Conditional Access in Azure AD

Provides an additional layer of security before allowing authenticated users to access data or other assets. It is implemented via policies created and manged in Azure AD, based on things like the user, the location, the device, and the applicaiton they are attempting to access.

Conditional Access Signals

User or group membership - policies are targeted to all users, a specific group, directory roles, or external guests

Named location - uses IP ranges. Tracking can be allowed or blocked from an entire country/region IP range.

Device - users with certain device platforms can be used (e.g. only you work laptop)

Application - specific attempts at accessing applications can trigger different policies

Real-time-sign-in risk detection - integration with other signals can identify risky sign-in behaviour. If it is triggered, the user can be prompted to change their password, or required to use MFA.

Cloud apps or actions - can include or exclude applications or user actions that are subject to policy

User risk - can be evaluated as part of Conditional Access policies. It represents the probability that a given identity or account is compromised. It can be configured for high, medium or low.

Access controls

When a Conditional Access policy is in effect, it decides whether to grant or block access, or require further verification. Decisions are:

- Block access
- Grant access OR

Require one or more conditions to be met before granting access:

- Require MFA
- Require device to be marked as compliant
- Require hybrid Azure AD joined device

- Require approved client app
- Require app protection policy
- Require a password change

Session controls can also be implemented e.g. whilst using apps, downloads, copying, and pasting are prohibited for sensitive documents. Or that if the device is not quite up to conditions, they can read, but not do anything else to the resources.

Benefits of Azure AD roles and role-based access control

Built in roles

There are many roles that come with a fixed set of permissions:

- Global administrator: have access to all administrative features of Azure AD. The person who signs up for the Azure AD tenant automatically becomes a global administrator.
- User administrator: users with this role can create and manage all aspects of users and groups. They can also manage support tickets and monitor service health
- Billing administrator: users with this role can make purchases, manage subscriptions and support tickets, and monitor service health.

The permissions for these built in roles cannot be modified.

Custom roles

A custom role definition is a collection of permissions you add from a preset list. It is a Two step process: create the custom role definition, then assign that roles to users or groups with a role assignment.

Custom roles require an Azure AD Premium P1 or P2 license.

Only grant needed access

It is best practice and more secure to grant users the least privilege to get their work done.

Categories of Azure AD roles

Azure AD specific roles: grant permissions to manage resources within Azure AD only (e.g. user admin, application admin, group admin)

Service specific roles: For major M365 services, Azure AD includes bulit-in service-specific roles that grant permissions to manage features within service. Examples are Exchange Admin, Intune Admin, Sharepoint Admin, and Teams Admin.

Cross-service role: Some roles within Azure Ad span services e.g. Security Admin across multiple M365 services. Or the Compliance Admin to manage compliance related settings in M365 Compliance Center, Exchange etc.

Difference between Azure AD RBAC and Azure RBAC

Azure AD RBAC: Azure AD controls access to Azure AD resources such as **users, groups, applications**

Azure RBAC: controls access to Azure resources such as **virtual machines or storage using Azure Resource Management**