2 - Creating Custom Security Attributes in Microsoft Azure

Additional information about this functionality is available at: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/public-preview-conditional-access-filters-for-apps/ba-p/2365680

What is a "Custom Security Attribute"

Simply, the custom security attribute lets you stick a Post-It Note with anything you want written on it onto an Enterprise app, a user, or any other Azure or Azure AD resources. Once you've tagged it, you can use that tag for things like applying conditional access policies or exempting apps or users from the policy.

Why do you need a Custom Security Attribute

The most common need is to be able to tag an application that would not otherwise be able to have an Azure Conditional Access policy applied or exempted. It may be useful as a way to group a bunch of applications together to apply a specific policy too.

For Apple device administrators, the most common need is with the Jamf Connect application. Custom Security Attributes can be used to exempt the non-interactive background local password check performed periodically by Jamf Connect from being subject to a multi-factor authentication challenge. This eliminates false "failed" login attempts in Azure AD and users possibly being marked with risky sign-ins. [LINK: Modifying Jamf Connect to apply Azure Conditional Access Policies]

Manage a Custom Security Attribute (Preview)

Role permissions required

If you have not already, add the role permissions for your administrator user to include:

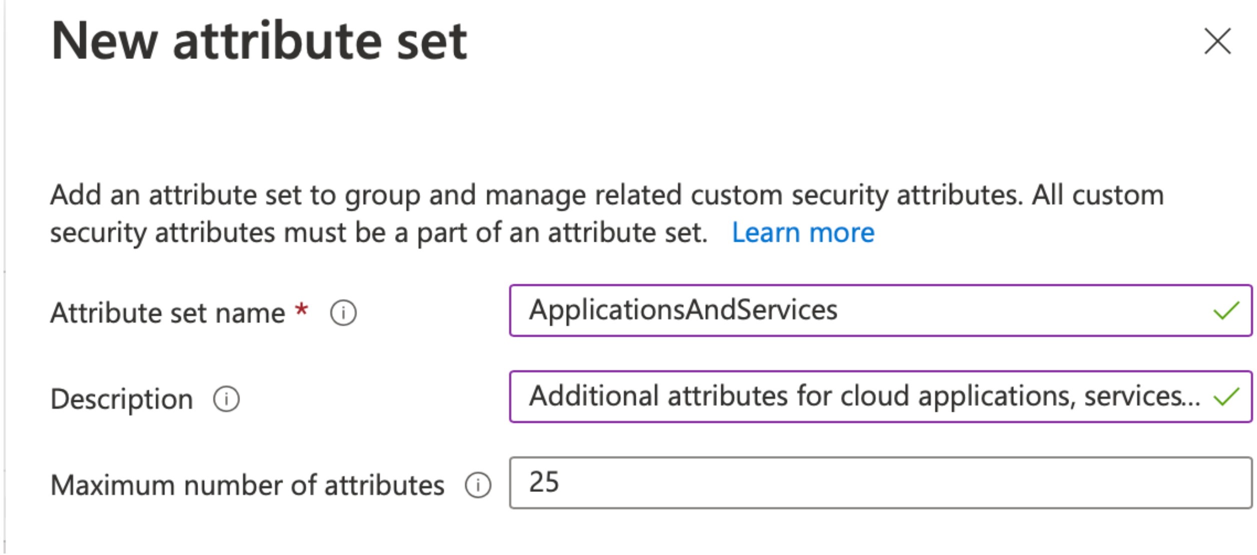
- Attribute assignment administrator
- Attribute assignment reader
- Attribute definition administrator
- Attribute definition reader

Navigate to Azure Active Directory → Roles and administrators. Your user must be given access to all four of the roles to continue. Global administrator role does not automatically come with these permissions.

