JUMPSEC

Reverse Engineering a Rumour

Story behind weaponising the Intune Conditional Access Bypass
Sunny Chau - Bsides HK 2025

Agenda

Tell a cool 2 part story

Part 1 - reverse engineering

Part 2 - making friends

And not delay lunch for everyone too much ;)

$whoami

Consultant @ JUMPSEC Adv Sim , joined 2022

Loves all things cloud

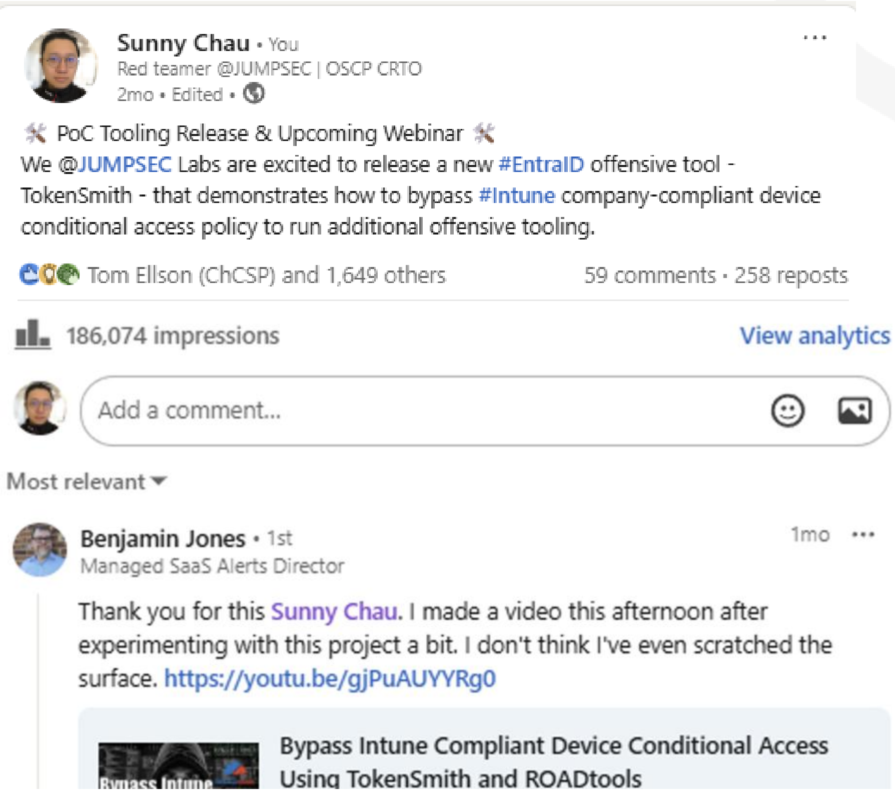
Loves math rock

@gladstomych

sunnyc@jumpsec.com

JUMPSEC

Let's set the stage



Sunny Chau • You
Red teamer @JUMPSEC | OSCP CRTO
2mo • Edited •

🛠 PoC Tooling Release & Upcoming Webinar 🛠
We @JUMPSEC Labs are excited to release a new #EntraID offensive tool - TokenSmith - that demonstrates how to bypass #Intune company-compliant device conditional access policy to run additional offensive tooling.

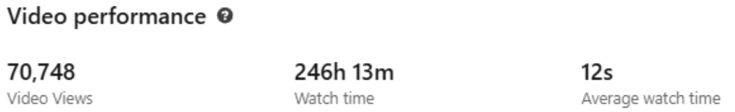
Tom Ellson (ChCSP) and 1,649 others · 59 comments · 258 reposts

186,074 impressions · View analytics

Benjamin Jones • 1st · 1mo
Managed SaaS Alerts Director

Thank you for this Sunny Chau. I made a video this afternoon after experimenting with this project a bit. I don't think I've even scratched the surface. https://youtu.be/gjPuAUYYRg0

Bypass Intune Compliant Device Conditional Access Using TokenSmith and ROADtools



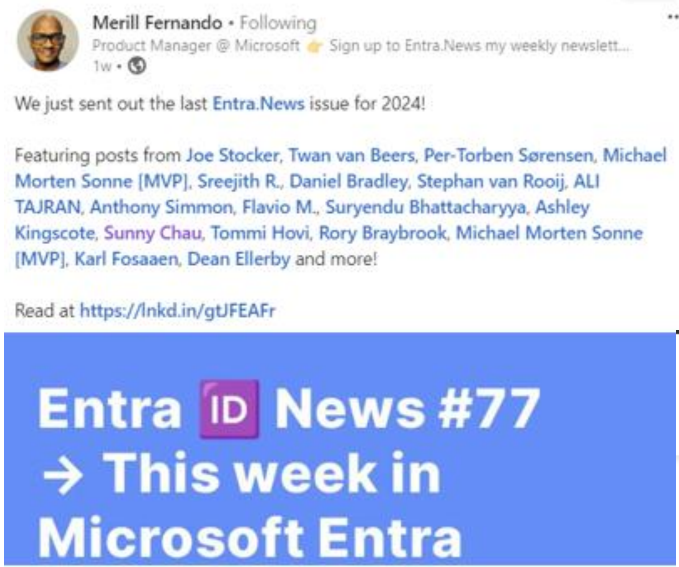
Video performance

70,748	246h 13m	12s
Video Views	Watch time	Average watch time

(post drop – 27th Dec)

(which was day after Boxing day ....)

Community reaction?

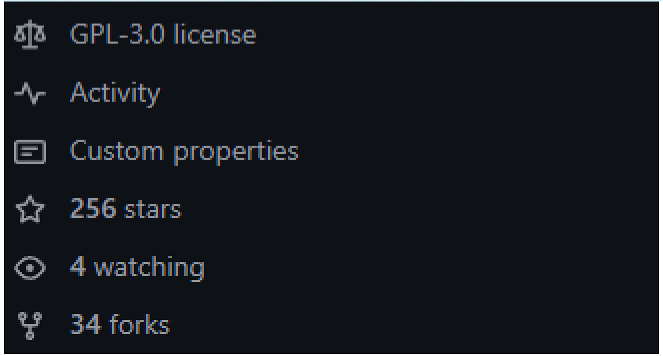


Merill Fernando • Following
Product Manager @ Microsoft 👉 Sign up to Entra.News my weekly newslett...
1w •

We just sent out the last Entra.News issue for 2024!

Featuring posts from Joe Stocker, Twan van Beers, Per-Torben Sørensen, Michael Morten Sonne [MVP], Sreejith R., Daniel Bradley, Stephan van Rooij, ALI TAJRAN, Anthony Simmon, Flavio M., Suryendu Bhattacharyya, Ashley Kingscote, Sunny Chau, Tommi Hovi, Rory Braybrook, Michael Morten Sonne [MVP], Karl Fosaaen, Dean Ellerby and more!

Read at https://lnkd.in/gtJFEAFr



GPL-3.0 license

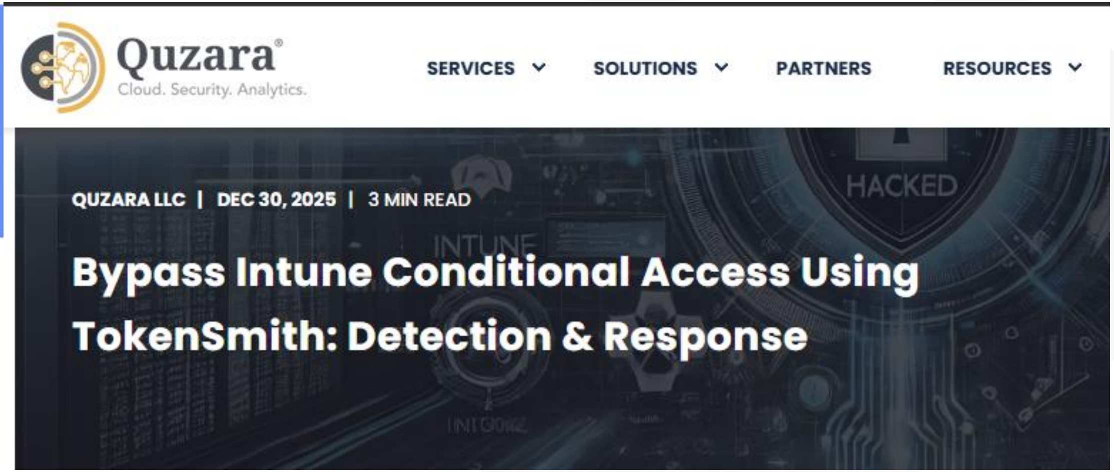
Activity

Custom properties

256 stars

4 watching

34 forks



QUZARA LLC | DEC 30, 2025 | 3 MIN READ

Bypass Intune Conditional Access Using TokenSmith: Detection & Response

Let’s rewind the clock a little bit

Timeline

11th Nov – First Rumour

…

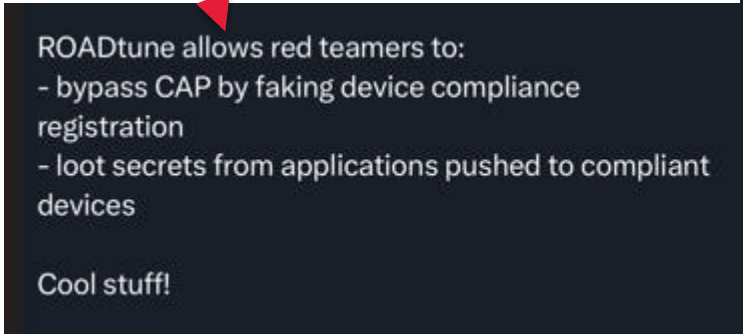
[The fun part]

…

27th Dec – Post Drop + went viral

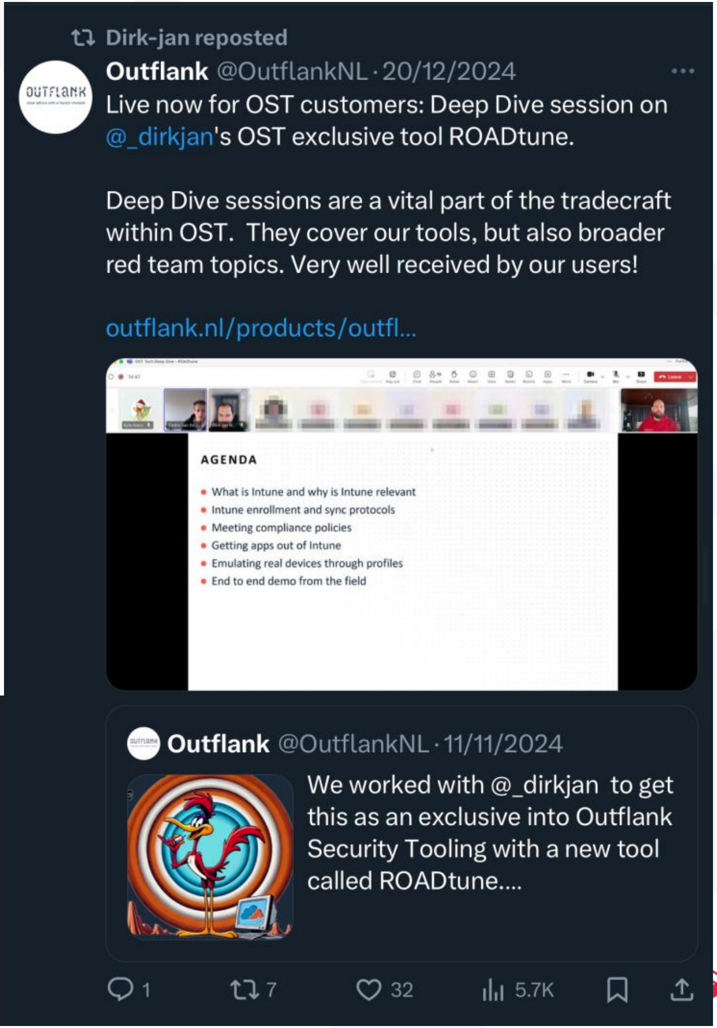
Initial rumour

11th Nov – Pay-walled bypass



ROADtune allows red teamers to:
- bypass CAP by faking device compliance registration
- loot secrets from applications pushed to compliant devices

Cool stuff!



Dirk-jan reposted

Outflank @OutflankNL · 20/12/2024

Live now for OST customers: Deep Dive session on @_dirkjan's OST exclusive tool ROADtune.

Deep Dive sessions are a vital part of the tradecraft within OST. They cover our tools, but also broader red team topics. Very well received by our users!

outflank.nl/products/outfl...

AGENDA

- What is Intune and why is Intune relevant
- Intune enrollment and sync protocols
- Meeting compliance policies
- Getting apps out of Intune
- Emulating real devices through profiles
- End to end demo from the field

Outflank @OutflankNL · 11/11/2024

We worked with @_dirkjan to get this as an exclusive into Outflank Security Tooling with a new tool called ROADtune....

What are Entra ID CAPs?

