Control Access to Power Apps and Power Automate with Azure AD Conditional Access Policies

By Developer Support

Published: 2020-05-09 · Archived: 2026-04-05 22:34:53 UTC

May 9th, 2020

❤️ 3 reactions

Cloud Solution Architects

App Dev Manager Roger Lamb and Dev Consultant Adam Toth detail how to control access to Power Apps and Power Automate using Azure AD Conditional Access Policies.

UPDATE 9/9/2022: Microsoft Product Support requested an update to this article to indicate that blocking only one of these products at a time could introduce various issues and is not supported. If you are going to use this policy to block Power Platform features, make sure you block both Power Automate and Power Apps at the same time. The reason is that some features of one application are dependencies for another, for example some Power Automate UI features require Power Apps functionality under the cover to work (Solutions, Dataverse, etc), and those UI operations may fail if you block Power Apps but try and use the Power Automate Portal.

Overview

As companies begin adoption of Microsoft 365 citizen developer platforms, such as Microsoft Power Apps and Power Automate (Flow), there is a growing demand to control access to these platforms. Governance and administration best-practices are paramount to ensuring only authorized users have access to critical systems. When combined with multiple organizations and users, varying levels of access, and the need for user-level permissions, maintaining Power Apps and Power Automate solutions may be a challenge.

Each Microsoft 365 tenant has a default environment provisioned for use with PowerApps and Power Automate, where any licensed user can contribute Power Apps and Power Automate workflows immediately. There is currently no mechanism to restrict the Maker role (i.e. who can create Power Apps and Power Automate workflows) in the Default environment, so many companies look for the ability to limit access to these systems

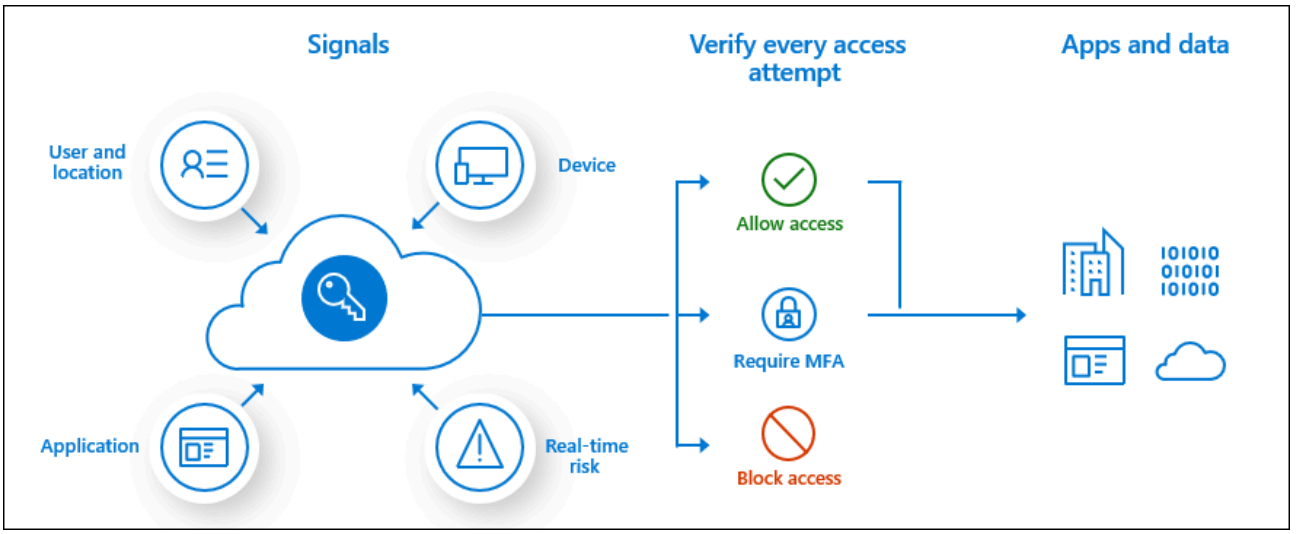
until a fully-featured governance and administration process is put in place, or until the platform has been vetted through pilot rollouts to limited numbers of users.

Fortunately, this can easily be achieved using Microsoft Azure Active Directory (AD) Conditional Access Policies.

About Conditional Access Policies

Conditional Access Policies in Azure AD are a flexible way for administrators to control access to Microsoft-based services for end users. The diagram below illustrates how to wire up Conditional Access policies to restrict access to end users for both PowerApps and Power Automate.

Conditional Access policies at their simplest form are if-then statements: if a user wants to access a resource, then they must complete an action.



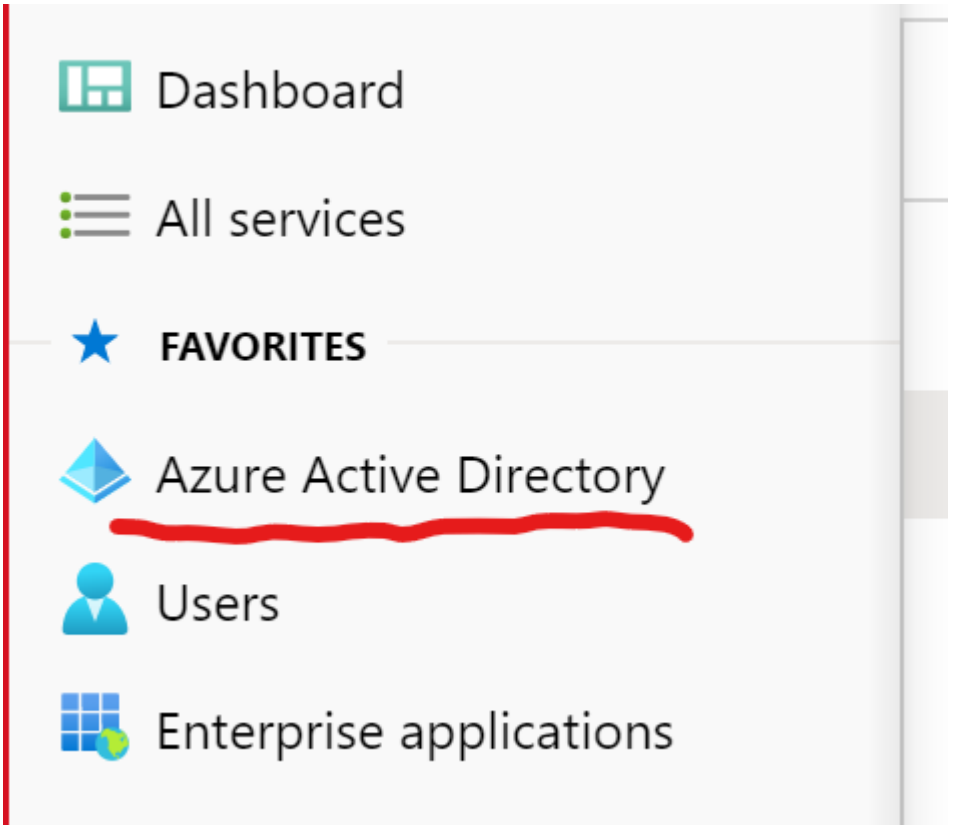
Find out more about Conditional Access (CA) policies here.

