMtaL1FgutHsymQ",
  "tid": "4c1a1e11-a052-4346-9091-807fc856e66e",
  "unique_name": "vaisha.bernard@eye.security",
  "upn": "vaisha.bernard@eye.security",
  "uti": "YkUnNSNnO0ec7M2x1iRGAA",
  "ver": "1.0",
  "wids": [
    "c430b396-e693-46cc-96f3-db01bf8bb62a",
    "5d6b6bb7-de71-4623-b4af-96380a352509"
  ],
  "xms_ftd": "SgMETP26g1pxu-akzQtmEEHIdTDsJLzZL5Ap09qEYqoBc3dlZGVuYy1kc21z",
  "xms_idrel": "1 6",
  "xms_tdbr": "EU"
}.[Signature]
```


Header

```
7 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Il9qTndqZVNudlRUSzhYRWRyNVFVUGtCUkxMbyIsImtpZ
CI6Il9qTndqZVNudlRUSzhYRWRyNVFVUGtCUkxMbyJ9.eyJhdWQiOiJjNDRiNDA4MyOzYmIwLTQ5YzEtYjQ3ZC05N
zRlNTNjYmPmM2MiLCJpc3MiOiJodHRwczovL3NOcy53aW5kb3dzLm5ldC8OYzFhMWUxMS1hMDUyLTQzNDYtOTA5MS
O4MDdmYzg1NmU2NmUvIiwiaWFOIjoxNzUxOTcyMTYzLCJuYmYiOjE3NTE5NzIxNjMsImV4cCI6MTc1MTk3NjkyOCw
iYWNyIjoiMSIsImFpbyI6IkFkUUFLLzhaQUFBQUVTbG05LzhnOWt3RjlCdlBvbm1rdDl3cGh5QnRnaE9ZdkxGUkOw
cUxaLytlV2l2bnIyZlQ5ei9VN3RTMGdUTDJWQnVxTXB1bDJ6QUMrcWd3RzlEVitOVWFZROJ5RGE0M3hueStYdkxOM
kxybXRMOW83dVVhdS95Rml6TFY2SUdIWk45bHZQLzhPc3R5eFlaWVRIam5LS1NiMTJwY1ZCMkVVSHhSbmIxNzBOYk
tmM1JkY2EveTJqaC9WLzlYZklVakNYcVVSeFhvRWs5OVl2cXJuZldqWkJLVDB5am5qeXo5ZWltVXVwRUdPWVdhMzZ
oaON4L3p5TUVsRFVSRlhRc3BKWE5LR2hMZWR4Ti8vVHhXUmluT2ZnPTOiLCJhbXIiOlsicnNhIiwibWZhIl0sImFw
cGlkIjoiYzQ0YjQwODMtM2JiMC00OWMxLWION2QtOTc0ZTUzY2JkZjNjIiwiYXBwaWRhY3IiOiIyIiwiZGV2aWNla
WQiOiJmNzJmOWU2MyImNTFjLTRiNjEtYWY4NS00OWI2ZGZjNmEwNzkiLCJmY
JnaXZlb19uYW1lIjoiVmFpc2hhIiwiaWROeXAiOiJ1c2VyIiwiaXBhZGRyIj
iOiJWYWlzaGEgQmVybmFyZCB8IEV5ZSBTZWN1cmlOeSIsIm9pZCI6IjM4NzA
MWYxY2E5NWU2NSIsInBlaWQiOiIxMDAzMjAwMDlDMUE3NzdFIiwicmgiOiIx
UZibWJvTkFTOFN3TzhGSnRIMlhUbFBMM3p5dEFlOTBBQS4iLCJzY3AiOiJPcmdhbm16YXRpb24uUmVhZC5BbGwgUG
9saWN5LlJlYWRXcmlOZS5BcHBsaWNhdGlvbkNvbmZpZ3VyYXRpb24gVXNlci5SZWFkIiwic2lkIjoiMDA2YjczZTk
tYzMyZiIlZmI2LTUwNjQtNmExMWZlMmJkZGYOIiwic3ViIjoiSllwMXZrYVhnOHVTek5CX24yUmxWc3BaWDhkT3hN
dGFMMUZndXRIc3ltUSIsInRpZCI6IjRjMWExZTExLWEwNTItNDMONiO5MDkxLTgwN2ZjODU2ZTY2ZSIsInVuaXF1Z
V9uYW1lIjoidmFpc2hhLmJlcm5hcmRAZXllLnN1Y3VyaXR5IiwidXBuIjoidmFpc2hhLmJlcm5hcmRAZXllLnN1Y3
VyaXR5IiwidXRpIjoiWWtVbk5TTm5PMGVjNOOyeDFpUkdBQSIsInZlciI6IjEuMCIsIndpZHMiOlsiYzQzMGIzOTY
tZTY5MyOONmNjLTk2ZjMtZGIwMWJmOGJiNjJhIiwiNWQ2YjZiYjctZGU3MSOONjIzLWIOYWYtOTYzODBhMzUyNTA5
IlOsInhtc19mdGQiOiJTZO1FVFAyNmcxcHh1LWFrelFObUVFSElkVERzSkx6Wkw1QXAwOXFFWXFvQmMzZGxaR1Z1W
Xkxa2MyMXoiLCJ4bXNfaWRyZWwiOiIxIDYiLCJ4bXNfdGRici16IkVVInO.
```

Payload

Signature

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",
}.
  "exp": 1751976928,
  "acr": "1",
  "aio":
"AdQAK/8ZAAAAESlm9/8g9kwF9BwPonmkwIwphyBtghOYvLFRM0qLZ/+eWmvnr2fT9z/U7tS0gTL2VBuqMpel2zAC+
zLV6IGHZN9lvP/8OstyxYZYTHjnKJSu12pcVB2EUHxRnb170NbKf3Rdca/y2jh/V/9XfIUjCXqURxXoEk99YvqrngW
pJXNKGhLedxN//TxWRinOfg==",
  "amr": [
    "rsa",
  "given_name": "Vaisha",
  "idtyp": "user",
  "ipaddr":
  "name": "Vaisha Bernard | Eye Security",
  "oid": "38708b91-6c68-4152-9aaf-f41f1ca95e65",
  "puid": "100320009C1A777E",
  "rh": "1.AXQAER4aTFKgRkOQkYB_yFbmboNAS8SwO8FJtH2XTlPL3zytAe90AA.",
  "scp": "Organization.Read.All Policy.ReadWrite.ApplicationConfiguration User.Read",
  "sid": "006b73e9-c32f-efb6-5064-6a11fe2bddf4",
  "sub": "JYp1vkaXg8uSzNB_n2RlVspZX8dOxMtaL1FgutHsymQ",
  "tid": "4c1a1e11-a052-4346-9091-807fc856e66e",
  "unique_name": "vaisha.bernard@eye.security",
  "upn": "vaisha.bernard@eye.security",
  "uti": "YkUnNSNnO0ec7M2x1iRGAA",
  "ver": "1.0",
  "wids": [
    "c430b396-e693-46cc-96f3-db01bf8bb62a",
    "5d6b6bb7-de71-4623-b4af-96380a352509"
  ],
  "xms_ftd": "SgMETP26g1pxu-akzQtmEEHIdTDsJLzZL5Ap09qEYqoBc3dlZGVuYy1kc21z",
  "xms_idrel": "1 6",
  "xms_tdbr": "EU"
}.[Signature]
```


"aud": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",

"appid": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",
  "kid": "_jNwjeSnvTTK8XEdr5QUPkBRLLo"
```

"iss": "https://sts.windows.net/4c1a1e11-a052-4346-9091-807fc856e66e/",

```
  "acr": "1",
  "aio":
"AdQAK/8ZAAAAESlm9/8g9kwF9BwPonmkwIwphyBtghOYvLFRM0qLZ/+eWmvnr2fT9z/U7tS0gTL2VBuqMpel2zAC+
zLV6IGHZN9lvP/8OstyxYZYTHjnKJSu12pcVB2EUHxRnb170NbKf3Rdca/y2jh/V/9XfIUjCXqURxXoEk99YvqrngW
pJXNKGhLedxN//TxWRinOfg==",
  "amr": [
    "rsa",
    "mfa"
  ],
  "appid": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
  "appidacr": "2",
  "deviceid": "f72f9e63-f51c-4b61-af85-49b6dfc6a079",
  "family_name": "Bernard",
  "given_name": "Vaisha",
  "idtyp": "user",
  "ipaddr":
  "name": "Vaisha Bernard | Eye Security",
  "oid": "38708b91-6c68-4152-9aaf-f41f1ca95e65",
  "puid": "100320009C1A777E",
  "rh": "1.AXQAER4aTFKgRkOQkYB_yFbmboNAS8SwO8FJtH2XTlPL3zytAe90AA.",
  "scp": "Organization.Read.All Policy.ReadWrite.ApplicationConfiguration User.Read",
  "sid": "006b73e9-c32f-efb6-5064-6a11fe2bddf4",
  "sub": "JYp1vkaXg8uSzNB_n2RlVspZX8dOxMtaL1FgutHsymQ",
  "tid": "4c1a1e11-a052-4346-9091-807fc856e66e",
  "unique_name": "vaisha.bernard@eye.security",
  "upn": "vaisha.bernard@eye.security",
  "uti": "YkUnNSNnO0ec7M2x1iRGAA",
  "ver": "1.0",
  "wids": [
    "c430b396-e693-46cc-96f3-db01bf8bb62a",
    "5d6b6bb7-de71-4623-b4af-96380a352509"
  ],
  "xms_ftd": "SgMETP26g1pxu-akzQtmEEHIdTDsJLzZL5Ap09qEYqoBc3dlZGVuYy1kc21z",
  "xms_idrel": "1 6",
  "xms_tdbr": "EU"
}.[Signature]
```

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",
  "kid": "_jNwjeSnvTTK8XEdr5QUPkBRLLo"
}.{
  "aud": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
  "iss": "https://sts.windows.net/4c1a1e11-a052-4346-9091-807fc856e66e/",
  "iat": 1751972163,
  "nbf": 1751972163,
  "exp": 1751976928,
  "acr": "1",
  "aio":
"AdQAK/8ZAAAAESlm9/8g9kwF9BwPonmkwIwphyBtghOYvLFRM0qLZ/+eWmvnr2fT9z/U7tS0gTL2VBuqMpel2zAC+
zLV6IGHZN9lvP/8OstyxYZYTHjnKJSu12pcVB2EUHxRnb170NbKf3Rdca/y2jh/V/9XfIUjCXqURxXoEk99YvqrngW
pJXNKGhLedxN//TxWRinOfg==",
  "amr": [
    "rsa",
    "mfa"
  ],
  "appid": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
  "appidacr": "2",
  "deviceid": "f72f9e63-f51c-4b61-af85-49b6dfc6a079",
  "family_name": "Bernard",
  "given_name": "Vaisha",
  "idtyp": "user",
  "ipaddr":
  "name": "Vaisha Bernard | Eye Security",
  "oid": "38708b91-6c68-4152-9aaf-f41f1ca95e65",
  "puid": "100320009C1A777E",
  "scp": "Organization.Read.All Policy.ReadWrite.ApplicationConfiguration User.Read",
  "unique_name": "vaisha.bernard@eye.security",
  "upn": "vaisha.bernard@eye.security",
  "uti": "YkUnNSNnO0ec7M2x1iRGAA",
  "ver": "1.0",
  "wids": [
    "c430b396-e693-46cc-96f3-db01bf8bb62a",
    "5d6b6bb7-de71-4623-b4af-96380a352509"
  ],
  "xms_ftd": "SgMETP26g1pxu-akzQtmEEHIdTDsJLzZL5Ap09qEYqoBc3dlZGVuYy1kc21z",
  "xms_idrel": "1 6",
  "xms_tdbr": "EU"
}.[Signature]
```

