



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





Sunny Chau • You
Red teamer @JUMPSEC | OSCP CRTO
2mo • Edited • 1

...

🛠 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 Ellison (ChCSP) and 1,649 others

59 comments • 258 reposts

186,074 impressions

[View analytics](#)



Add a comment...



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

Let's set the stage

Video performance

70,748
Video Views

246h 13m
Watch time

12s
Average watch time

(post drop - 27th Dec)

(which was day after Boxing day)



Merrill Fernando • Following
Product Manager @ Microsoft 🌐 Sign up to Entra.News my weekly newsletter...
1w • ④

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

Community reaction?



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...

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....

1 7 32 5.7K

JUMPSEC

What are Entra ID CAPs?

Think of CAP as this

Hole is for users

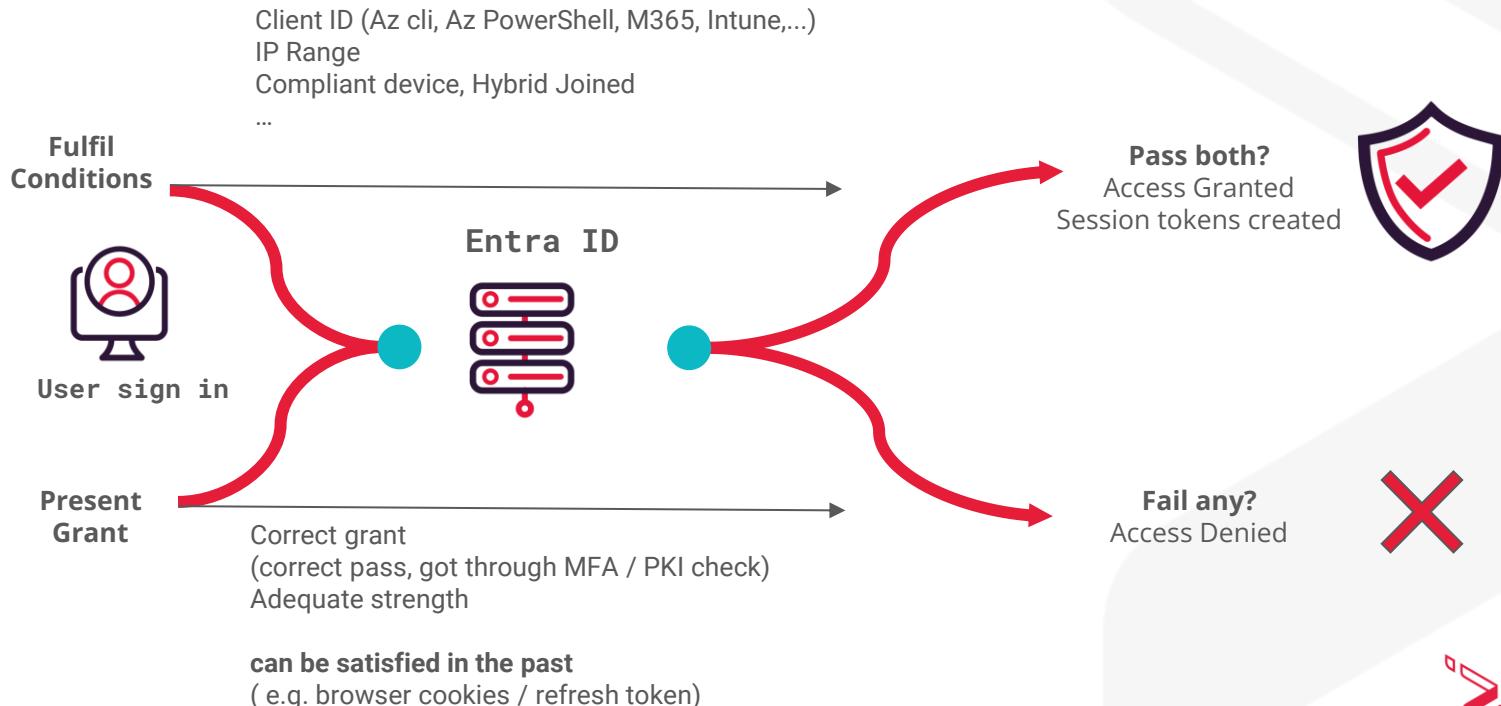
Yellow wall for bad guys

Rumour:

Requiring Company device?
No more



Pictorially



1 mo Later Rumour became reality

The slide features the Black Hat Europe 2024 logo at the top left. Below it, the text "DECEMBER 11-12, 2024" and "BRIEFINGS". The main title is "Unveiling the Power of Intune: Leveraging Intune for Breaking Into Your Cloud and On-Prem". The speaker's name, "Yuya Chudo", is centered below the title.