Create a Custom Security Attribute Set

Reference: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/custom-security-attributes-overview

Navigate to Azure Active Directory → Custom security attributes (Preview). Select the option to "+ Add 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 * ApplicationsAndServices

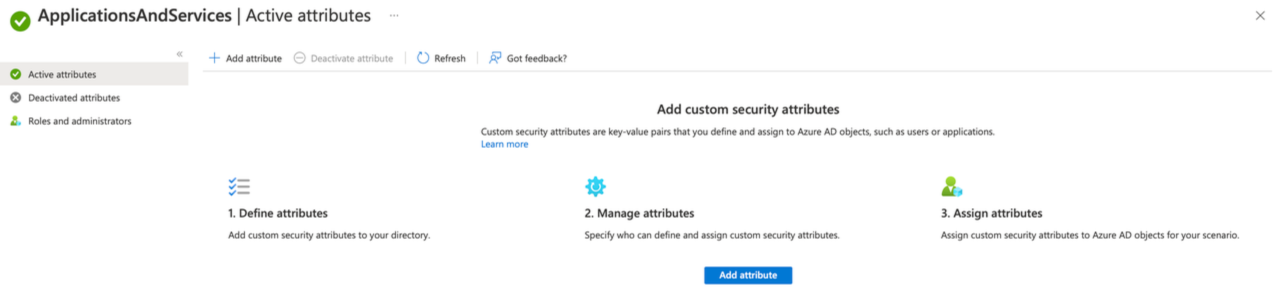
Description Additional attributes for cloud applications, services...

Maximum number of attributes 25

The attribute set can be named anything containing only letters, numbers, and no special characters. You can have several attributes in one set, up to 500. Attribute sets cannot be renamed or deleted after creation. Some good practices may be to create attribute sets for:

- Applications and Services
- Users
- Azure AD Resources
- Azure Resources

After naming, select “Add” at the bottom of the screen to save. Once created, select the name of your attribute set to add individual attributes up to the maximum you defined for the set.



ApplicationsAndServices | Active attributes

Add custom security attributes

Custom security attributes are key-value pairs that you define and assign to Azure AD 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 Azure AD objects for your scenario.

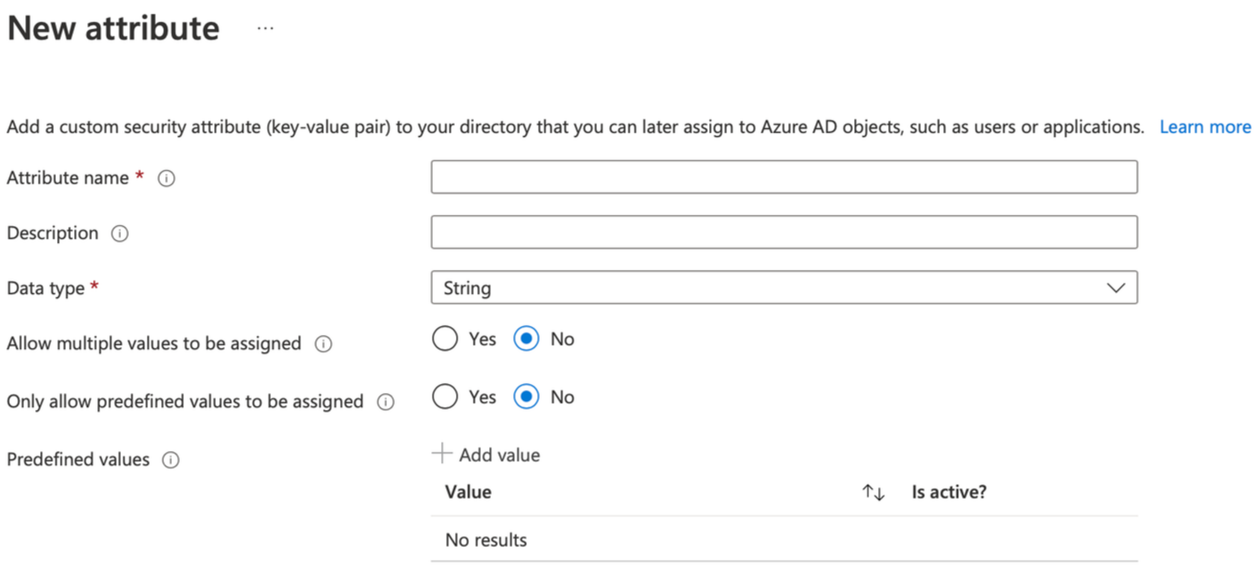
Create a Custom Security Attribute

Select “+ Add attribute” to add an attribute. Attributes can contain:

- Strings
- Boolean values
- Integers

Furthermore, you can allow the value to be set by the administrator or restrict the value to a preselected set of values.