Think of CAP as this

Hole is for users

Yellow wall for bad guys

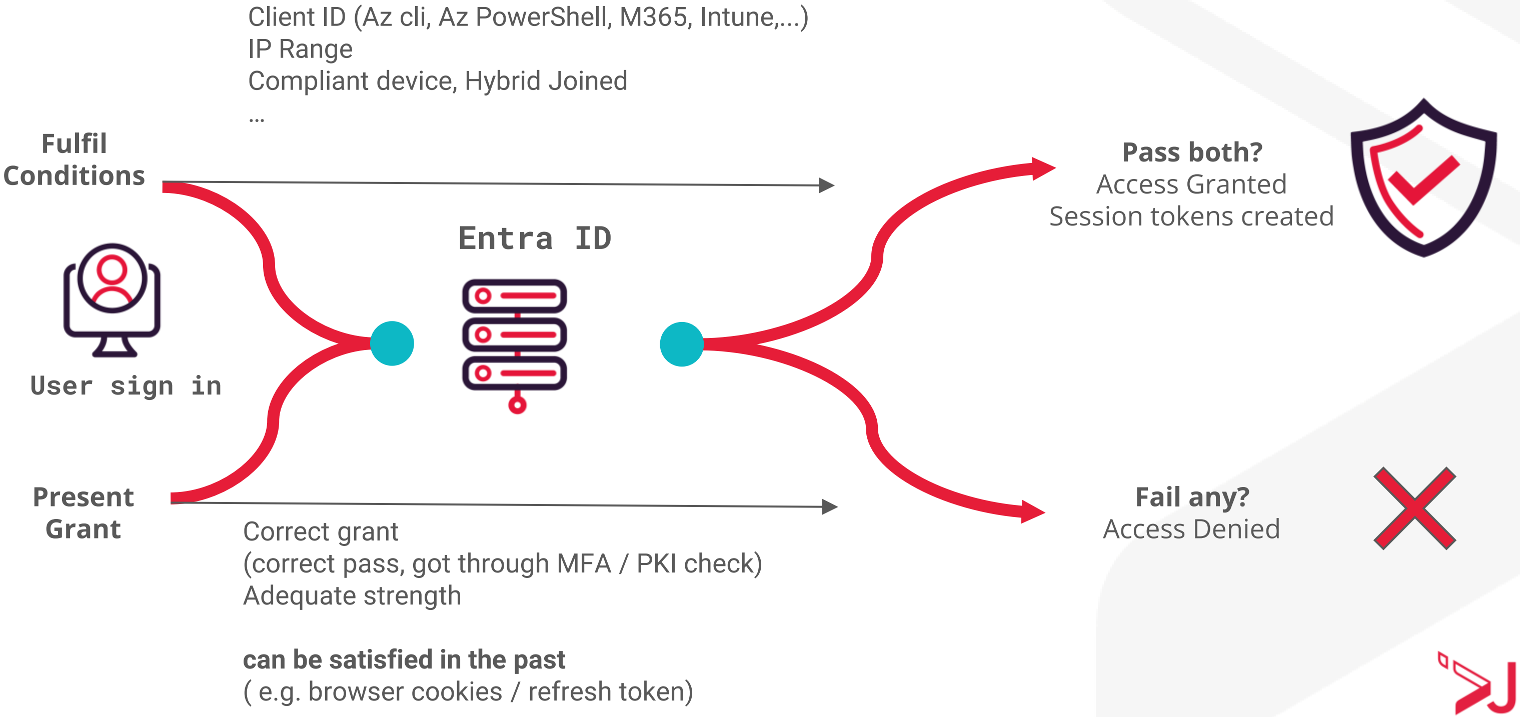
JUMPSEC

CAP gap?

The block rules (wall) has to fit exactly as a negative of the access restriction

Sometimes unexpected gaps appear in edge cases

Pictorially



Client ID (Az cli, Az PowerShell, M365, Intune,...)
IP Range
Compliant device, Hybrid Joined
…

Fulfil Conditions

User sign in

Entra ID

Present Grant

Correct grant
(correct pass, got through MFA / PKI check)
Adequate strength

can be satisfied in the past
(e.g. browser cookies / refresh token)

Pass both?
Access Granted
Session tokens created

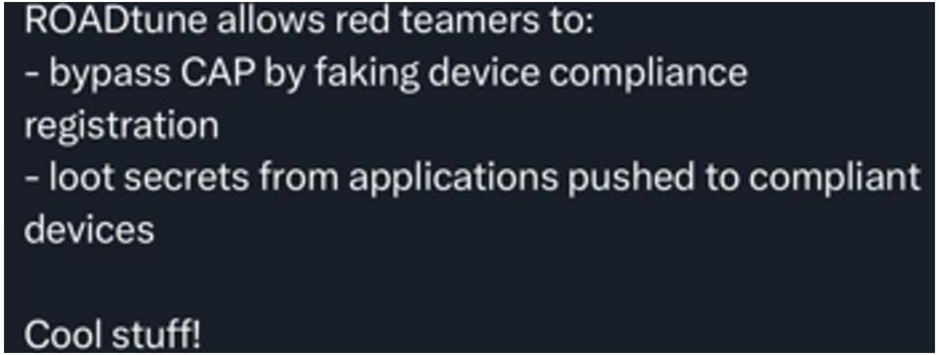
Fail any?
Access Denied

What is an enrolled device?

Starter device needs enrollment

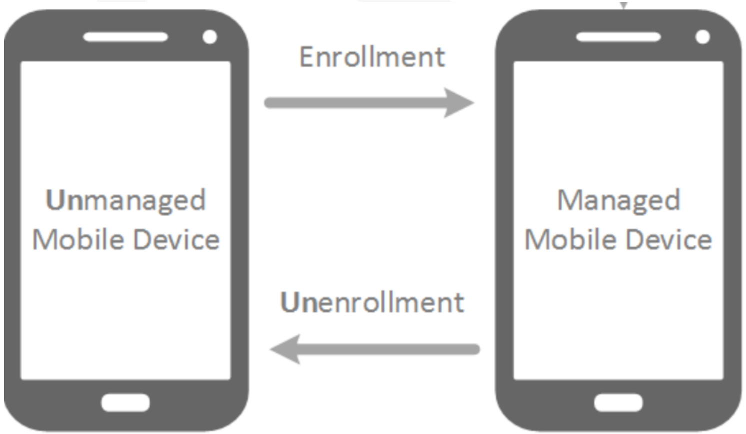
The enrollment mechanism cannot 'require' a managed device

(don't want to get into the compliant vs joined details but there are difference)



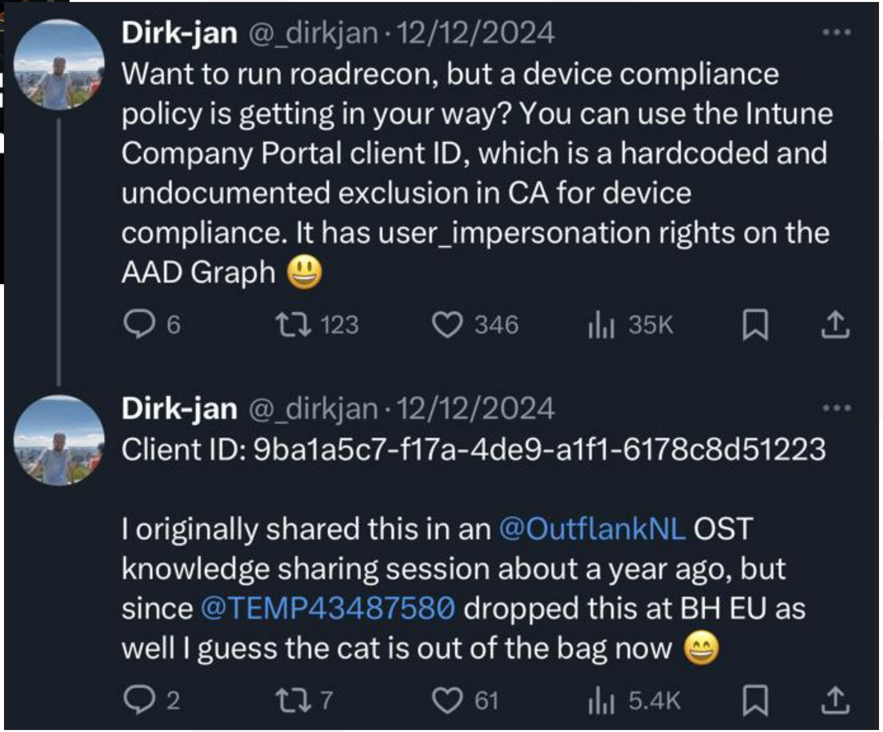
ROADtune allows red teamers to:
- bypass CAP by faking device compliance registration
- loot secrets from applications pushed to compliant devices

Cool stuff!



1 mo Later Rumour became reality

black hat
EUROPE 2024
DECEMBER 11-12, 2024
BRIEFINGS
Unveiling the Power of Intune:
Leveraging Intune for Breaking Into Your Cloud and On-Prem
Yuya Chudo



Dirk-jan @_dirkjan · 12/12/2024

Want to run roadrecon, but a device compliance policy is getting in your way? You can use the Intune Company Portal client ID, which is a hardcoded and undocumented exclusion in CA for device compliance. It has user_impersonation rights on the AAD Graph 😃

6 123 346 35K

Dirk-jan @_dirkjan · 12/12/2024

Client ID: 9ba1a5c7-f17a-4de9-a1f1-6178c8d51223

I originally shared this in an @OutflankNL OST knowledge sharing session about a year ago, but since @TEMP43487580 dropped this at BH EU as well I guess the cat is out of the bag now 😄

2 7 61 5.4K

Quick Recap

Black Hat EU 24’ - Yuya Chudo - ‘Unveiling the Power of Intune’

‘9ba1a5c7-f17a-4de9-a1f1- 6178c8d51223’ [Intune Company Portal]

- Can be used to bypass compliant & hybrid joined
- Can be used to enroll devices
- Access Token can access Graph API… (think GraphRunner or ROADtools)

At the time we didn’t know the redirect URI nor have the BH slides

How would you approach this?

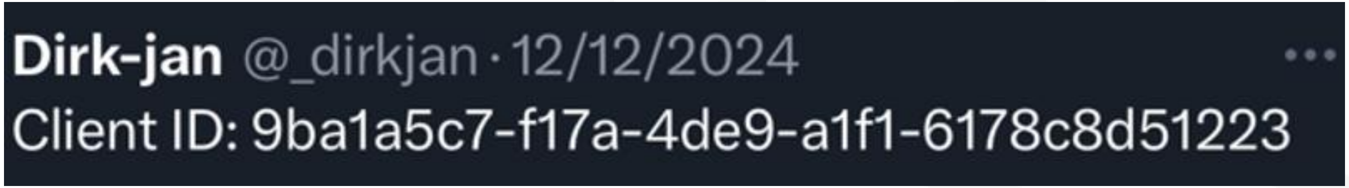
WHAT – being able to run ROADtools (& others)

HOW - Authenticate into Entra ID with compliant device CAP, without using a compliant device

The red team, using a Microsoft 0-day on the next engagement

Knowns & Unknowns

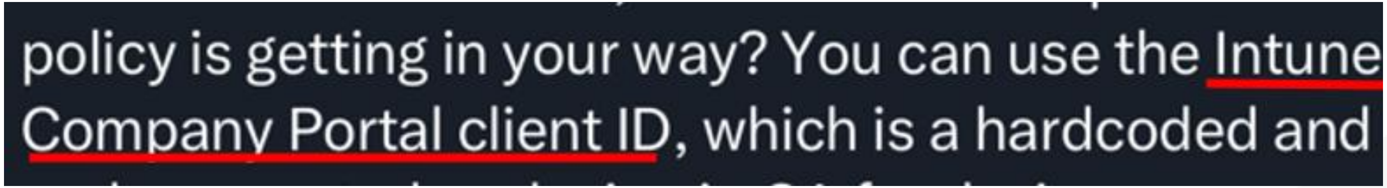
- Client ID



Dirk-jan @_dirkjan · 12/12/2024

Client ID: 9ba1a5c7-f17a-4de9-a1f1-6178c8d51223

- Client Name

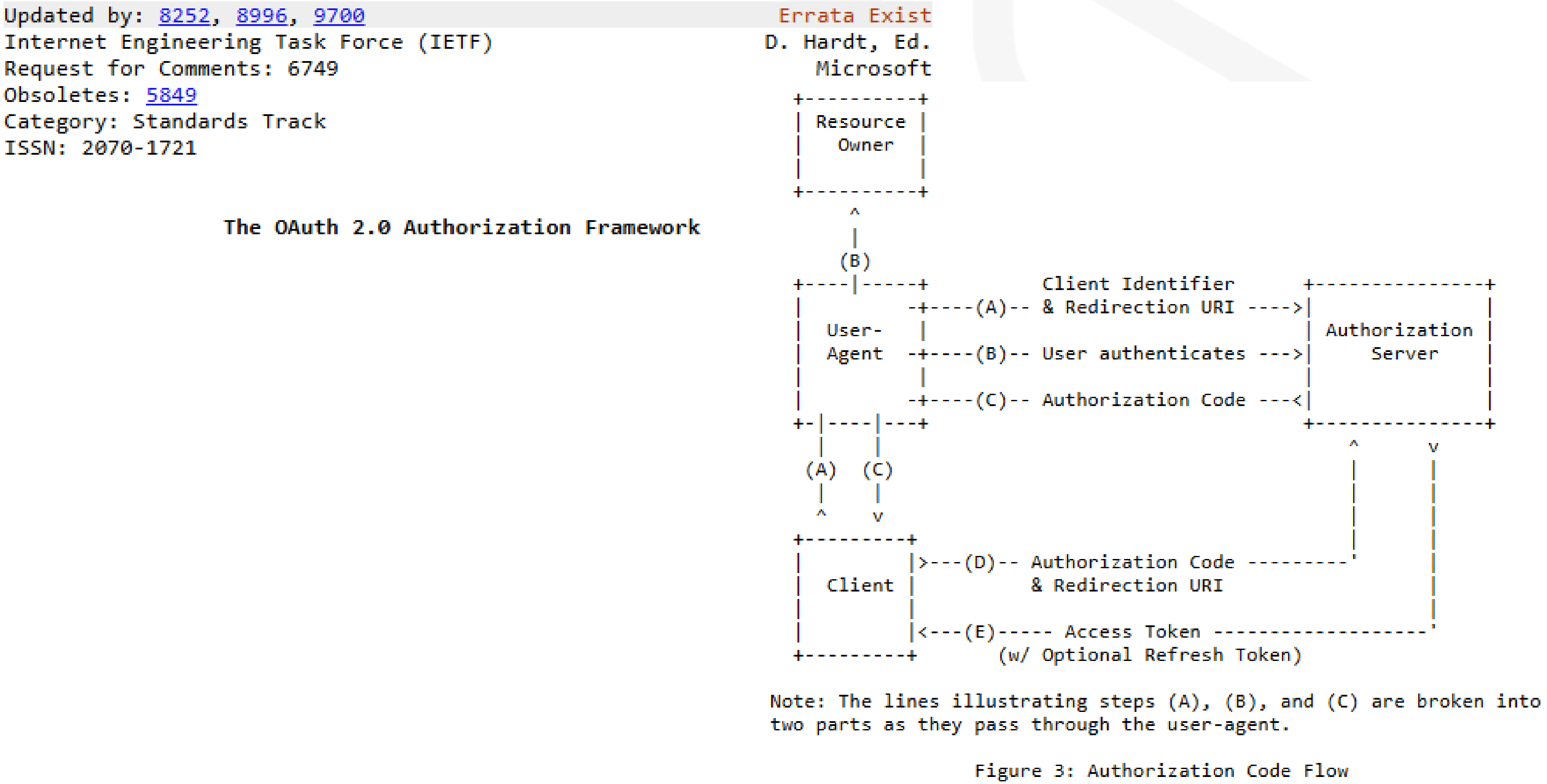


policy is getting in your way? You can use the Intune Company Portal client ID, which is a hardcoded and

How OAuth2 works in Entra

- **Grant: Authorize Code flow (code)**
- Grant: refresh_token
- Grant: Device code flow
- (some others)

