

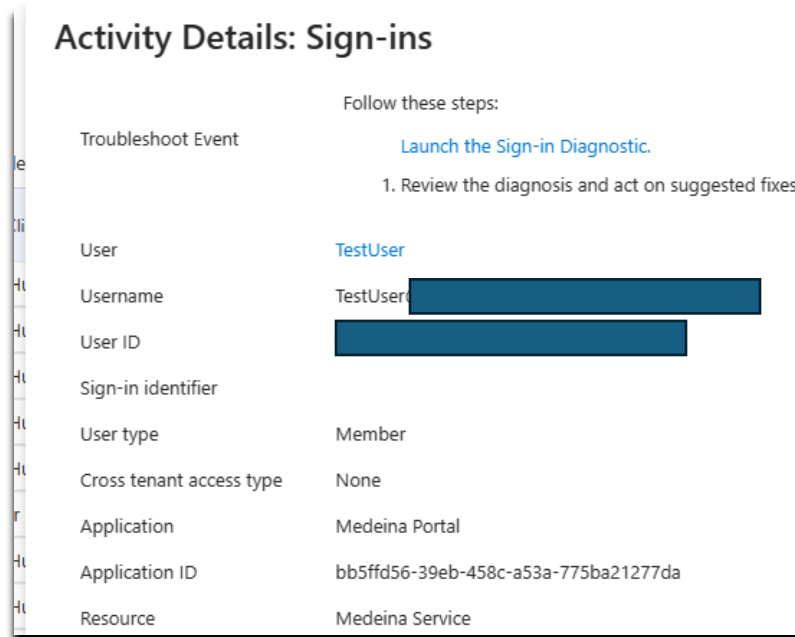
## For Early Access Preview Program Only - How to Control / Restrict Access to the Security Copilot “Stand Alone” Portal (Model is slated to change for General Availability)

### 1) **Create a Targetable Service Principal via Powershell**

\*\*Ensure proper permissions and current scope is selected when connecting to

```
new-mgserviceprincipal -appid bb5ffd56-39eb-458c-a53a-775ba21277da
```

You can verify this App ID in Entra ID by reviewing a sign-in log into “Medeina Portal”



**Activity Details: Sign-ins**

Follow these steps:

Troubleshoot Event [Launch the Sign-in Diagnostic.](#)

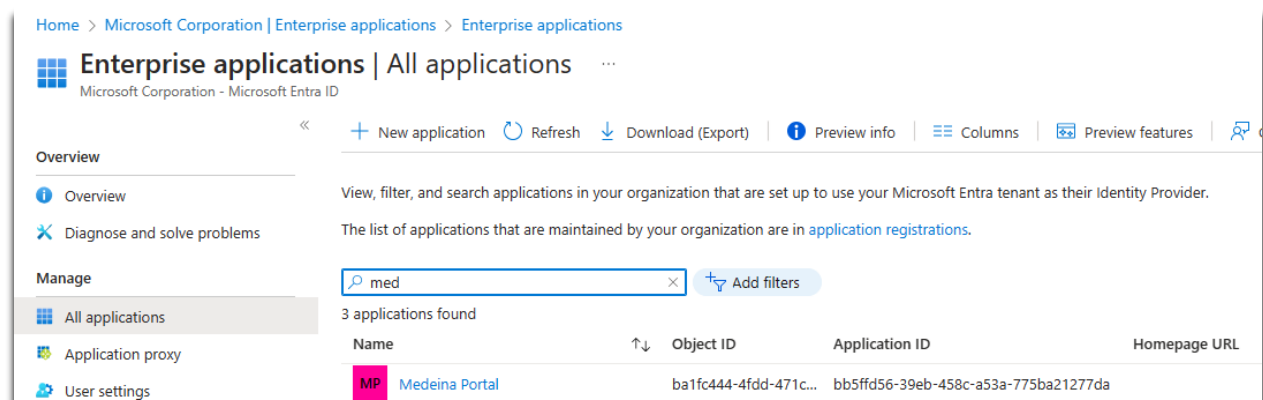
1. Review the diagnosis and act on suggested fixes.

User	TestUser
Username	TestUser
User ID	
Sign-in identifier	
User type	Member
Cross tenant access type	None
Application	Medeina Portal
Application ID	bb5ffd56-39eb-458c-a53a-775ba21277da
Resource	Medeina Service

Additional info on MS Graph Powershell.

[Migrate from Azure AD PowerShell to Microsoft Graph PowerShell. | Microsoft Learn](#)  
[Connect-MgGraph \(Microsoft.Graph.Authentication\) | Microsoft Learn](#)

After creating the SP via powershell, you will see it here under Enterprise Apps in Entra.



