**Introduction to Microsoft Entra ID**

Microsoft Entra ID is a cloud-based identity and access management service from Microsoft. It helps organizations manage who can access what resources, like apps and data, in a secure way. Think of it as a digital gatekeeper for your company's online tools. It used to be called Azure Active Directory, but it's been rebranded to Microsoft Entra ID to cover a broader family of security products. As of 2025, it includes advanced features like risk-based access controls and integration with new authentication methods. It's designed for modern work, supporting remote employees, cloud apps, and even partnerships with external users.

* **Why Use It?**: It simplifies sign-ins, boosts security with features like multifactor authentication (MFA), and scales easily for businesses of any size. It powers access to Microsoft services like Microsoft 365, Azure, and thousands of other apps.
* **Core Benefits**: Provides single sign-on (SSO) so users log in once for multiple apps; automates user management; and protects against threats with smart detection. In 2025, new updates include better support for passkeys and QR code sign-ins for frontline workers.
* **Who It's For**: Businesses using cloud services, hybrid setups (mix of on-premises and cloud), or needing to manage external collaborators.
* **Recent Updates (2025)**: Microsoft has rolled out features like optional application-based authentication for Entra Connect, auditing for admin events, and enhanced **Conditional Access with real-time risk assessments**. There's also a hardening update requiring TLS 1.2 by April 2025, and new roles like People Administrator.

**Key Concepts in Microsoft Entra ID**

These are the building blocks of how Entra ID works. Understanding them helps you see how identities are handled in the cloud.

* **Identity**: This is anything that needs to prove who or what it is to access resources. It could be a person (user), an app, or even a device. For example, a username and password combo is a basic identity.
* **Account**: An identity with extra details attached, like contact info or job role. You can't have an account without an identity—it's like a profile built on top.
* **Microsoft Entra Account**: A specific type of account created in Entra ID or linked Microsoft services (e.g., Microsoft 365). It's also called a "work or school account" and is stored securely in the cloud.
* **Tenant (or Directory)**: A private space for your organization in Entra ID. When you sign up for a Microsoft cloud service, a tenant is auto-created. It's like your company's own secure bubble where you manage users, groups, and apps. Terms "tenant" and "directory" are often used interchangeably—one tenant equals one directory.
  + **Single Tenant vs. Multitenant**: Single means dedicated access for one org; multitenant shares resources across orgs but keeps data separate.
  + **Custom Domains**: Starts with a default like "yourcompany.onmicrosoft.com," but you can add your own domain (e.g., "[user@yourcompany.com](mailto:user@yourcompany.com)") for easier recognition.
* **Azure Subscription**: This is how you pay for Azure services—it's linked to your tenant but separate. You can have multiple subscriptions for different billing needs.
* **Microsoft Account (MSA)**: Personal accounts for consumer stuff like Outlook or Xbox—not for business use in Entra ID.
* **Authentication Methods**: Ways to verify identities, including passwords, MFA (e.g., app notifications, codes), passwordless options like FIDO2 passkeys (expanded support in November 2025), and even QR codes for frontline workers.

**Comparison: Microsoft Entra ID vs. Active Directory Domain Services (AD DS)**

Entra ID is cloud-focused, while AD DS is for on-premises networks. They're similar in managing users but differ in how they work and what they support.

* **Similarities**:
  + Both handle user creation (manual or automated) and group-based permissions.
  + Support credential management like passwords and certificates.
  + Can integrate: Entra ID syncs with AD DS via tools like Entra Connect for hybrid setups.
* **Differences in Structure and Management**:
  + Entra ID is flat—no folders (OUs) or policies (GPOs) like in AD DS. It's managed as a service; Microsoft handles the backend, so you focus on users and policies.
  + AD DS requires you to manage servers, patching, and infrastructure yourself (or via VMs in Azure).
  + Entra ID uses role-based access control (RBAC) with built-in roles; AD DS uses domains and groups for delegation.
* **Protocols and Authentication**:
  + Entra ID uses modern web protocols like HTTP/HTTPS, SAML, OAuth, and OpenID Connect , great for cloud apps and federation (e.g., sign in with Facebook).
  + AD DS relies on older protocols like LDAP, NTLM, and Kerberos, better for legacy on-premises apps.
* **User and Device Management**:
  + Entra ID excels at external users (B2B guests) and mobile devices via Intune; supports managed identities for apps.
  + AD DS is strong for Windows servers and on-premises devices but needs extras for mobiles or externals.
* **Security Features**:
  + Entra ID has built-in MFA, smart lockout, and risk-based access; AD DS has basic password policies but lacks cloud smarts.
* **Use Cases**:
  + Choose Entra ID for cloud/hybrid environments, SaaS apps, and remote work.
  + Use AD DS for traditional on-premises networks; combine both for hybrid identity.

**Licensing Plans for Microsoft Entra ID**

Entra ID comes in tiers: Free (basic), P1 (advanced management), P2 (premium security), and the Suite (all-in-one bundle). Features build on each other—pick based on your needs like MFA or governance.