OAuth2 mechanism & RTFM



Updated by: 8252, 8996, 9700 Errata Exist

Internet Engineering Task Force (IETF) D. Hardt, Ed.
Request for Comments: 6749 Microsoft
Obsoletes: 5849
Category: Standards Track
ISSN: 2070-1721

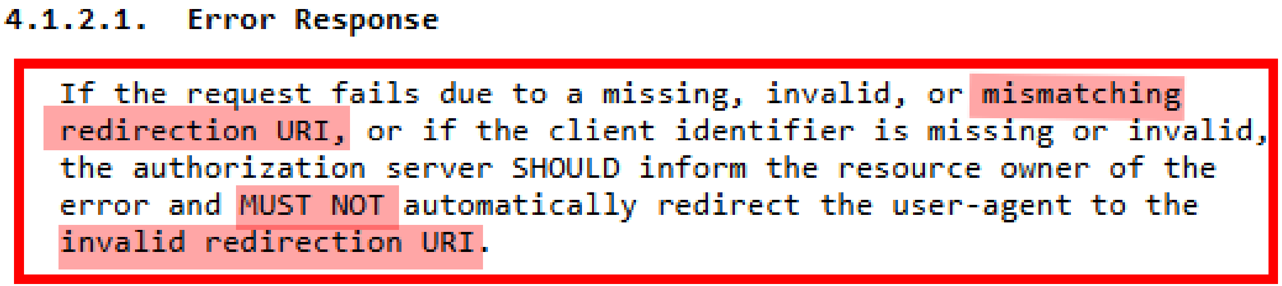
The OAuth 2.0 Authorization Framework

```
+----------+
| Resource |
|   Owner  |
|          |
+----------+
     ^
     |
    (B)
+----|-----+          Client Identifier      +---------------+
|         -+----(A)-- & Redirection URI ---->|               |
|  User-   |                                 | Authorization |
|  Agent  -+----(B)-- User authenticates --->|     Server    |
|          |                                 |               |
|         -+----(C)-- Authorization Code ---<|               |
+-|----|---+                                 +---------------+
  |    |                                         ^      v
 (A)  (C)                                        |      |
  |    |                                         |      |
  ^    v                                         |      |
+---------+                                      |      |
|         |>---(D)-- Authorization Code ---------'      |
|  Client |          & Redirection URI                  |
|         |                                             |
|         |<---(E)----- Access Token -------------------'
+---------+       (w/ Optional Refresh Token)
```

Note: The lines illustrating steps (A), (B), and (C) are broken into two parts as they pass through the user-agent.

Figure 3: Authorization Code Flow

Most Important Error Relevant to us



4.1.2.1. Error Response

If the request fails due to a missing, invalid, or mismatching redirection URI, or if the client identifier is missing or invalid, the authorization server SHOULD inform the resource owner of the error and MUST NOT automatically redirect the user-agent to the invalid redirection URI.

OAuth2 Code flow URL

https://login.microsoftonline.com/common/**oauth2/v2.0/authorize**?

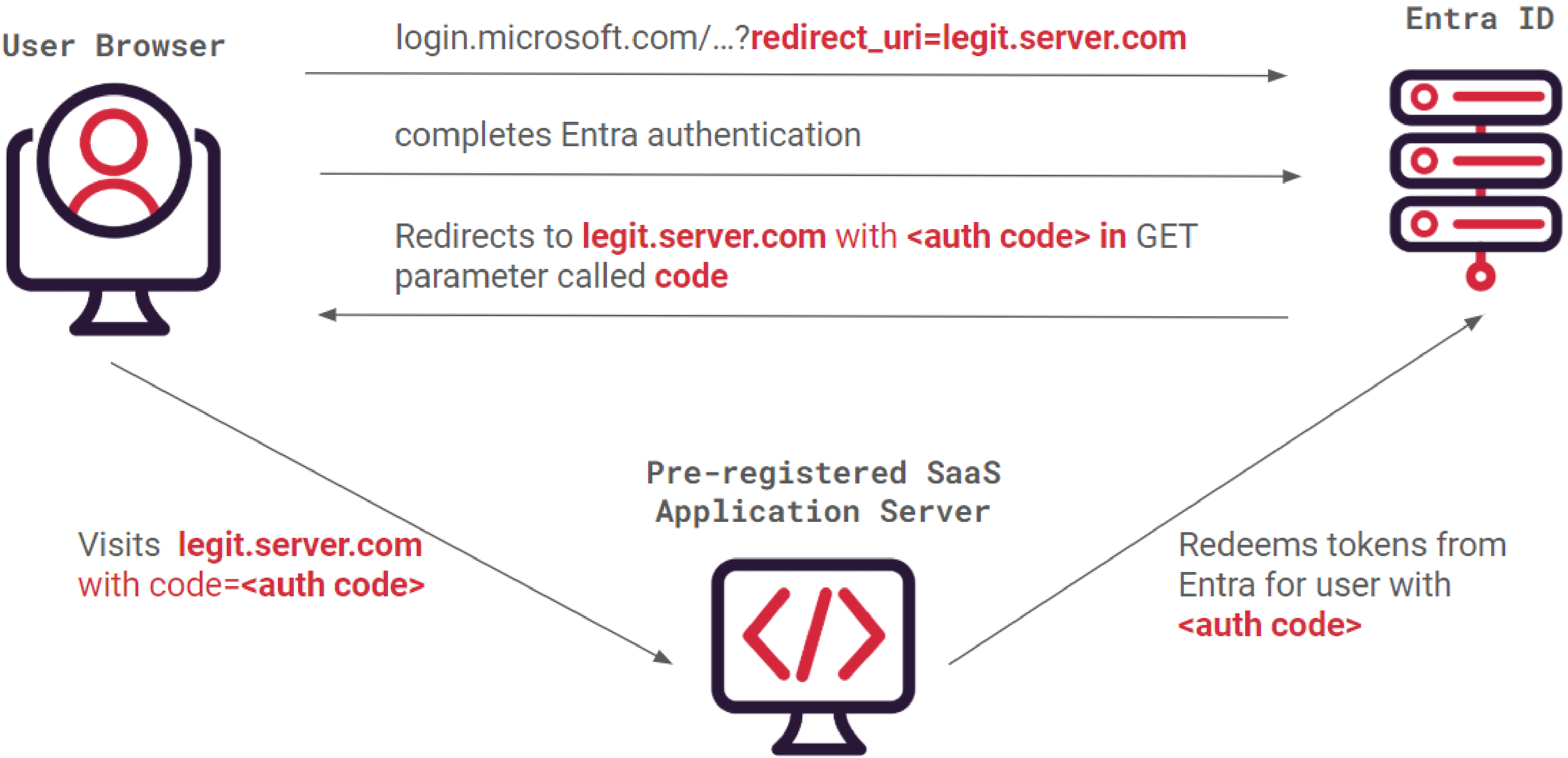
client_id=4765445b-32c6-49b0-83e6-1d93765276ca&

redirect_uri=https://www.office.com/landingv2&

response_type=code&

scope=openid%20profile%20https://www.office.com/v2/OfficeHome.All&

response_mode=form_post...



User Browser

Entra ID

login.microsoft.com/...?**redirect_uri=legit.server.com**

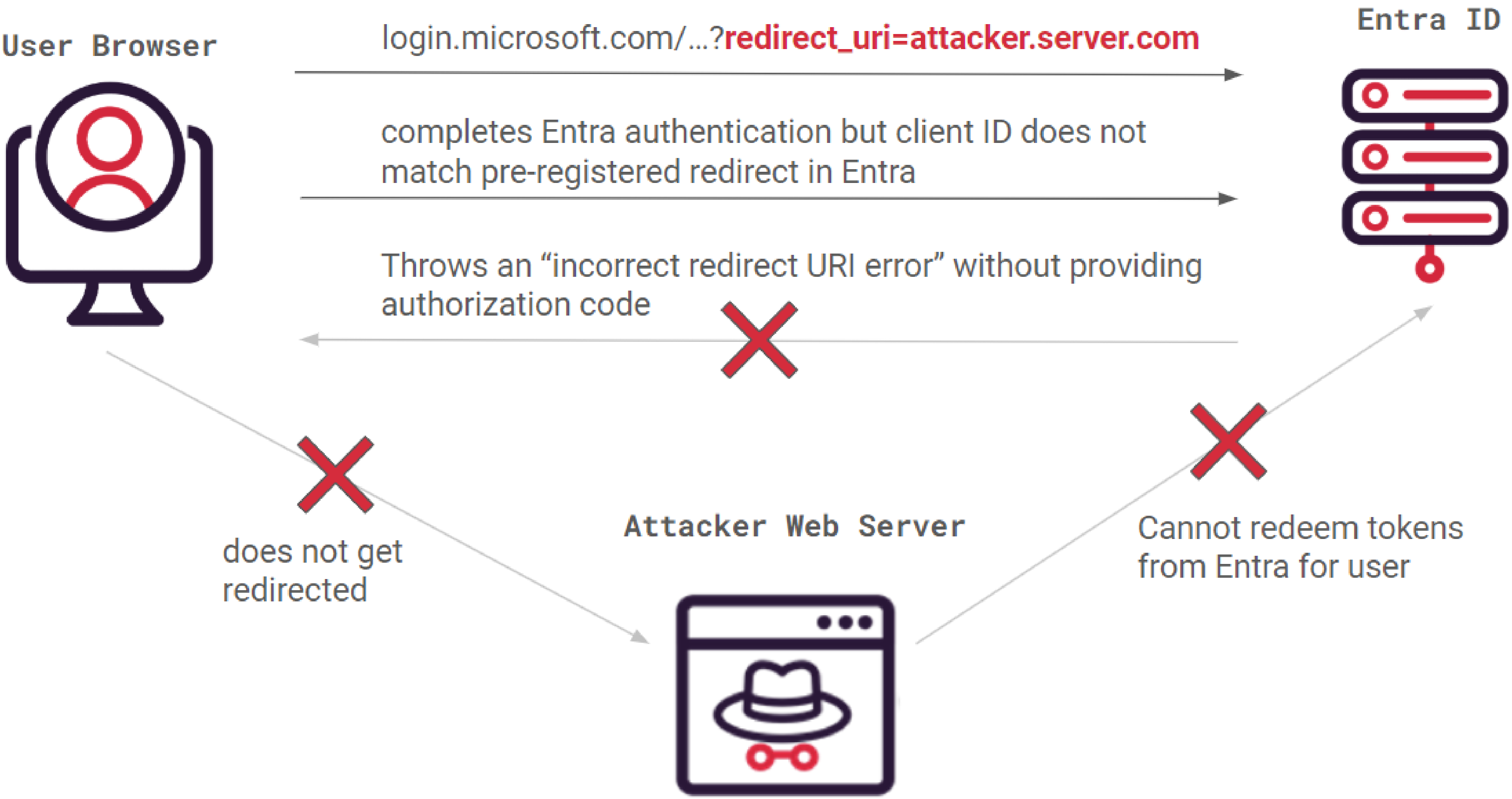
completes Entra authentication

Redirects to **legit.server.com** with **<auth code> in** GET parameter called **code**

Pre-registered SaaS Application Server

Visits **legit.server.com** with code=**<auth code>**

Redeems tokens from Entra for user with **<auth code>**



User Browser

Entra ID

login.microsoft.com/…?**redirect_uri=attacker.server.com**

completes Entra authentication but client ID does not match pre-registered redirect in Entra

Throws an “incorrect redirect URI error” without providing authorization code

does not get redirected

Attacker Web Server

Cannot redeem tokens from Entra for user

Message after RTFM

Redirect URI is not Arbitrary

Microsoft doesn’t publishes their first party App redirs

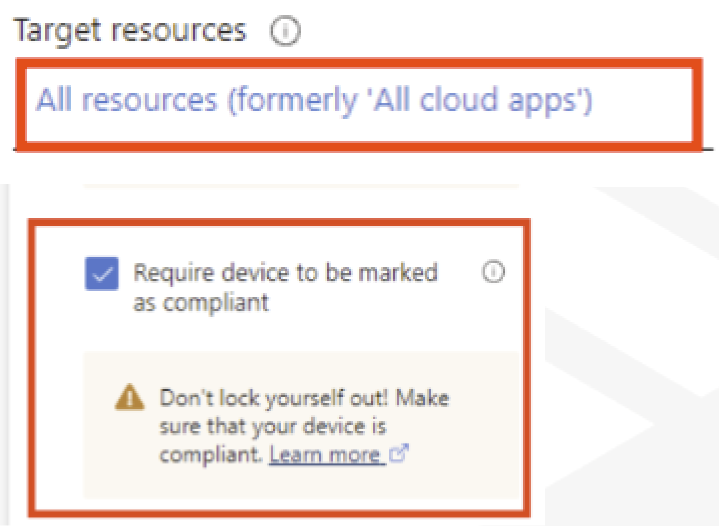
So this is probably the main thing we need to rev eng

Research Setup

Research Entra ID tenant with appropriate license

CAP rule require compliant device for all ‘Cloud Apps’

And …



Target resources

All resources (formerly 'All cloud apps')

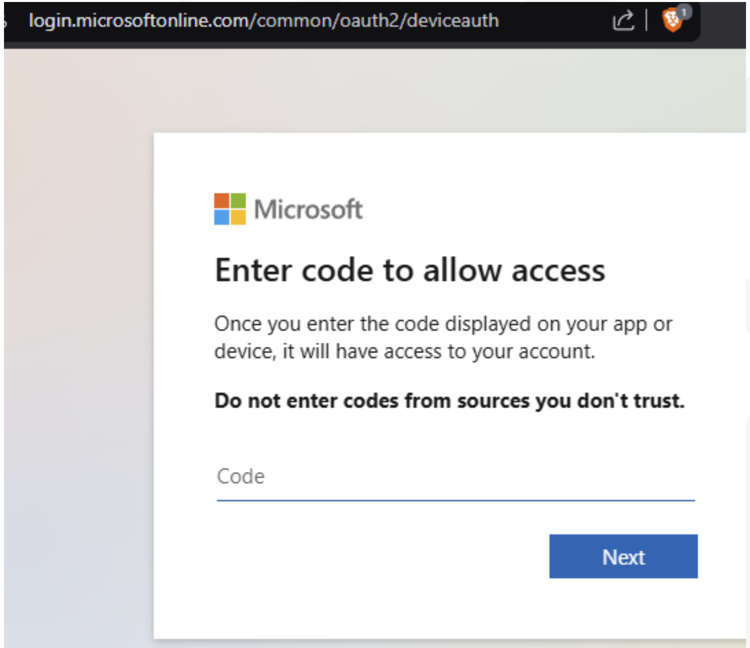
☑ Require device to be marked as compliant

⚠ Don't lock yourself out! Make sure that your device is compliant. Learn more

Approach one – device code

Because .. it has the name 'device' in it

You can specify client ID when initiating a device code sign in



login.microsoftonline.com/common/oauth2/deviceauth

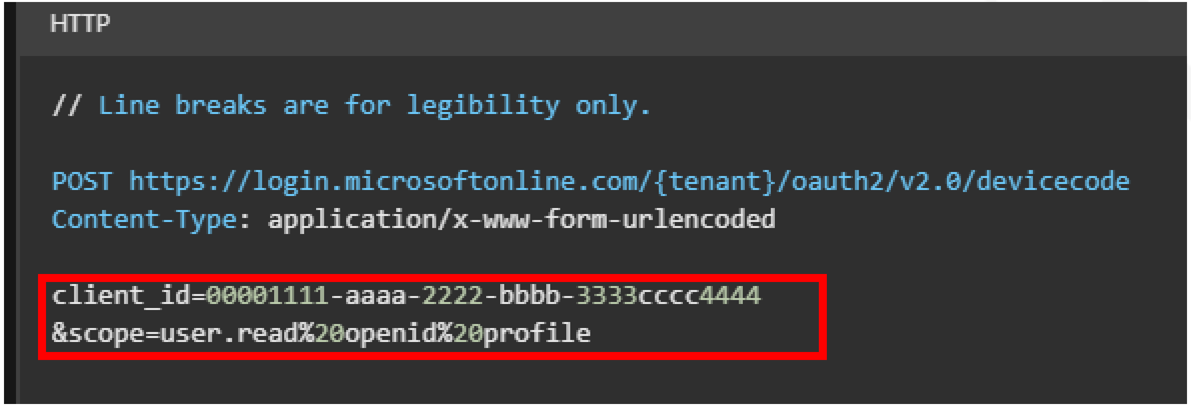
Microsoft

Enter code to allow access

Once you enter the code displayed on your app or device, it will have access to your account.