Conditional Access Policies are available to tenants that subscribe to Azure AD Premium capabilities, including Azure AD Premium P1, P2, or Microsoft 365 Business license.

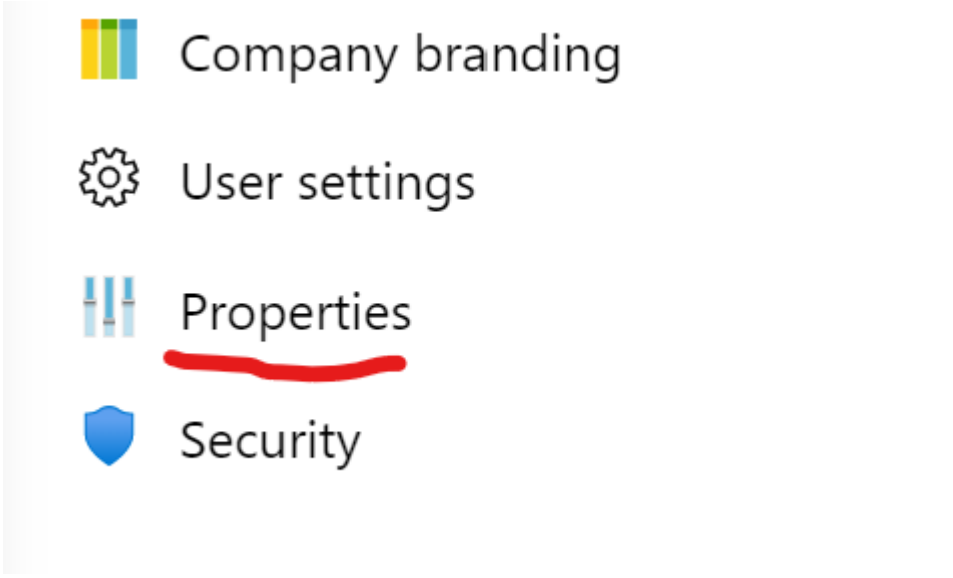
For more information on comparisons of Azure Active Directory P1 and P2 licenses as well as pricing please review the documentation here.

Create a Conditional Access Policy

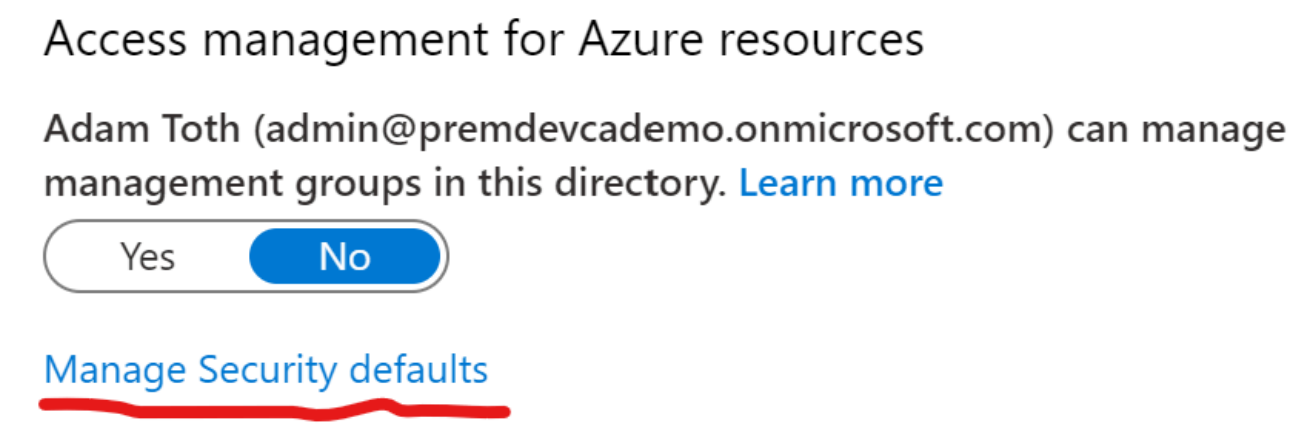
To create a Conditional Access Policy, first access the Azure portal and navigate to the Azure Active Directory blade. Access this through portal.azure.com or from the Admin Center links in the Office365 Administration Center.

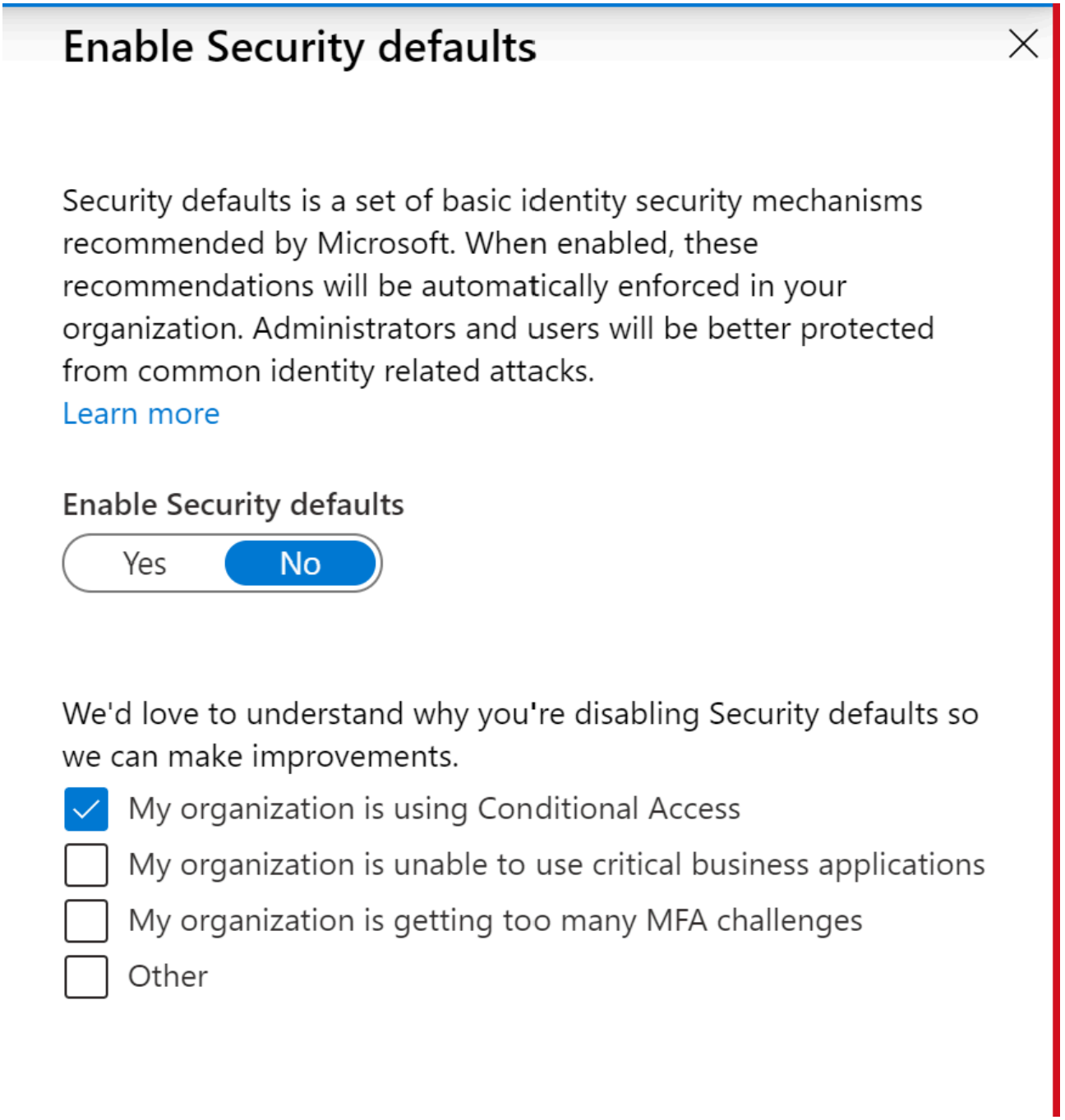


Once in the Azure AD management blade, select **Properties**.