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

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

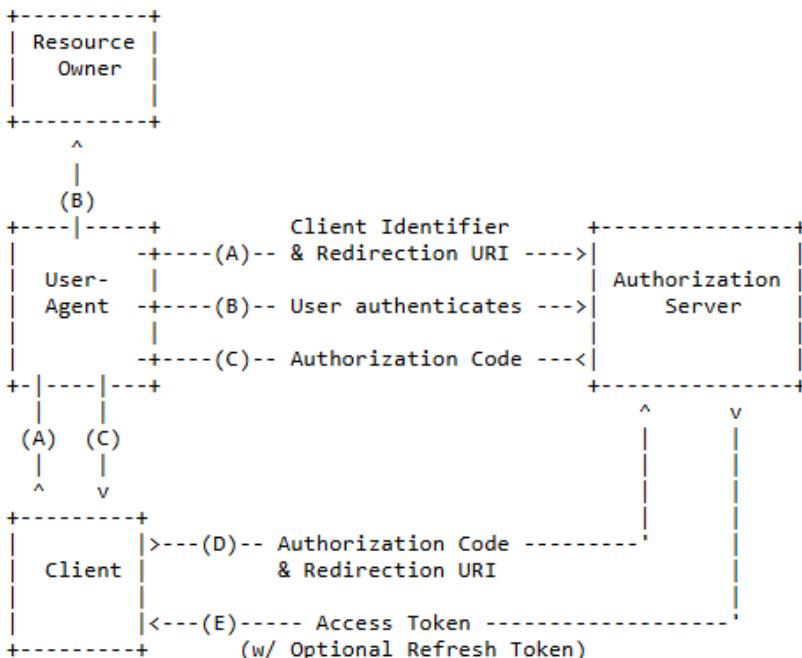
ISSN: 2070-1721

Errata Exist

D. Hardt, Ed.

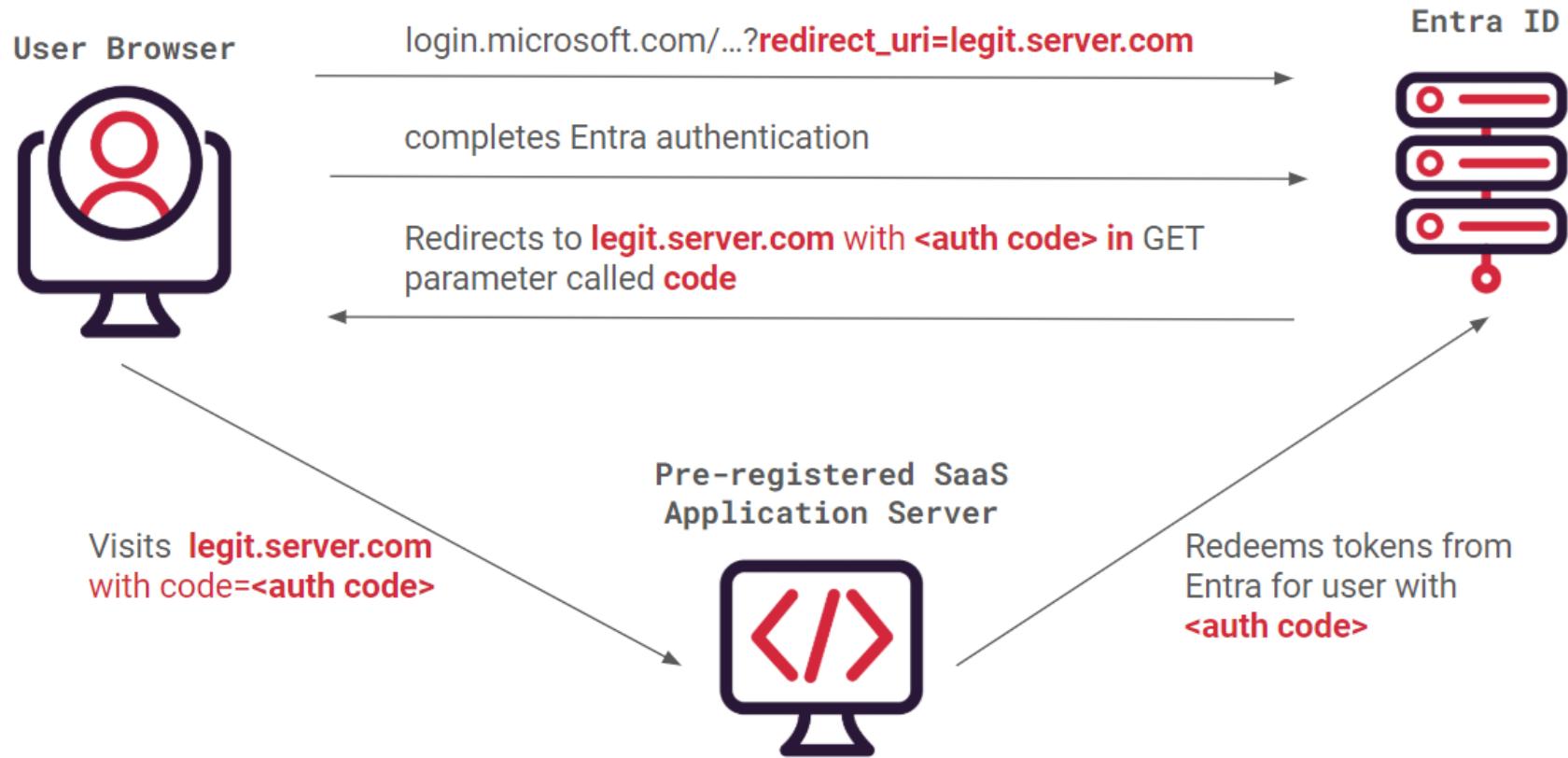
Microsoft

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

