



# Reverse Engineering a Rumour

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

# \$whoami

Head of Adv Simulation @JUMPSEC, joined 2022

Loves all things cloud

Loves math rock



@gladstomych

[sunnyc@jumpsec.com](mailto:sunnyc@jumpsec.com)



# Let's set the stage

## Video performance 📊


70,748  
Video Views

246h 13m  
Watch time



12s  
Average watch time


(post drop – 27<sup>th</sup> Dec)




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

**Sunny Chau** • You  
Red teamer @JUMPSEC | OSCP CRT0  
2mo • Edited • 📌


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

  Tom Ellison (ChCSP) and 1,649 others  
59 comments • 258 reposts


 186,074 impressions [View analytics](#)

Most relevant ▾

**Benjamin Jones** • 1st  
Managed SaaS Alerts Director  
1mo ...

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

# Community reaction?



Merill Fernando • Following

Product Manager @ Microsoft Sign up to Entra.News my weekly newsletter...  
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>

## Entra ID News #77 → This week in Microsoft Entra

🔗 GPL-3.0 license

📈 Activity

📁 Custom properties

★ 256 stars

👁 4 watching

🍴 34 forks



Quzara®  
Cloud. Security. Analytics.

SERVICES ▾

SOLUTIONS ▾

PARTNERS

RESOURCES ▾

QUZARA LLC | DEC 30, 2025 | 3 MIN READ

## Bypass Intune Conditional Access Using TokenSmith: Detection & Response

# Initial rumour

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

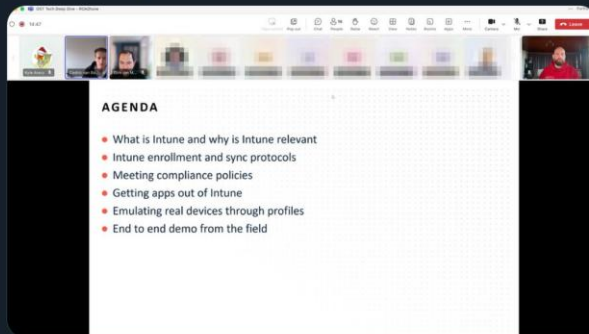


**Outflank** @OutflankNL · 20/12/2024

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...](https://outflank.nl/products/outfl...)