On the Properties screen, select the **Manage Security Defaults** option at the bottom.


Access management for Azure resources
Adam Toth (admin@premdevcademo.onmicrosoft.com) can manage management groups in this directory. Learn more
Yes
No
Manage Security defaults

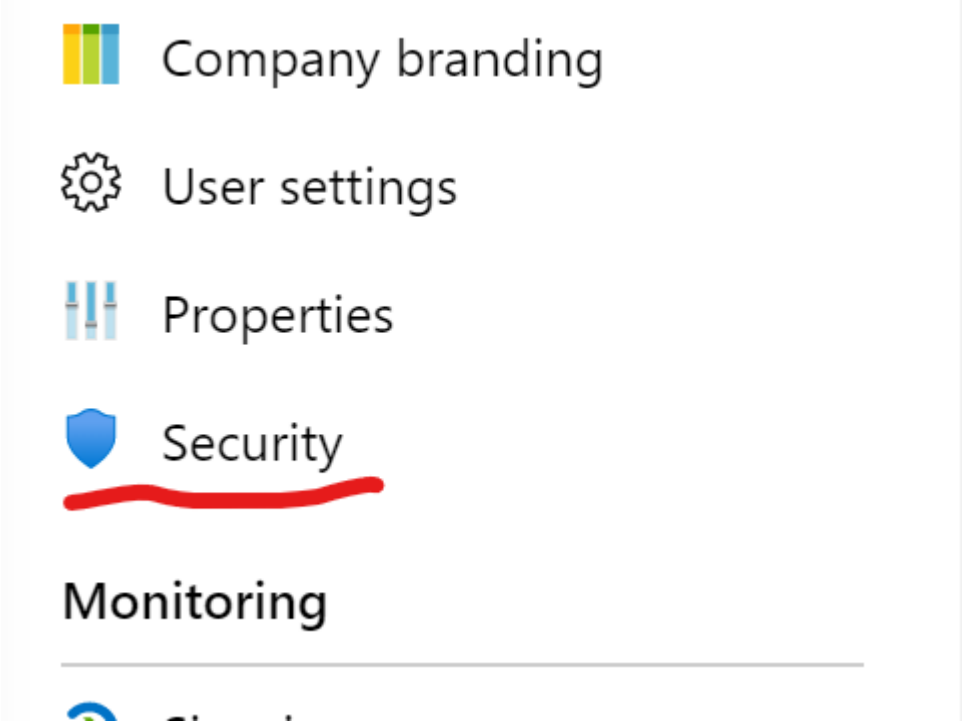

Enable Security defaults
Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.
Learn more
Enable Security defaults
Yes
No
We'd love to understand why you're disabling Security defaults so we can make improvements.
My organization is using Conditional Access
My organization is unable to use critical business applications
My organization is getting too many MFA challenges
Other

Make sure that **Enable Security defaults** is **off** in order to use Conditional Access Policies.

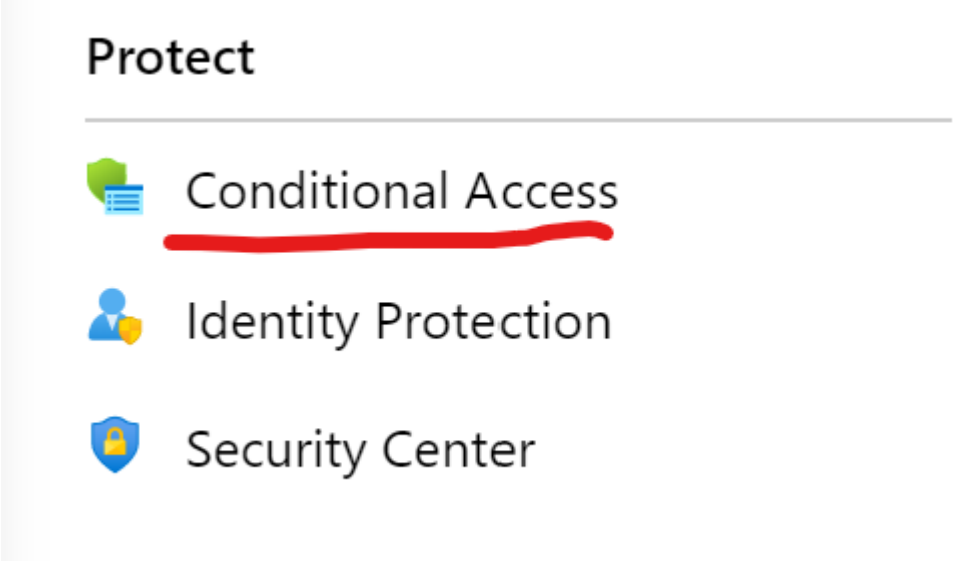
For more information about Security Defaults, see this link.

Once the defaults are turned off (they may already be off if Conditional Access has been used for other purposes, such as MFA and location-based access policies), the policy for accessing PowerApps and Power Automate (Flow) can be configured

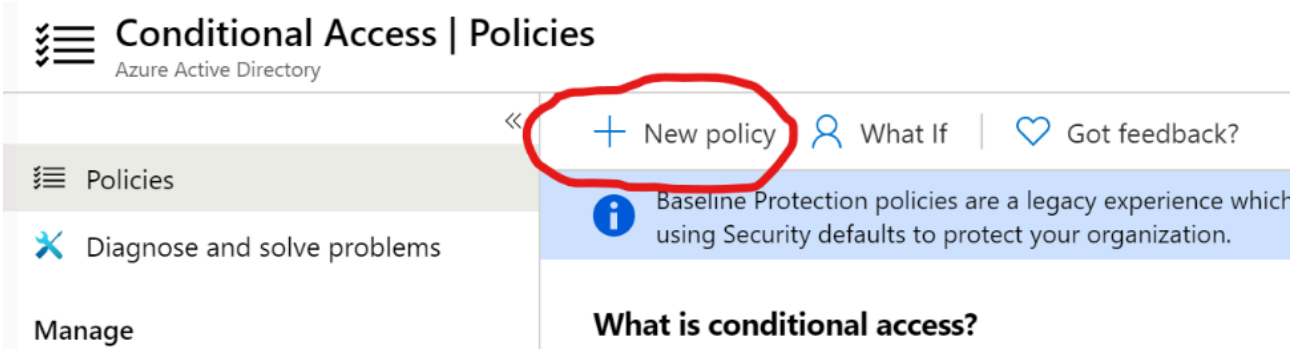
Return to the **Azure Active Directory** blade and select **Security**.



