Block Legacy Authentication for Exchange Online using the Graph Explorer

An Azure AD Solution Guide

**Note :**

The current guide is based on the **Private Preview** and some options might change in future

This guide walks you through how to modify an existing Conditional Access Policy to block Legacy Authentication for Exchange Online using Graph API. This user is required to have appropriate roles to complete the operations, example Global admin/Conditional Access Administrator. However, you might need Global Admin the first time if you need to enable the Canary endpoint.

# Desired Outcome

You should be able to update the existing CA Policies and verify the change using the Graph Explorer.

# Pre-requisites

1. Enable Canary Endpoint for the Graph Explorer.

Enable and assign permissions to Access the CA APIs using the Canary endpoint.

1. Login as **Global Administrator**
2. Navigate to [https://developer.microsoft.com/graph/graph-explorer/#mode=canary](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdeveloper.microsoft.com%2Fgraph%2Fgraph-explorer%2F%23mode%3Dcanary&data=04%7C01%7Cjeevan.bisht%40microsoft.com%7Cec5c4feb91364f1b7ccc08d6a1c25145%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636874253293385317%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C-1&sdata=2j3f6Sf4l6OHd0W05CIUh7cMJ%2B0F%2BgsZ3eYWRr9sYl8%3D&reserved=0)
3. Sign in by clicking the “Sign In with Microsoft” button on the sidebar to the left
4. After signing in, the button should be replaced with the user’s name and UPN. Below the UPN, there should be a link called *modify permissions*
5. Select *Directory.AccessAsUser.All* and *Policy.ReadWrite.ConditionalAccess*  in the list that comes up and click on *Modify Permissions*
6. You might need to sign-in again and consent to the permissions being granted to the app

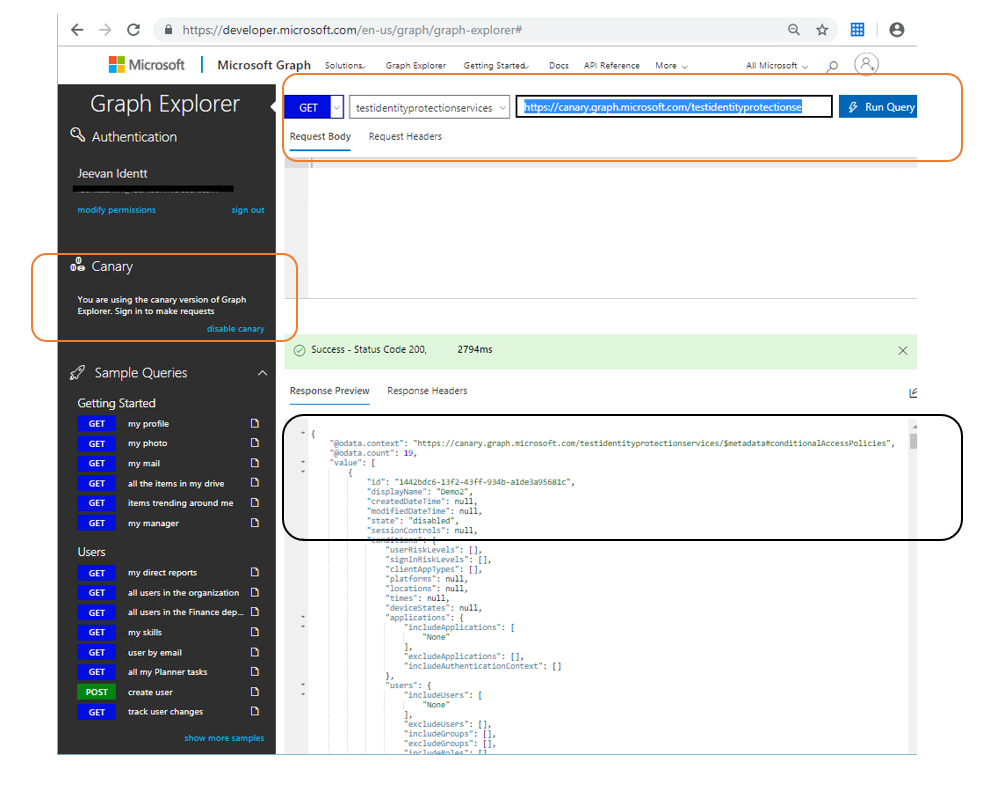
You should now be able to query the CA ([https://canary.graph.microsoft.com/testidentityprotectionservices/conditionalaccesspolicies](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcanary.graph.microsoft.com%2Ftestidentityprotectionservices%2Fconditionalaccesspolicies&data=04%7C01%7Cjeevan.bisht%40microsoft.com%7Cec5c4feb91364f1b7ccc08d6a1c25145%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636874253293395309%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C-1&sdata=8Qy87oI%2F%2BMK8g%2Fqc5RSHjJUbZ2p63Qw3nzJpyWVeGHg%3D&reserved=0))