**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....



1



7



32



5.7K



# What are Entra ID CAPs?

Think of CAP as this

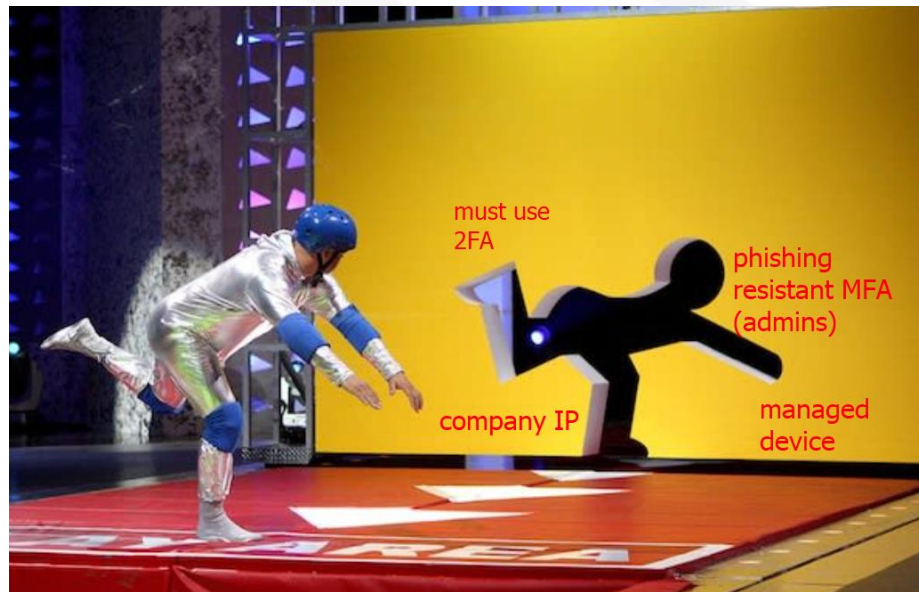
Hole is for users

Yellow wall for bad guys

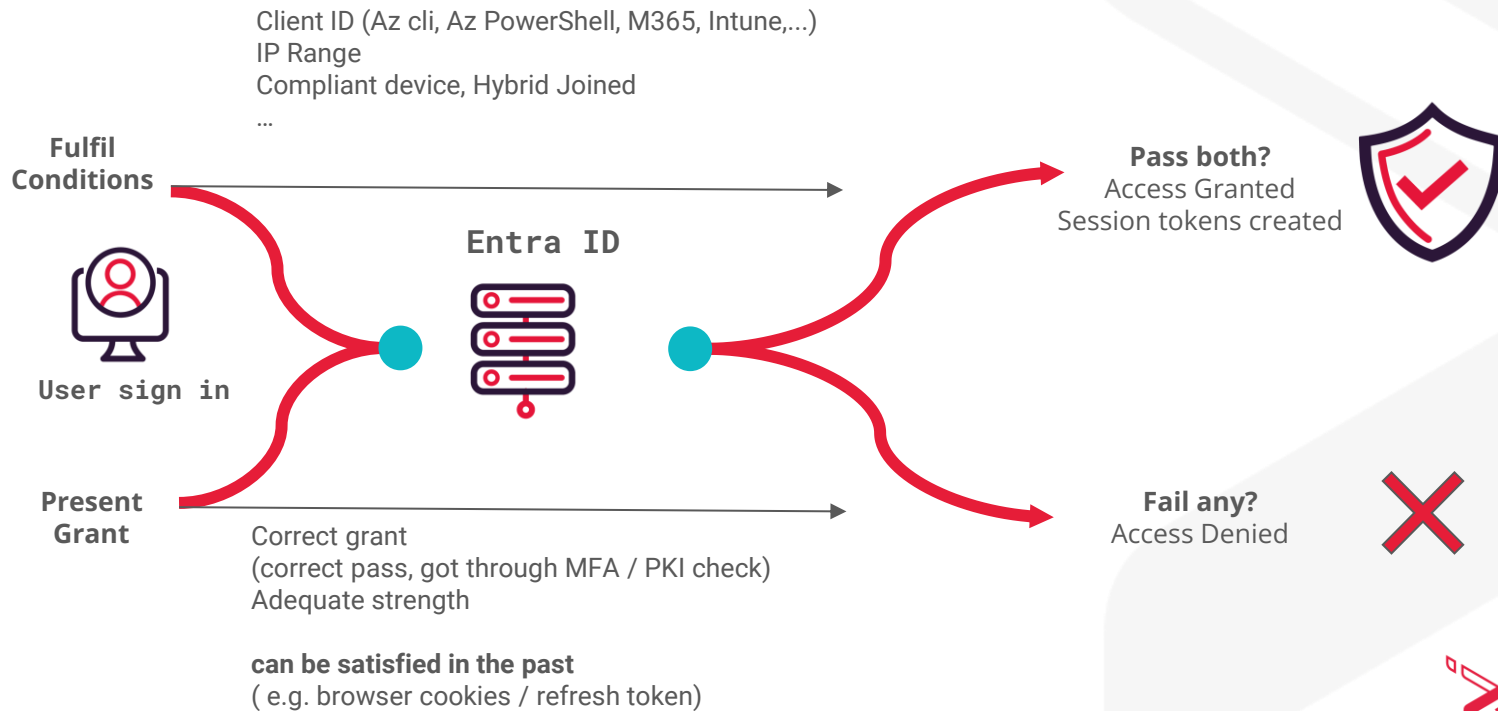
Rumour:

Requiring Company device?

No more



# Pictorially





# 1 mo Later Rumour became reality





# Quick Recap

## HINT 1:

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

## HINT 2:

**[Intune Company Portal]**

At the time we didn't have the BH slides



# How would you approach this?

**WHAT** – being able to run offensive tools

**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

# 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](#)

Internet Engineering Task Force (IETF)

Request for Comments: 6749

Obsoletes: [5849](#)