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",
  "kid": "_jNwjeSnvTTK8XEdr5QUPkBRLLo"
}.{
  "aud": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
  "iss": "https://sts.windows.net/4c1a1e11-a052-4346-9091-807fc856e66e/",
  "iat": 1751972163,
  "nbf": 1751972163,
  "exp": 1751976928,
  "acr": "1",
  "aio":
"AdQAK/8ZAAAAESlm9/8g9kwF9BwPonmkwIwphyBtghOYvLFRM0qLZ/+eWmvnr2fT9z/U7tS0gTL2VBuqMpel2zAC+
zLV6IGHZN9lvP/8OstyxYZYTHjnKJSu12pcVB2EUHxRnb170NbKf3Rdca/y2jh/V/9XfIUjCXqURxXoEk99YvqrngW
pJXNKGhLedxN//TxWRinOfg==",
  "amr": [
    "rsa",
    "mfa"
  ],
  "appid": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
  "appidacr": "2",
  "d
  "f
  "g
  "i
  "i
  "n
  "o
  "p
  "r
  "s
  "s
  "s
  "t
  "u
  "u
  "u
  "v
  "w
  ],
  "xms_ftd": "SgMETP26g1pxu-akzQtmEEHIdTDsJLzZL5Ap09qEYqoBc3dlZGVuYy1kc21z",
  "xms_idrel": "1 6",
  "xms_tdbr": "EU"
}.[Signature]
```

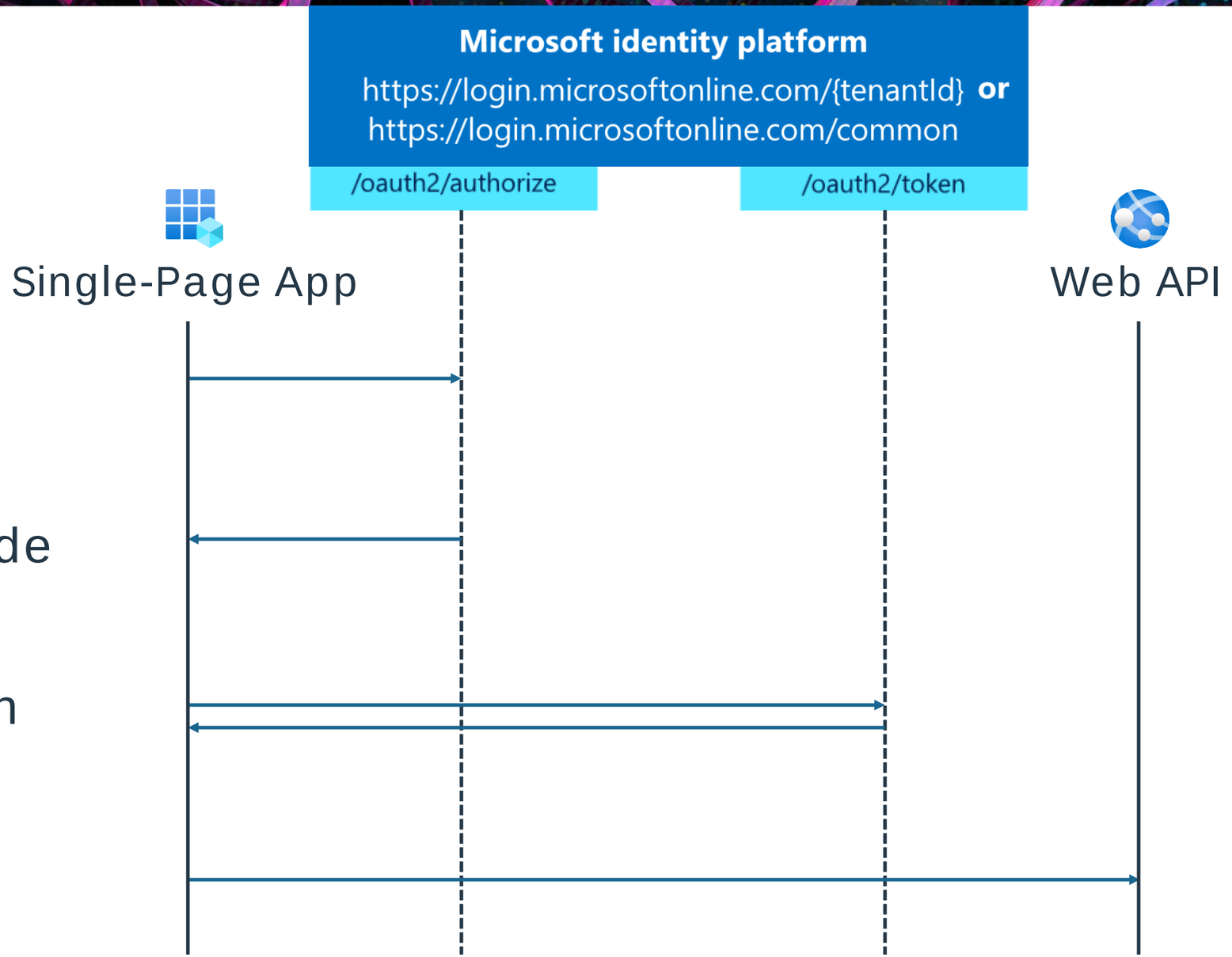


```
"oid": "38708b91-6c68-4152-9aaf-f41f1ca95e65",
"name": "Vaisha Bernard | Eye Security",
"unique_name": "vaisha.bernard@eye.security",
"upn": "vaisha.bernard@eye.security",
```

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",
  "kid": "_jNwjeSnvTTK8XEdr5QUPkBRLLo"
}.{
  "aud": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
  "iss": "https://sts.windows.net/4c1a1e11-a052-4346-9091-807fc856e66e/",
  "iat": 1751972163,
  "nbf": 1751972163,
  "exp": 1751976928,
  "acr": "1",
  "aio":
"AdQAK/8ZAAAAESlm9/8g9kwF9BwPonmkwIwphyBtghOYvLFRM0qLZ/+eWmvnr2fT9z/U7tS0gTL2VBuqMpel2zAC+
zLV6IGHZN9lvP/8OstyxYZYTHjnKJSu12pcVB2EUHxRnb170NbKf3Rdca/y2jh/V/9XfIUjCXqURxXoEk99YvqrngW
pJXNKGhLedxN//TxWRinOfg==",
  "amr": [
    "rsa",
    "mfa"
  ],
  "appid": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
  "appidacr": "2",
  "deviceid": "f72f9e63-f51c-4b61-af85-49b6dfc6a079",
  "family_name": "Bernard",
  "given_name": "Vaisha",
  "idtyp": "user",
  "ipaddr":
  "name": "Vaisha Bernard | Eye Security",
  "oid": "38708b91-6c68-4152-9aaf-f41f1ca95e65",
  "puid": "100320009C1A777E",
  "rh": "1.AXQAER4aTFKgRkOQkYB_yFbmboNAS8SwO8FJtH2XTlPL3zytAe90AA.",
  "scp": "Organization.Read.All Policy.ReadWrite.ApplicationConfiguration User.Read",
  "sid": "006b73e9-c32f-efb6-5064-6a11fe2bddf4",
  "sub": "JYp1vkaXg8uSzNB_n2RlVspZX8dOxMtaL1FgutHsymQ",
  "tid": "4c1a1e11-a052-4346-9091-807fc856e66e",
  "unique_name": "vaisha.bernard@eye.security",
  "upn": "vaisha.bernard@eye.security",
  "uti": "YkUeNSNnO0ec7M2x1iRGAA"
  "
  "
  ],
  "xms_ftd": "SgMETP26g1pxu-akzQtmEEHIdTDsJLzZL5Ap09qEYqoBc3dlZGVuYy1kc21z",
  "xms_idrel": "1 6",
  "xms_tdbr": "EU"
}.[Signature]
```


"tid": "4c1a1e11-a052-4346-9091-807fc856e66e",

1. Sign-in & Consent
2. Get Authorization Code
3. Request Access Token
4. Call Web API



Multi-Tenant Applications

Home > App registrations >

Register an application ...