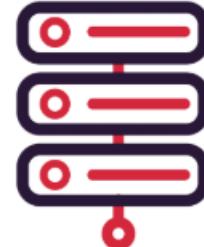


login.microsoft.com/...?redirect_uri=attacker.server.com

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



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')

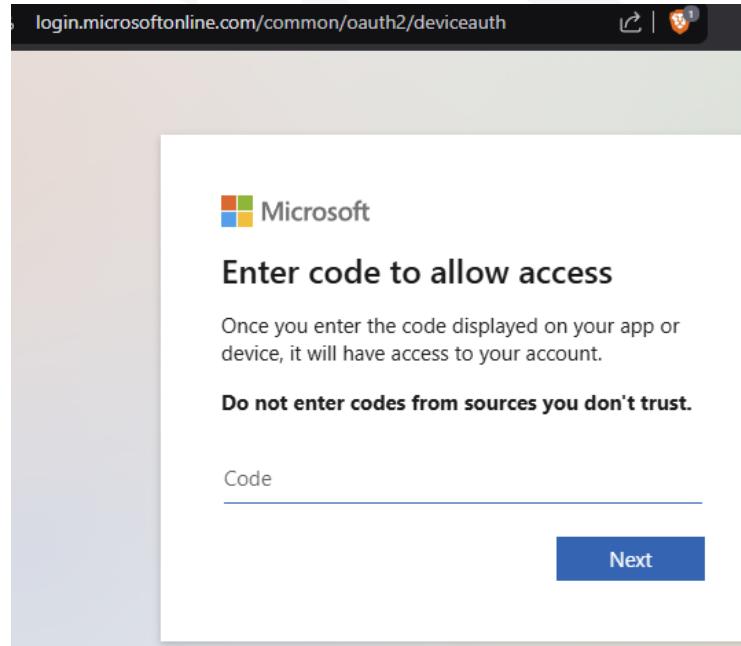
Require device to be marked as compliant ⓘ