1. Login as a Global Administrator or Conditional Access Administrator if your canary endpoint is already enabled.

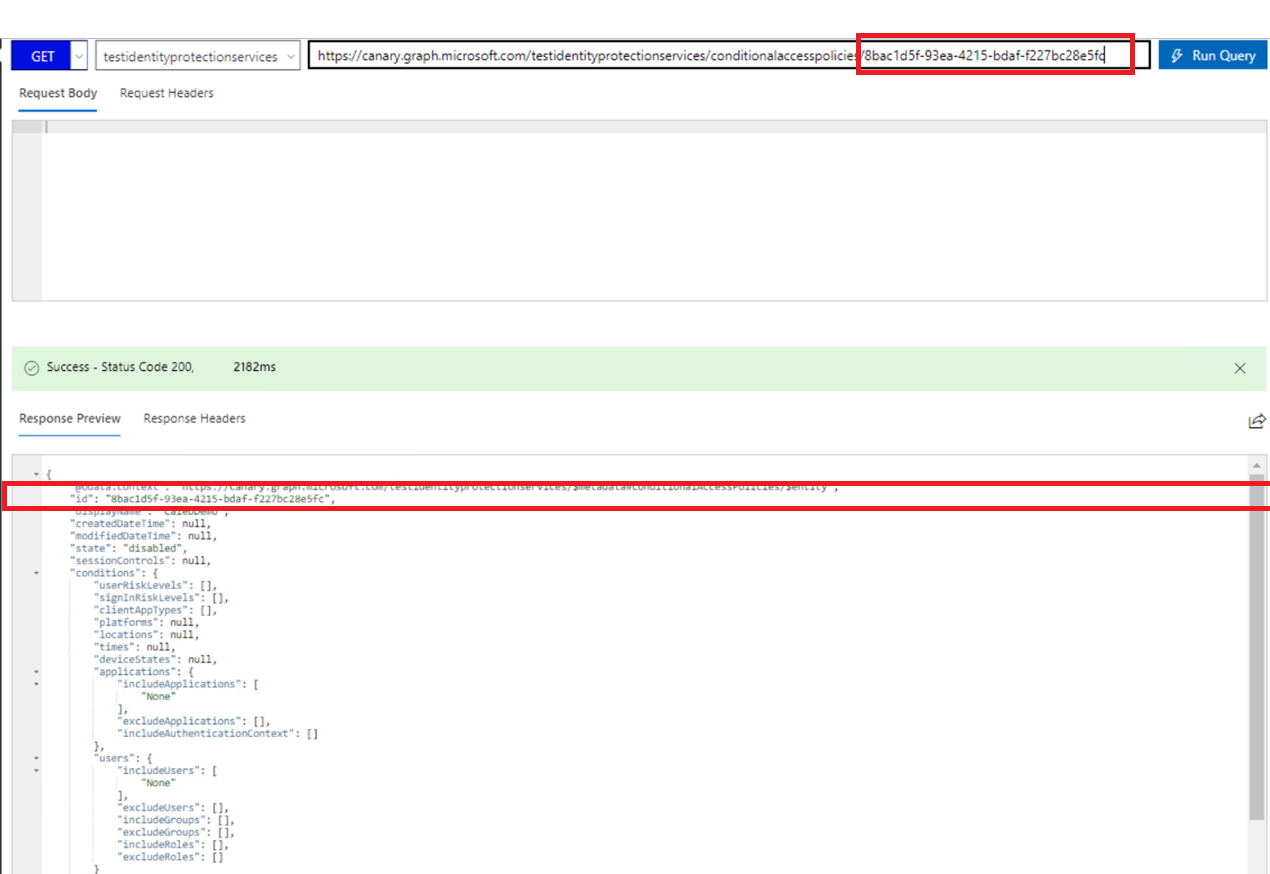
# Steps to implement

***Task 1: Get the required Policy Conditional Access Policies***

1. Log in to [https://developer.microsoft.com/en-us/graph/graph-explorer#](https://developer.microsoft.com/en-us/graph/graph-explorer)
2. Run the **GET** query against the [https://canary.graph.microsoft.com/testidentityprotectionservices/conditionalaccesspolicies](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcanary.graph.microsoft.com%2Ftestidentityprotectionservices%2Fconditionalaccesspolicies&data=04%7C01%7Cjeevan.bisht%40microsoft.com%7Cec5c4feb91364f1b7ccc08d6a1c25145%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636874253293395309%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C-1&sdata=8Qy87oI%2F%2BMK8g%2Fqc5RSHjJUbZ2p63Qw3nzJpyWVeGHg%3D&reserved=0) endpoint



1. Identify the Conditional Access Policy ID(s) using the **ApplicationPrincipalID**, see **appendix** on how to find the ApplicationPrincipalID for the Application.
2. Get the contents of specific policy by appending the /{ID} in the /conditionalaccesspolicies endpoint.