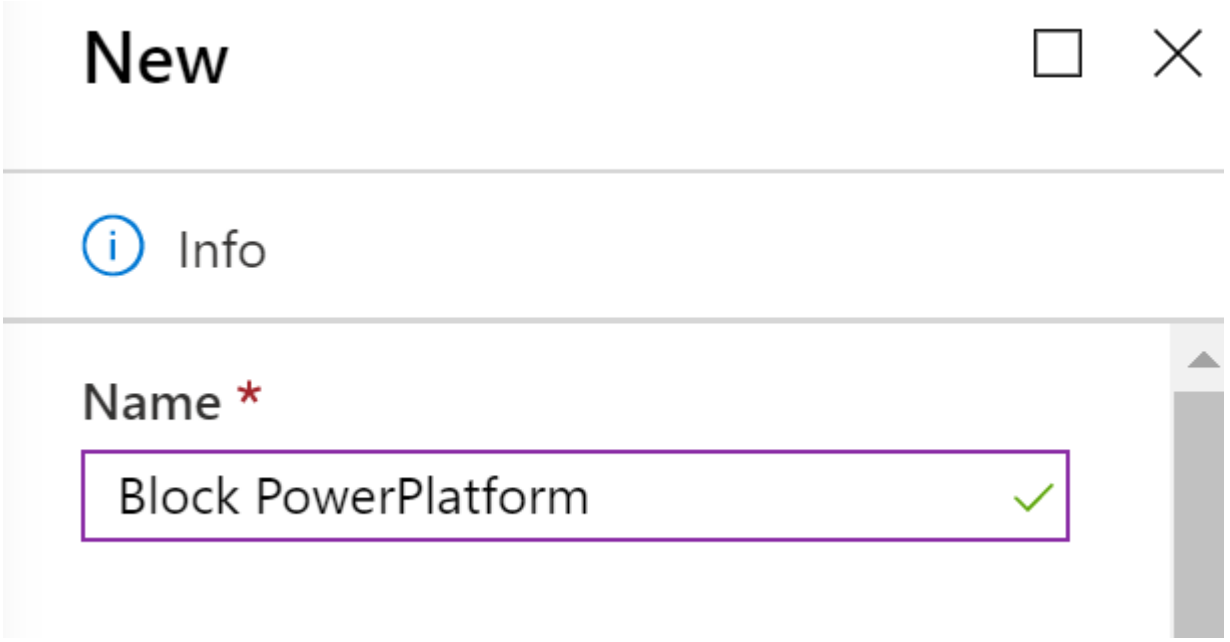
In the next blade, select **Conditional Access**.



In the next screen, click the **New policy** button to create a new policy:

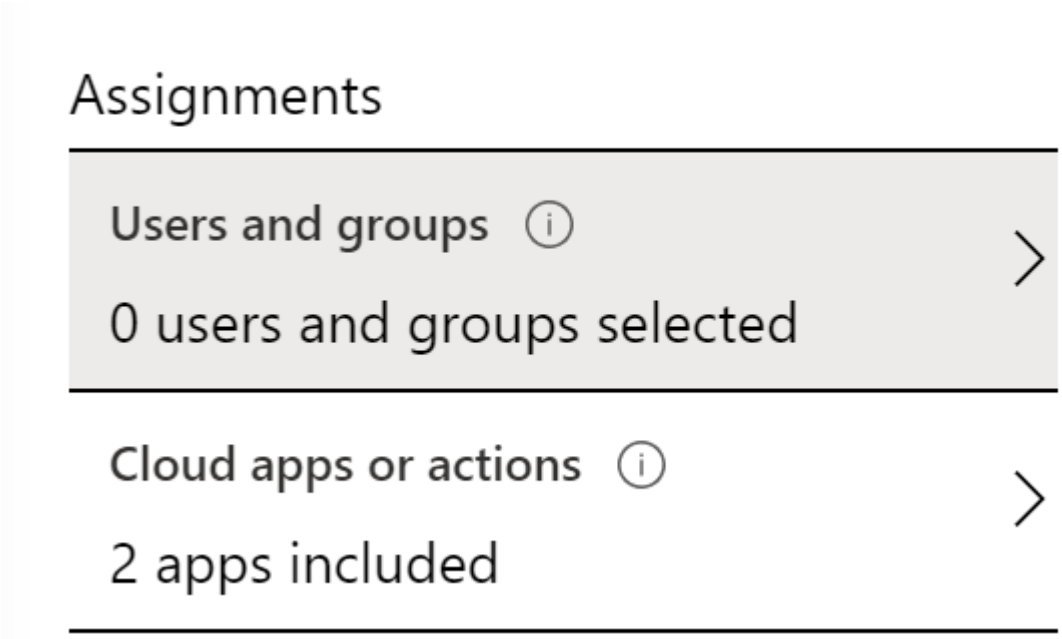


Name the new policy:



To configure a new Conditional Access Policy, 1) Define who/what the policy applies to, and 2) Define what actions to take for anything that matches Step 1.

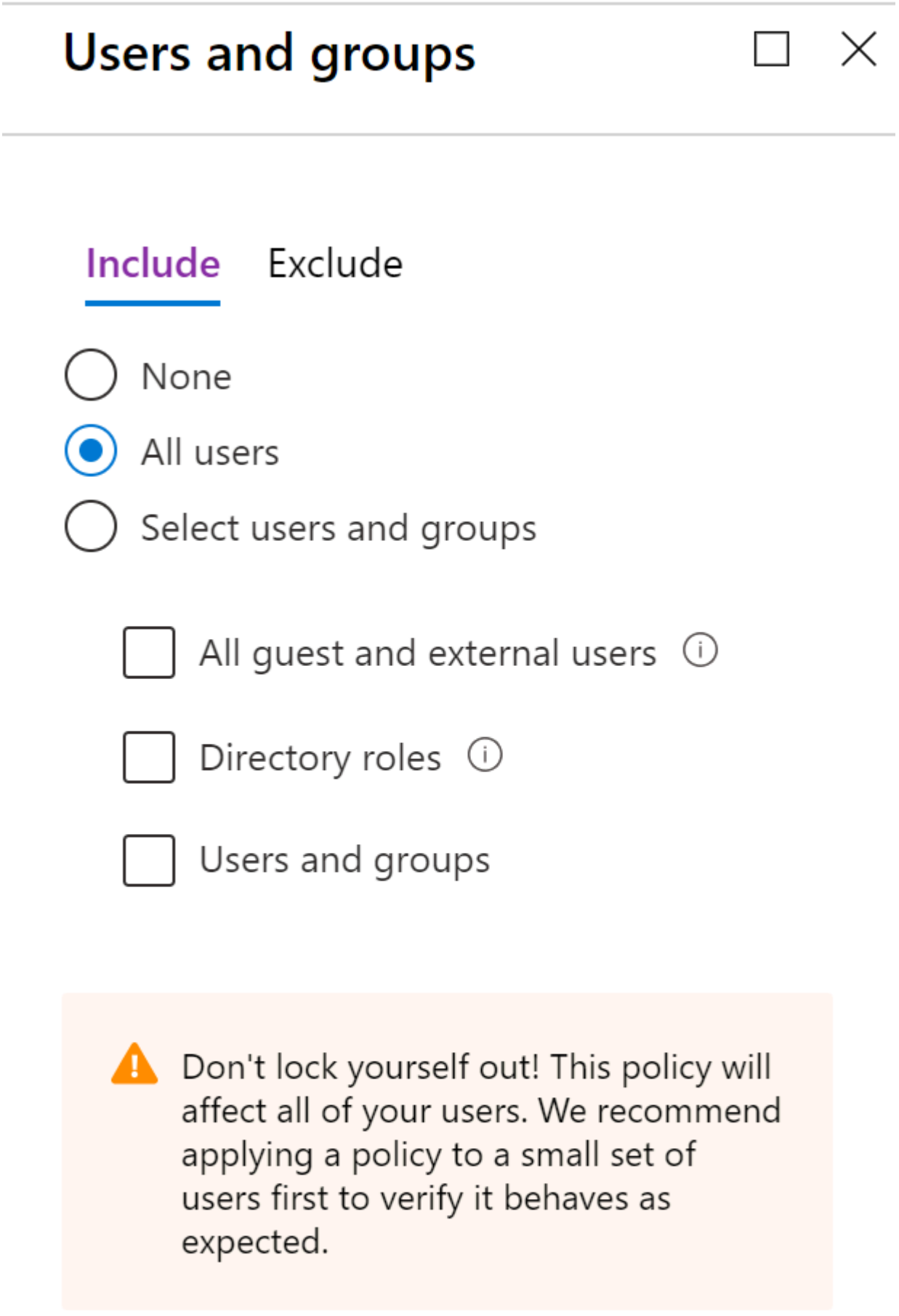
Step 1. Configure the users that this new policy applies to. Under **Assignments**, select **Users and Groups**.