NOTE: In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown.



New attribute

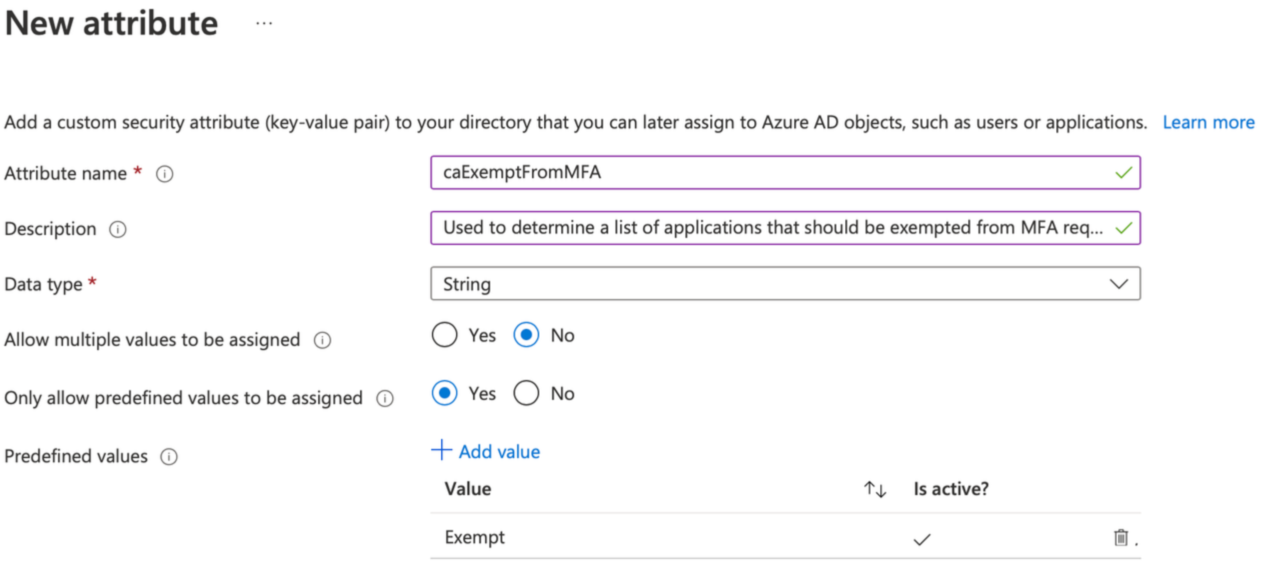
Add a custom security attribute (key-value pair) to your directory that you can later assign to Azure AD objects, such as users or applications. Learn more

Attribute name *	
Description	
Data type *	String
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	

Attribute example with a string value

In this example, we'll create an attribute to denote applications which should be exempt from conditional access policies that enforce Multi-factor Authentication requirements. We'll name the attribute `isExemptMFA` and set the data type to a String value. (Boolean and integer values are not supported while this feature is in Preview.)



New attribute ...

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

Attribute name * ⓘ: caExemptFromMFA ✓

Description ⓘ: Used to determine a list of applications that should be exempted from MFA req... ✓