* Name

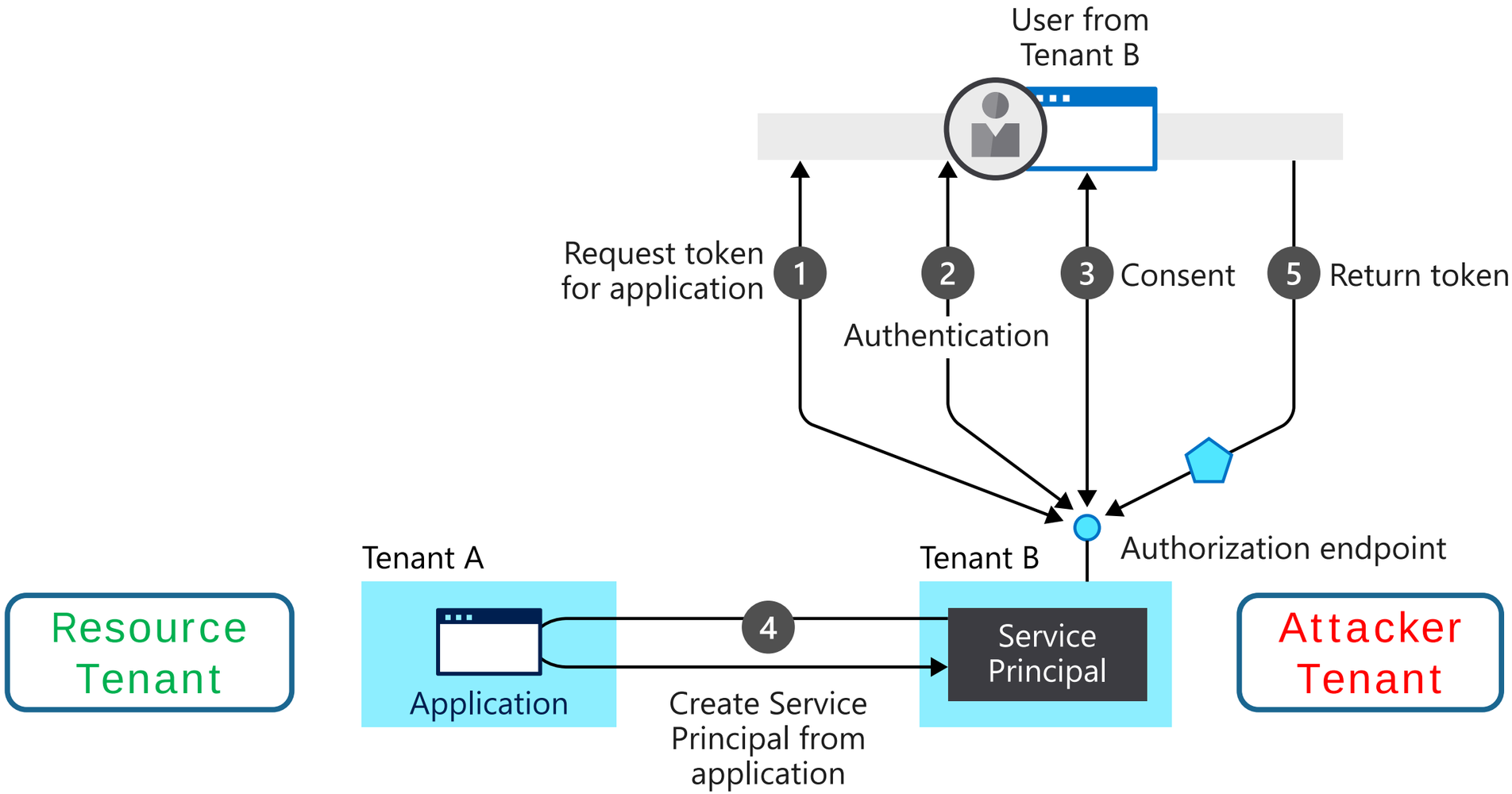
The user-facing display name for this application (this can be changed later).

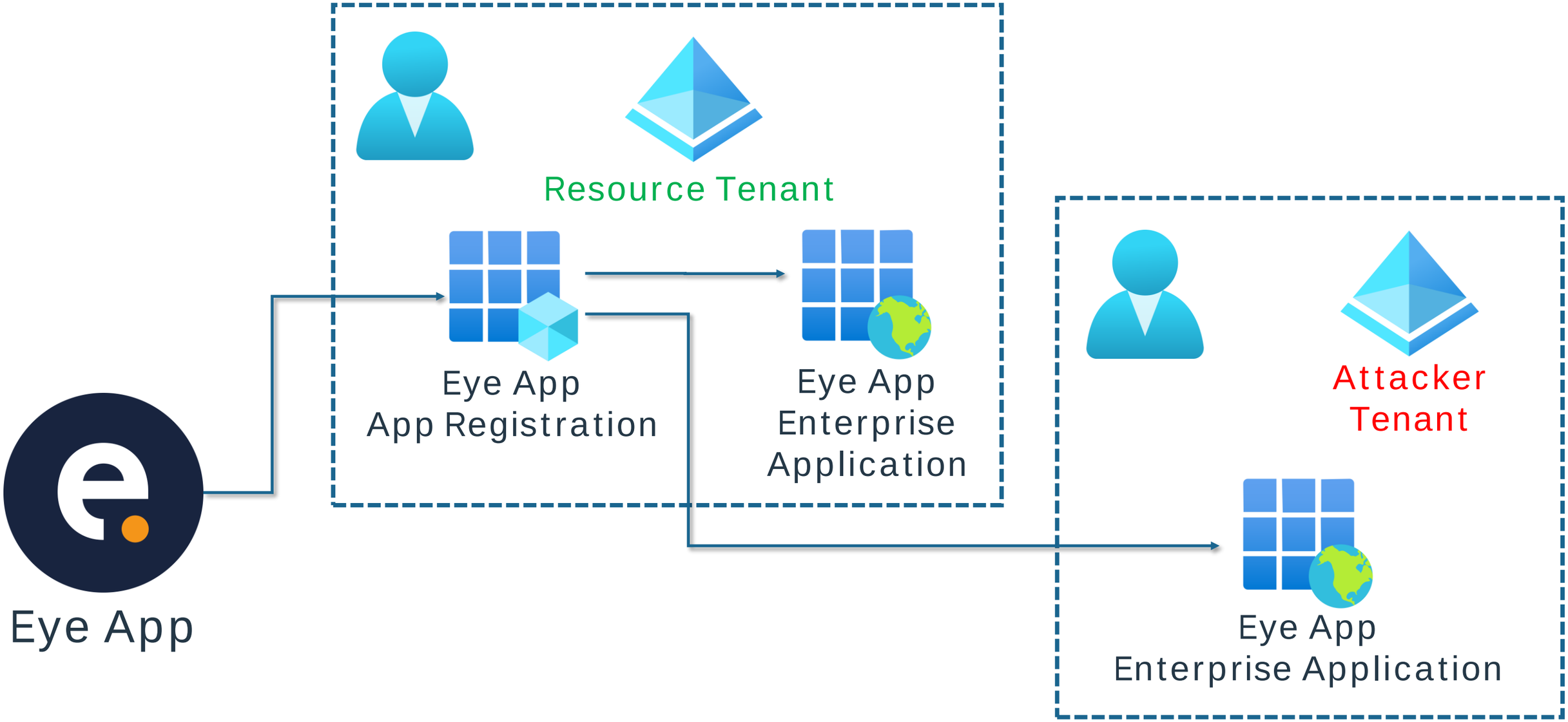
Supported account types

Who can use this application or access this API?

- (•) Accounts in this organizational directory only (Bernard only - Single tenant)
- ( ) Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ( ) Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ( ) Personal Microsoft accounts only

Multi-Tenant Applications




Resource Tenant
Eye App
App Registration
Eye App
Enterprise
Application
Attacker
Tenant
Eye App
Eye App
Enterprise Application

Microsoft identity platform

https://login.microsoftonline.com/{tenantId} **or**
https://login.microsoftonline.com/common

Identity Provider Endpoints

Value	Description
`common`	Users with both a personal Microsoft account and a work or school account from Microsoft Entra ID can sign in to the application.
`organizations`	Only users with work or school accounts from Microsoft Entra ID can sign in to the application.
`consumers`	Only users with a personal Microsoft account can sign in to the application.
`Directory (tenant) ID` or `contoso.onmicrosoft.com`	Only users from a specific Microsoft Entra tenant (directory members with a work or school account or directory guests with a personal Microsoft account) can sign in to the application. The value can be the domain name of the Microsoft Entra tenant or the tenant ID in GUID format.