Category: Standards Track

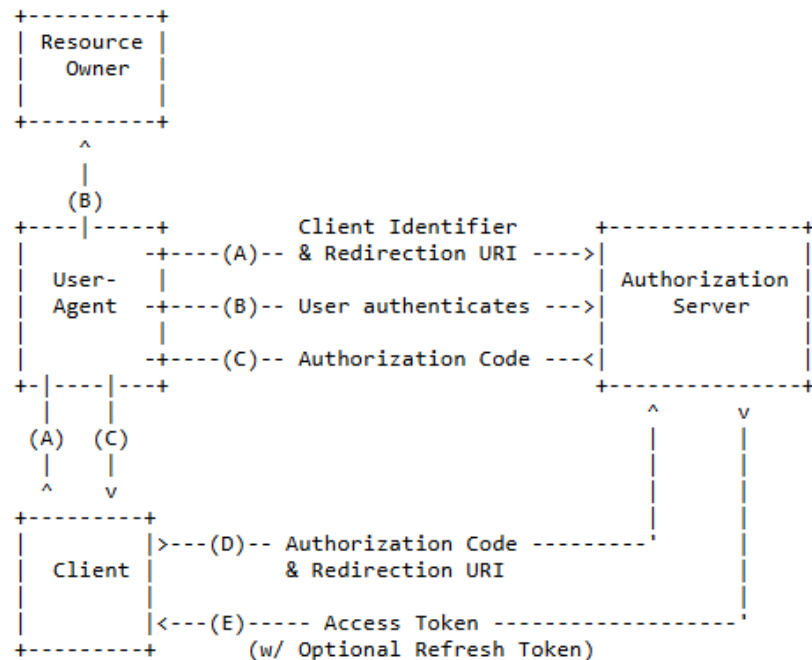
ISSN: 2070-1721

Errata Exist

D. Hardt, Ed.

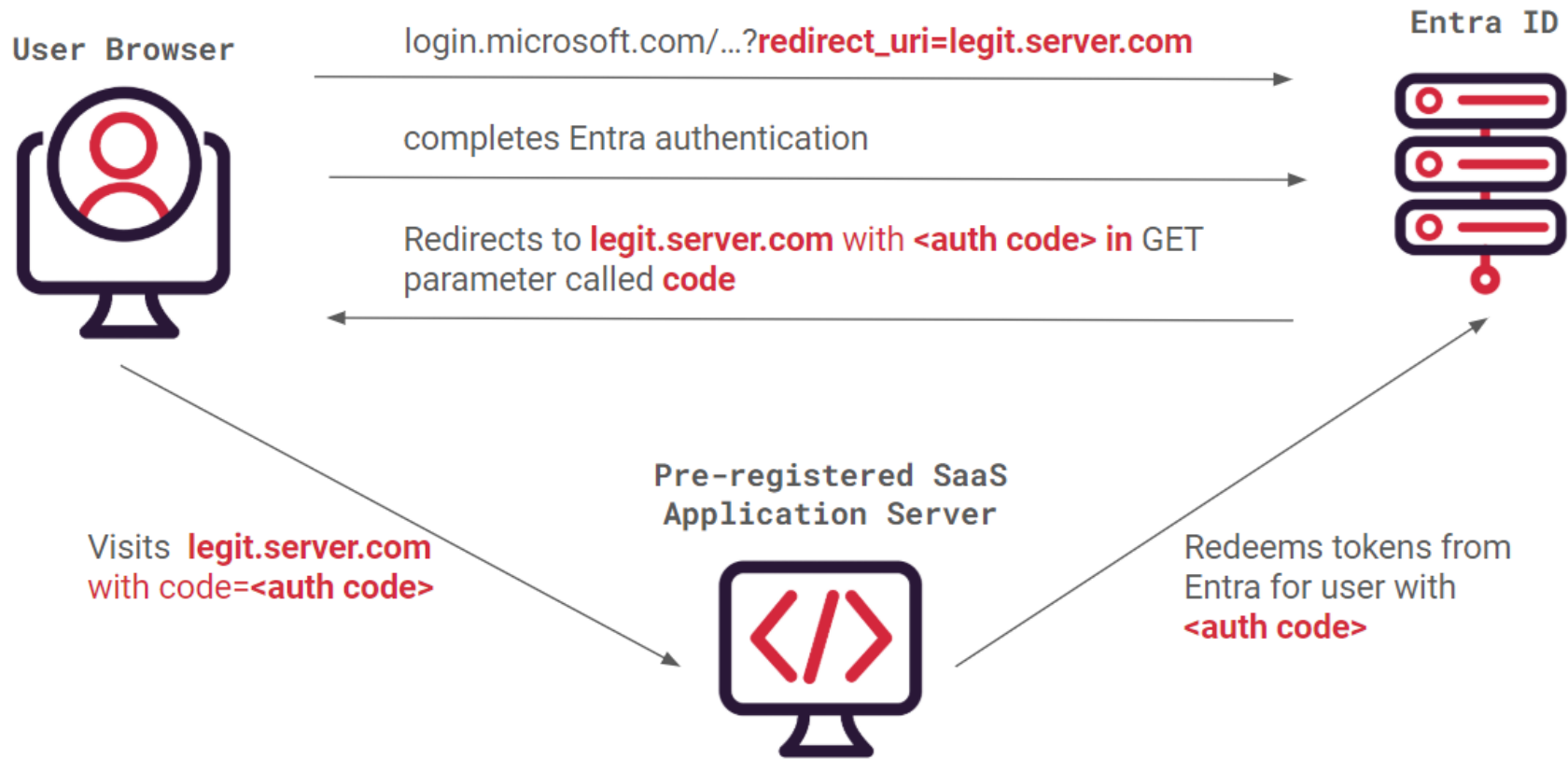
Microsoft

## The OAuth 2.0 Authorization Framework



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



User Browser

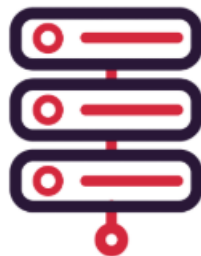


login.microsoft.com/...?redirect\_uri=attacker.server.com

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

Throws an "incorrect redirect URI error" without providing authorization code

Entra ID



Attacker Web Server



does not get redirected

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 ⓘ

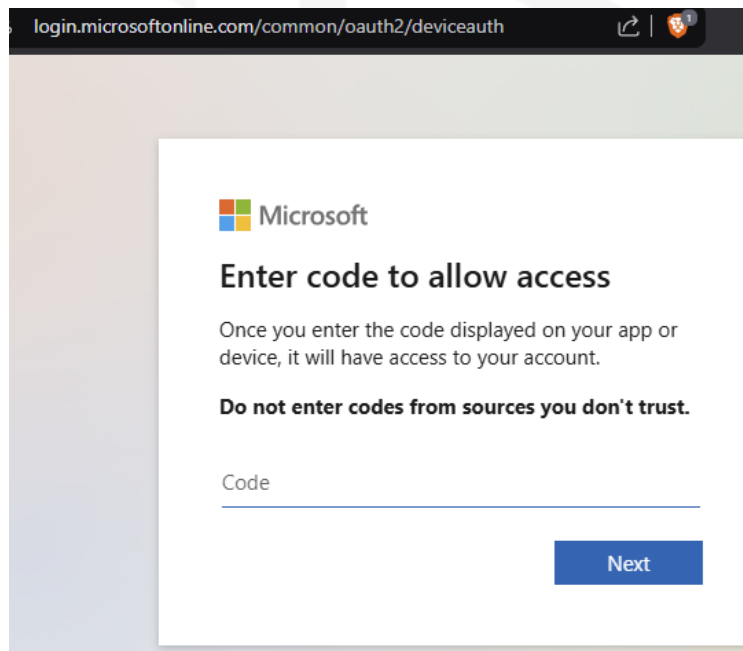


Don't lock yourself out! Make sure that your device is compliant. [Learn more](#) ⓘ

# Approach one – device code

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

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



The screenshot shows a web browser window with the address bar displaying 'login.microsoftonline.com/common/oauth2/deviceauth'. The page content features the Microsoft logo at the top, followed by the heading 'Enter code to allow access'. Below this, a message states: 'Once you enter the code displayed on your app or device, it will have access to your account.' A warning in bold text reads: 'Do not enter codes from sources you don't trust.' There is a text input field labeled 'Code' and a blue 'Next' button at the bottom right.