Data type *: String

Allow multiple values to be assigned ⓘ: ○ Yes ● No

Only allow predefined values to be assigned ⓘ: ● Yes ○ No

Predefined values ⓘ: + Add value

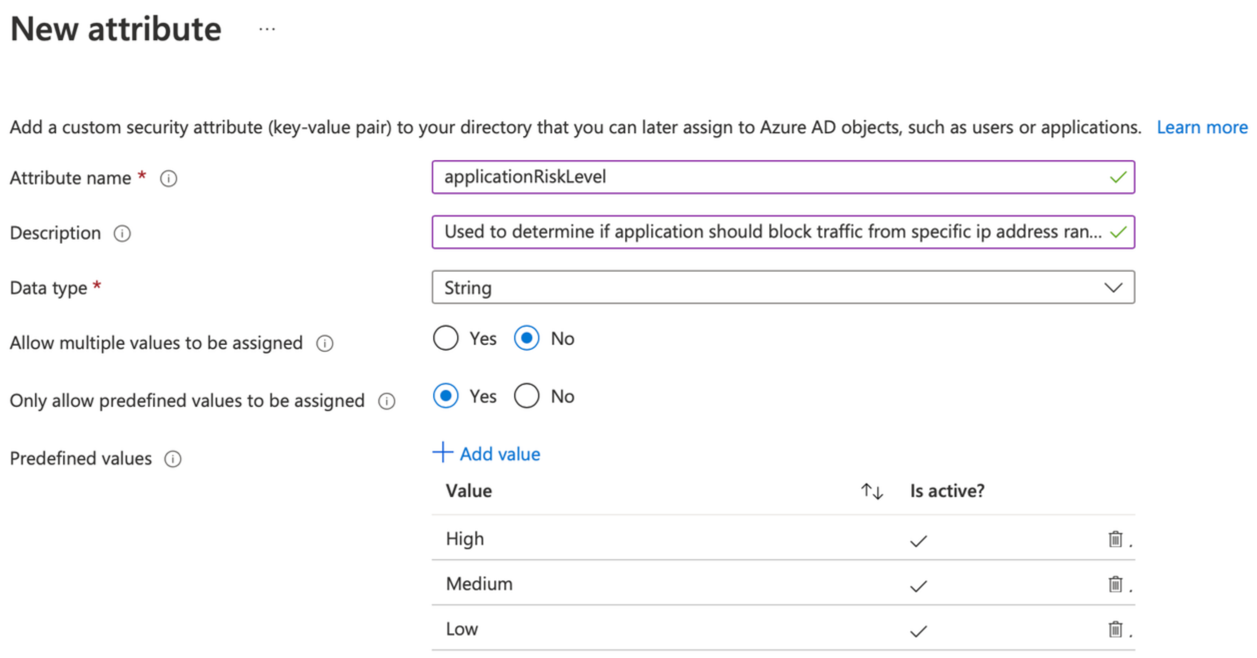
Value	Is active?
Exempt	✓

To simulate a boolean value while in preview, we will add a Data type of "String", allow only predefined values to be assigned, and add a predefined value of "Exempt." If the app contains a value of "Exempt," the value is assumed "true". If the value is missing, the value is assumed "false" and therefore should be subject to an MFA policy.

Confirm your naming, description, and spelling. Attributes are limited and cannot be deleted after creation; they can only be deactivated. Use the "Save" button at the bottom of the screen to save the attribute.

Attribute example with a set of predefined values

In this example, we'll create an attribute to denote applications risk level as determined by our security department. Applications with a medium or high risk value may want to be blocked if traffic is originating from a country deemed a high security risk. Applications with a high risk value may only be accessed through a private access network address range.



New attribute ...

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

Attribute name *	applicationRiskLevel
Description	Used to determine if application should block traffic from specific ip address ran...
Data type *	String
Allow multiple values to be assigned	○ Yes ● No
Only allow predefined values to be assigned	● Yes ○ No
Predefined values	+ Add value