⚠ 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



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



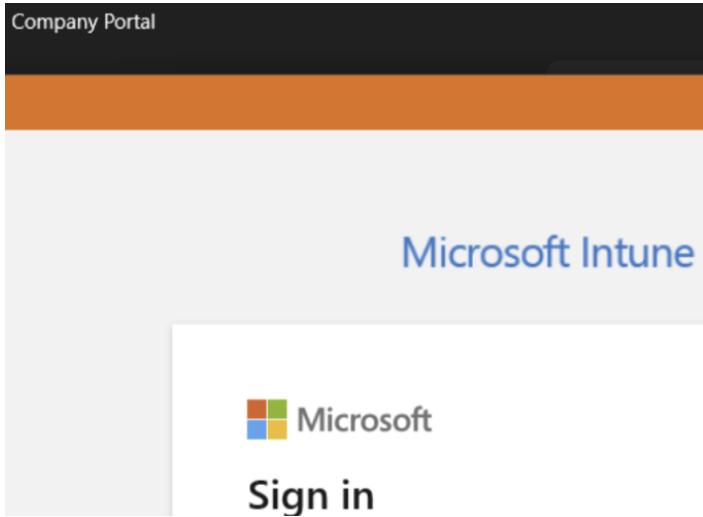
derpy.fonder

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

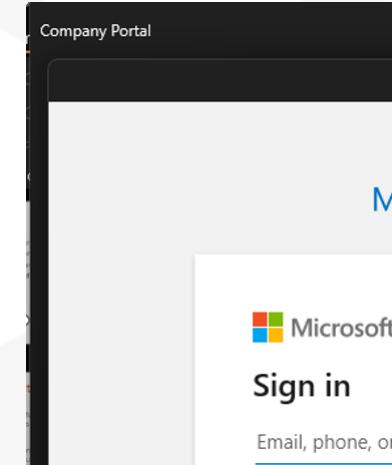
Username	derpy.fonder@contoso.com
User ID	f1e033d0-1a2f-4330-8a20-1a2f43308a20
Sign-in identifier	
Session ID	
User type	Member
Cross tenant access type	None
Application	Microsoft Intune Company Portal
Application ID	9ba1a5c7-f17a-4de9-a1f1-6178c8d51223

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** redirect 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 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

The screenshot shows the Windows Control Panel under 'Network & internet' with 'Proxy' selected. A message at the top states: 'Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.' Below this, there are two main sections: 'Automatic proxy setup' (with 'Automatically detect settings') and 'Manual proxy' (with 'Use a proxy'). Under 'Manual proxy', the 'On' button is selected. A callout box highlights the 'Edit proxy server' section, which contains 'Use a proxy server' (with an 'On' toggle switch), 'Proxy IP address' (set to '127.0.0.1'), and 'Port' (set to '8080'). To the right of the settings window is the Burp Suite Professional logo, featuring a blue lightning bolt icon and the text 'Burp Suite Professional'.

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

Add	Running	Interface	Invisible	Redirect	Certificate
Edit	<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host
Remove					

install Burp's cert onto root store

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

[Import / export CA certificate](#)

[Regenerate CA certificate](#)

Okay – System level https proxy working

The screenshot illustrates a system-level HTTPS proxy setup. At the top, a browser developer tools Network tab shows two requests to 'https://example.com' (GET /) with responses 200 OK and 1620 bytes of HTML content. Below this, the Request and Response panes show the raw HTTP/2 traffic. The Request pane includes headers like Host: example.com and User-Agent: PowerOfLoveAndFriendShip. The Response pane shows the full HTML response, including the title 'Example Domain'. A red arrow points from the PowerShell session at the bottom to the User-Agent header in the Request pane. The PowerShell session itself shows the command 'iwr https://example.com -UserAgent "PowerOfLoveAndFriendShip"' and its output, which includes the status code 200, status description OK, and the content of the HTML response.

