


1- Entra ID

Entra Id

- cloud-based *identity and access management* service,
 - enables your employees access *external resources*.
 - Resources like M365, Azure portal, other SaaS applications.
 - Also helps them access *internal resources* like apps on your corporate intranet.
 - resource -  [\(161\) Microsoft Entra ID Beginner's Tutorial \(Azure Active Directory\) - YouTube](#)
 - using same sign-in credentials to securely access all of your online services for work.
 - ! Its primary job is to help you prove you are who you say you are.
 - @ once that verified which is a process called authentication.
 - @ You can access services that you have permissions to use, refer to as authorization
-

Identity and Access Management

Meaning

ensures the *right people*, *right machine* get access to the right resources at the *right time*

- First a person, machine or software component needs to prove *they're who* or *what they claim to be*.
- Then they are allowed or denied to access to use certain resource.

Identity

An identity is a collection of unique identifiers or attributes that represent a human, software component, machine, asset, or resource in a computer system.

Identifiers like

- Email add
- Sign-in creds
- Bank acc no
- MAC address or IP address

- **!** Identities are used to authenticate and authorize to resources, communicate with other humans, conduct transactions and other purposes.

3 types of identities

1. Human identities
2. Workload identities
3. device identities

Authentication

- process of challenging a person, software component, or hardware devices for credentials in order to *verify their identity* or *prove they're who or what they claim to be*
- shortened to **AuthN**

MFA

- a security measure to provide more than one piece of evidence to verify their identities.
 - Something they *know*.
 - Something they *have*.
 - Something they *are*.

SSO

authenticate their identities once and silently accessing the resources that rely on the same identity.

- **!** The IAM system acts as a source of identity truth for the other resources available to the user.
- removes the need for signing on to multiple, separate target systems.

Authorization

- Validates that the user, machine or software component has been granted access to certain resources.
- shortened to **AuthZ**

Authentication vs Authorization

Authentication



Confirms users are who they say they are

Authorization



Validates users have permission to complete the attempted action

#Authentication	#Authorization
Can be thought of as a gatekeeper, allowing access only to those who provide valid credentials.	Can be thought of as a guard, ensuring that only those with the proper clearance can enter certain areas.
Verifies whether a user, machine, or software is who or what they claim to be.	Determines if the user, machine, or software is allowed to access a particular resource.
Challenges the user, machine, or software for verifiable credentials (for example, passwords, biometric identifiers, or certificates).	Determines what level of access a user, machine, or software has.
Done before authorization.	Done after successful authentication.
Information is transferred in an ID token.	Information is transferred in an access token.
Often uses the OpenID Connect (OIDC) (which is built on the OAuth 2.0 protocol) or SAML protocols.	Often uses the OAuth 2.0 protocol.

- Individual permissions are collected into **#roles** which can be granted to individual users.

Identity Provider

#identity_provider *creates, maintains and manages* identity information while offering authentication, authorization and auditing services.

[source](#)

- Info that's used to authenticate the user, with a server is stored and managed centrally by the identity provider.
- using the central identity provider, orgs can establish authN and AuthZ policies, monitor user behavior, identify suspicious activities and reduce malicious attacks.
- Microsoft Entra ID is an Example of a **cloud based identity provider**.