* **Free Plan** (Included with Azure/Microsoft 365 subscriptions):
  + Unlimited SSO for SaaS apps.
  + Basic MFA and self-service password changes.
  + User/group management and on-premises sync.
  + Basic reports, no advanced governance.
* **P1 Plan** (Builds on Free; required for Suite):
  + Advanced group features (dynamic groups, policies).
  + Conditional Access for smarter sign-ins.
  + Automated provisioning to apps (HR-driven too).
  + Self-service portals for passwords and groups.
  + Global password protection and reports.
* **P2 Plan** (Builds on P1; special pricing with annual commitment):
  + Risk-based Conditional Access (e.g., block risky sign-ins).
  + Privileged Identity Management (PIM) for just-in-time admin access.
  + Identity Protection with real-time risk detection.
  + Access reviews and entitlement management.
* **Microsoft Entra Suite** ($12/user/month, annual; includes P1/P2):
  + Full governance: Lifecycle workflows, machine learning reviews.
  + Verified ID for credentials (e.g., facial matching).
  + Network access controls like Tenant Restrictions.
  + High-assurance features for sensitive data.

**Self-Service Password Reset (SSPR)**

SSPR lets users fix their own passwords without calling IT, saves time and reduces help desk tickets. It's configurable and works in cloud or hybrid setups.

* **How It Works**:
  + Users go to a portal (aka.ms/sspr) to reset/change passwords.
  + System checks if SSPR is enabled, verifies methods, and updates passwords (even on-premises via writeback).
  + Emails notify users/admins of changes; no data is stored long-term.
* **Configuration Steps**:
  + Enable in Entra admin center; require registration during sign-in.
  + Set reconfirmation period (e.g., every 180 days) to keep info fresh.
  + For hybrid: Use Entra Connect for password writeback.
  + Allow account unlock without full reset.
* **Authentication Methods**:
  + Require 1-2 methods: Mobile app (notification/code), email, phone (mobile/office), security questions, OATH tokens.
  + Best to use 2+ for backup; can't rely only on authenticator app for single-method setups.
* **Best Practices**:
  + Force registration to avoid surprises.
  + Enable notifications and combine with MFA.
  + Test in hybrid environments; use for admins with strong policies.

**Managing User Accounts**

Users are the core of identity—create them for employees, guests, or externals. Manage as Global or User Admin.

* **Creating Users**:
  + In Entra admin center: Go to Users > New user.
  + Basics: User principal name (e.g., user@domain), display name, password (auto or manual), enable account.
  + Properties: Job title, department, manager, contact info, age group (for parental controls), location.
  + Assignments: Add to groups/roles (up to 20), administrative units (1).
  + For Guests: Invite via email; they accept and link externally.
  + External Tenants: Use email sign-in; no roles for externals.
* **Managing Users**:
  + Update profiles: Add pictures, job info; view sign-in/audit logs.
  + Restore deleted users within 30 days.
  + Bulk Operations: Download CSV template, edit, upload for mass creates/updates/deletes.
* **Deleting Users**:
  + Select user > Delete; User Admin can delete most, but Privileged Admins handle higher roles.
  + Check dependencies (e.g., owned groups) first.

**Managing Group Accounts**

Groups bundle users for easier access control—assign permissions once to the group.

* **Group Types**:
  + Security: For controlling access to resources like apps or files.
  + Microsoft 365: For collaboration (e.g., Teams, email distribution).
* **Membership Types**:
  + Assigned: Manually add/remove members.
  + Dynamic: Auto-add based on rules (e.g., department = "Sales").
* **Creating Groups**:
  + In admin center: Groups > New group; name it, choose type/membership.
  + Add members/owners during or after creation.
* **Managing Groups**:
  + View all groups; search and see members.
  + Update properties, add/remove users dynamically.
  + Use for licenses: Assign to group for auto-distribution.

**Assigning Licenses to Users and Groups**

Licenses unlock paid features—manage in Microsoft 365 Admin Center or PowerShell.

* **Basics**:
  + Free services (e.g., basic Entra ID) don't need licenses; paid ones (e.g., P1/P2) do.
  + Each user/group needs a license for access.
* **Assigning to Users**:
  + Select user > Licenses > Assign; choose plan, set location.
  + Bulk: Upload CSV for multiple.
* **Assigning to Groups**:
  + Create group, assign license—auto-applies to members.
  + Dynamic groups make this scalable.
* **Managing Licenses**:
  + View usage, change plans, remove licenses.
  + Monitor in portal for expirations or over-assignments.

**Hybrid Identity and Advanced Topics**

For mixed on-premises/cloud setups, use Entra Connect to sync identities—new 2025 features include app-based auth and auditing.

* **Hybrid Setup**: Sync AD DS users to Entra ID; single identity for all.
* **Administrative Units**: Scope admin roles to subsets (e.g., by department)—needs P1/P2.
* **Bulk Updates**: CSV for mass user/group changes—great for large orgs.
* **Labs and Learning**: Practice in Azure labs: Create users/groups, assign licenses.