Value	Is active?
High	✓
Medium	✓
Low	✓

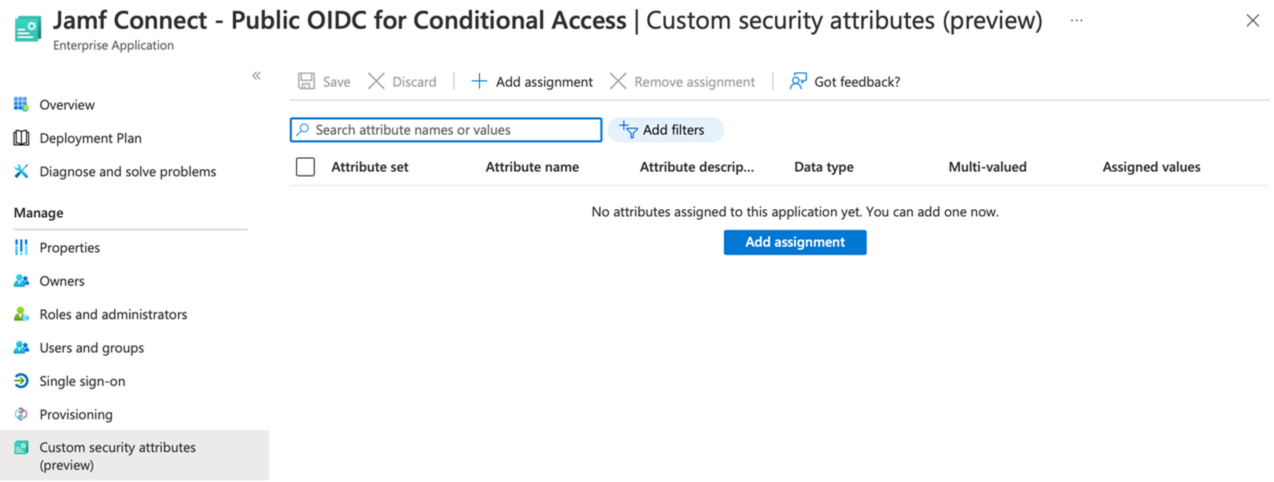
In this example, we'll name the attribute `applicationRiskLevel` and only allow for our predefined values of High, Medium, and Low to be assigned to the application.

Apply Custom Security Attribute to an Enterprise App

Once an attribute is created, it must be applied to an application. Navigate to Azure Active Directory → Enterprise applications. Select an application.

In our example, we'll apply the custom security attribute to the Jamf Connect app registration to mark it as a low risk application and exempt from multi-factor authentication requirements for our ongoing password checks.

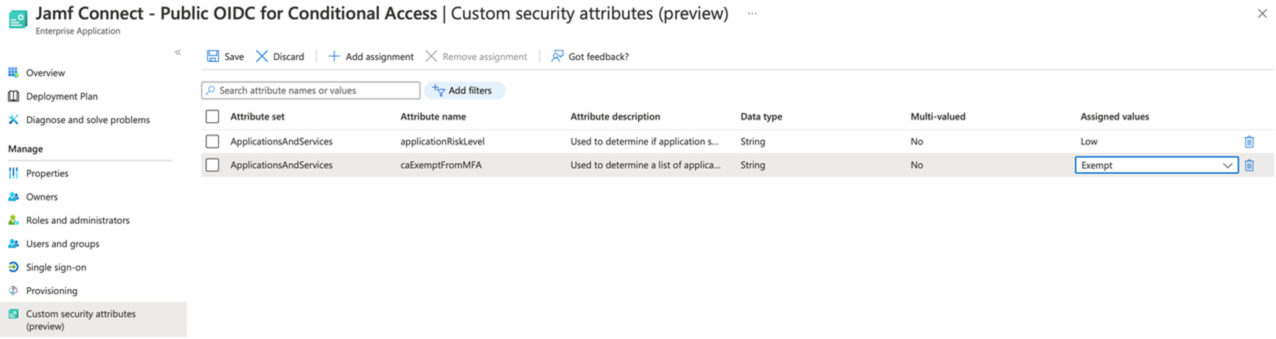
In the left hand navigation bar under the section "Manage", select the option for "Custom security attributes (preview)". Use the "Add assignment" option to add an attribute set.



□	Attribute set	Attribute name	Attribute descrip...	Data type	Multi-valued	Assigned values

No attributes assigned to this application yet. You can add one now.

Once an Attribute set is selected, Attribute names and their predefined values can be added individually to the application. Select the “Save” option after adding attributes.



□	Attribute set	Attribute name	Attribute description	Data type	Multi-valued	Assigned values
□	ApplicationsAndServices	applicationRiskLevel	Used to determine if application s...	String	No	Low
□	ApplicationsAndServices	caExemptFromMFA	Used to determine a list of applica...	String	No	Exempt

To apply the custom security attribute to create an conditional access policy for Jamf Connect, continue to “https://github.com/jamf/jamfconnect/blob/main/azure_conditional_access/3_-_Use_Custom_Security_Attributes_to_apply_an_exc.pdf “