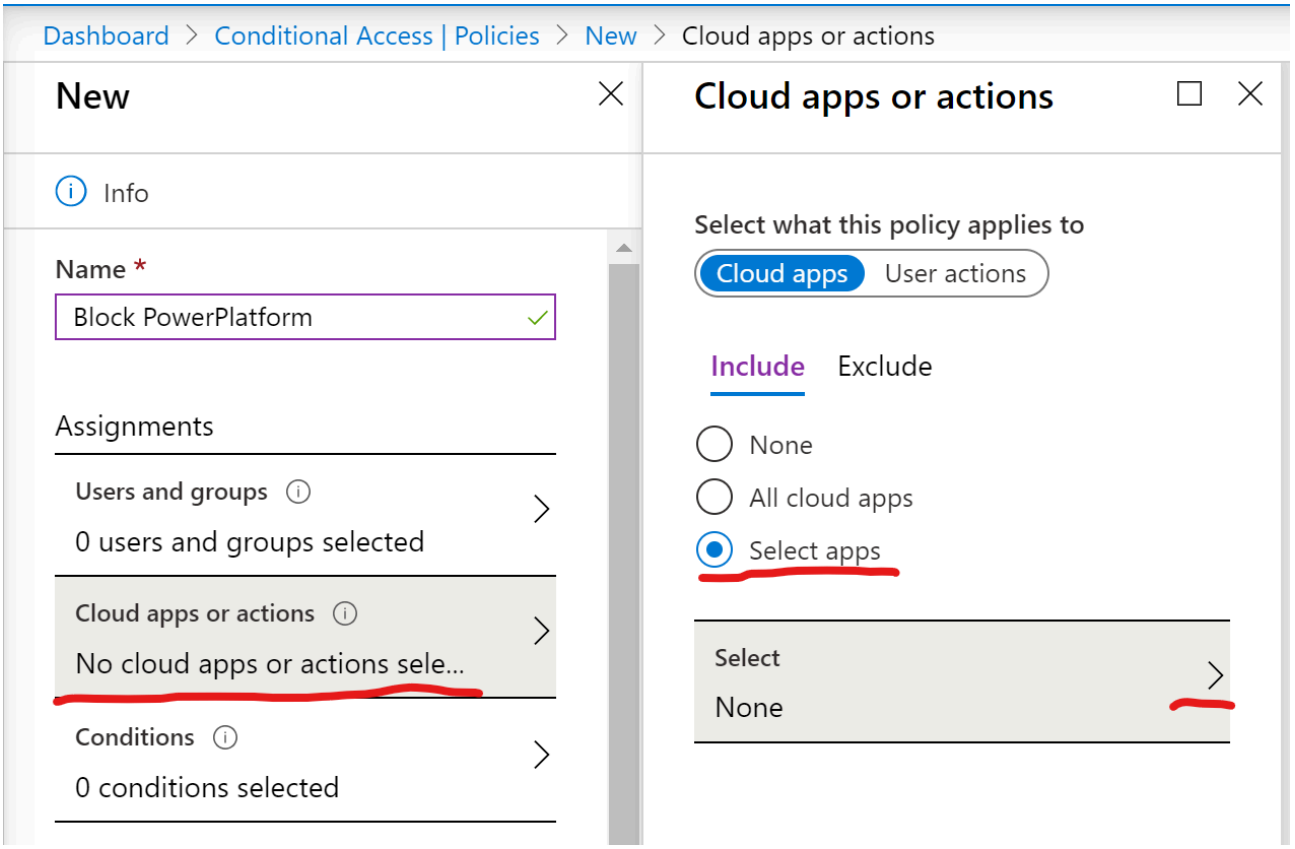
Select which users and groups to **Include** and **Exclude** from the new policy. In the following example, access to PowerApps and Flow is blocked for most users and is enabled only for **Pilot** users.

Since the new policy is intended to block access to most users, for the **Include** setting, select **All Users and Groups**, and for the **Exclude** setting select any desired pilot users and any Power Platform services administrators that need to have access (and any break-glass accounts).