# 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



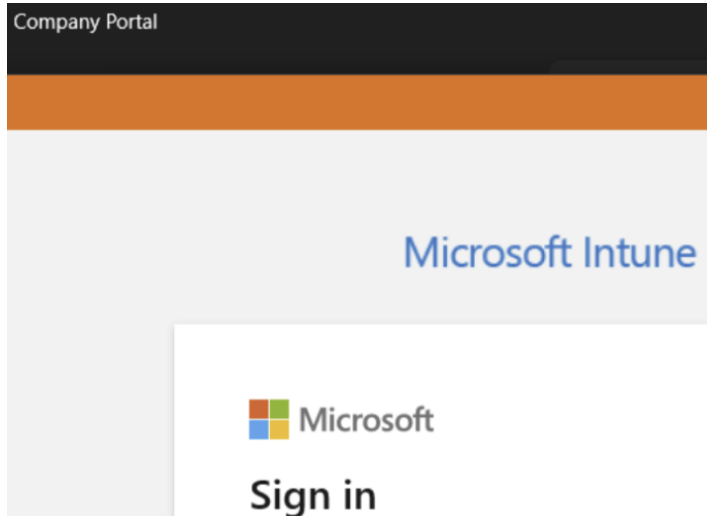
derpy.fonder

## 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...



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@
User ID	1
Sign-in identifier	
Session ID	
User type	Member
Cross tenant access type	None
Application	Microsoft Intune Company Portal
Application ID	9ba1a5c7-f17a-4de9-a1f1-6178c8d51223

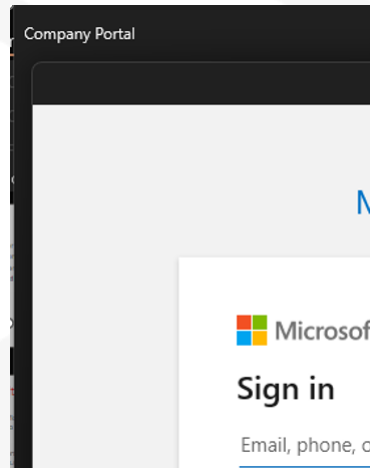
User	↑↓ Application	↑↓ Status	in-app browser	IP address
Derpy Fonder	Microsoft Intune Co...	Success		
Derpy Fonder	Microsoft Intune Co...	Failure		