Do not enter codes from sources you don't trust.

MSDN for ref



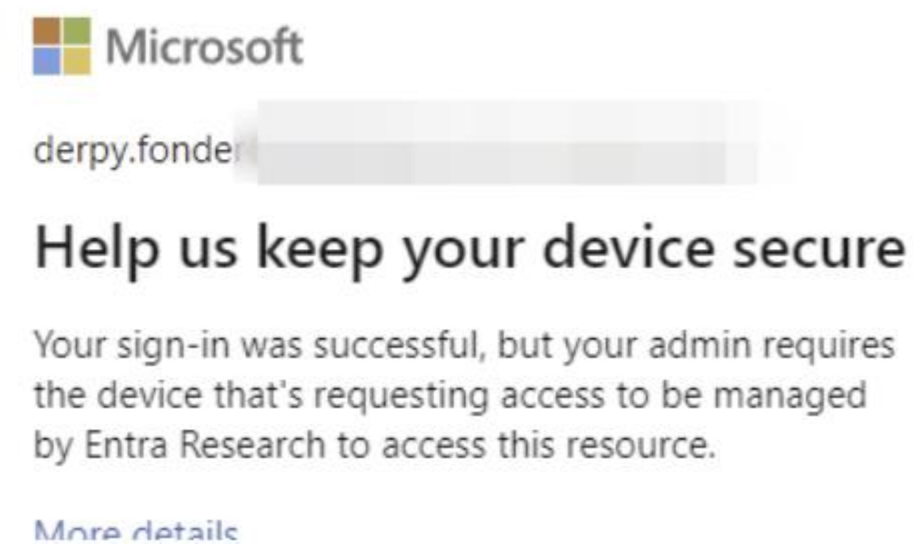
HTTP

```
// Line breaks are for legibility only.

POST https://login.microsoftonline.com/{tenant}/oauth2/v2.0/devicecode
Content-Type: application/x-www-form-urlencoded

client_id=00001111-aaaa-2222-bbbb-3333cccc4444
&scope=user.read%20openid%20profile
```

We’re blocked

Review of logs:

Did not satisfy



Microsoft

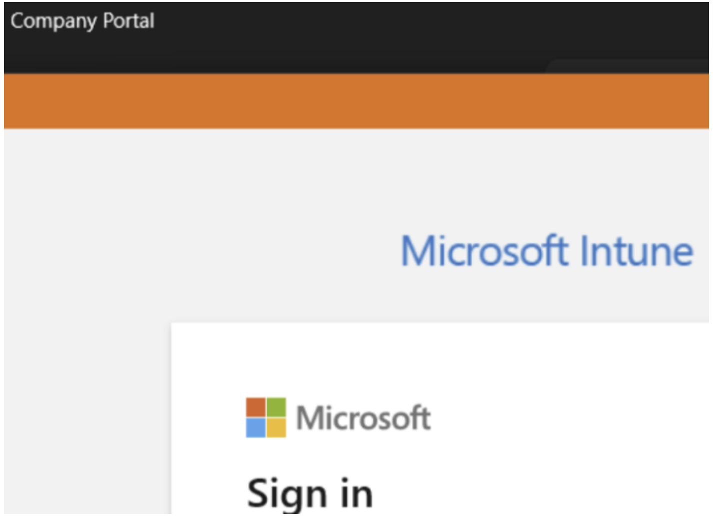
derpy.fonde[redacted]

Help us keep your device secure

Your sign-in was successful, but your admin requires the device that's requesting access to be managed by Entra Research to access this resource.

More details

Here we go, Company Portal App...

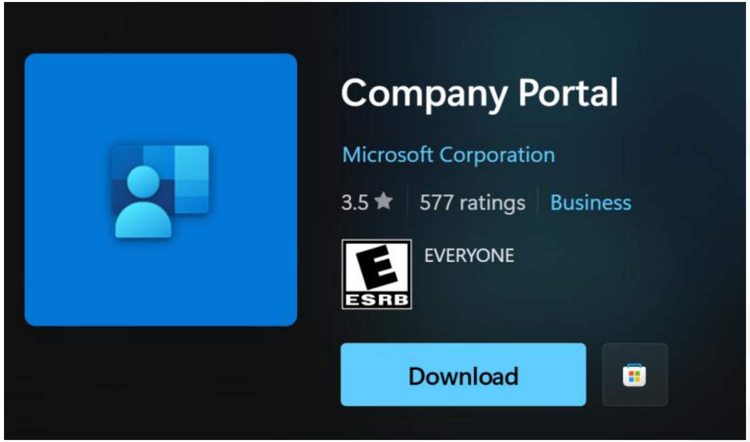


Company Portal

Microsoft Intune

Microsoft

Sign in



Company Portal

Microsoft Corporation

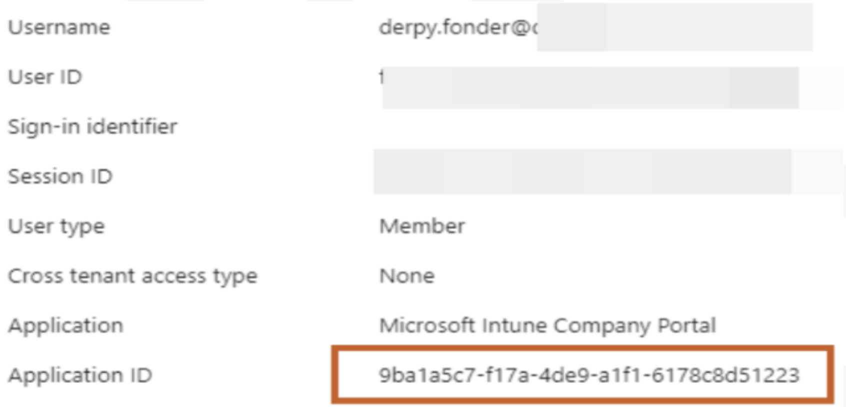
3.5 ★ | 577 ratings | Business

EVERYONE

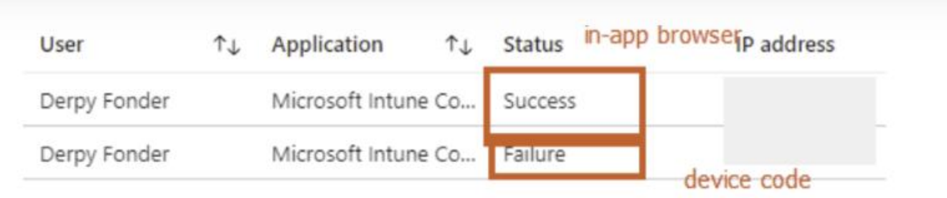
What would be your approach?

Approach 2 – Using the App as Is

- Yes we could sign in!
- Review logs
- But we didn't know how it worked



Username	derpy.fonder@[redacted]
User ID	[redacted]
Sign-in identifier	
Session ID	[redacted]
User type	Member
Cross tenant access type	None
Application	Microsoft Intune Company Portal
Application ID	9ba1a5c7-f17a-4de9-a1f1-6178c8d51223



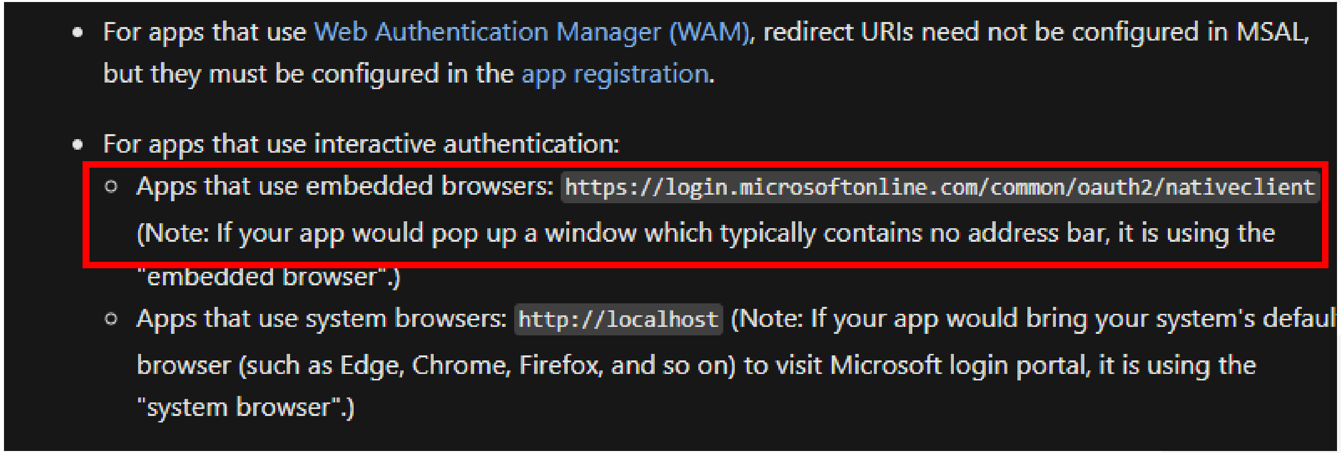
User ↑↓	Application ↑↓	Status	IP address
Derpy Fonder	Microsoft Intune Co...	Success	[redacted]
Derpy Fonder	Microsoft Intune Co...	Failure	[redacted]

in-app browser

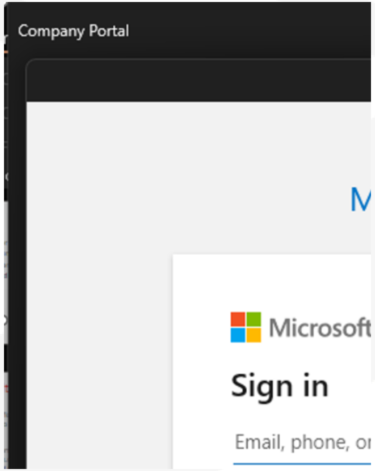
device code

Approach 3 – Trying other known Redir URIs

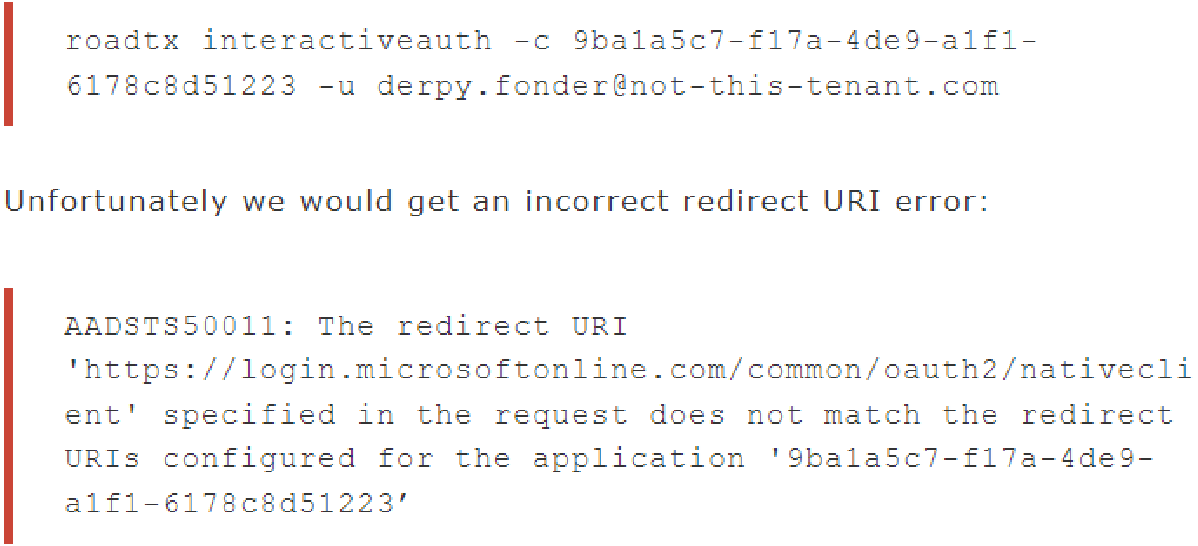
The nativeclient redir is used by Az PowerShell / Cli, Teams, …



- For apps that use Web Authentication Manager (WAM), redirect URIs need not be configured in MSAL, but they must be configured in the app registration.
- For apps that use interactive authentication:
  - Apps that use embedded browsers: `https://login.microsoftonline.com/common/oauth2/nativeclient` (Note: If your app would pop up a window which typically contains no address bar, it is using the "embedded browser".)
  - Apps that use system browsers: `http://localhost` (Note: If your app would bring your system's defaul browser (such as Edge, Chrome, Firefox, and so on) to visit Microsoft login portal, it is using the "system browser".)