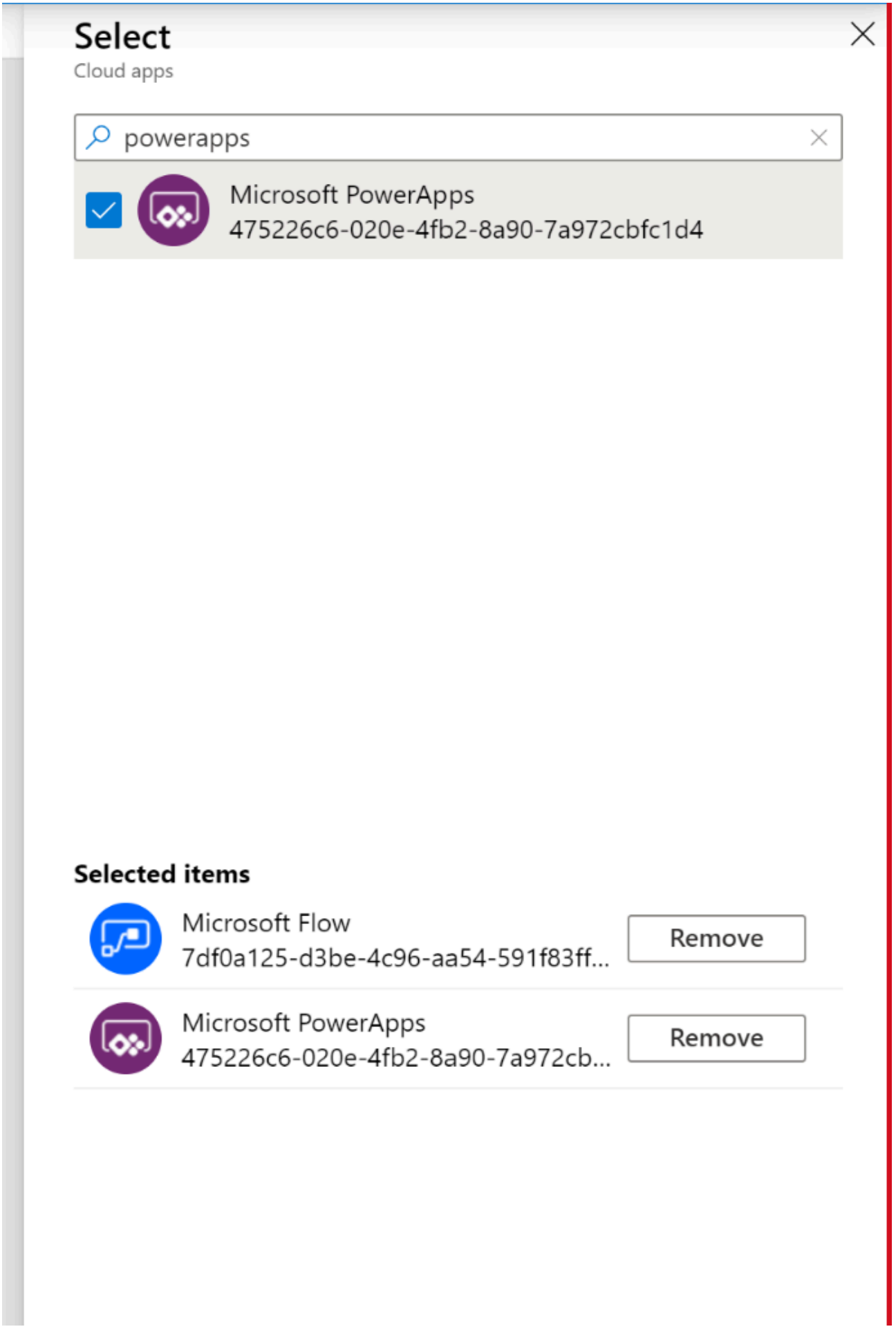
IMPORTANT NOTE: Be careful here to avoid locking out administrator. Check out this guide for best practices on configuring CA policies, and this guide for Block Access and exclusions.

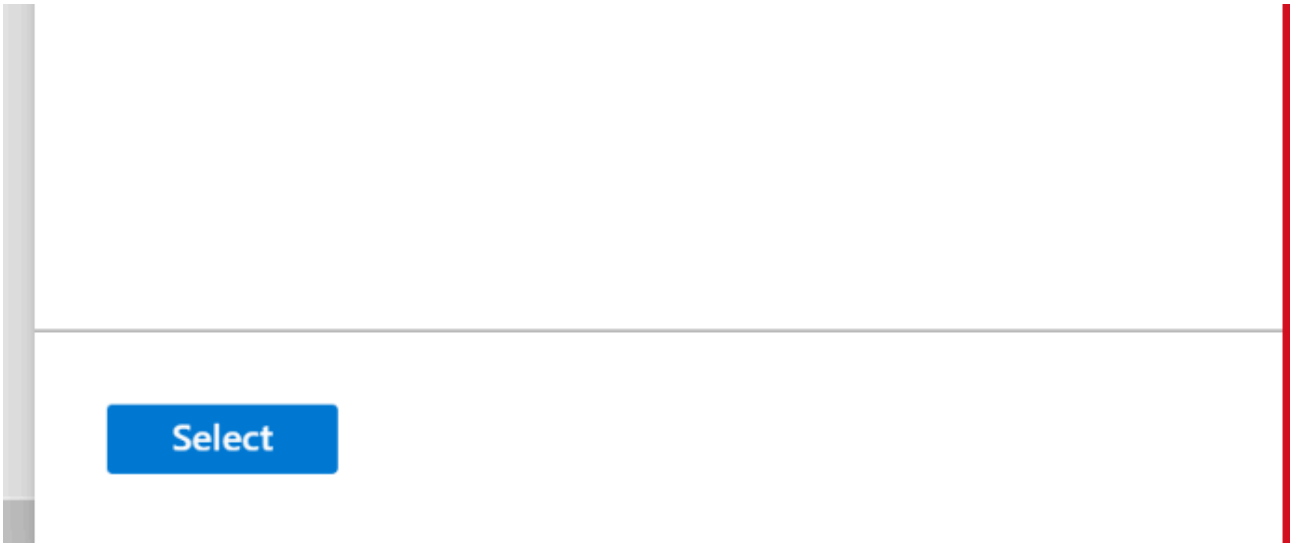

Users and groups
Include
Exclude
None
All users
Select users and groups
All guest and external users
Directory roles
Users and groups
Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

Once the users have been configured, select the **Cloud Apps** that the new policy will apply to.

