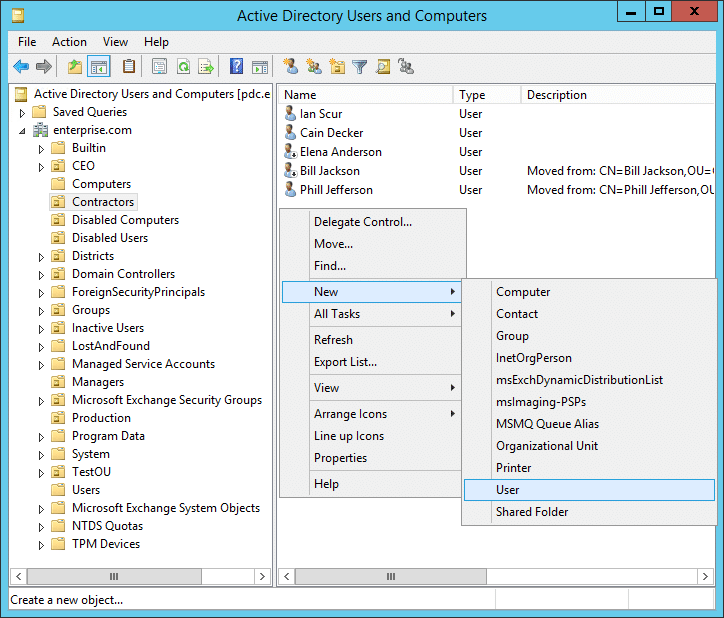
**1.What is Active Directory?**

Active Directory or (AD) is a directory service that was created by Microsoft for Windows domain services. It is used as a central area for controlling network assets such user accounts, computers, printers, and software. Network admins will use AD to create and manage a user’s account, help add security guidelines, and manage the users access to specific network resources.



One of Actives Directory’s biggest upsides is that it makes it very easy to manage user accounts and access permissions. Admins have the ability to create user accounts, specify what access they have with that account, and which groups they can be placed in with each permission. They also can control user password and username very easily through AD. This makes it not only possible, but very easy for businesses to enforce security policies and limit user or group rights-based access to network resources.

**2. Policies**

Diving further into groups and policies, AD provides group policy administration, which will let admins create and apply policies to a group or the whole network. These regulations may cover user configurations, security-related settings, and procedures for installing and updating software. Group policies allow admins to maintain organization and security over an entire network by applying them to specific users, groups, or even computers.

**3. DNS Resolution**

Another helpful feature that AD provides is DNS resolution services. Computers and other devices may locate network resources thanks to DNS resolution, which converts domain names into IP addresses. A DNS server is part of AD and offers name resolution services to network clients. This is vital to an organization’s infrastructure as it is the difference between public and private internet.

**4. Certificates**

AD is also more than capable of using certificate services which let admins create and control digital certificates that can be used to create a secure connections between people and their devices. It can also be used to secure programs on the network and to confirm their identities. Email, web traffic, and other network applications can all be secured using certificate services.

Overall, Active Directory is one of the most useful tools in an IT setting and can help manage an entire company’s infrastructure, and assist a business in securing their networks. AD is a flexible and effective tool that can be tailored to satisfy the particular requirements of any organization.

Iainfoulds. “Active Directory Domain Services Overview.” *Microsoft Learn*, https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview.

Shyamsundar, Teju. “What Is Two-Factor Authentication (2FA)? .” *Okta*, Okta Inc., 9 Mar. 2022, https://www.okta.com/blog/2021/07/what-is-two-factor-authentication-2fa/.