


What Are Azure AD Custom Security Attributes?

 blog.netwrix.com/2022/02/10/what-are-azure-ad-custom-security-attributes

Kevin Joyce

Microsoft released a valuable new Azure feature in December of 2021: custom security attributes. This feature is still in preview.

Custom security attributes enable organizations to define new attributes to meet their needs. These attributes can be used to store information or, more notably, implement access controls with Azure attribute-based access control (ABAC).

Handpicked related content:

[\[On-demand Webinar\] 10 Best Practices for Securing AD and Azure AD](#)

Azure ABAC, which is also in preview, enables an organization to define access rules based on the value of an object's attribute. For example, you can grant access to a particular resource to all users that have the custom attribute 'Project' set to 'Beta'.

Adopting Azure custom security attributes is very easy. They are available tenant-wide, can support various data types, and can be single or multi-valued. They can be applied to users, applications and managed identities.

Handpicked related content:

[Top 5 Azure AD Security Best Practices](#)

How to Set Up Custom Security Attributes

Prerequisite

To configure Azure custom security attributes, you must have either the 'Attribute definition administrator' role or the 'Attribute assignment administrator' role. These are two of the four new roles related to custom security attributes:

Procedure

Let's suppose we want to create an attribute set named 'Access' to control access to resources in Azure AD. To create this attribute set and configure its custom attributes, take the following steps.

1. Navigate to the 'Custom security attributes' blade in Azure Active Directory and click the 'Add attribute set' button.



2. Configure the first attribute for the set. I've named it 'Level' since it will be used to ensure that only users who have been assigned a particular level have access to certain resources in Azure AD.

3. Now let's use the new attribute to govern access by controlling role assignments. The screenshot below shows how to configure a resource group to grant the 'Storage Blob Data Reader' role only when the principal attempting to access it has an 'Access_Level' attribute value of 1.

4. Last, I need to configure the 'Level' security attribute on all of the objects I want to be able to access this resource group with the data reader role. Here's how to assign the required value of 1 to this attribute for a particular user:

Limitations and Considerations

There seem to be some limitations with implementing custom security attributes for dynamic role assignments — the only roles that seem to be able to be granted conditions to access resources so far seem to be ones that contain actions related to storage blobs. This includes Storage Blob Data Contributor, Storage Blob Data Owner and Storage Blob Data Reader, as well as any custom roles that provide the same set of actions as those three roles.

Despite this limitation, the custom attribute functionality is a huge step forward toward making fine-grained access control available and easy to configure.

Kevin Joyce

Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University of Pennsylvania.