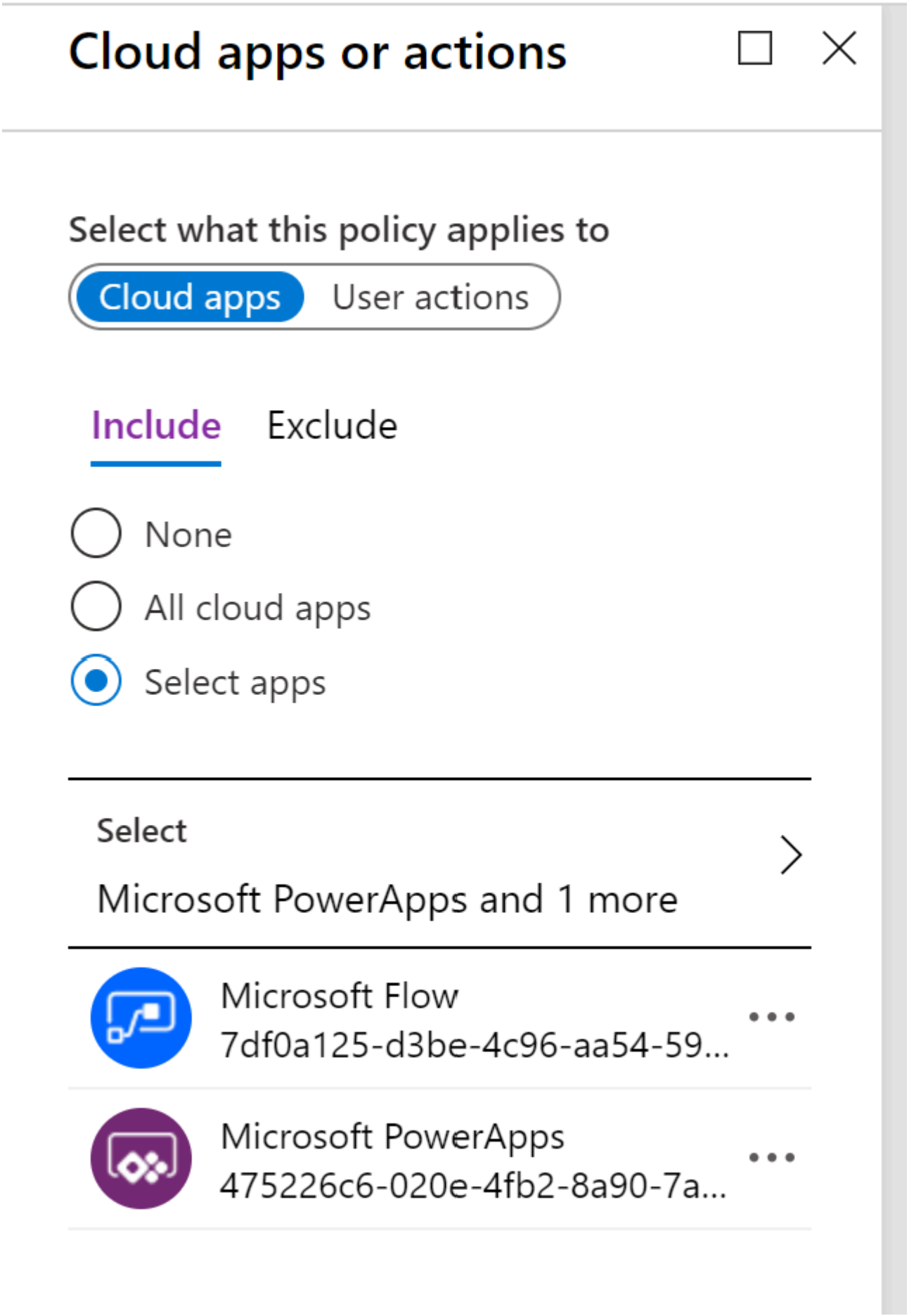


Click **Select apps** and then the arrow to select. In the search bar on the following screen, look first for **PowerApps**, and check it to select it, then search for **Microsoft Flow**, and select it as well. Both items should show as selected.


Select
Cloud apps
powerapps
Microsoft PowerApps
475226c6-020e-4fb2-8a90-7a972cbfc1d4
Selected items
Microsoft Flow
7df0a125-d3be-4c96-aa54-591f83ff...
Remove
Microsoft PowerApps
475226c6-020e-4fb2-8a90-7a972cb...
Remove

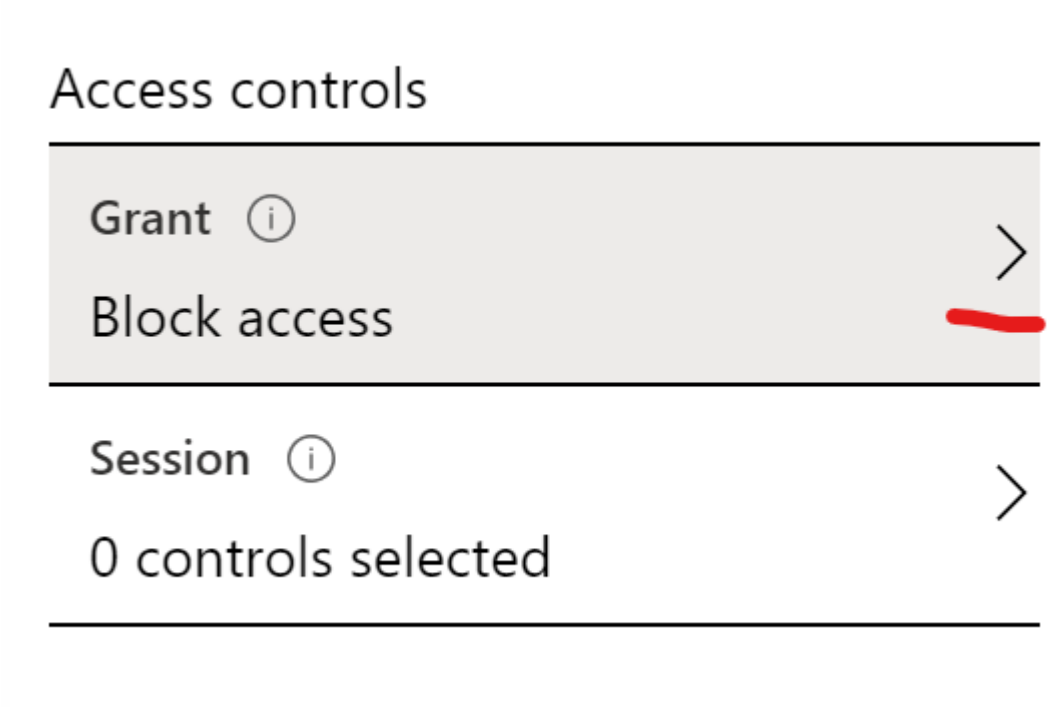


Click **Select** at the bottom of the screen. The two apps should now appear as part of the policy.