Got hit by the RFC specified error



```
roadtx interactiveauth -c 9ba1a5c7-f17a-4de9-a1f1-
6178c8d51223 -u derpy.fonder@not-this-tenant.com
```

Unfortunately we would get an incorrect redirect URI error:

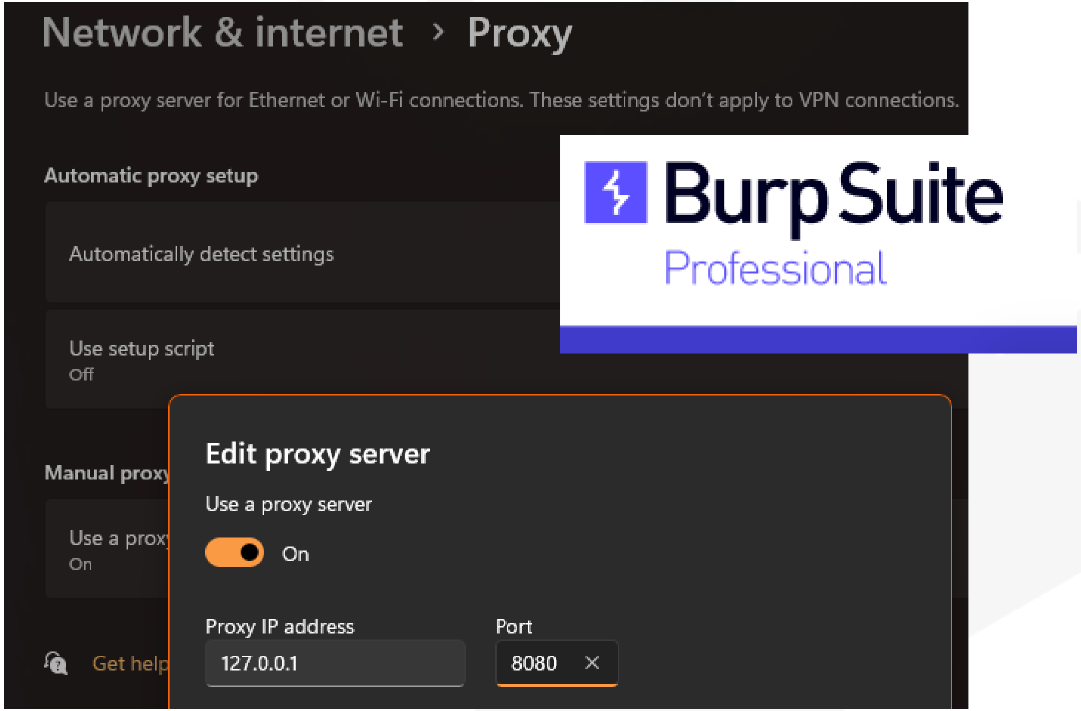
```
AADSTS50011: The redirect URI
'https://login.microsoftonline.com/common/oauth2/nativecli
ent' specified in the request does not match the redirect
URIs configured for the application '9ba1a5c7-f17a-4de9-
a1f1-6178c8d51223'
```

Approach 4 – Trying to get TLS layer HTTP proxy working

Burp suite

System proxy

CA cert



Network & internet › Proxy

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatic proxy setup

Automatically detect settings

Use setup script
Off

Manual prox

Use a prox
On

Get help

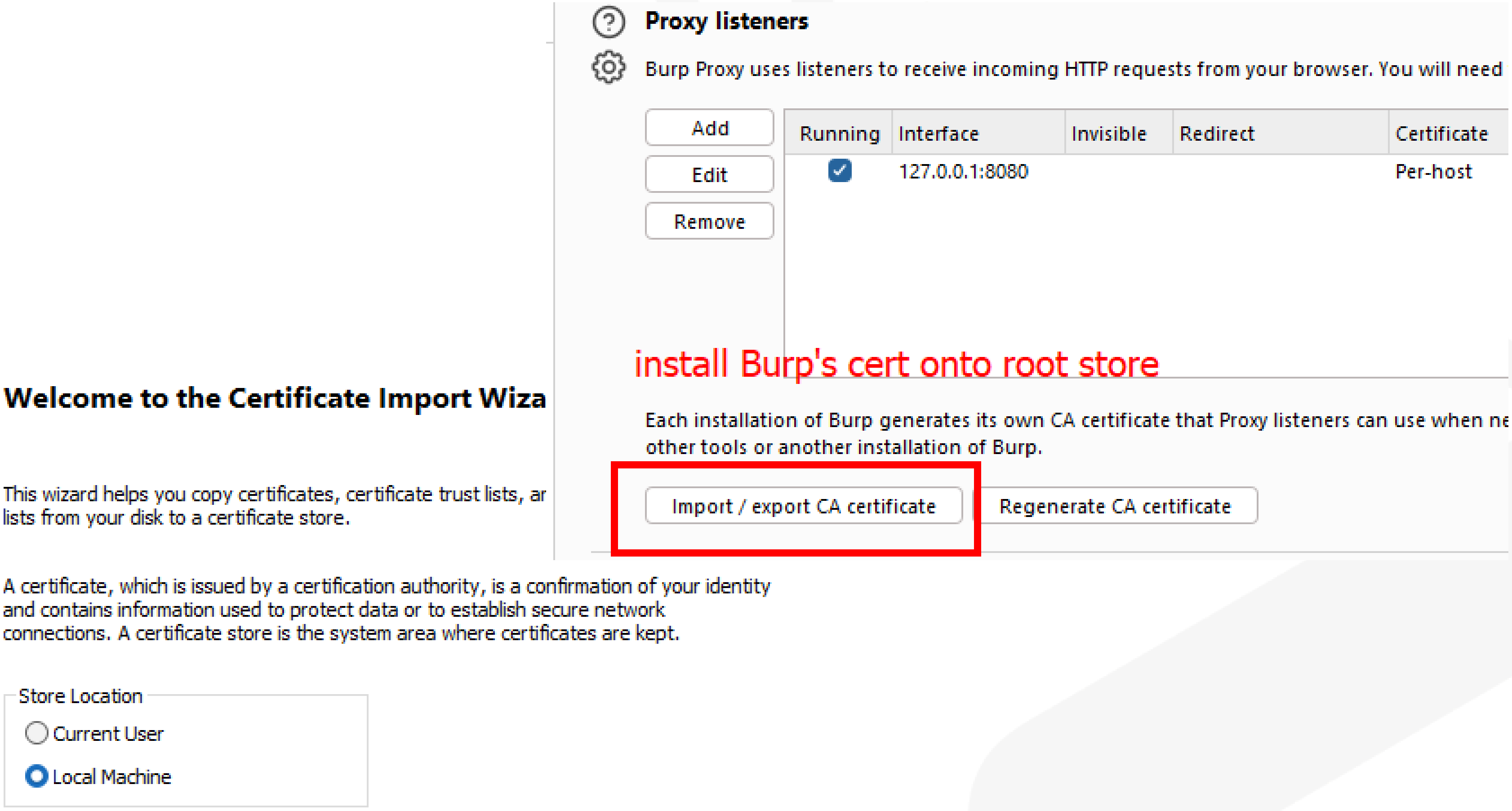
Edit proxy server

Use a proxy server

On

Proxy IP address: 127.0.0.1

Port: 8080



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

install Burp's cert onto root store

Each installation of Burp generates its own CA certificate that Proxy listeners can use when ne
other tools or another installation of Burp.

Welcome to the Certificate Import Wiza

This wizard helps you copy certificates, certificate trust lists, ar
lists from your disk to a certificate store.

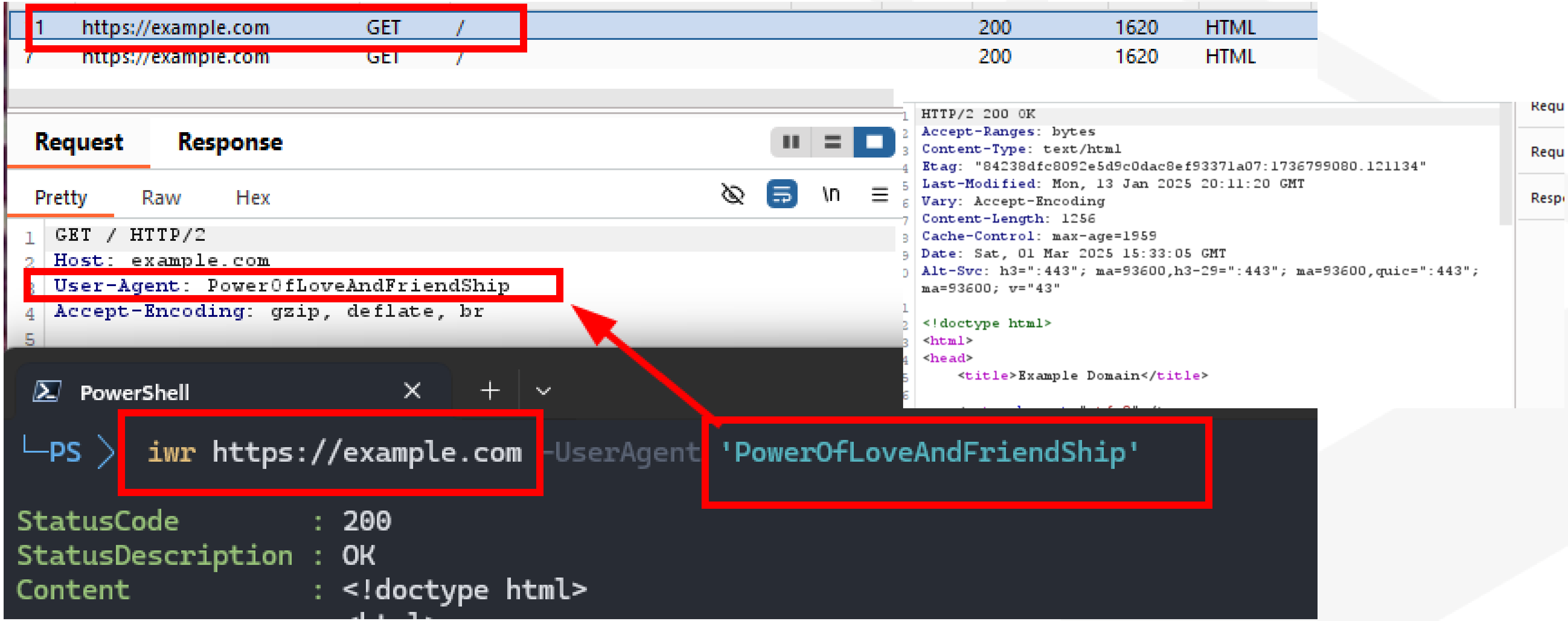
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

○ Current User

● Local Machine

Okay – System level https proxy working



```
1   https://example.com   GET   /   200   1620   HTML
7   https://example.com   GET   /   200   1620   HTML
```

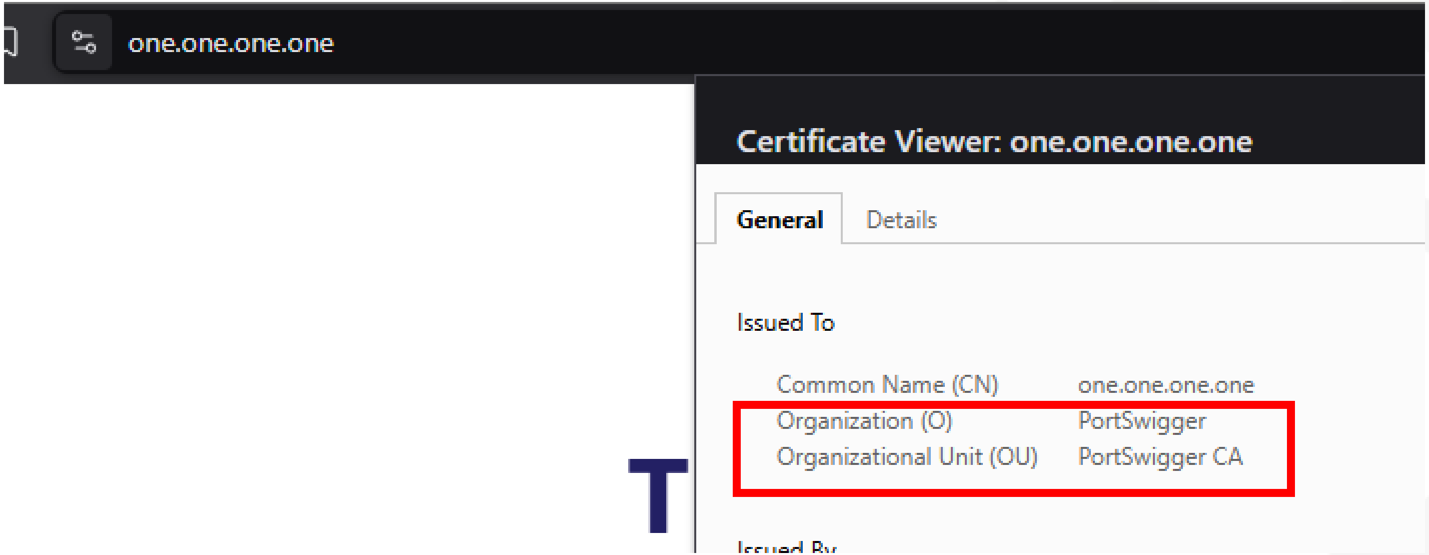
```
GET / HTTP/2
Host: example.com
User-Agent: PowerOfLoveAndFriendShip
Accept-Encoding: gzip, deflate, br
```

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: text/html
Etag: "84238dfc8092e5d9c0dac8ef93371a07:1736799080.121134"
Last-Modified: Mon, 13 Jan 2025 20:11:20 GMT
Vary: Accept-Encoding
Content-Length: 1256
Cache-Control: max-age=1959
Date: Sat, 01 Mar 2025 15:33:05 GMT
Alt-Svc: h3=":443"; ma=93600,h3-29=":443"; ma=93600,quic=":443";
ma=93600; v="43"

<!doctype html>
<html>
<head>
    <title>Example Domain</title>
```

```
└PS > iwr https://example.com -UserAgent 'PowerOfLoveAndFriendShip'