1. Save the contents into a file as .JSON (optional)

***Task 2: Updating a CA Policy***

1. Extract the Policy from the Backup or using the GET Operation

**Below is the sample extract**

{

"displayName": "CalebDemo",

"state": "disabled",

"sessionControls": null,

"conditions": {

"userRiskLevels": [],

"signInRiskLevels": [],

"clientAppTypes": [],

"platforms": null,

"locations": null,

"times": null,

"deviceStates": null,

"applications": {

"includeApplications": [

"00000002-0000-0ff1-ce00-000000000000"

],

"excludeApplications": [],

"includeAuthenticationContext": []

},

"users": {

"includeUsers": [

"None"

],

"excludeUsers": [],

"includeGroups": [],

"excludeGroups": [],

"includeRoles": [],

"excludeRoles": []

}

},

"grantControls": {

"operator": "OR",

"builtInControls": [

"mfa"

],

"customAuthenticationFactors": [],

"termsOfUse": []

}

}

1. Prep the Policy for the **PATCH** operation

2a. We Need to remove 4 Fields while preserving the entire policy

* **@odata.context**
* **id**
* **createdDateTime**
* **modifiedDateTime**

2b. update the required field.

In this case we need to update 2 things

* **IncludeApplications** (in our example – EXO **00000002-0000-0ff1-ce00-000000000000** )
* **builtInControls** to **block**
* **clientAppTypes** to **others**

Below is the example of the above policy being prepped for MFA.

{

"displayName": "CalebDemo",

"state": "disabled",

"sessionControls": null,

"conditions": {

"userRiskLevels": [],

"signInRiskLevels": [],

"clientAppTypes": [

"other"

],

"platforms": null,

"locations": null,

"times": null,

"deviceStates": null,

"applications": {

"includeApplications": [

"00000002-0000-0ff1-ce00-000000000000"

],

"excludeApplications": [],

"includeAuthenticationContext": []

},

"users": {

"includeUsers": [

"None"

],

"excludeUsers": [],

"includeGroups": [],

"excludeGroups": [],

"includeRoles": [],

"excludeRoles": []

}

},

"grantControls": {

"operator": "OR",

"builtInControls": [

"block"

],

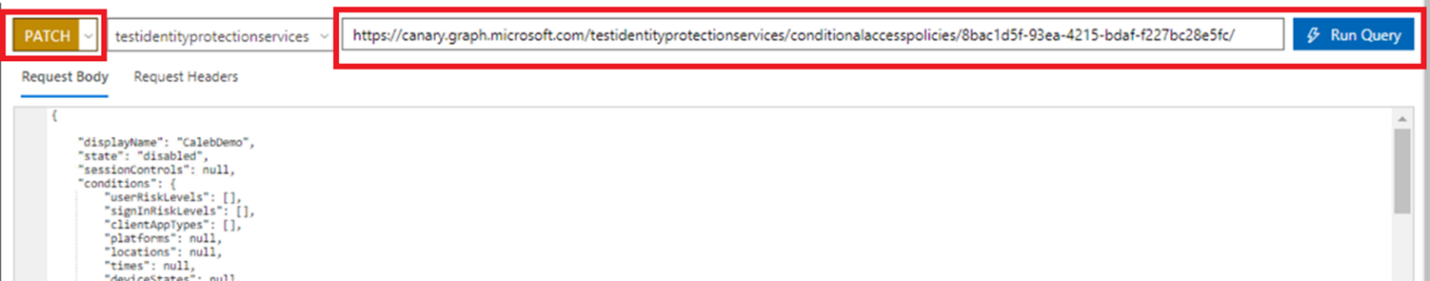
"customAuthenticationFactors": [],

"termsOfUse": []