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 default 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 9bala5c7-f17a-4de9-alf1-6178c8d51223 -u derpy.fonder@not-this-tenant.com
```

Unfortunately we would get an incorrect redirect URI error:

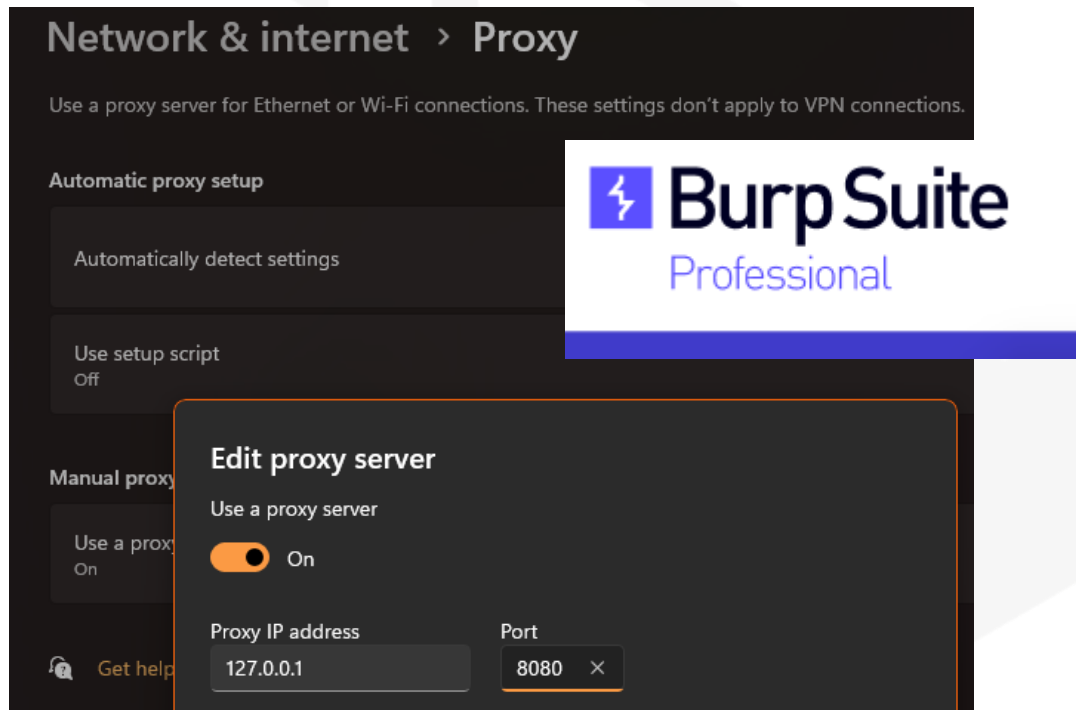
```
AADSTS50011: The redirect URI  
'https://login.microsoftonline.com/common/oauth2/nativecli  
ent' specified in the request does not match the redirect  
URIs configured for the application '9bala5c7-f17a-4de9-  
alf1-6178c8d51223'
```

# Approach 4 – Trying to get TLS layer HTTP proxy working

Burp suite

System proxy

CA cert



## Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, or 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

### Proxy listeners



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

<input type="button" value="Add"/>	<input type="checkbox"/>				
<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host
<input type="button" value="Remove"/>					

install Burp's cert onto root store

Each installation of Burp generates its own CA certificate that Proxy listeners can use when needed. This certificate is not installed by default, so you must install it manually. You can also regenerate the certificate if you need to.

# Okay – System level https proxy working

The screenshot displays a web browser's developer tools interface. At the top, a table lists network requests. The first request is highlighted with a red box:

#	URL	Method	Status	Size	Type
1	https://example.com	GET	200	1620	HTML
7	https://example.com	GET	200	1620	HTML

Below the table, the 'Request' and 'Response' tabs are visible. The 'Request' tab is selected, showing the following details:

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

The 'Response' tab shows the following details:

- 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"

Below the developer tools, a PowerShell terminal window is open. The command and its output are highlighted with red boxes:

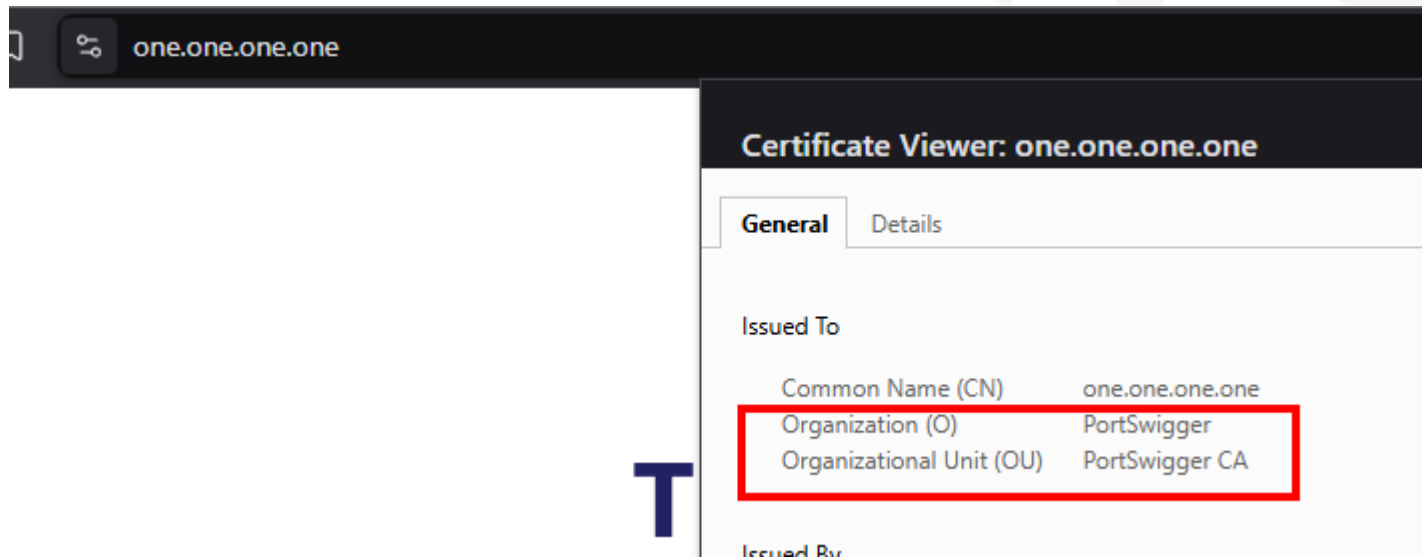
```
PS > iwr https://example.com -UserAgent 'PowerOfLoveAndFriendShip'