Home > Microsoft Corporation | Enterprise applications > Enterprise applications

## Enterprise applications | All applications

Microsoft Corporation - Microsoft Entra ID

« + New application Refresh Download (Export) Preview info Columns Preview features

**Overview**

Overview View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider. The list of applications that are maintained by your organization are in [application registrations](#).

**Manage**

med Add filters

3 applications found

Name	Object ID	Application ID	Homepage URL
MP Medeina Portal	ba1fc444-4fdd-471c...	bb5ffd56-39eb-458c-a53a-775ba21277da	

For Early Access Preview Program Only - How to Control / Restrict Access to the Security Copilot “Stand Alone” Portal (Model is slated to change for General Availability)

2) Create the Custom Security Attribute in Entra ID.

Info here on Custom Security Attributes.

[What are custom security attributes in Microsoft Entra ID? \(Preview\) | Microsoft Learn](#)

[Add or deactivate custom security attribute definitions in Microsoft Entra ID \(Preview\) | Microsoft Learn](#)

\*\* Must have the appropriate roles to enable, create, and assign attributes

Home > Roles and administrators | All roles

Microsoft Corporation - Microsoft Entra ID

« + New custom role Delete custom role Download assignments Refresh Preview features Got feedback?

Get just-in-time access to a role when you need it using PIM. Learn more about PIM →

① Your Role: Global Administrator and 2 other roles

Administrative roles  
Administrative roles are used for granting access for privileged actions in Microsoft Entra ID. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Microsoft Entra ID not related to application configuration. [Learn more.](#)

[Learn more about Microsoft Entra ID role-based access control](#)

attribute Add filters

Role	↑↓	Description	Privileged	↑↓	Ass...↑↓	Type
<input type="checkbox"/> Attribute Assignment Administrator		Assign custom security attribute keys and values to supported Microsoft Entra objects.			1	Built-in
<input type="checkbox"/> Attribute Assignment Reader		Read custom security attribute keys and values for supported Microsoft Entra objects.			0	Built-in
<input type="checkbox"/> Attribute Definition Administrator		Define and manage the definition of custom security attributes.			1	Built-in

a) Create Attribute Set

New attribute set

Add an attribute set to group and manage related custom security attributes. All custom security attributes must be a part of an attribute set. [Learn more](#)

Attribute set name \* ⓘ

Description ⓘ

Maximum number of attributes ⓘ

Microsoft Corporation | Custom security attributes

Microsoft Entra ID

« + Add attribute set Refresh Got feedback?

Search attribute set name

Attribute set name	↑↓	Description	Maximum number of attributes
<a href="#">RestrictAccessToSecurityCopilot</a>		RestrictAccessToSecurityCopilot	25

## For Early Access Preview Program Only - How to Control / Restrict Access to the Security Copilot “Stand Alone” Portal (Model is slated to change for General Availability)

### b) Add New Attribute to the set

« + Add attribute - Deactivate attribute Refresh Got feedback?

Active attributes  
Deactivated attributes  
Roles and administrators

### Add custom security attributes

Custom security attributes are key-value pairs that you define and assign to Microsoft Entra objects, such as users or applications. [Learn more](#)

- 1. Define attributes**  
Add custom security attributes to your directory.
- 2. Manage attributes**  
Specify who can define and assign custom security attributes.
- 3. Assign attributes**  
Assign custom security attributes to Microsoft Entra objects for your scenario.

[Add attribute](#)

### New attribute ...

Add a custom security attribute (key-value pair) to your directory that you can later assign to Microsoft Entra objects, such as users or applications. [Learn more](#)

Attribute name \* ⓘ

Description ⓘ

Data type \*

Allow multiple values to be assigned ⓘ ☐ Yes ☒ No

Only allow predefined values to be assigned ⓘ ☐ Yes ☒ No

Predefined values ⓘ

+ Add value

Value	Is active?
No results	

Below example only:

### RestrictAccess ...

Add a custom security attribute (key-value pair) to your directory that you can later assign to Microsoft Entra objects, such as users or applications. [Learn more](#)

Attribute name ⓘ

Description ⓘ

Data type

Allow multiple values to be assigned ⓘ ☐ Yes ☒ No

Only allow predefined values to be assigned ⓘ ☐ Yes ☒ No

Predefined values ⓘ

+ Add value

Value	Is active?
No results	

### 3) Target the App with a Conditional Access Policy.

a) Choose to Exclude or Include based upon your Conditional Access approach.