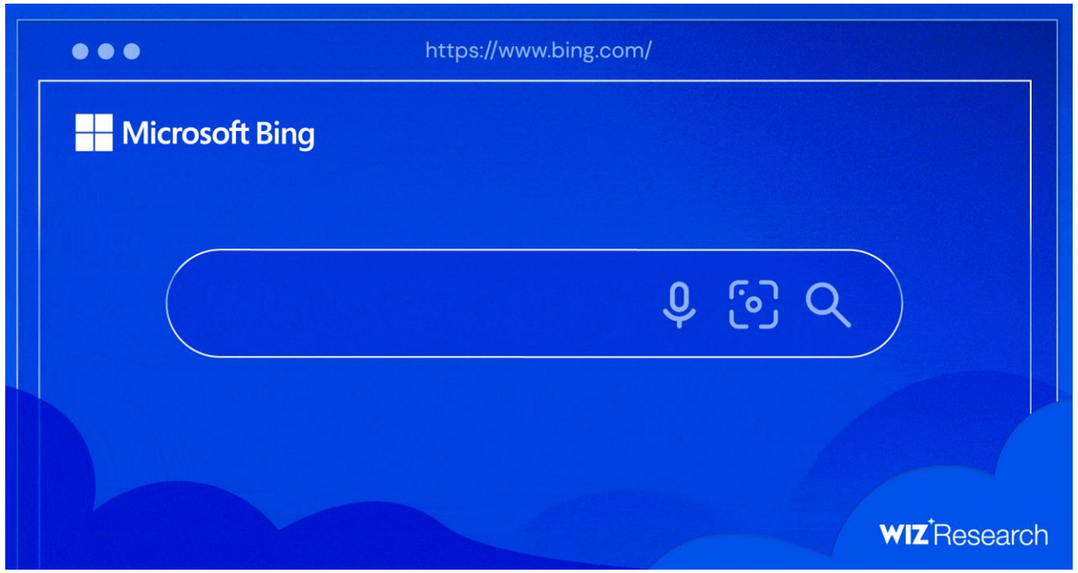
Identity Provider Endpoints

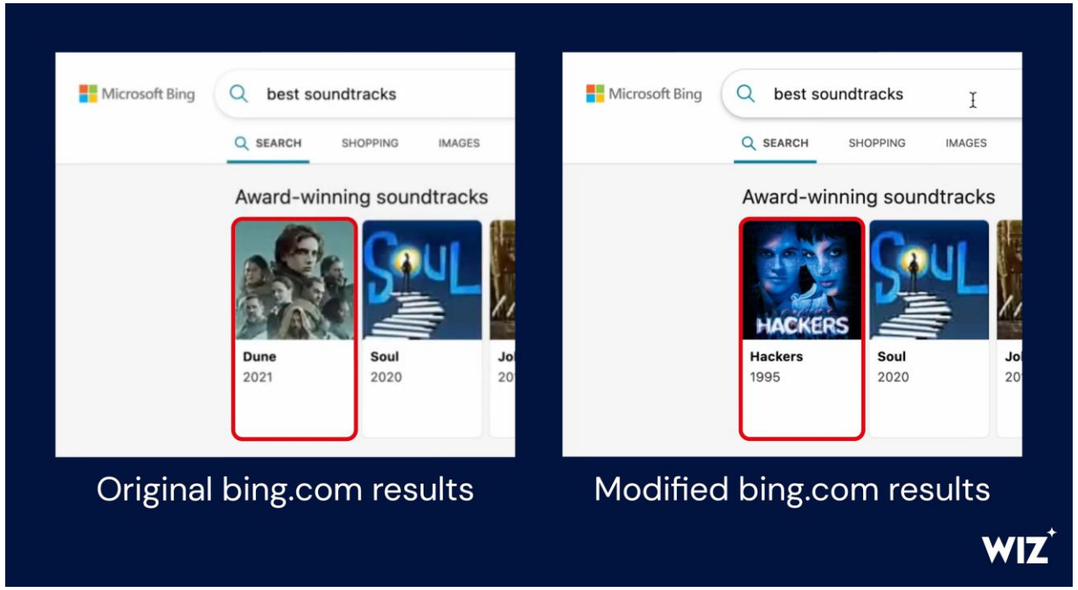
- https://login.microsoftonline.com/common/
- https://login.microsoftonline.com/organizations/
- https://login.microsoftonline.com/eye.security/
- https://login.microsoftonline.com/eyecs.onmicrosoft.com/
- https://login.microsoftonline.com/4c1a1e11-a052-4346-9091-807fc856e66e/

- For me, all the same!

Previous Research

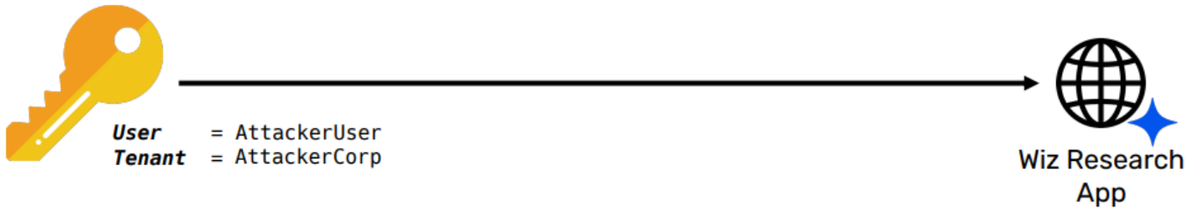
- BlackHat 2023
- Hillai Ben-Sasson (@hillai) of Wiz Research: BingBang
- Multi-Tenant Applications
- Authorization code flow





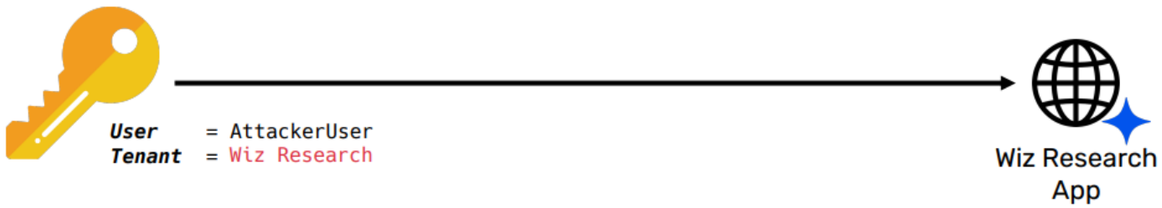
Previous Research

- Replace **attacker tenant** with **resource tenant** during authentication



ACCESS DENIED

- Token issued by **resource tenant** IdP (Microsoft)



ACCESS GRANTED

- 25% of applications vulnerable

Previous Research

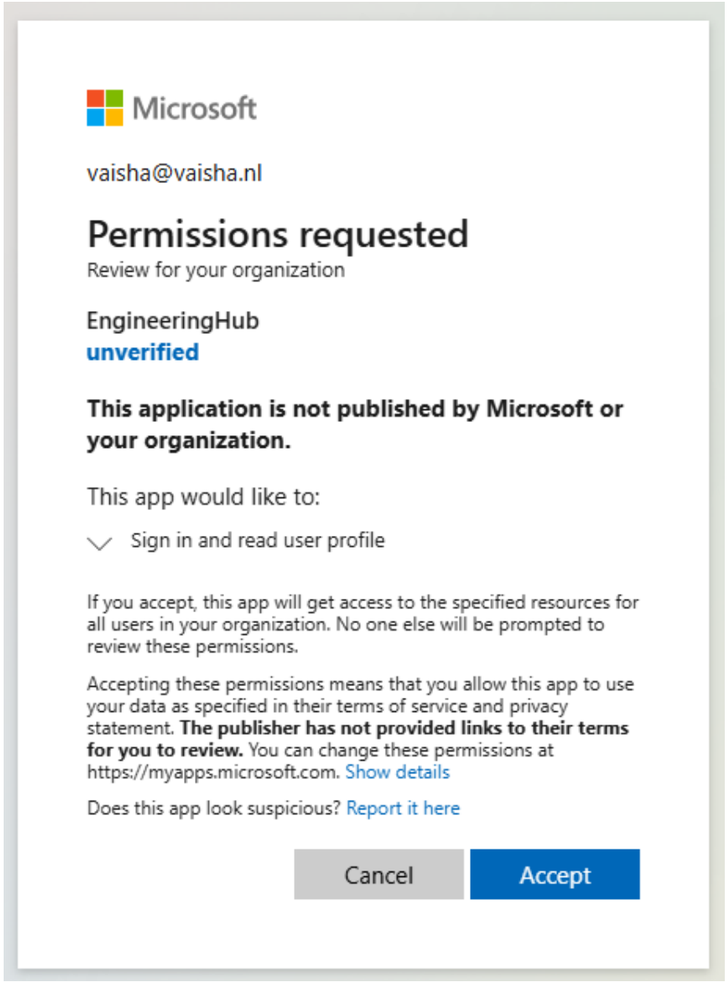
- MSRC Mitigations
  - "Azure AD has been updated to **stop issuing access tokens** to clients that are **not registered in the resource tenants**. This **prevents this issue from happening** even if an application does not correctly handle the authorization check."
  - "...implement recommended authorization checks"

- Wiz Recommendations
  - Reduce multi-tenant exposure (still valid)
  - Require user assignment
  - Implement Conditional Access Policies

"So why could I still login to the Engineering Hub?"

Vulnerable Misconfigurations

- Web app redirects to /common endpoint
- Login & consent prompt to consent app executes in **attacker tenant**
- Obtains token for app_id/aud of EngineeringHub, issued by **attacker tenant**



Vulnerable Misconfigurations

- User assignment? Conditional Access Policies? Applied in **attacker tenant**

- Authenticated ✅
- Authorized ✅
- **But by who? The attacker tenant!**

- Web application did not validate “iss" or “tid"
- **Who’s responsible?**

Access to Internal Microsoft Applications

- microsoft.com
- azure.com, .net
- office365.com
- office.com, .net,
- windows.net,
- .ms

- **102,672 (sub)domains**

Access to Internal Microsoft Applications

- 70,043 resolved to IP
- 41,890 responded to HTTPS
- 1,406 used Entra ID
  - 877 client-side redirects (javascript, sign-in buttons)
  - 529 HTTP 30X redirects

(and 327 swagger interfaces)

Access to Internal Microsoft Applications

- 762 to /<tenant> endpoint
  - /microsoft.com
  - /microsoft.onmicrosoft.com
  - /72f988bf-86f1-41af-91ab-2d7cd011db47
- 410 to /common
- 133 to /organizations
- 3 to /consumers

Access to Internal Microsoft Applications

- Parse client_id, check for multi-tenancy
- https://graph.windows.net/myorganization/applicationRefs/<APP_ID>/?api-version=1.6-internal
  - "availableToOtherTenants“ = true
- 176 multi-tenant applications

Access to Internal Microsoft Applications

- Most of them were requests to the /<tenant> endpoint
  - No account there
  - But they are Multi-Tenant applications…
  - **How to login?**

`Directory (tenant) ID` or `contoso.onmicrosoft.com`	Only users from a specific Microsoft Entra tenant (directory members with a work or school account or directory guests with a personal Microsoft account) can sign in to the application. The value can be the domain name of the Microsoft Entra tenant or the tenant ID in GUID format.

