






Microsoft Entra Product Family (AZ-104 Context)

1. Overview

Microsoft Entra is a unified identity and access solution that includes several services. For AZ-104, you'll mostly focus on **Microsoft Entra ID** (formerly Azure Active Directory), but it's important to know what other products exist and how they might relate to enterprise identity scenarios.

2. Key Products in the Entra Family

Product	Description	AZ-104 Relevance
Microsoft Entra ID	Core identity and access management (formerly Azure AD)	 High — manage users, groups, RBAC, MFA, Conditional Access
Microsoft Entra ID Governance	Identity lifecycle, access reviews, entitlement management	 Medium — indirectly relevant, appears in lifecycle and access control questions
Microsoft Entra Permissions Management	CIEM for least privilege across multi-cloud	 Low — not directly tested in AZ-104
Microsoft Entra Verified ID	Decentralized identity solution for verifiable credentials	 Low — not part of AZ-104 scope
Microsoft Entra External ID	Secure access for external users (B2B/B2C)	 Medium — B2B is sometimes touched in hybrid identity scenarios
Microsoft Entra Workload ID	Manage identities for apps and services (non-human)	 Low — minor relevance in automation/service principal topics

3. Real-World Scenarios (AZ-104 Focused)

◆ Scenario 1: Secure Access with Microsoft Entra ID

You are tasked with securing access to Azure resources. You must implement authentication, MFA, and least privilege access.

Solution:

- Use **Microsoft Entra ID** to create users and groups
 - Assign **RBAC** roles at the resource group or subscription level
 - Configure **MFA** and **Conditional Access** policies
-

◆ Scenario 2: Lifecycle Management

Your organization wants to automatically remove access for employees who leave the company.

Solution (Enterprise Setting):

- Use **Microsoft Entra ID Governance** to implement **access reviews** and **automated lifecycle workflows**

(Note: You're not required to configure these in AZ-104, but knowing their purpose supports understanding of the identity governance concept.)

◆ Scenario 3: Manage Service Principals

You deploy an Azure Function App that needs to read data from a storage account. It needs to authenticate securely.

Solution:

- Use **Microsoft Entra Workload ID** (behind the scenes this uses service principals or managed identities)
 - Assign a **Storage Blob Data Reader** role to the app's managed identity
-

4. Azure Portal Pathways

Most Entra services are accessible via:

➔ **Microsoft Entra Admin Center:** <https://entra.microsoft.com>

In the portal:

- **Microsoft Entra ID** → Users, Groups, Roles, Devices
 - **Identity Governance** → Lifecycle workflows, Access Reviews, Entitlement Management
 - **Workload Identities** → Applications and managed identities
 - **Permissions Management** → Not commonly configured by admins taking AZ-104
-

5. **AZ-104 Exam Tips**

- Focus on **Microsoft Entra ID**, including:
 - User/group management
 - Role assignments (RBAC)
 - MFA & Conditional Access
 - Azure AD Connect
 - Identity Protection (basic risk detection)
 - **Understand** the names and **purposes** of other Entra products but don't worry about in-depth configurations.
 - Expect questions around:
 - Granting access using RBAC + Entra ID
 - Implementing secure access policies
 - Managing identities in hybrid environments
-

Summary for AZ-104

Focus Area	Entra Product
Identity and access for Azure	Microsoft Entra ID
Role-based access to Azure resources	Microsoft Entra ID + Azure RBAC
MFA and conditional access	Microsoft Entra ID
Hybrid identity (on-prem + cloud)	Microsoft Entra ID + Azure AD Connect
Non-human identities (apps, scripts)	Microsoft Entra Workload ID
Identity governance and compliance	Microsoft Entra ID Governance (theory only)