```

The output of the command is:

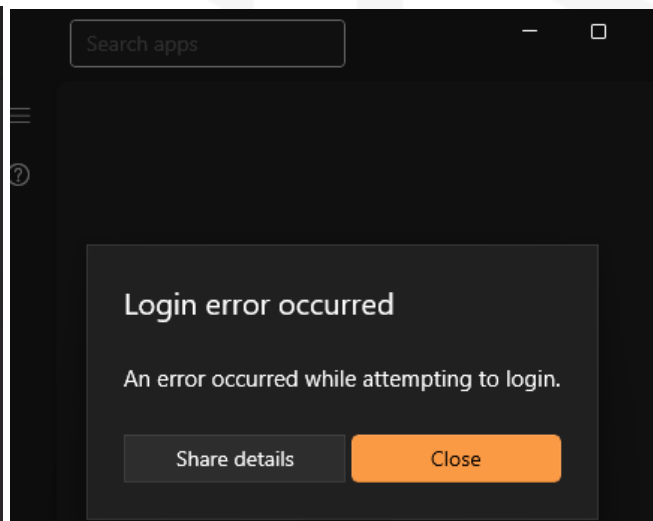
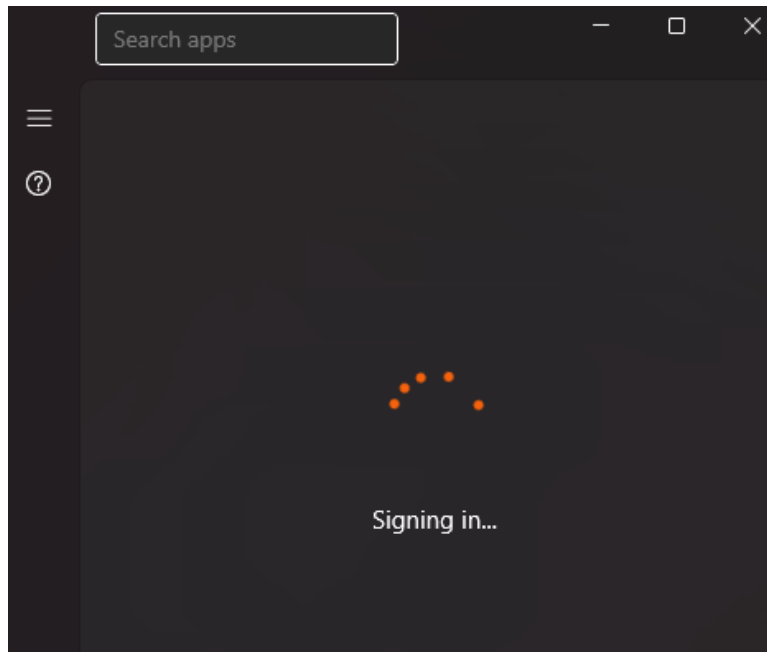
```
StatusCode      : 200  
StatusDescription : OK  
Content         : <!doctype html>
```



# CA is auto switched & Trusted



But for what we needed ... it did not work out





Reason?  
mTLS check?

Proxy  
detection?

# Google to the rescue

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




ZeroTouch.ai

### Supercharged Real-time Intune Companion

- Install & Auto update 15K Apps
- Intuitive, sequenced, & optimized Autopilot
- Remote Desktop & Remote Shell

Single-Tenant | M



## 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 tried to **Repair** or Reset Company Portal App to fix the issue? The Intune company portal **application** is no



## 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:**

**XMLHttpRequest::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 URL: [ms-appx-web://Microsoft.AAD.BrokerPlugin/S-1-15-2-2666988183-](ms-appx-web://Microsoft.AAD.BrokerPlugin/S-1-15-2-2666988183-1750391847-2906264630-3525785777-2857982319-3063633125-1907478113)

[1750391847-2906264630-3525785777-2857982319-3063633125-1907478113](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

General Details

Error: 0xCA30194 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-75db1a2c88098&add\\_account=multiple&prompt=login&response\\_mode=form\\_post&windows\\_api\\_version=2.0.1](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-75db1a2c88098&add_account=multiple&prompt=login&response_mode=form_post&windows_api_version=2.0.1)  
HTTP Error: 404  
Content-Type: text/html

Authentication requirement    Multifactor authentication

Status    Success

Continuous access evaluation    No

Additional Details    MFA completed in Azure AD

Follow these steps:

Troubleshoot Event

[Launch the Sign-in Diagnostic.](#)

1. Review the diagnosis and act on suggested fixes.

User    Derpy Fonder

Username    derpy.fonder@

#### 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
```