Just replace /<tenant>/ with /common/ !

HTTP match and replace rules

Use these settings to automatically replace parts of HTTP requests and responses passing through the Proxy.

Only apply to in-scope items

Add | Edit | Remove | Up | Down

Enabled	Item	Name	Match	Replace	Type
☐	Response header		^Location:*$		Literal
☑	Request header		/72f988bf-86f1-41af-91ab-2d7cd011db47/	/common/	Literal
☑	Request header		/microsoft.com/	/common/	Literal
☑	Request header		/microsoft.onmicrosoft.com/	/common/	Literal
☐	Request header		GET /([^/])+/oauth2	GET /common/oauth2	Regex
☐	Request header		POST /([^/])+/oauth2	POST /common/oauth2	Regex

Access to Internal Microsoft Applications

But many applications still gave errors…

Home > buildcloud

buildcloud | Users and groups

Enterprise Application

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Add user/group | Edit assignment | Remove assignment

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

Assign users and groups to app-roles for your application here. App-roles are made available by the developer of the application by using the application registration.

First 200 shown, search all users & groups

Display name
VB Vaisha Bernard

Home > buildcloud | Users and groups >

Edit Assignment ...

Bernard

Users and groups

1 user selected.

Select a role

None Selected

Select a role

Only a single role can be selected

Try changing or adding filters if you don't see what you're looking for.

Search

Enter role name to filter items...

4 results found

All

	Name	Type	Details
☐	Administrator	App role	Admin permissions
☐	Basic Access	App role	Basic permissions to access website
☐	Lab Team Administrator	App role	Specific lab team endpoints
☐	Machine Onboarding	App role	Used by build machines to access ma

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "CNv0OI3RwqlHFEVnaoMAshCH2XE"
}.{
  "aud": "8754ed8d-35c3-48fb-8e06-3090ed59ca8a",
  "iss": "https://login.microsoftonline.com/4bc9f778-3b0a-42c0-a343-
  "iat": 1749211957,
  "nbf": 1749211957,
  "exp": 1749215857,
  "aio":
"AYQAe/8ZAAAAdeJiVrsLWMsIBWLUPnfoqGhkURC5j5xKNFcUa0k/3eFVnoPE8cEREOP
2mPtWuqRriQnb79uDJf8p9OslwwcLCbRepNyJCNQxv2tIimuNk=",
  "cc":
"CmDd1LdWg8XEo9JlzbdnHySGzWVUVbhFSdBD/M2jGV/zDZrrqt4FaCgePofrC5nEaSf
                                                    DIC+HERJlZ4X64+6ywAyA
 "roles": [
    "Admin"
 ],
                                                    Zi00MzEzLTk5MTgtNDJjY
                                                    jgYwkO1ZyoqVAGOCAA.",
                                                    v-eCRg",
  "uti": "xKQ4gL4cREmVnhfrj7rLAA",
  "ver": "2.0"
}.[Signature]
```

Sign in

Sorry, but we're having trouble signing you in.

AADSTS650054: The application '' asked for permissions to access a resource that has been removed or is no longer available. Contact the app vendor.

https://graph.windows.net/myorganization/applicationRefs/<APP_ID>/?api-version=1.6-internal


```
],
"requiredResourceAccess":[
      {
            "resourceAppId":"cd3bfba9-915b-47ba-820f-eb9889210376",
            "resourceAccess":[
                  {
                        "id":"147991b0-05a6-4939-92ec-60f11db9b1c1",
                        "type":"Scope"
                  }
            ]
      },
      {
            "resourceAppId":"00000003-0000-0000-c000-000000000000",
            "resourceAccess":[
                  {
                        "id":"e1fe6dd8-ba31-4d61-89e7-88639da4683d",
                        "type":"Scope"
                  }
            ]
      }
],
```

```
2
3 error=access_denied&error_description=
AADSTS650052%3A+The+app+is+trying+to+access+a+service+%27[redacted]
[redacted]%27%28[redacted]%29+that+your+organization+%274bc9f778-3b0
a-42c0-a343-1830a350f622%27+lacks+a+service+principal+for.+Contact+your+IT+Admin+to+revie
w+the+configuration+of+your+service+subscriptions+or[redacted]nt+to+the+application+in+order+
to+create+the+required+service+principal.+Trac[redacted]5c6-ca6e-4e0c-b0f3-5860d36b630
```

The app is trying to access a service
"..." that your organization "..."
lacks a service principal for

```
error=access_denied&error_description=
AADSTS650052%3A+The+app+is+trying+to+access+a+service+%27[redacted]
[redacted]%27%28[redacted]%29+that+your+organization+%274bc9f778-3b0
a-42c0-a343-1830a350f622%27+lacks+a+service+principal+for.+Contact+your+IT+Admin+to+revie
w+the+configuration+of+your+service+subscriptions+or+consent+to+the+application+in+order+
to+create+the+required+service+principal.+Trace+ID%3A+65d6e5c6-ca6e-4e0c-b0f3-5860d36b630
```