**For Early Access Preview Program Only - How to Control / Restrict Access to the Security Copilot “Stand Alone” Portal (Model is slated to change for General Availability)**

The screenshot shows the configuration page for a Conditional Access policy named "CA004-Block-Security-Copilot-Portal". The page is divided into several sections:

- Header:** "CA004-Block-Security-Copilot-Portal" with a menu icon. Below it, "Conditional Access policy".
- Actions:** "Delete" (trash icon) and "View policy information" (eye icon).
- Descriptions:**
  - Left: "Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)"
  - Right: "Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)"
- Name:** A text box containing "CA004-Block-Security-Copilot-Portal".
- Assignments:**
  - Users:** A dropdown menu showing "All users included and specific users excluded".
  - Target resources:** A section with a "Configured" link.
  - Conditions:** A section with an information icon.
- Include/Exclude:** Two tabs. The "Exclude" tab is selected.
  - Select the users and groups to exempt from the policy:**
    - ☐ Guest or external users
    - ☐ Directory roles
    - ☒ Users and groups
  - Select excluded users and groups:** A section showing "1 user".

- b) Under Target Resources, Select Cloud Apps, Include “Select Apps”, Select Edit Filter and toggle “Yes” for configure in Edit Filter Menu. Choose Attribute, and complete Operator and Values. Select the attributes created.

## For Early Access Preview Program Only - How to Control / Restrict Access to the Security Copilot “Stand Alone” Portal (Model is slated to change for General Availability)

### CA004-Block-Security-Copilot-Portal

Conditional Access policy

[Delete](#) [View policy information](#)

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

Name \*  
CA004-Block-Security-Copilot-Portal

Assignments

Users [1](#)  
[All users included and specific users excluded](#)

Target resources [1](#)  
[Configured](#)

Conditions [1](#)  
[0 conditions selected](#)

Access controls

Grant [1](#)  
[Block access](#)

Control access based on all or specific network access traffic, cloud apps or actions. [Learn more](#)

Select what this policy applies to  
Cloud apps

**Include** Exclude

☐ None  
☐ All cloud apps  
☒ Select apps

Edit filter (Preview)  
[Configured](#)

Select  
[None](#)

## Edit filter (Preview)

[Configure](#) [1](#)

[Yes](#) [No](#)

Using custom security attributes you can use the rule builder or rule syntax text box to create or type Integer or Boolean will not be shown. [Learn more](#)

And/Or	Attribute	Operator
	<div><div></div><div>Choose an attribute</div></div>	
<a href="#">+ Add expression</a>	<div>RestrictAccessToSecurityCopilot</div> <div>RestrictAccess</div>	

Rule syntax [1](#)

## For Early Access Preview Program Only - How to Control / Restrict Access to the Security Copilot “Stand Alone” Portal (Model is slated to change for General Availability)

The screenshot shows the Azure portal interface for editing a Conditional Access policy. The left sidebar displays the policy details for 'CA004-Block-Security-Copilot-Portal', including its name, assignments (All users included and specific users excluded), target resources (Configured), conditions (0 conditions selected), access controls (Block access), and session controls (0 controls selected). The main pane shows the 'Edit filter (Preview)' window, which allows configuring filter rules. The 'Configure' button is set to 'Yes'. The rule builder shows a single rule with the attribute 'RestrictAccessToSecurityCopilot\_RestrictAccess', the operator 'Equals', and the value 'RestrictAccessTest'. The rule syntax is displayed as 'CustomSecurityAttribute.RestrictAccessToSecurityCopilot\_RestrictAccess -eq "RestrictAccessTest"'. The 'Add expression' button is visible below the rule builder.

**4)Test and Validate the CA policy;** Log in with user who is restricted or allowed depending on you configured the CA Policy

The screenshot shows the 'Activity Details: Sign-ins' window in the Azure portal. The window displays details for a failed sign-in attempt. The 'Basic info' tab is selected, showing the following information:

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Date		11/7/2023, 9:34:41 PM			
Request ID		6e540493-b460-42fd-bb14-87024fa30a01			
Correlation ID		9bcd0db-05d4-4f43-9f40-521b2bfefbe0			
Authentication requirement		Single-factor authentication			
Status		Failure			
Continuous access evaluation		No			
Original transfer method		None			
Sign-in error code		53003			
Failure reason		Access has been blocked by Conditional Access policies. The access policy does not allow token issuance.			
Additional Details		If this is unexpected, see the conditional access policy that applied to this request in the Azure Portal.			
Troubleshoot Event		Follow these steps: <a href="#">Launch the Sign-in Diagnostic.</a> 1. Review the diagnosis and act on suggested fixes.			
User		TestUser			
Username		TestUser			

**For Early Access Preview Program Only - How to Control / Restrict Access to the Security Copilot “Stand Alone” Portal (Model is slated to change for General Availability)**

Activity Details: Sign-ins

Basic info

Location

Device info

Authentication Details

Conditional Access

Report-only

...

Search

Policy Name	Grant Controls	Session Controls	Result
CA004-Block-Security-Copilot-...	Block		Failure