

Active Directory Basics

What It Is and What It's For - Simple Guide for IT Beginners

DOMAIN CONTROLLER
(Active Directory Server)

↓ Manages & Authenticates ↓

Users

Computers

Printers

File Shares

What is Active Directory?

Active Directory (AD) is Microsoft's directory service that acts like a digital phone book for your entire network. It stores information about users, computers, and resources, and controls who can access what.

Think of it Like...

A Security Guard at a Building: Active Directory is like having a security guard who knows everyone who works in the building, which floors they can access, and what resources they're allowed to use. When someone tries to log in or access something, AD checks if they're allowed to do so.

Primary Functions

- **Authentication:** Verifies who you are when you log in
- **Authorization:** Determines what you can access
- **Central Management:** Manage all users from one place
- **Single Sign-On:** Log in once, access everything you're allowed to

What AD Manages

- **User Accounts:** Employee login credentials
- **Computer Accounts:** All company computers
- **Groups:** Collections of users with similar needs
- **Resources:** Printers, file shares, applications
- **Security Policies:** Password rules, access controls

- **Group Policy:** Apply settings to many computers at once

Centralized Control

Manage all users, computers, and permissions from one central location instead of configuring each device individually.

Security

Enforce consistent security policies, password requirements, and access controls across the entire organization.

User Convenience

Users log in once and can access all resources they're authorized to use without entering passwords repeatedly.

Common Active Directory Objects

Users

Individual people who need to access network resources

Groups

Collections of users with similar access needs

Computers

All workstations and servers in the domain

Organizational Units

Containers to organize objects by department

Why is Active Directory Important?

Without AD:

Each computer needs local accounts, passwords are managed separately, sharing resources is difficult, and security is inconsistent across systems.

With AD:

One login works everywhere, centralized user management, consistent security policies, easy resource sharing, and simplified IT administration.

Business Benefits:

Reduced IT workload, improved security, better compliance, easier onboarding/offboarding of employees, and lower administrative costs.

User Benefits:

Single password to remember, seamless access to resources, consistent experience across all company computers, and automatic policy updates.

Real-World Example

New Employee Joins:

- IT creates one AD user account
- Adds user to appropriate groups (Sales, Marketing, etc.)
- Employee can immediately log into any company computer
- Automatically gets access to departmental resources
- Password policies are automatically enforced

When Employee Leaves

Simple Cleanup:

- Disable one AD account
- Employee loses access to everything immediately
- No need to visit every computer or system
- Account can be deleted after transition period
- All access is centrally revoked

Simple Summary: Active Directory is like having one master key that controls access to everything in your office. It makes managing users and security much easier for IT and provides a seamless experience for employees.

© Dan Mill Training - All Rights Reserved