StatusCode        : 200
StatusDescription : OK
Content           : <!doctype html>
```

JUMPSEC

CA is auto switched & Trusted



one.one.one.one

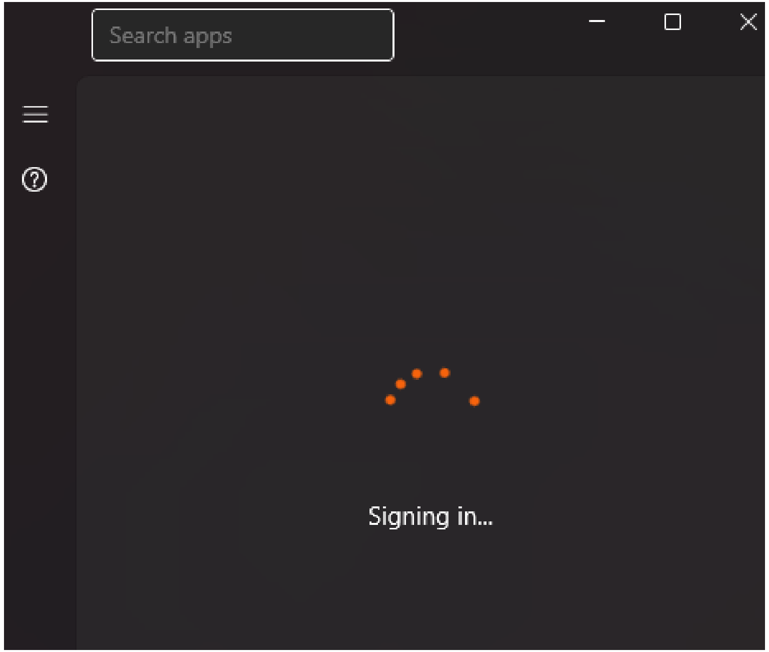
Certificate Viewer: one.one.one.one

Issued To

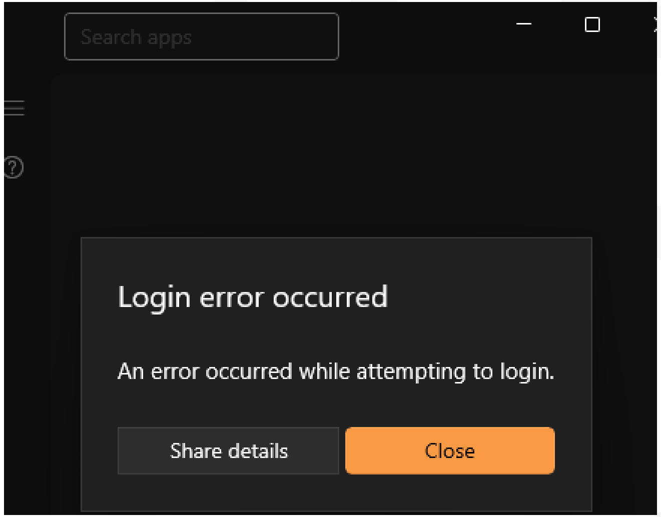
Common Name (CN)	one.one.one.one
Organization (O)	PortSwigger
Organizational Unit (OU)	PortSwigger CA

Issued By

But for what we needed … it did not work out



Signing in...



Login error occurred

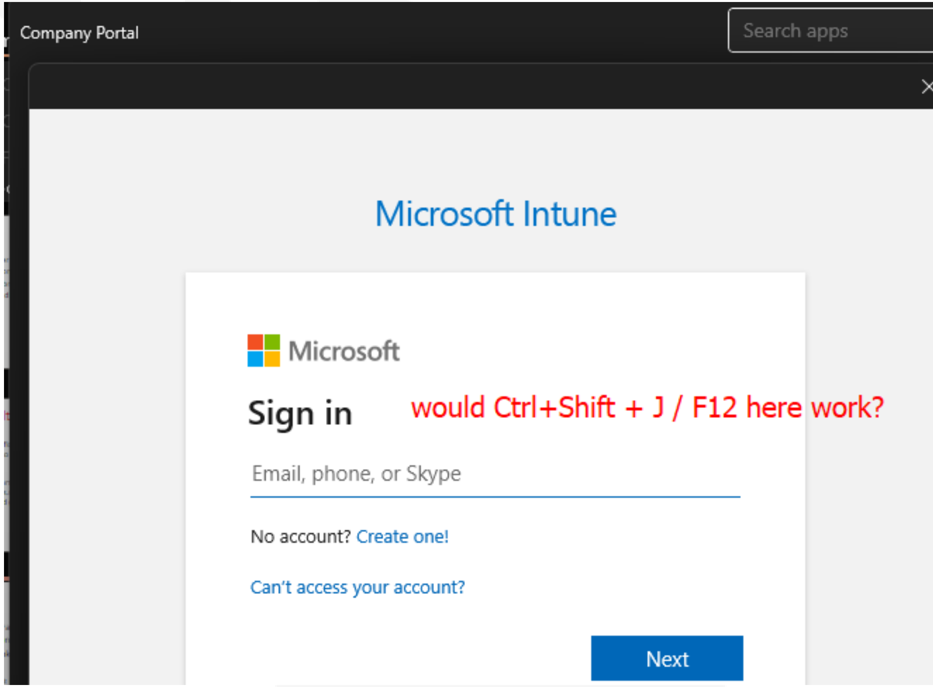
An error occurred while attempting to login.

Reason?
mTLS check?

Proxy
detection?

Approach x – Honorary Mentions

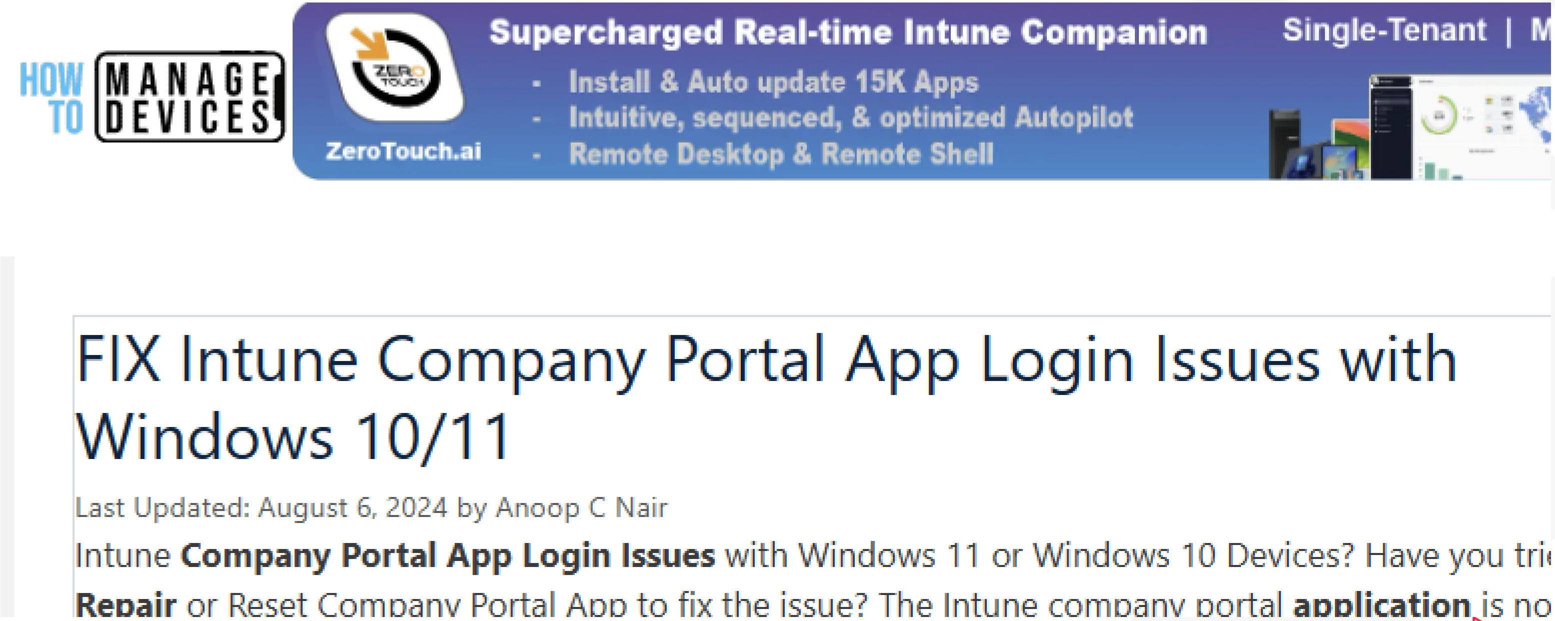
- Trying the Linux MS Company Portal Client
- Trying to start a developer console
- No logs to review lol



would Ctrl+Shift + J / F12 here work?

Google to the rescue

There must be those with enterprise SSL HTTP proxy with same issue?

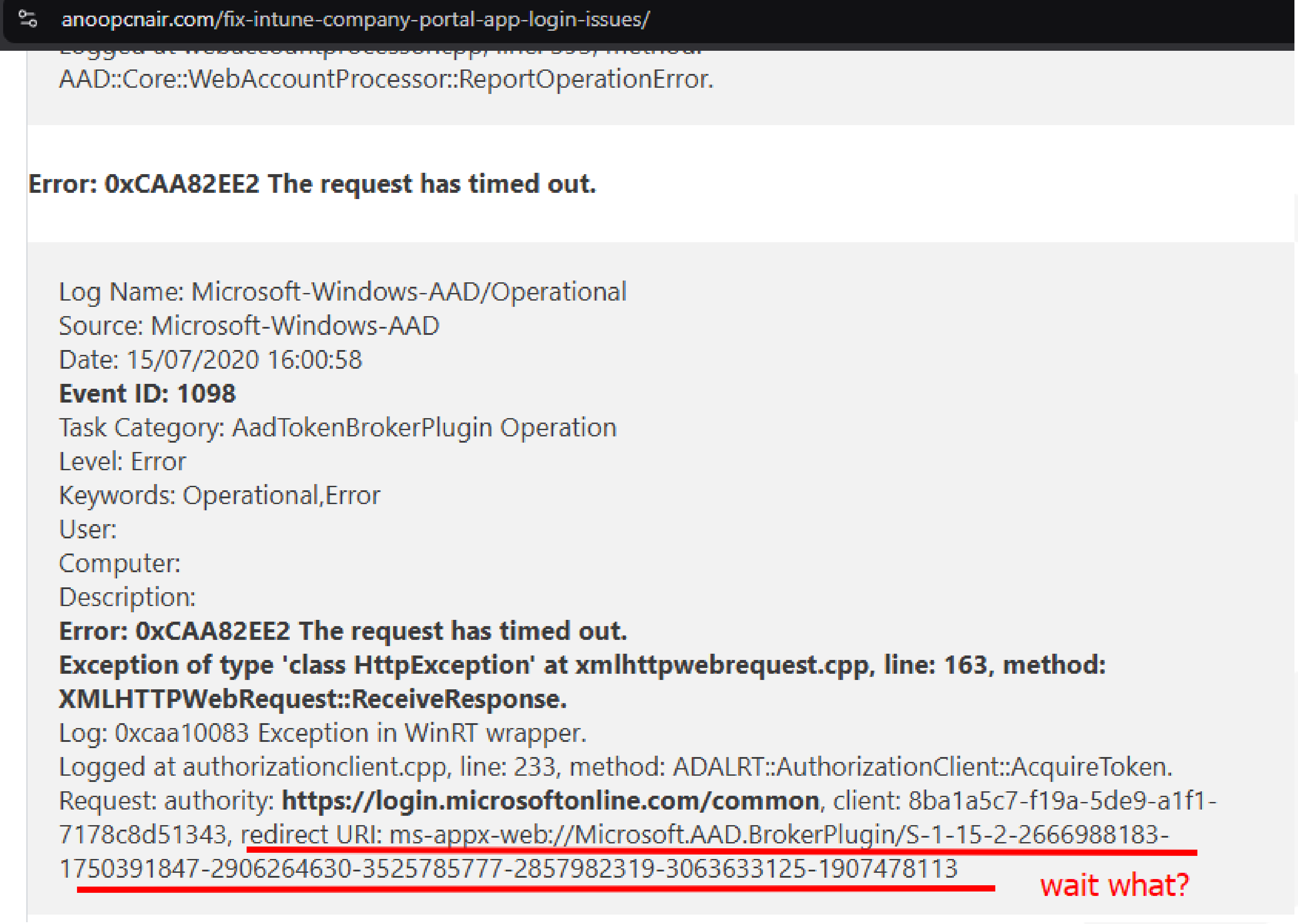


HOW TO MANAGE DEVICES

FIX Intune Company Portal App Login Issues with Windows 10/11

Last Updated: August 6, 2024 by Anoop C Nair

Intune **Company Portal App Login Issues** with Windows 11 or Windows 10 Devices? Have you tri **Repair** or Reset Company Portal App to fix the issue? The Intune company portal **application** is no



anoopcnair.com/fix-intune-company-portal-app-login-issues/

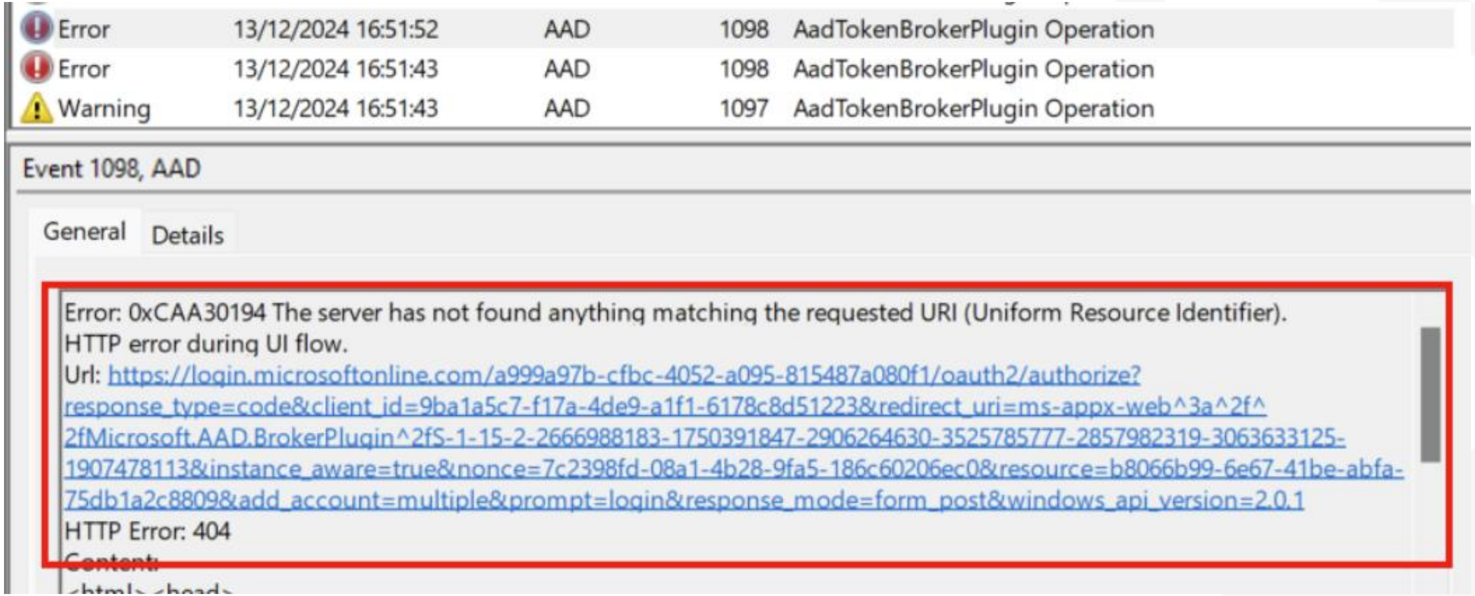
```
Logged at webaccountprocessor.cpp, line: [illegible], method:
AAD::Core::WebAccountProcessor::ReportOperationError.
```

Error: 0xCAA82EE2 The request has timed out.