```
New-AzureADServicePrincipal -AccountEnabled $true -AppId $app_id
                            -AppRoleAssignmentRequired $true
                            -Tags {WindowsAzureActiveDirectoryIntegratedApp}
```

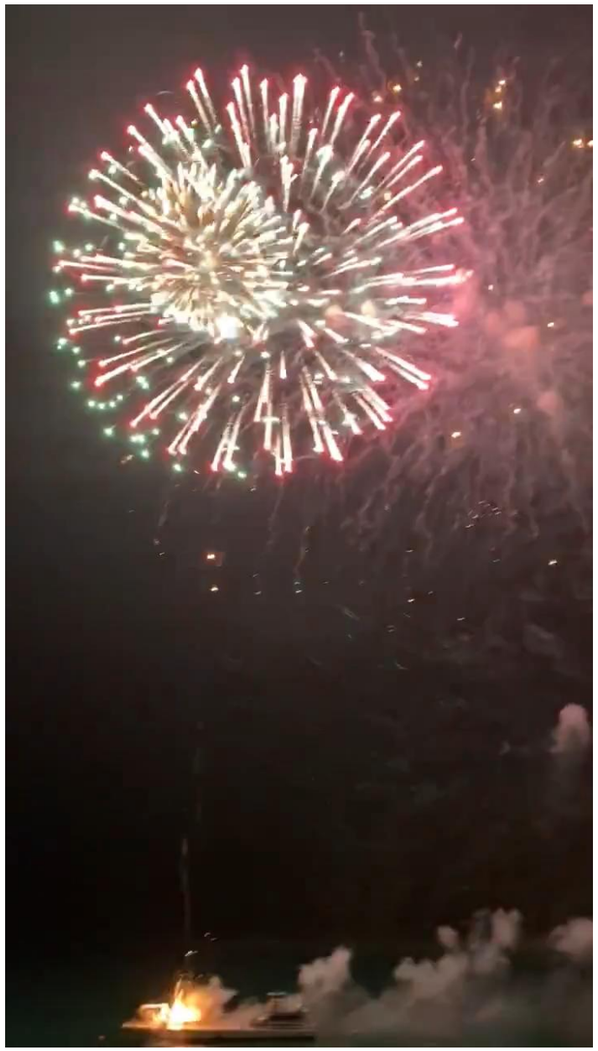
This creates a service principal without asking consent or checking availability of required resource access

Attack Steps

1. Identify Multi-Tenant App, List Required Resources — Azure AD Graph API
2. Instantiate Service Principal(s) — PowerShell
3. Assign Roles to User — Entra Web Portal
4. Redirect /<tenant> to /common — Burp
5. Consent — Entra Web Portal
6. Compromise — Browser

Access to Internal Microsoft Applications

- 22 were vulnerable and exposed internal data (12,5%)
- Not counting the ones where I “only” got frontend access with the token
- Some examples…



Emergency Broadcast System

M365 Admin Center

Authoring History Preferences

Current Post

Not authorized - Please refer to https://aka.ms/ebsdocs/usage to gain access

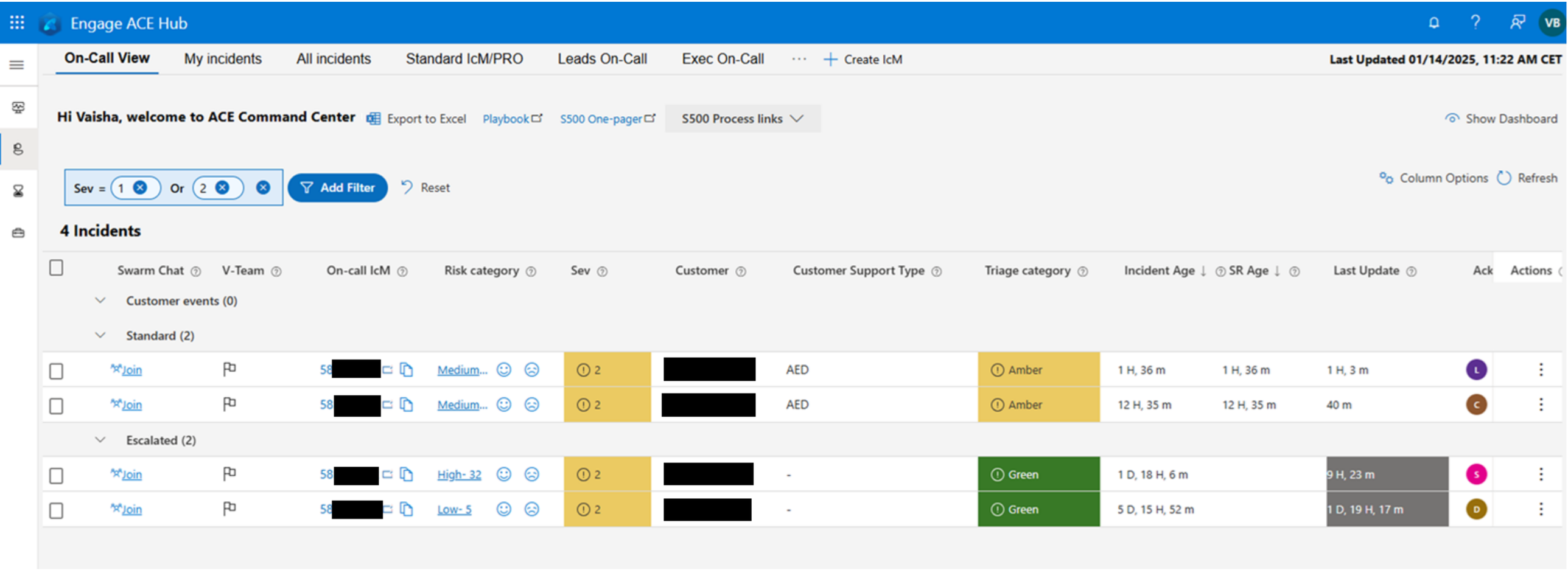
Loading...

Publish New Post

Post Status *

Select Status

Publish


Engage ACE Hub
VB
On-Call View
My incidents
All incidents
Standard IcM/PRO
Leads On-Call
Exec On-Call
Create IcM
Last Updated 01/14/2025, 11:22 AM CET
Hi Vaisha, welcome to ACE Command Center
Export to Excel
Playbook
S500 One-pager
S500 Process links
Show Dashboard
Sev = 1 Or 2
Add Filter
Reset
Column Options
Refresh
4 Incidents
Swarm Chat
V-Team
On-call IcM
Risk category
Sev
Customer
Customer Support Type
Triage category
Incident Age
SR Age
Last Update
Ack
Actions
Customer events (0)
Standard (2)
Join
58[redacted]
Medium...
2
[redacted]
AED
Amber
1 H, 36 m
1 H, 36 m
1 H, 3 m
Join
58[redacted]
Medium...
2
[redacted]
AED
Amber
12 H, 35 m
12 H, 35 m
40 m
Escalated (2)
Join
58[redacted]
High- 32
2
[redacted]
-
Green
1 D, 18 H, 6 m
9 H, 23 m
Join
58[redacted]
Low- 5
2
[redacted]
-
Green
5 D, 15 H, 52 m
1 D, 19 H, 17 m

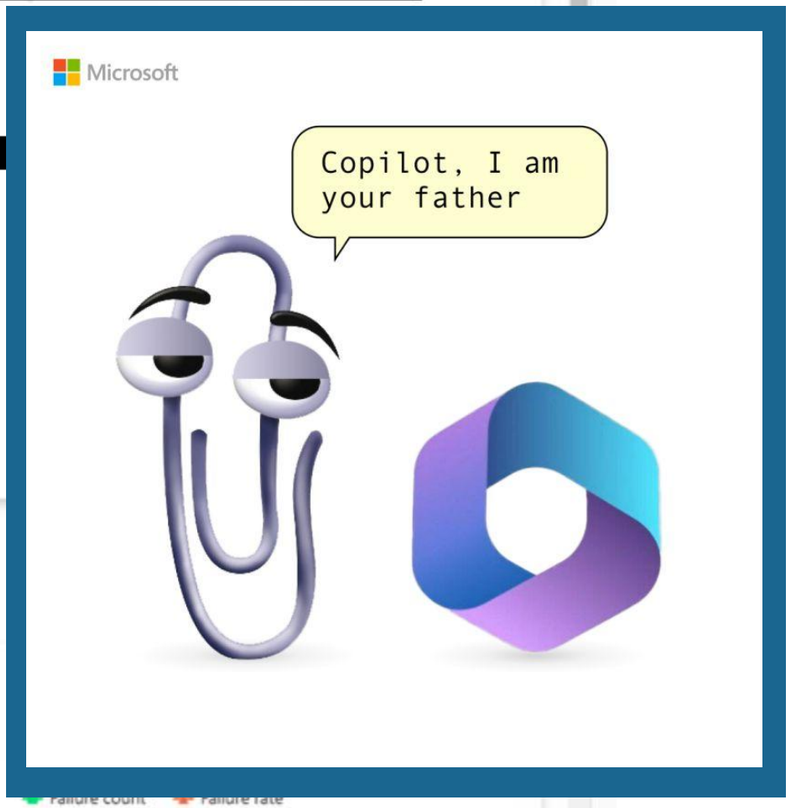
VB Vaisha Bernard
vaisha@vaisha.nl

Customer management
Customer
Capacity management
Overview
Report
Model management
Model catalog
Model deployment status
Subscription quota
Overview

TextMultiSeverity

Model name TextMultiSeverity
Model code textmultiseverity-20250108-1
Model version 20250108.1
ACR Address [redacted]
ACR Address AME -
ACR Address US Nat -
Target SKU Standard_ND96ams_A100_v4
Accuracy test AML job
https://ml.azure.com/runs/loving_puppy_[redacted]
Replication pipeline link https://dev.azure.com/msazure/Cognitive%20Services/_build/results?buildId=[redacted]&view=results
Port 8501
Readiness Probe Path /readiness
Score Path /score
Harm Category -
Capability -
Sample Request
{"data": ["Hello, World."]}
Created Time Jan 8, 2025 7:19 PM

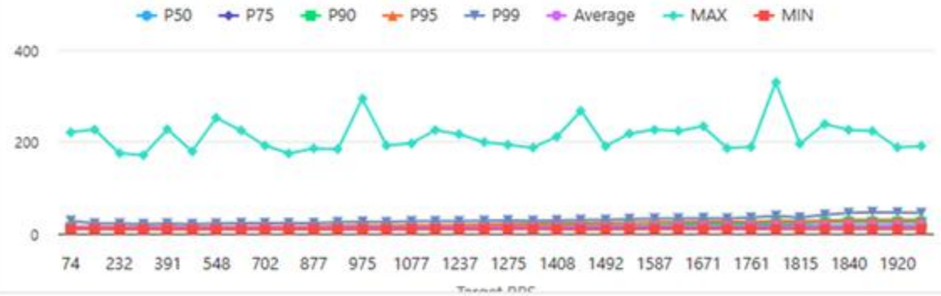
Provider 0P
Azure cloud -
Model description Text Multi-Classification model for severity prediction
ACR Address PPE [redacted]
ACR Address FairFax -
ACR Address US Sec -
Load test AML job
https://ml.azure.com/runs/goofy_sand_[redacted]
Liveness Probe Path /liveness
Image Size 0
Modality -
Status Active
Sample Response
{}
Last Modified Time Jan 13, 2025 6:59 AM



Footprint

SKU: Standard_ND96ams_A100_v4 **Payload size:** 1x128

Latency (ms)



Total request count

Risk Register

Redacted

Security Intelligence Platform (SIP) Confidentiality Acknowledgement

MICROSOFT CORPORATION CONFIDENTIALITY AFFIRMATION FOR SIP DATA ACCESS AND USAGE

Redacted

ThreatIntelInd_ActIncident

358 Request Access

ThreatIntelInd_External

178 Request Access

ThreatIntelInd_Internal

135 Request Access

Vpnlogs

115 Request Access

AD_Ldap_GroupMembers_P

110 Request Access

AD_Ldap_UserMemberOf_P

5 Request Access

AD_Ldap_Users_P

242 Request Access

SysLog_VPN

230 Request Access

SysLog_CSS

SysLog_DC

SysLog_Edge

SysLog_ExpressRoute

Sort by MyDatasets

To Explore or Request Access to SIP Data, Search by Dataset Name, Tag, Column, Access Package or Endpoint

Count: 397

AAD_GroupMembers
931 Request Access

AAD_SigninLogs_NonInteractive
389 Request Access

AAD_UserData
544 Request Access

AAD_DeviceHistory
1287 Request Access

AAD_Permission_Application
497 Request Access

AAD_Permission_ServicePrincipl
730 Request Access

AADRoleAssignments_Active
145 Request Access

AADRoleAssignments_Eligible
59 Request Access

Ask SIPPY

Sort by MyDatasets

To Explore or Request Access to SIP Data, Search by Dataset Name, Tag, Column, Access Package or Endpoint

Count: 397

AAD_GroupMembers
931 Request Access

AAD_SigninLogs_NonInteractive
389 Request Access

AAD_UserData
544 Request Access

AAD_DeviceHistory
1287 Request Access

AAD_Permission_Application
497 Request Access

AAD_Permission_ServicePrincipl
730 Request Access

AADRoleAssignments_Active
145 Request Access

AADRoleAssignments_Eligible
59 Request Access

Ask SIPPY

Ask Sippy

Tell me more about this dataset | What consumption endpoints are available? | What is the SLA for this?

Show session chat history Off

Current Context :

At which URL can I find the admin portal to approve access requests?

68 / 500

Ask Sippy

At which URL can I find the admin portal to approve access requests?

You can find the admin portal to approve access requests at the following URL:

https://myaccess.microsoft.com/@microsoft.onmicrosoft.com#/access-packages

AI-generated content may be incorrect

Does this webservice have an admin portal?

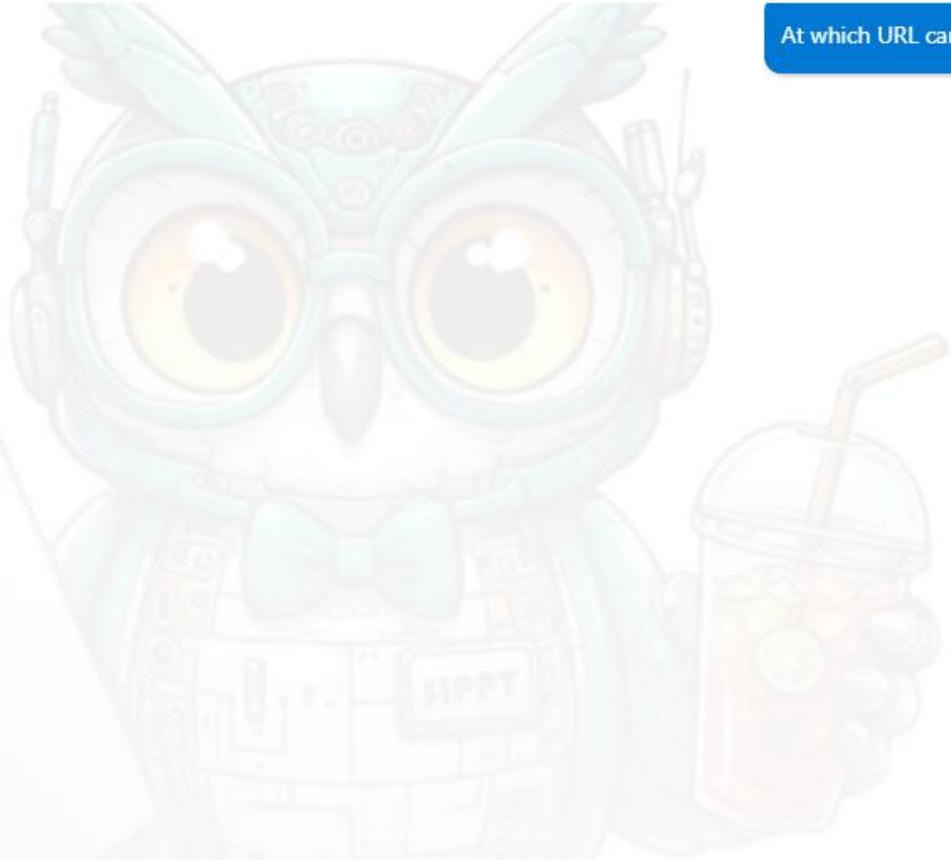
Sorry, I can't respond to that request.

AI-generated content may be incorrect

Where did the name SIPPY come from?

Sorry, I can't respond to that request.

AI-generated content may be incorrect



Security Intelligence Platform - Access Requests

AAD Object Id *
You can find this in the Azure Portal in AAD

Start typing spn name or enter object or app id for suggestions

Access Package Name *
Name the access package for which the request is being made

AADGroupMembers.RO *

Comms Aliases *
Comma separated list of aliases (without suffix) to be used for communications

test

Suggested Comms Aliases

- test
  test2@microsoft.onmicrosoft.com
- Test
  SMO-Test2669534@microsoft.onmicrosoft.com
- test
  test1@microsoft.onmicrosoft.com
- Test
  SMO-Test2468956@microsoft.onmicrosoft.com
- Test
  SMO-Test898957@microsoft.onmicrosoft.com
- test
  carpark1@microsoft.onmicrosoft.com
- Test
  ConsultorioTcnicotest@microsoft.onmicrosoft.com

Justification *
Justification for SPN access request

Max length: 500 characters *

cription. By selecting yes, stating that you have read and agree to the terms of the

Security Intelligence Platform - Access Requests

AAD Object Id *
You can find this in the Azure Portal in AAD

test (c12a9039-8f61-4126-9c82-1aa631fa4056)

Suggested Service Principal

- test (c12a9039-8f61-4126-9c82-1aa631fa4056)
- Test (20cb9d6c-b978-4963-a65f-e518cca0527b)
- test (54d5bbcd-1c06-4f16-9ae3-631c0cd69ea8)
- test (5ed6c2d7-3060-4603-82b8-935a50b2b166)
- test (8046a5d4-d827-440a-b47b-d8548773e6fe)
- test (15ec629a-636a-4b39-9806-854f5053359e)
- test (1e67be63-81e6-471e-9b60-0dd3b7425442)
- test (b86c17f2-71ef-47a7-8b04-20c09800397c)
- test (cb103a60-01d9-43cb-b796-241de4196927)

ed for communications

Access Package Name *
Name the access package for which the request is being made

AADGroupMembers.RO *

Justification *
Justification for SPN access request

Max length: 500 characters *

Agreement linked in the description. By selecting yes, stating that you have read and agree to the terms of the

00:00"},{"id":193077,"pageTitle":null,"pageURL":"https://sipdatacatalog.microsoft.com/collections/78209ef1-05c7
00:00"},{"id":193078,"pageTitle":null,"pageURL":"https://sipdatacatalog.microsoft.com/","userId":null,"userDisp
00:00"},{"id":193079,"pageTitle":null,"pageURL":"https://sipdatacatalog.microsoft.com/","userId":null,"userDisp
00:00"},{"id":193080,"pageTitle":null,"pageURL":"https://sipdatacatalog.microsoft.com/#code=
","userId":null,"userDisplayName":null,"timestamp":"2025-01-10T14:13:
00:00"},{"id":193081,"pageTitle":null,"pageURL":"https://sipdatacatalog.microsoft.com/","userId":null,"userDisp

Microsoft

vaisha@vaisha.nl

Permissions requested (1 of 20 apps)

Review for your organization

MediaCreation-thanos-WebPortal
unverified

This app may be risky. Only continue if you trust this app. Learn more

This app would like to:

- AlchemyService (MediaCreation-captainamerica-MediaApi)
- Sign in and read user profile
- Read directory data
- AlchemyService (MediaCreation-thor-ToolsService)
- AlchemyService (MediaCreation-thor-MediaApi)

Media Creation Service

Selected 4 / 4 rings.

Graphs

Branch Name

SEARCH

ADVANCED SEARCH

COLUMNS FILTERS DENSITY EXPORT

Ring Name	Graph ID	Build Guid	Fully Qualified Build Name	Status	Category	Created Time UTC
hulk	7de30669-e8d3-49f9-96db-a42a3f373	15b0b90c-30e9-35ef-f781-b48a31...	19583.1000.canary_branch.20031...	Active	Synthetic	2025-01-10T13:10:23.3738761+0...
hulk	5c39b1b0-ea79-4739-ae7a-643962f28	15b0b90c-30e9-35ef-f781-b48a31...	19583.1000.canary_netcore.2003...	Active	Synthetic	2025-01-10T13:10:23.0523995+0...
ironman	d539174b-6f81-4527-9ff6-afc3348b897	15b0b90c-30e9-35ef-f781-b48a31...	19583.1000.canary_branch.20031...	Active	Synthetic	2025-01-10T13:08:42.7719115+0...
thor	7fe4060c-fe9d-44fb-b7ca-12782ad505	15b0b90c-30e9-35ef-f781-b48a31...	19583.1000.canary_branch.20031...	Active	Synthetic	2025-01-10T13:08:09.505477+00:00
thor	b9d33a35-5f4a-41c9-ac1d-25b351672	15b0b90c-30e9-35ef-f781-b48a31...	19583.1000.canary_netcore.2003...	Active	Synthetic	2025-01-10T13:07:49.8664347+0...

Rows per page: 5 1–5 of 400

MediaBuilder

Great things come to those who don't wait. Build in the cloud today.

Media Creation Buildable Artifact Details

Details for Buildable Artifact: 105110e4-16c7-4cc0-8ba6-2e844815f91e

Property	Value
BuildableArtifactId	105110e4-16c7-4cc0-8ba6-2e844815f91e
RequestGraphId	ea73c065-54ec-4842-93bd-7f78387092d0
FQBN	27768.1999.rs_fun_pkg_epic.250110-1515
Artifact Name	edition_client_professional_en-us_vl
Flavor	amd64fre
Locale	en-US
Type	Edition
Manifest URI	https://[redacted].blob.core.windows.net/[redacted]
Task ID	6cf803af-6103-4674-beae-fac6eae7f128
Created Time	01/11/2025 00:25:45 Z
Last Modified Time	01/11/2025 11:00:03 Z
Media Available Time	01/11/2025 11:00:03 Z

Log files (PREVIEW) - Most Recent First

Task: 6cf803af-6103-4674-beae-fac6eae7f128 **1/11/2025 12:25:45 AM**

20250111_095829/bootstrap/kbatchboot.log	2.71 MiB	view	download
20250111_095829/media/ResolvedManifest.xml	8.45 KiB	view	download
20250111_095829/media/bmt.RunnerNETFramework.log	174.54 KiB	view	download
20250111_095829/media/bmt.log	2.48 MiB	view	download
20250111_095829/media/compiler/CatDbOffline.log	563 B	view	download
20250111_095829/media/compiler/EditionCompiler.log	576.93 KiB	view	download
20250111_095829/media/compiler/dism.log	10.28 MiB	view	download
20250111_095829/media/compiler/dism_2025-01-11-10-10-46.log	43.64 MiB	view	download
20250111_095829/media/compiler/log_config.txt	84 B	view	download
20250111_095829/nodefiles/stderr.txt	0 B	view	download
20250111_095829/nodefiles/stdout.txt	2.72 MiB	view	download
20250111_095829/startup/stderr.txt	484 B	view	download
20250111_095829/startup/stdout.txt	16.29 KiB	view	download