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

Request Response

Pretty Raw Hex

```
1 GET / HTTP/2
2 Host: example.com
3 User-Agent: PowerOfLoveAndFriendShip
4 Accept-Encoding: gzip, deflate, br
5
```

PowerShell

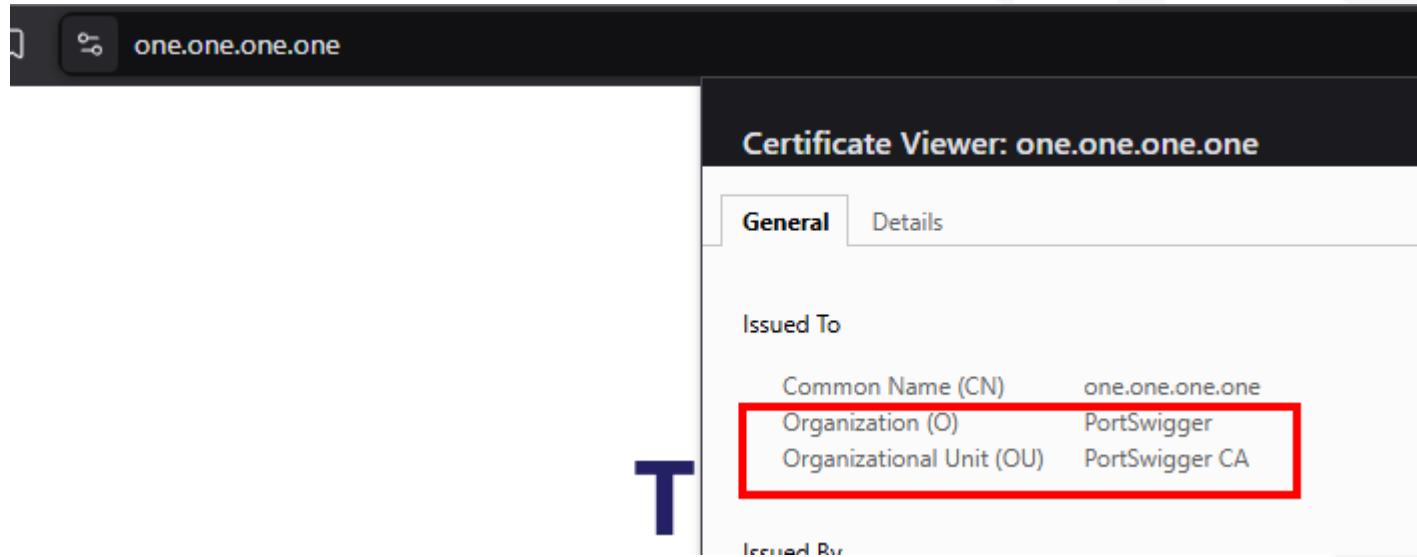
```
iwr https://example.com -UserAgent "PowerOfLoveAndFriendShip"
```

