**Setup Entra ID**

When implementing Azure into the Entra ID or what used to be known as Azure Active Directory, then there are several technical artifacts and configurations required. These two integrate mainly to support authentication, identification and security in the cloud platforms. Below are the main technical artifacts and steps required for integration:

A screenshot of a computer

Description automatically generated

Fig Ozmart Entra ID Setup

1. Azure Entra ID Tenant An existing tenant in Entra ID is mandatory to build an integration with Azure resources. This specific tenant caters for the Identity and Access Management (IAM) for users, groups and applications that are in Azure.
2. App Registration For applications to connect with Entra ID, it is required that an app registration be made. This registration creates an application (client) ID which is used to refer to the application within the Entra ID.
3. API Permissions and Consent The app uses permissions to access several resources in Azure. These permissions are given via the concept known as API permissions. Some of the permissions may be granted if the administrator consents.
4. API Permissions and Consent The use of the app entails granting of permissions for accessing the various Azure resources. These permissions are received with the help of API permissions. Some permissions may require admin permission to be granted.
5. Role Assignments (RBAC) In order for the service principal or user groups to be able to access certain Azure resources, roles can only be assigned using Azure RBAC. It enables giving the right role to access the right resource.
6. Conditional Access Policies Conditional access policies can be set in order to allow to use Azure services. These policies, further set prerequisites through which users or apps can use resources.
7. Enterprise Applications When it comes to third party SaaS or on-premises application, you can set up applications in Entra ID Identity as the Enterprise applications to control access, policies and SSO.
8. User and Group Management To integrate, one needs to create or synchronize users and groups either by performing online manual work or by synchronizing the Azure AD Connect with the on-premises Active Directory.
9. Identity Guard and Surveillance There are other monitoring tools such as Azure AD Identity Protection and Azure Monitor that shall help real-time threat and anomaly detection of users.