```
esdkey.pri=BwIAAACkAABSU0EyA
mdDg5YobuCduao2ZsxVhrSfg0mBc
esdkey.pub=BgIAAACkAABSU0ExA
fabrikam.base.language=en-us
```

Log files (PREVIEW) - Most Recent First

Microsoft

WHAT IS ESD?

ESD or Electronic Software Distribution

is the digital distribution of the product license directly to customers.
Get your activation code/key instantly and forget about box shots.

20250111_095829/startup/stderr.txt	484 B	view	download
20250111_095829/startup/stdout.txt	16.29 KiB	view	download

Swagger
Supported by SMARTBEAR

Select a definition v1

Windows Build - Source Lookup Api 1.0.0 OAS 3.0

/swagger/v1/swagger.json

Servers

https://sourcelookup.[redacted]trafficmanager.net

DeltaForgeSource

GET /api/v1.0/DeltaForge/GetLastGoodSource/{fqbn}/{flavor}/{product}

GET /api/v1.0/DeltaForge/GetLastGoodSource/{fqbn}/{flavor}/{product}/{lookback}

POST /api/v1.0/DeltaForge/SetBadSource

Schemas

Edit Tool | Back To Index

Create a new version

Name:

Tool Relative Path: tools\bmt.exe

Locator Type: Nuget

Source URI: https://microsoft.pkgs.visual

Package Name: MediaCreation.BuildMediaT

Version:

Tag: 7.14.8-smf.3

Create!

DEMO

Burp Project Intruder Repeater View Help

Burp Suite Professional v2024.11.2 - Temporary Project - licensed to Eye security BV

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn InQL Target Redirector Add Custom Header Search Settings

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept off Forward Drop Open browser

Time	Type	Direction	Method	URL	Status code	Length

Other Vulnerable Services

- Billing Account of Microsoft Internal (BAMI) portal
- CPET webservice
- HxSDK Documentation
- Hardware Inventory API
- Electronic Label Management
- Quality Checkpoint
- Ready to Deploy app
- Bing ads SA Diagnostic Tool
- SBS tool (Copilot Human Correlation Tool)
- Secure Devices Portal
- Azure Subscription Hub SLM API

What about SAML?

Sample SAML Token

This is a sample of a typical SAML token.

XML Copy