}

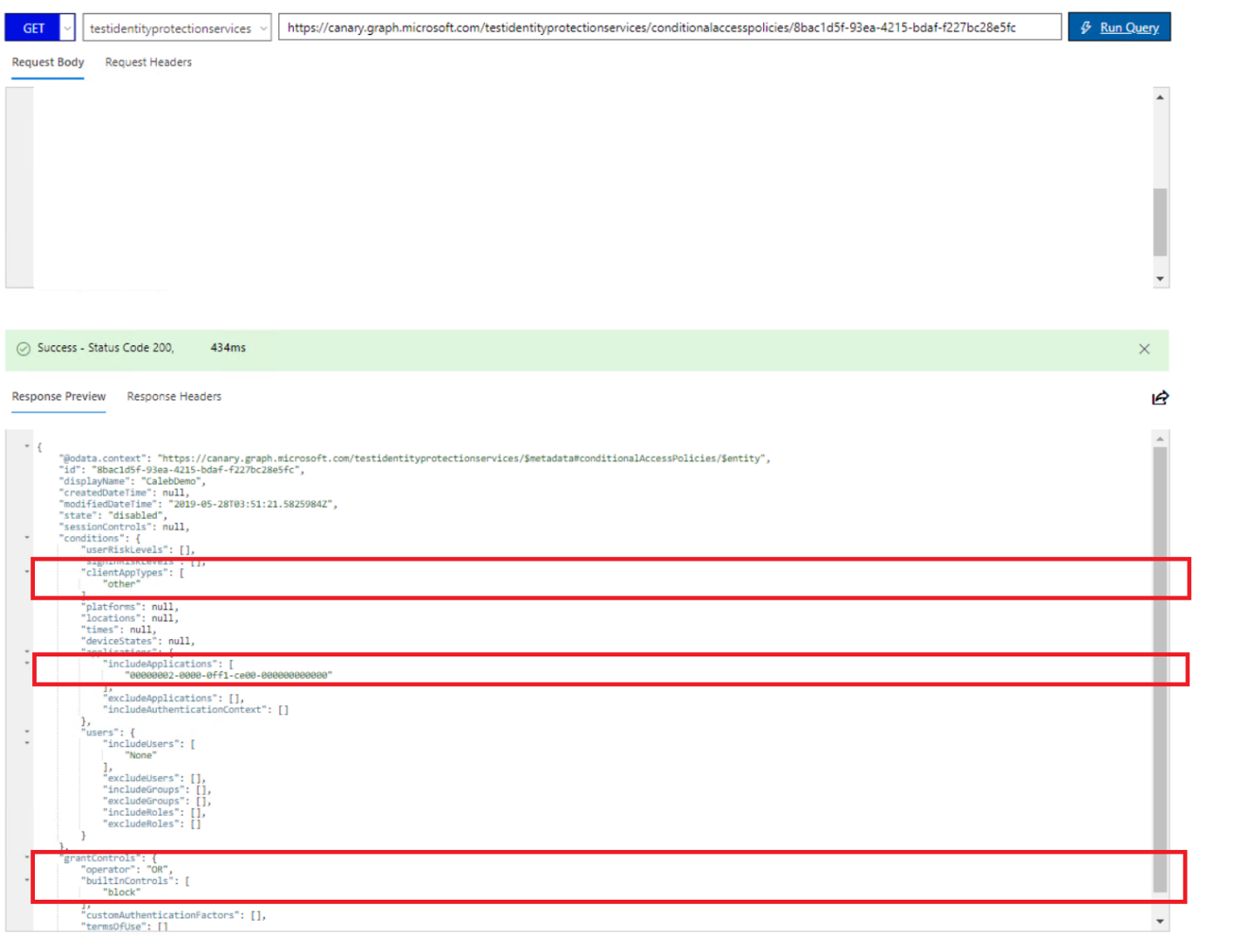
}

1. Perform a **PATCH** Operation with above Policy. Copy the content of the Policy in the **RequestBody** and click on **RunQuery** button



If the operation was successful you will get HTTP 204 return code

1. Verify in the Azure AD Conditional Access Policy Console or by running the GET query.



# Appendix

Below is the list of common queries that be used to identify the dependent resources.

## ## Applications

Applications supported for Conditional Access ( Excluding 3rd Party SaaS apps and Azure AD Application Proxy)

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/technical-reference#microsoft-cloud-applications>

**Using Graph**

https://canary.graph.microsoft.com/beta/serviceprincipals?$select=AppDisplayName,appid

https://canary.graph.microsoft.com/beta/serviceprincipals?$filter=startswith(displayName,'Microsoft Intune')

**Using PowerShell**

Get-MsolServicePrincipal | ft DisplayName, AppPrincipalId -AutoSize

## ## Directory Roles

Role Definition : <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles>

**Using Graph**

https://canary.graph.microsoft.com/beta/directoryroles

**Using PowerShell**

Get-AzureADDirectoryRoleTemplate | Where-Object {$\_.DisplayName -eq "B2C IEF Keyset Administrator"}

## ## Group

**Using Graph**

https://canary.graph.microsoft.com/beta/groups?$select=DisplayName,id

**PowerShell**

Get-MsolGroup | ft objectid, signinname, displayname

**Note:** There might be a schema change soon causing some of the fields to have a different name, you might need to modify that if you have an older export of the CA Policies JSON.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2018 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.