```
Log Name: Microsoft-Windows-AAD/Operational
Source: Microsoft-Windows-AAD
Date: 15/07/2020 16:00:58
Event ID: 1098
Task Category: AadTokenBrokerPlugin Operation
Level: Error
Keywords: Operational,Error
User:
Computer:
Description:
Error: 0xCAA82EE2 The request has timed out.
Exception of type 'class HttpException' at xmlhttpwebrequest.cpp, line: 163, method:
XMLHTTPWebRequest::ReceiveResponse.
Log: 0xcaa10083 Exception in WinRT wrapper.
Logged at authorizationclient.cpp, line: 233, method: ADALRT::AuthorizationClient::AcquireToken.
Request: authority: https://login.microsoftonline.com/common, client: 8ba1a5c7-f19a-5de9-a1f1-
7178c8d51343, redirect URI: ms-appx-web://Microsoft.AAD.BrokerPlugin/S-1-15-2-2666988183-
1750391847-2906264630-3525785777-2857982319-3063633125-1907478113
```

wait what?

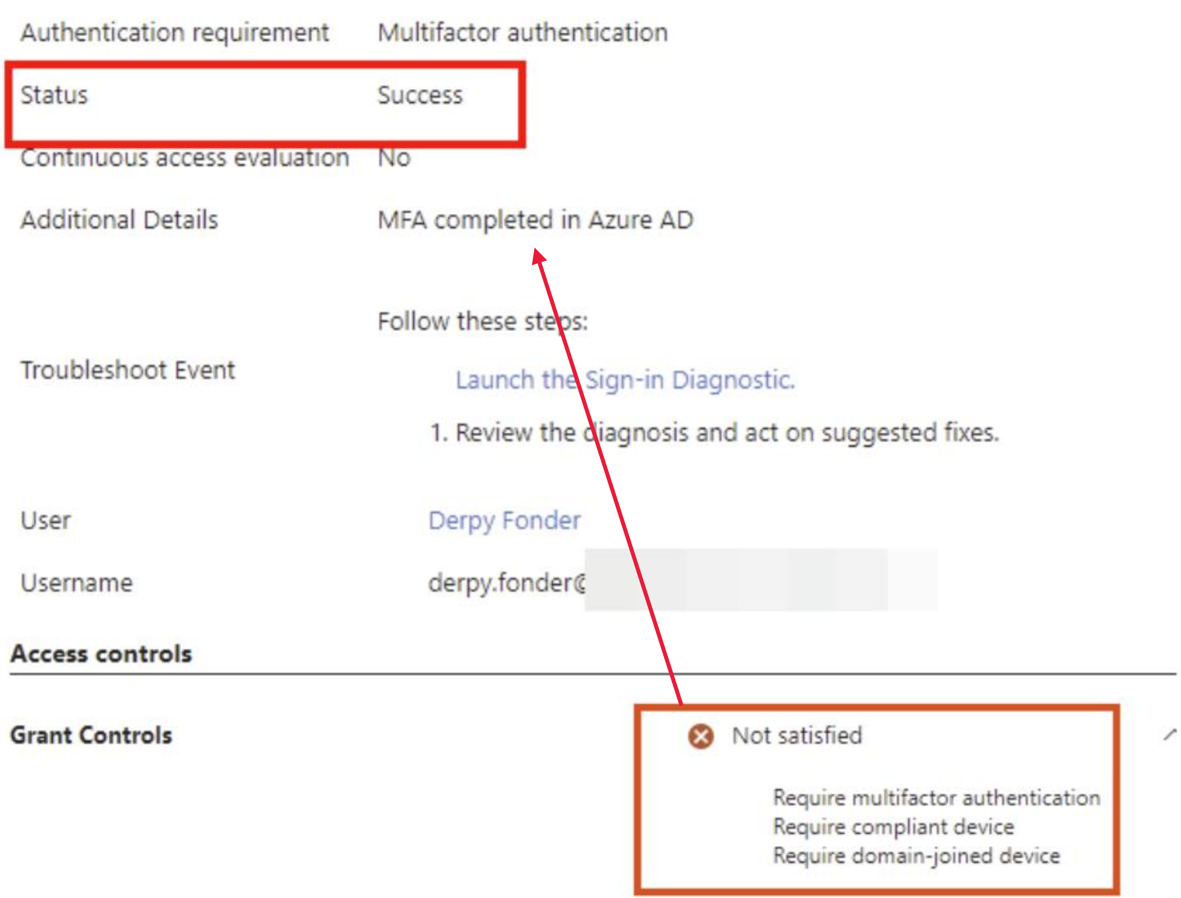
It was in the error logs



```
Error     13/12/2024 16:51:52   AAD   1098   AadTokenBrokerPlugin Operation
Error     13/12/2024 16:51:43   AAD   1098   AadTokenBrokerPlugin Operation
Warning   13/12/2024 16:51:43   AAD   1097   AadTokenBrokerPlugin Operation
```

Event 1098, AAD

```
Error: 0xCAA30194 The server has not found anything matching the requested URI (Uniform Resource Identifier).
HTTP error during UI flow.
Url: https://login.microsoftonline.com/a999a97b-cfbc-4052-a095-815487a080f1/oauth2/authorize?
response_type=code&client_id=9ba1a5c7-f17a-4de9-a1f1-6178c8d51223&redirect_uri=ms-appx-web^3a^2f^
2fMicrosoft.AAD.BrokerPlugin^2fS-1-15-2-2666988183-1750391847-2906264630-3525785777-2857982319-3063633125-
1907478113&instance_aware=true&nonce=7c2398fd-08a1-4b28-9fa5-186c60206ec0&resource=b8066b99-6e67-41be-abfa-
75db1a2c8809&add_account=multiple&prompt=login&response_mode=form_post&windows_api_version=2.0.1
HTTP Error: 404
Content:
<html><head>
```

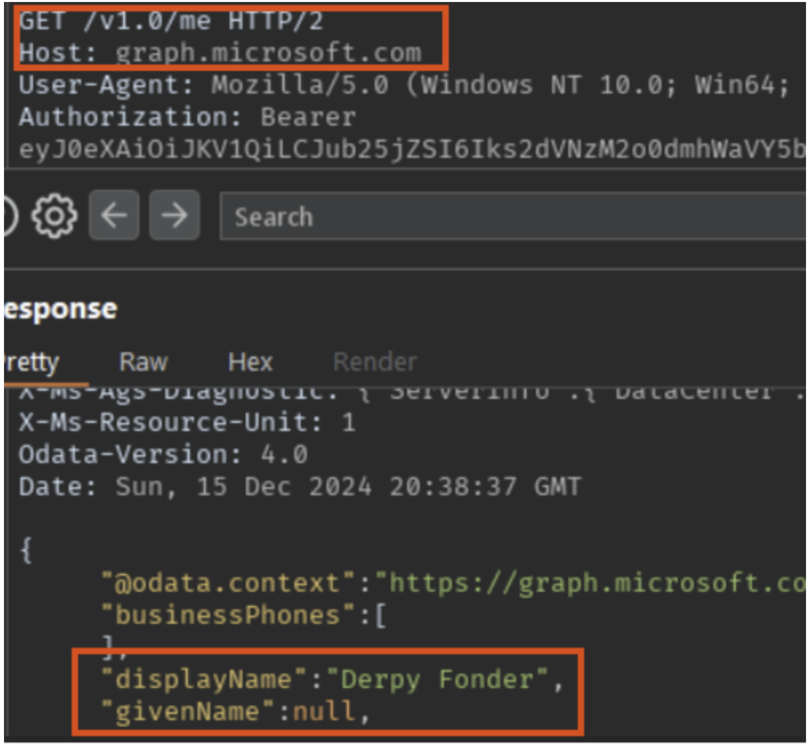


Authentication requirement	Multifactor authentication
Status	Success
Continuous access evaluation	No
Additional Details	MFA completed in Azure AD
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.
User	Derpy Fonder
Username	derpy.fonder@[redacted]

Access controls

Grant Controls	Not satisfied Require multifactor authentication Require compliant device Require domain-joined device

Weaponisation – so it talked to Graph API

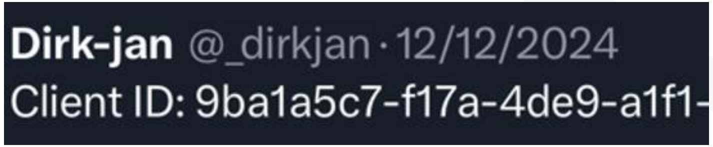


```
GET /v1.0/me HTTP/2
Host: graph.microsoft.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJub25jZSI6Iks2dVNzM2o0dmhWaVY5b
```

```
X-Ms-Ags-Diagnostic: { ServerInfo :{ DataCenter :
X-Ms-Resource-Unit: 1
Odata-Version: 4.0
Date: Sun, 15 Dec 2024 20:38:37 GMT

{
     "@odata.context":"https://graph.microsoft.co
     "businessPhones":[
     ],
     "displayName":"Derpy Fonder",
     "givenName":null,
```

Timestamp – 13th Dec

One day after Dirk-jan leaked



Dirk-jan @_dirkjan · 12/12/2024
Client ID: 9ba1a5c7-f17a-4de9-a1f1-

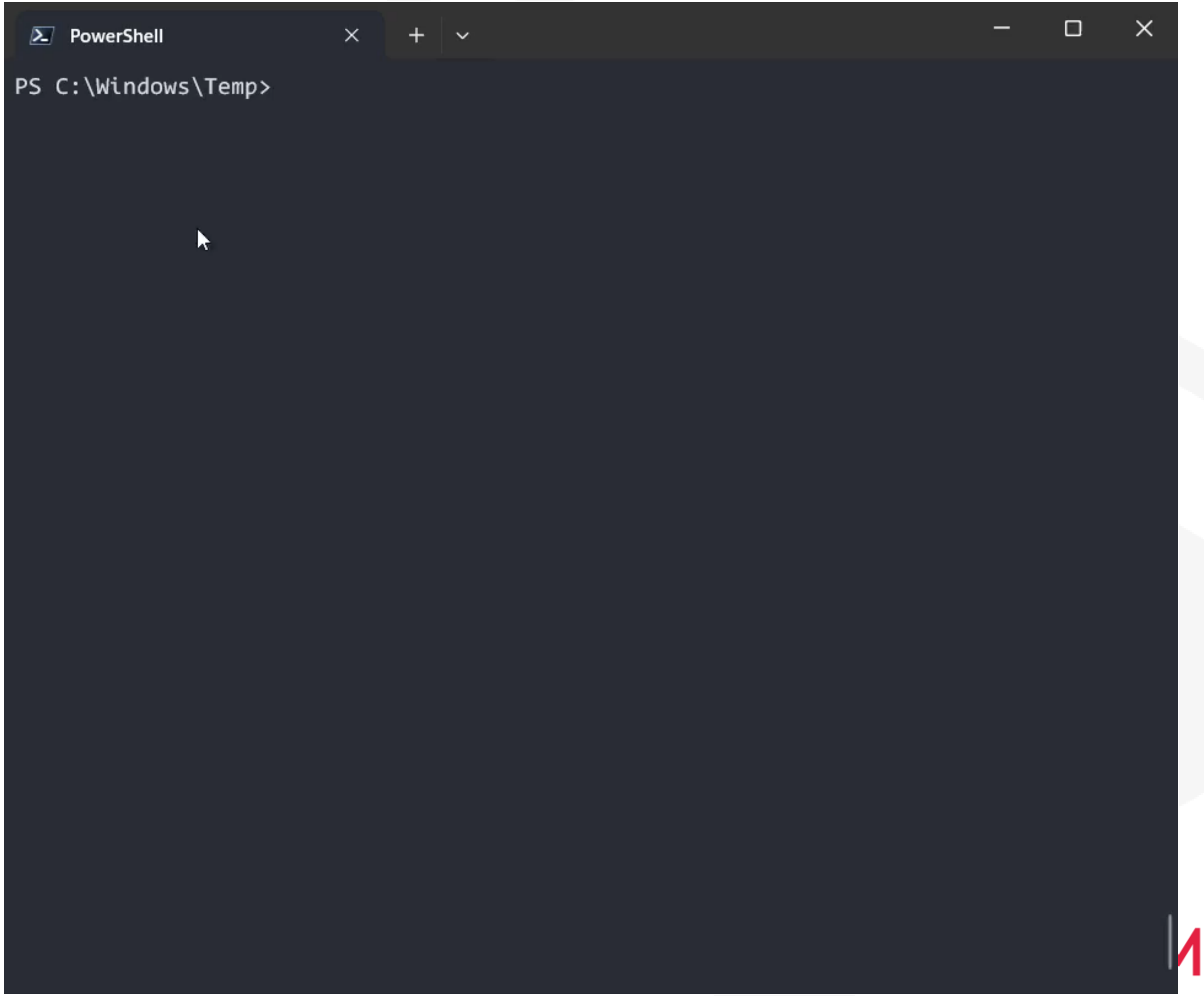
So we just weaponised it in 1 week…?

Just kidding

Code base was 85% there at the time

Was a generic offensive Entra ID auth tool

Demo time