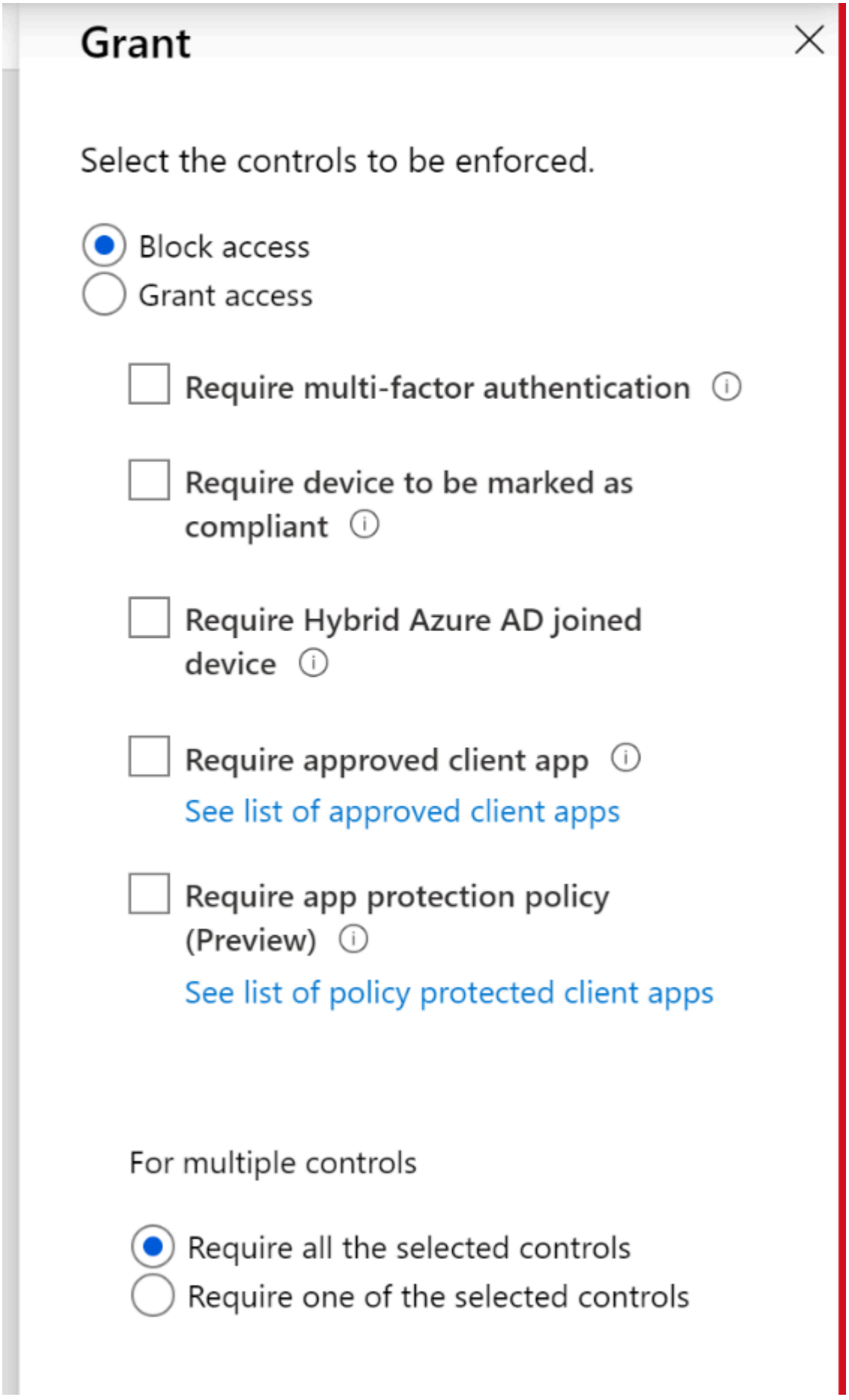

Cloud apps or actions
Select what this policy applies to
Cloud apps
User actions
Include
Exclude
None
All cloud apps
Select apps
Select
Microsoft PowerApps and 1 more
Microsoft Flow
7df0a125-d3be-4c96-aa54-59...
Microsoft PowerApps
475226c6-020e-4fb2-8a90-7a...

Step 2. Once the users have been configured, the next step to create the new policies is to define what to do when the conditions are met. In this case, the purpose of the policy is to block access to these apps for most users but allow access for pilot users and admins.

Select the **Grant** option under **Access controls** and click the arrow.

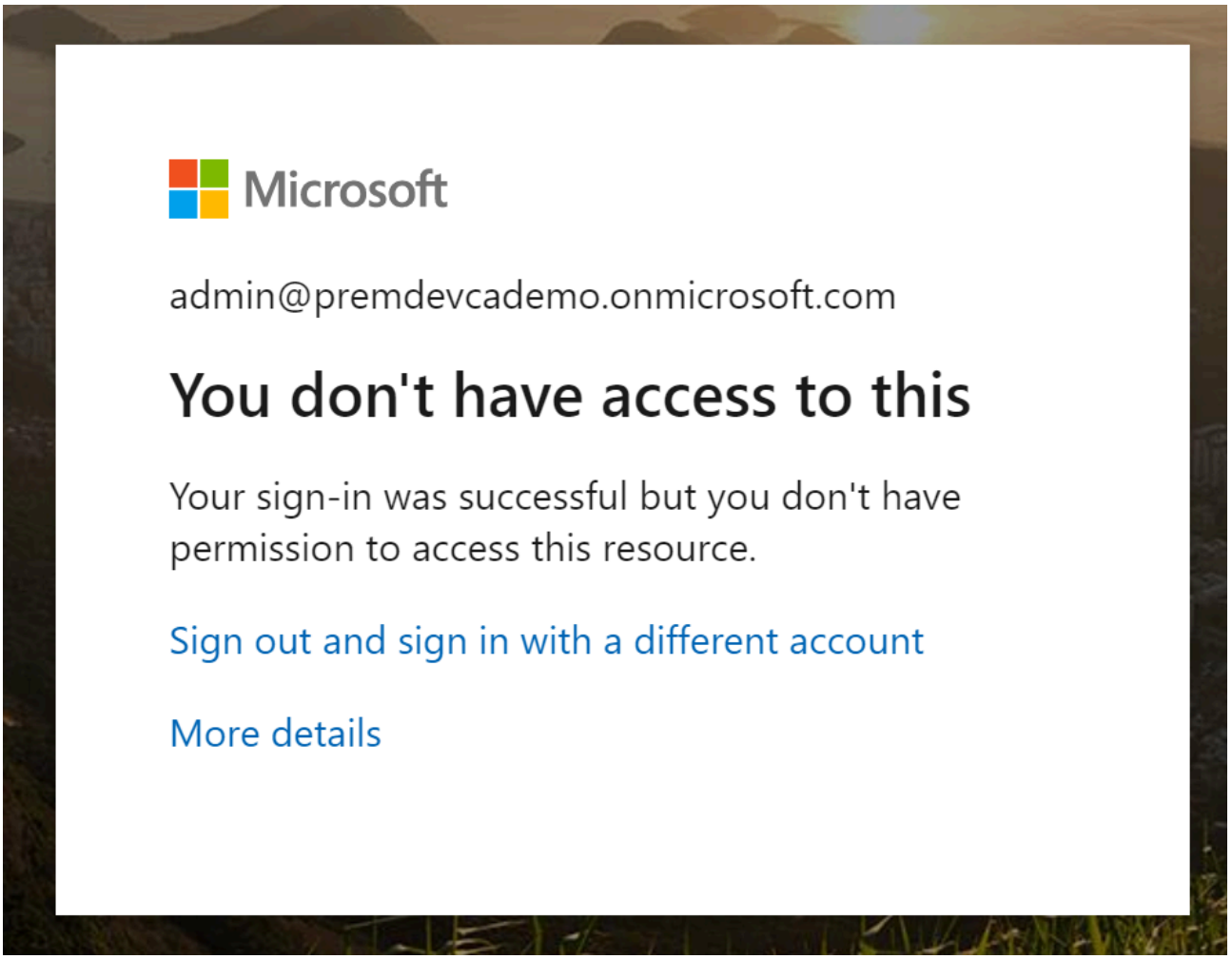


In the **Grant** screen, select **Block access**.


Grant
Select the controls to be enforced.
Block access
Grant access
Require multi-factor authentication
Require device to be marked as compliant
Require Hybrid Azure AD joined device
Require approved client app
See list of approved client apps
Require app protection policy (Preview)
See list of policy protected client apps
For multiple controls
Require all the selected controls
Require one of the selected controls

The policy is now configured and ready for deployment. To activate the policy, select **On** under **Enable Policy**.

Once the new policy is on, if any users try and access PowerApps or Power Automate (Flow), they will receive the following message upon logging in:



Summary

With just a few quick steps using the Azure AD Conditional Access Policy, it is easy to limit access to PowerApps and Power Automate. This quick fix allows time for companies to evaluate the platform, experiment with pilot

users, and take the time to implement governance and administration best practices.

Additional resources for Power Platform governance and administration topics:

- Power Platform CoE Starter Kit
- Power Platform Governance White Paper

Category

Topics

Author

Cloud Solution Architects

Microsoft Developer Support helps software developers rapidly build and deploy quality applications for Microsoft platforms.