IAM

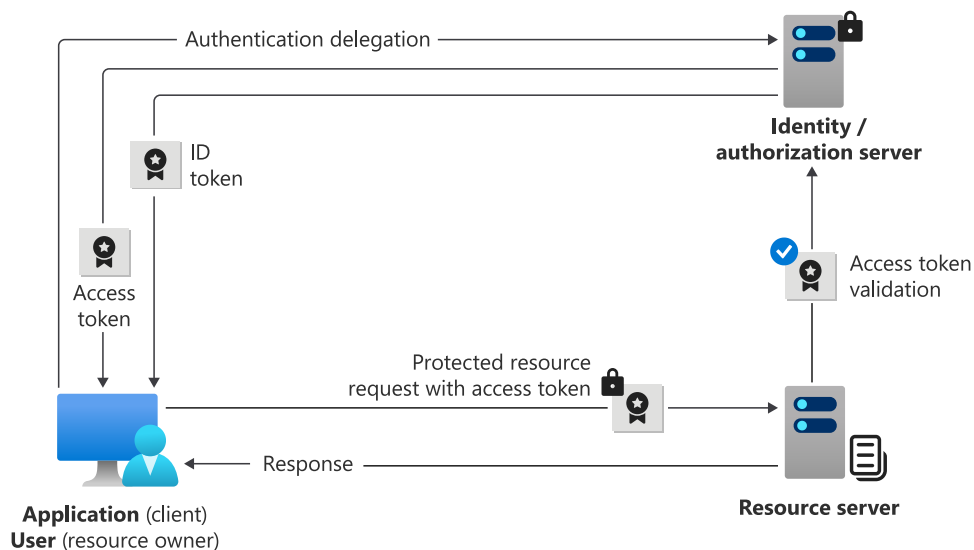
functionalities provided by IAM

1. Identity Management
 2. Identity federation
 3. provisioning and deprovisioning users
 4. Authentication of users
 5. Authorization of users
 6. Access Control
 7. Reports and monitoring
-

source - bard

original source - [source](#)

1. The user **initiates an authentication** request with the identity provider/authorization server.
2. The identity provider/authorization server verifies the user's credentials.
3. If the credentials are valid, the identity provider/authorization server sends an ID token and an access token to the client application.
4. The client application sends the access token to the protected resource server.
5. The protected resource server validates the access token.
6. If the access token is valid, the protected resource server grants the user access to the resource.



Authentication

2. The user **initiates an authentication** request with the identity provider/authorization server from the client application. This means that the user enters their credentials, such as their username and password, into the client application.

3. The client application sends the user's credentials to the identity provider/authorization server.
4. The identity provider/authorization server verifies the user's credentials. If the credentials are valid, the identity provider/authorization server sends an ID token back to the client application.
5. The ID token contains information about the user, such as their username and email address. The client application stores the ID token securely.

Authorization

2. The user tries to access a protected resource, such as a website or an application.
3. The client application sends the ID token to the identity provider/authorization server.
4. The identity provider/authorization server verifies the ID token and obtains end-user consent.
5. If the ID token is valid and the user has consented, the identity provider/authorization server grants the client application authorization to access the protected resource.
6. Authorization is provided in an access token, which is also sent back to the client application.
7. The client application sends the access token to the protected resource server.
8. The protected resource server validates the access token. If the access token is valid, the protected resource server grants the user access to the resource.

Example

Let's say that you are trying to access a confidential document on a website. The website is the protected resource server. The identity provider/authorization server is a separate server that is responsible for authenticating users and authorizing them to access resources.

1. You enter your username and password into the website.
2. The website sends your username and password to the identity provider/authorization server.
3. The identity provider/authorization server verifies your username and password. If your credentials are valid, the identity provider/authorization server sends an ID token back to the website.
4. The website stores the ID token securely.
5. You click on a link to access the confidential document.
6. The website sends the ID token to the identity provider/authorization server.
7. The identity provider/authorization server verifies the ID token and obtains your consent to access the confidential document.
8. If the ID token is valid and you have consented, the identity provider/authorization server grants the website authorization to access the confidential document.
9. Authorization is provided in an access token, which is also sent back to the website.
10. The website sends the access token to the protected resource server.
11. The protected resource server validates the access token. If the access token is valid, the protected resource server grants you access to the confidential document.

Standards of AuthN and AuthZ

Authentication and authorization Standards

Tenant

- Your new `#tenant` represents your organization.
- When you create a new *Microsoft Entra Tenant* You become the first user of the tenant.
- As a first user, you are automatically assigned the *Global Administrator* role.
- Microsoft Entra tenants come with an initial domain name like *domainname.onmicrosoft.com*.

Change the directory of subscription

- changing the directory doesn't transfer some resources, like
- **!** All Azure RBAC assignments are deleted
- **!** All classic subscription administrators also lose access.