```
PS C:\Windows\Temp>
```

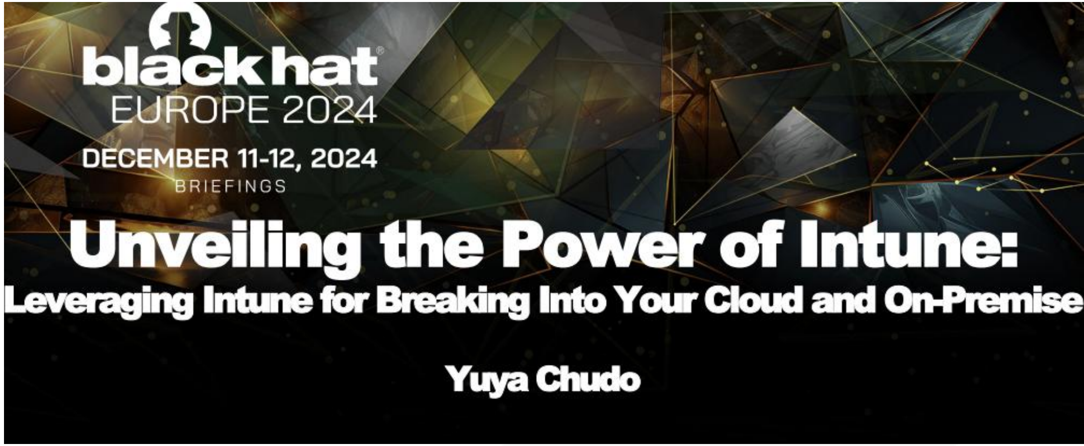
Story around Release

Comms it was all comms

Vendor side

Responsible disclosure?

Fortunately Yuya already told MS



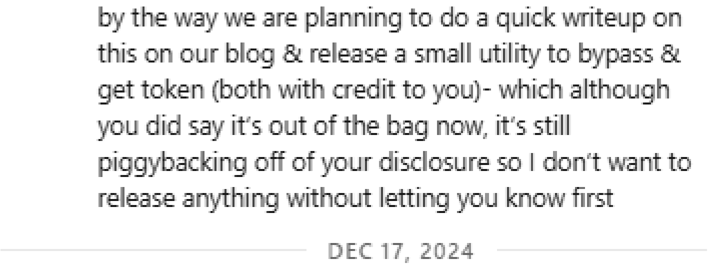
black hat®
EUROPE 2024
DECEMBER 11-12, 2024
BRIEFINGS

Unveiling the Power of Intune:
Leveraging Intune for Breaking Into Your Cloud and On-Premise

Yuya Chudo

Community Side

Me:



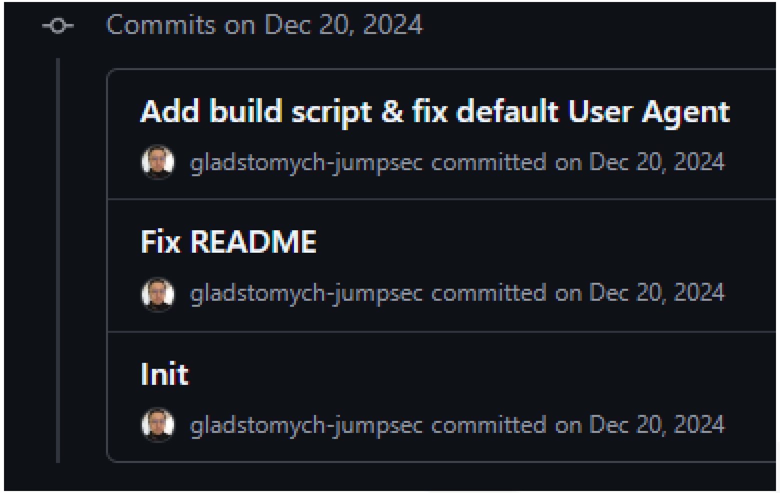
by the way we are planning to do a quick writeup on this on our blog & release a small utility to bypass & get token (both with credit to you)- which although you did say it's out of the bag now, it's still piggybacking off of your disclosure so I don't want to release anything without letting you know first

DEC 17, 2024

Of course! :) let me know when it's up

Dirk-jan

Holidays

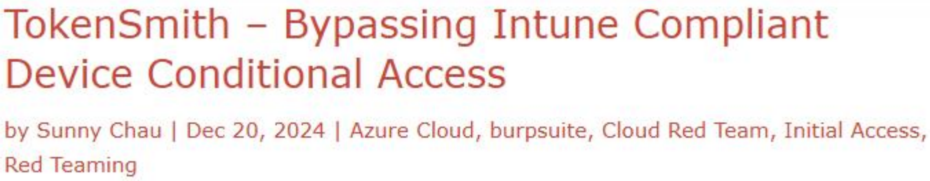


Commits on Dec 20, 2024

Add build script & fix default User Agent
gladstomych-jumpsec committed on Dec 20, 2024

Fix README
gladstomych-jumpsec committed on Dec 20, 2024

Init
gladstomych-jumpsec committed on Dec 20, 2024



TokenSmith – Bypassing Intune Compliant Device Conditional Access

by Sunny Chau | Dec 20, 2024 | Azure Cloud, burpsuite, Cloud Red Team, Initial Access, Red Teaming

Timeline so far

11th Nov – First rumour

12th Dec – Disclosure of vulnerable client ID

13th Dec – Initial research Done

17th Dec – Code written

20th Dec – Blog post + Repo out

No promotions on socials cos it

Was the holiday season

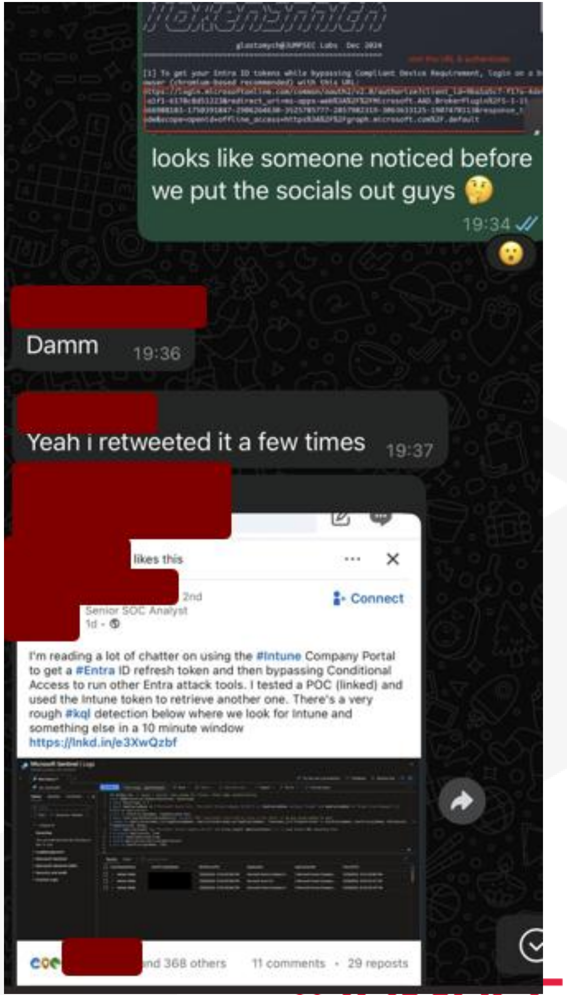
‘Drama’ right after Boxing Day

(and how it was handled)

I was chilling and enjoying Christmas

27th Dec night - My boss on our WhatApp group:

‘Hey there are a bunch of people sharing the news without crediting us’



glastomych@JUMPSEC Labs Dec 2024

[1] To get your Entra ID tokens while bypassing Compliant Device Requirement, login on a b
owser (chromium-based recommended) with this URL:

https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id= [illegible]
[illegible]&redirect_uri=ms-appx-web%3A%2F%2FMicrosoft.AAD.BrokerPlugin%2FS-1-15 [illegible]
[illegible]&response_ [illegible]
[illegible]&scope=openid+offline_access+https%3A%2F%2Fgraph.microsoft.com%2F.default

looks like someone noticed before we put the socials out guys 🤔

19:34 ✓✓

😮

[redacted]

Damm 19:36

[redacted]

Yeah i retweeted it a few times 19:37

[redacted]

likes this

2nd

Senior SOC Analyst

1d · 🌐

Connect

I'm reading a lot of chatter on using the #Intune Company Portal to get a #Entra ID refresh token and then bypassing Conditional Access to run other Entra attack tools. I tested a POC (linked) and used the Intune token to retrieve another one. There's a very rough #kql detection below where we look for Intune and something else in a 10 minute window https://lnkd.in/e3XwQzbf

[redacted]

nd 368 others 11 comments · 29 reposts

And how it was handled

Me

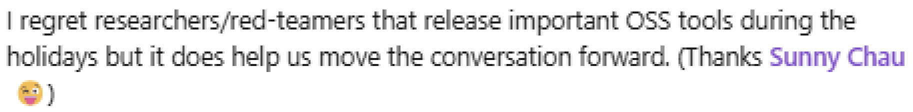
Hey *****,
Thank you for covering our tool :)
I released it a week ago without any social media because of the holiday seasons ...

That said, would you mind adding credit to us in your post as the author of the PoC?

*****[KOL]

Yes totally understand. No problem. great tool Btw!

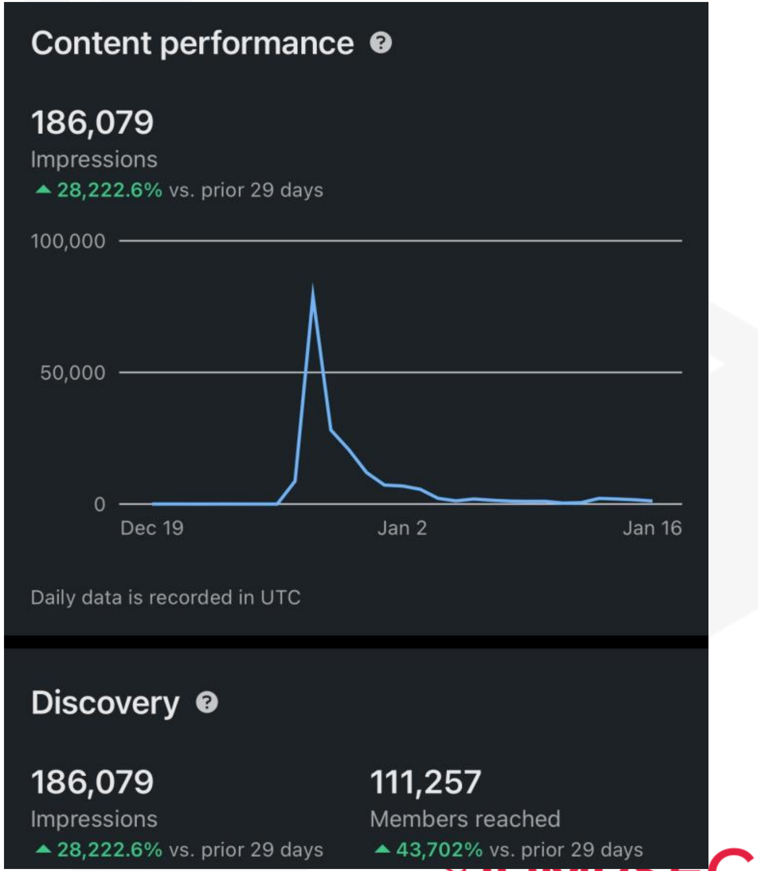
Nice guy though



I regret researchers/red-teamers that release important OSS tools during the holidays but it does help us move the conversation forward. (Thanks Sunny Chau 😜)

our own post was reshared by ***** soon as it went up

It was a super stressful night on 27th Dec



Content performance ?

186,079

Impressions

▲ 28,222.6% vs. prior 29 days

Daily data is recorded in UTC

Discovery ?

186,079	111,257
Impressions	Members reached
▲ 28,222.6% vs. prior 29 days	▲ 43,702% vs. prior 29 days

The shadow patch

Roughly 20th Feb 2025

Microsoft quietly reduced the scope for the token you could get from company portal

Noticeably more narrow than the original, notably only

ServicePrincipalEndpoint.Read & **User.Read**

on top of the Intune related ones.

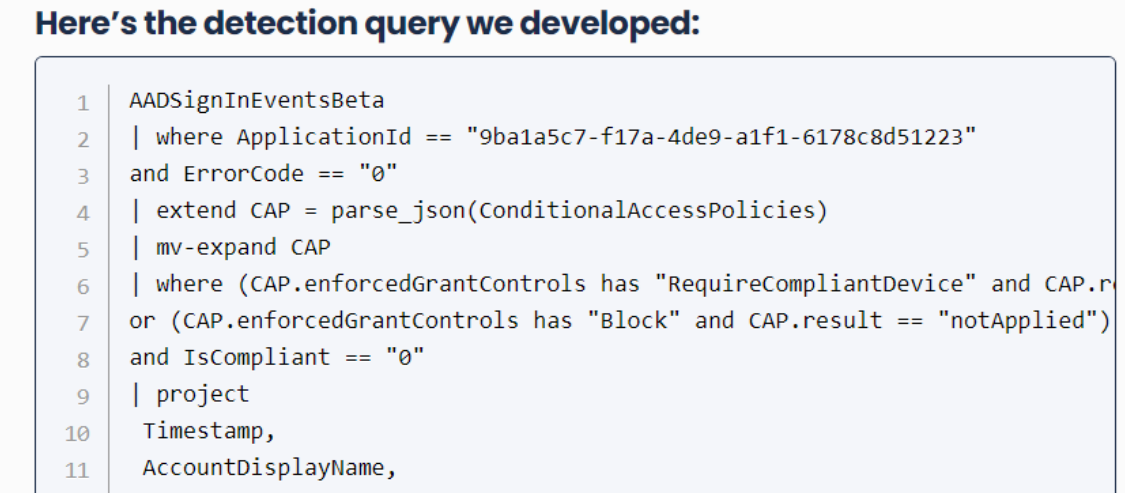
Also Tokensmith's executable has become 'malware'

What happens now

- Detection for client ID
- Watch for rouge device being registered

How to Defend against it?

Detection work: https://quzara.com/blog/bypass-intune-conditional-access-using-tokensmith-detection-response



Here’s the detection query we developed:

```
AADSignInEventsBeta
| where ApplicationId == "9ba1a5c7-f17a-4de9-a1f1-6178c8d51223"
and ErrorCode == "0"
| extend CAP = parse_json(ConditionalAccessPolicies)
| mv-expand CAP
| where (CAP.enforcedGrantControls has "RequireCompliantDevice" and CAP.r
or (CAP.enforcedGrantControls has "Block" and CAP.result == "notApplied")
and IsCompliant == "0"
| project
 Timestamp,
 AccountDisplayName,
```

Takeaways

Threat actors & KOLs monitor company blogs

Half written passion projects could be suddenly weaponised

Don’t be shy to talk to people & ask (nicely) - make friends along the way!

Thank you & QnA

I won’t keep you away from lunch any longer ;)

If you wanna check out the work:

https://labs.jumpsec.com/tokensmith-bypassing-intune-compliant-device-conditional-access/

https://github.com/JumpsecLabs/TokenSmith