Status Code : 200
Status Description : OK
Content : <!doctype html>

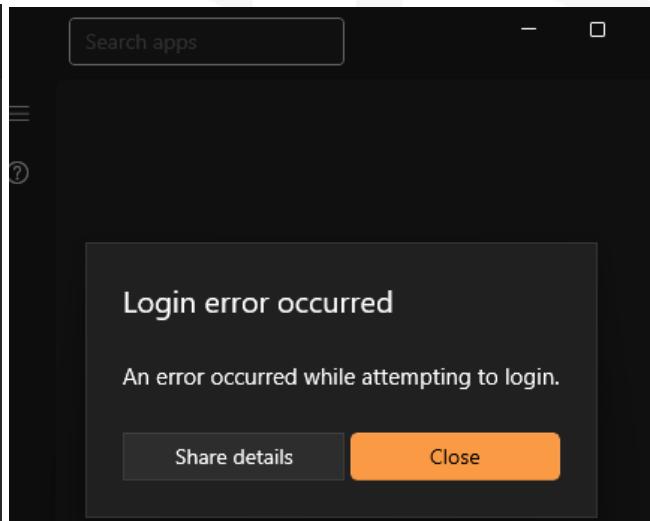
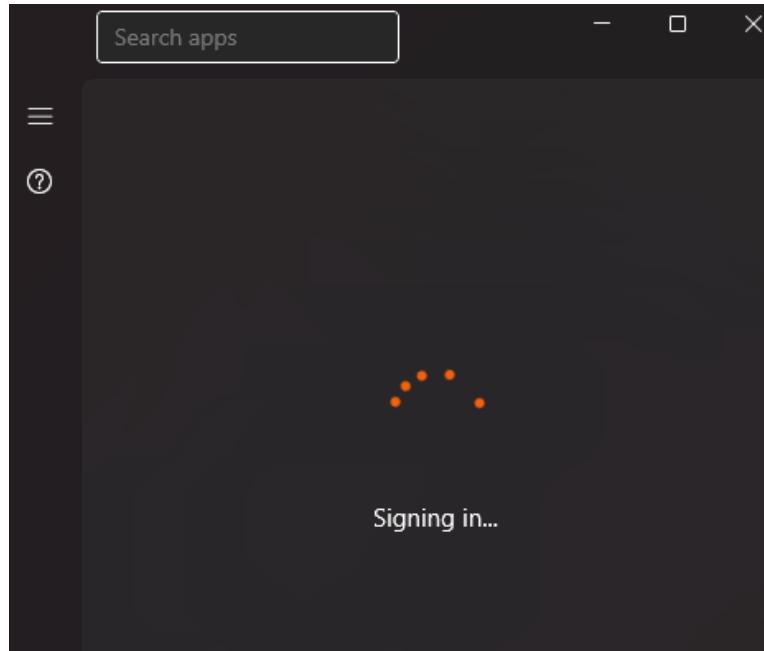
```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Type: text/html
Etag: "84238dfc8092e5d9c0dac8ef93371a07:1736799080.121134"
Last-Modified: Mon, 13 Jan 2025 20:11:20 GMT
Vary: Accept-Encoding
Content-Length: 1256
Cache-Control: max-age=1955
Date: Sat, 01 Mar 2025 15:33:05 GMT
Alt-Svc: h3=":443"; ma=93600,h3-29=:443; ma=93600,quic=:443; ma=93600; v="43"

<!doctype html>
<html>
<head>
    <title>Example Domain</title>
</head>
<body>
    This is a test server (https://example.com).
    </body>
</html>
```

CA is auto switched & Trusted



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

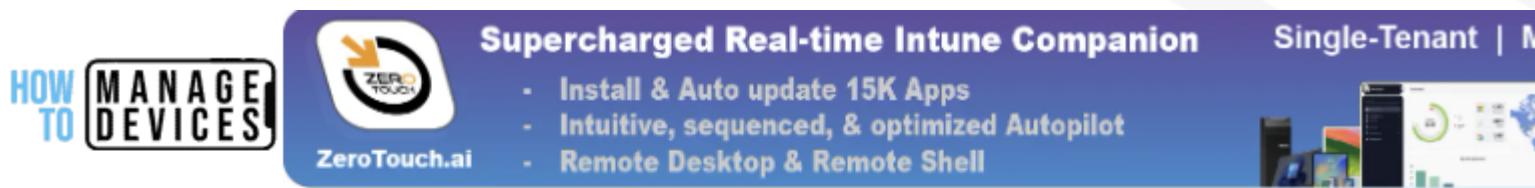


Reason?
mTLS check?

Proxy
detection?

Google to the rescue

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



The advertisement features a blue header with white text. On the left, there's a logo with 'HOW TO' above a box containing 'MANAGE DEVICES'. Next to it is the ZeroTouch.ai logo, which includes a circular icon with a yellow arrow pointing right and the text 'ZEROTOUCH'. The main title 'Supercharged Real-time Intune Companion' is centered. Below it is a bulleted list of features: 'Install & Auto update 15K Apps', 'Intuitive, sequenced, & optimized Autopilot', and 'Remote Desktop & Remote Shell'. To the right, the text 'Single-Tenant | M...' is visible, along with a small image showing multiple devices and a dashboard.

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

Logged at webaccountprocessorapp, line: 163, 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

General Details

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

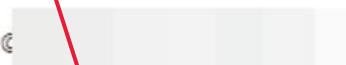
Additional Details MFA completed in Azure AD

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

(response)
pretty Raw Hex Render
X-Ms-Diagnostics: 1 serverinfo 1 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...?