Settings Navigation Search

response

pretty Raw Hex Render

```
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 – 13<sup>th</sup> 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

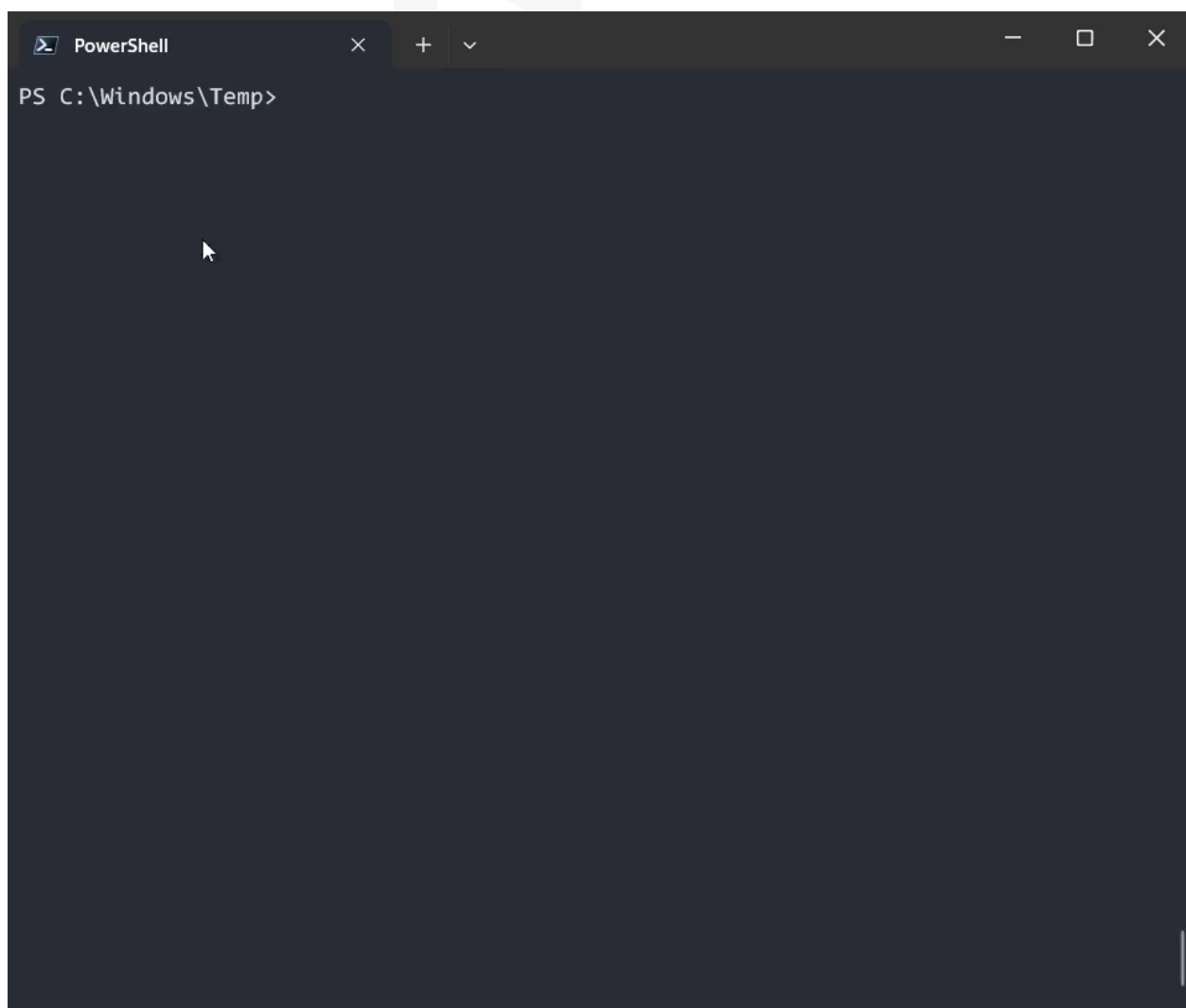
Code base was 85% there at the time

Was a generic offensive Entra ID auth tool





Demo  
time



# Story around Release

Comms it was all comms

Making friends by releasing around Christmas

# Vendor side

Responsible disclosure?

Fortunately Yuya  
already told MS



# The shadow patch

Roughly 20<sup>th</sup> 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'

# 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:

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

# Thank you & QnA

If you like what we do ...

If you wanna check out the work:

<https://github.com/JumpsecLabs/TokenSmith>

<https://labs.jumpsec.com>