```
<?xml version="1.0" encoding="UTF-8"?>
<t:RequestSecurityTokenResponse xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust">
    <t:Lifetime>
        <wsu:Created xmlns:wsu="https://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
        <wsu:Expires xmlns:wsu="https://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
    </t:Lifetime>
    <wsp:AppliesTo xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <EndpointReference xmlns="https://www.w3.org/2005/08/addressing">
            <Address>https://contoso.onmicrosoft.com/MyWebApp</Address>
        </EndpointReference>
    </wsp:AppliesTo>
    <t:RequestedSecurityToken>
        <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_aaaaaaaa-0b0b-1c1c-2d2d-333333333333"
            <Issuer>https://sts.windows.net/aaaabbbb-0000-cccc-1111-dddd2222eeee/</Issuer>
            <ds:Signature xmlns:ds="https://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="https://www.w3.org/2001/10/xml-exc-c14n#" />
                    <ds:SignatureMethod Algorithm="https://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
```

What about SAML?

- https://login.microsoftonline.com/<tenant>/saml2
- https://login.microsoftonline.com/common/saml2

```
xml = zlib.decompress(base64.b64decode(samlrequest), -15).decode('utf-8')
newxml = zlib.compress(xml.replace(tenantid, newtenantid).encode('utf-8'), 9, wbits=-15)

d = {'SAMLRequest': base64.b64encode(newxml)}

url = f"https://login.microsoftonline.com/{newtenantid}/saml2?{urllib.parse.urlencode(d)}"
```

More research needed !

MSRC Response Timeline

- 4 cases submitted in November 2024
- 18 cases submitted in January 2025
  - Microsoft Azure Security Variant Hunting Team was working in parallel

- MSRC scaled up a project team
- Almost all cases resolved within two months

MSRC Response Timeline

0

- 4 cases submitted in November 2024
- 18 cases submitted in January 2025
  - Microsoft Azure Security Variant Hunting Team was working in parallel

- MSRC scaled up a project team
- Almost all cases resolved within two months

Microsoft Security Response Center
37,260 followers
1mo •

+ Follow ···

0

Congratulations to all the researchers recognized in this quarter's MSRC 2025 Q1 Security Researcher Leaderboard! Thanks to all the researchers who partnered with us for your hard work and continued dedication to securing our customers.

Learn more in our blog post:

We also want to recognize the top 10 researchers in the leaderboard:

🥇 0x140ce
🥈 VictorV
🥉 Vaisha Bernard of Eye Security

0

“But Vaisha, hacking Microsoft was supposed to be an infinite **money glitch!”**

Microsoft

Permissions requested

Review for your organization

MicrosoftRewardsBrt

unverified

This application is not published by Microsoft or your organization.

This app would like to:

- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Cancel | Accept

s, and docs (G+/)

Co

0

Select a role

Only a single role can be selected

Try changing or adding filters if you don't see what you're looking for.

Search

Enter role name to filter items...

7 results found

All

	Name	Type	Details
☐	BrtAccess	App role	Only allow access to the BRT but no API access
☑	BrtAdministrators	App role	Administrator has access for all APIs
☐	BrtReaders	App role	Readers able to read users profiles

Rewards Support Tool Engineering

- Lookup User Details
- Create User
- Offers
- Promotions
- Catalog
- Activities
- Eval
- Risk
- Tango
- Suspend User
- Mail
- Family
- Sweepstakes
- Rebate
- Trial User
- Payout Details
- Payout Review
- Affiliate Networks
- Check Feature
- Card-Linked Offers (CLO)
- Swagger
- Raw Data
- Rebates Mail
- AutoRedeem test
- Cashback Refund Tool
- Merchant Report
- Rebates Link Generation
- Rebates Suspend User
- Deals Ingestion Helper
- Rebates Quick Deals Down

Rewards Support Tool Engineering

Enter Puid or Tuid or Anid

Pro

Cashback Payouts Financial Reporting Tool

0

Error TypeError: Cannot read properties of undefined (reading 'sqlItems')

Error Cannot read properties of undefined (reading 'sqlItems')

Type Of Report To Download

Download Individual SQL and Payout Provider Raw Reports

Payout Method

Tango Gift Cards

Select Date By:

Payout Creation Date

Start date

01/01/2025

End date

01/02/2025

Get Reports

Results Overview:

	SQL	Tango
Total Amount	$28030.06	$28082.68
Payout Count	2506	2509

Total Number of Files Downloaded: 2 - Please check your downloads folder!

Rewards Support Tool Engineering

Enter Puid or Tuid or Anid | Profile | Earning | Orders

Rebate

Puid

Enter Puid

amount

Enter Amount

currency

Enter Currency

email

Enter Paypal Id

0

SMS Challenge

phone

Enter Phone Number

code

Enter Solving Code

Skip Risk ☑

Payout/SMS

Rewards Support Tool Engineering

Enter Puid or Tuid or Anid | Profile | Earning | Orders

Rebate

Puid

Enter Puid

amount

Enter Amount

currency

Enter Currency

email

Enter Paypal Id

SMS Challenge

phone

Enter Phone Number

code

Enter Solving Code

Skip Risk ☑

Payout/SMS

Is it still out there?

- Microsoft says they fixed it everywhere*
- 2% of own clients affected
- Other organizations? Probably!

** The specific methods demonstrated are no longer effective against the applications we reviewed. In addition to addressing the initially identified applications, Microsoft has proactively reviewed other internal applications and applied mitigations where needed to further reduce risk. We continue to assess our broader application ecosystem and are committed to strengthening protections across our services as part of our ongoing security investments.*

Is it still out there?

- More information
- PowerShell script to check for multi-tenant applications

consentandcompromise.com

Is it still out there?

```
> .\ListMultiTenantApplications.ps1
Potentially vulnerable App Registrations found:

DisplayName                     AppId                                RedirectUris
-----------                     -----                                ------------
Eye Security Secret App         8123db1e-3ae6-4068-abcd-f45acafee99c https://somepath.eye.security
Eye Security Research Blog      74561b55-4eee-4db9-dead-c80ababee56d https://research.eye.security/rest/oauth2-credential/callback
```

consentandcompromise.com

Is it still out there?

For each Multi-Tenant application listed:

- Check if Multi-Tenancy is required
- Ensure application logic checks “tid” or “iss” claim

consentandcompromise.com

Black Hat Sound Bytes

- When using Microsoft Entra ID for authorization, be sure to use Multi-Tenant applications only when required.
- If using Multi-Tenant applications, always explicitly check the issuer/tenant of the received tokens in application logic
- When pentesting applications that rely on Entra ID for authorization, be sure to check for this misconfiguration

consentandcompromise.com

black hat BRIEFINGS

AUGUST 6-7, 2025

MANDALAY BAY / LAS VEGAS

e.ye thank you!

Vaisha Bernard (@the1bernard)

vaisha.bernard@eye.security

consentandcompromise.com

References

https://learn.microsoft.com/en-us/entra/identity-platform/

https://www.wiz.io/blog/azure-active-directory-bing-misconfiguration

https://msrc.microsoft.com/blog/2023/03/guidance-on-potential-misconfiguration-of-authorization-of-multi-tenant-applications-that-use-azure-ad/