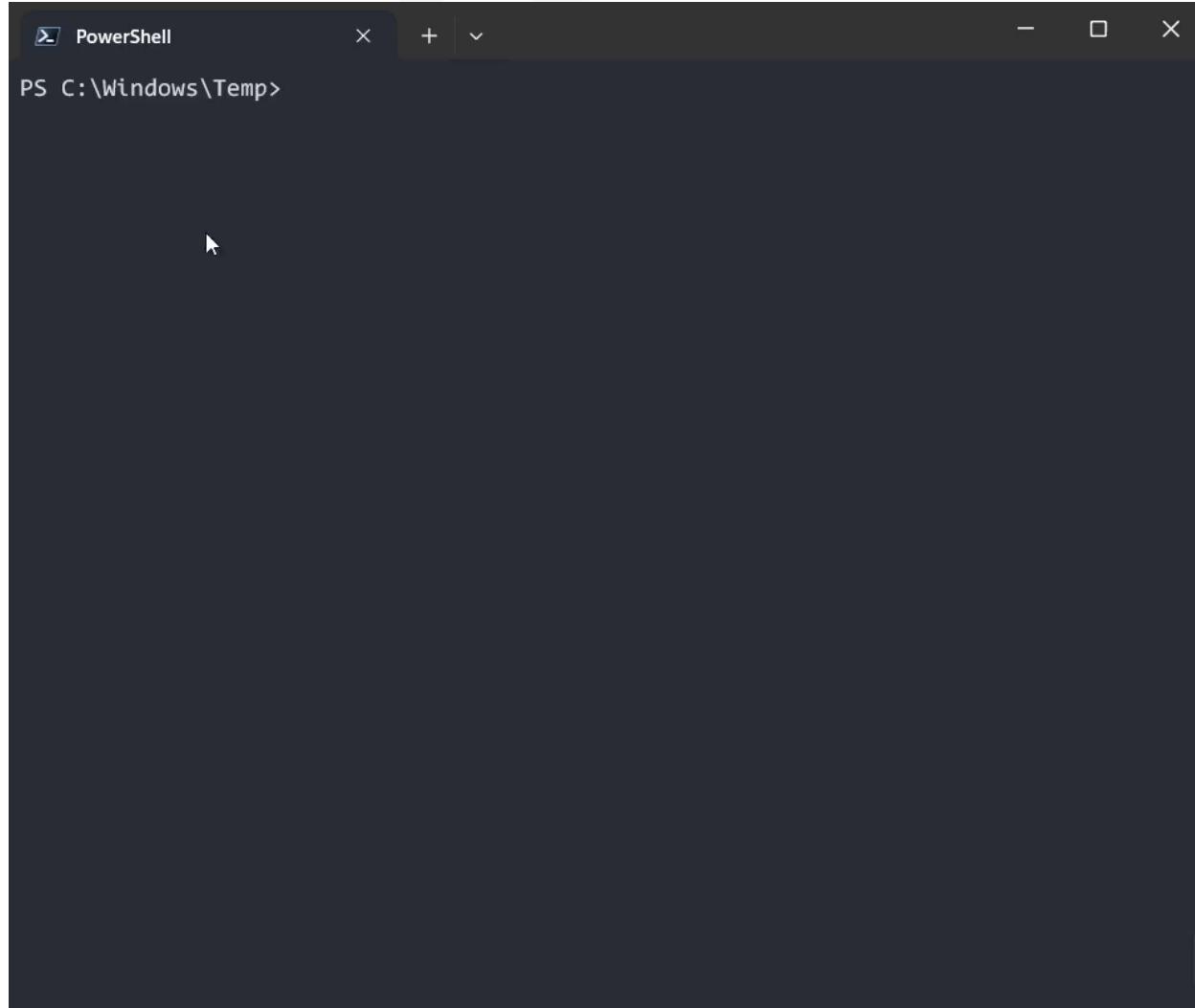
Just kidding

Code base was 85% there at the time

Was a generic offensive Entra ID auth tool



Demo time



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 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**'

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 TokenNameSmith](https://github.com/JumpsecLabs	TokenNameSmith)

<https://labs.jumpsec.com>