E-Guide

Azure Active Directory vs. Classic AD

TechTarget | SearchWindows Server

In this E-Guide:

How to use Azure Active Directory differently than classic AD

Learn how to spot the differences between the Microsoft Azure edition of Active Directory and classic Windows Active Directory – and how to use those differences to your advantage.

How to use Azure Active Directory differently than classic AD

Stuart Burns, Virtualization and Linux expert

Active Directory for Azure makes a large leap from the on-site AD that Windows administrators know well. While it leaves a lot behind, Azure Active Directory gives administrators ways to extend AD into cloud resources and achieve critical connections, such as application federation, once they know how to use it.

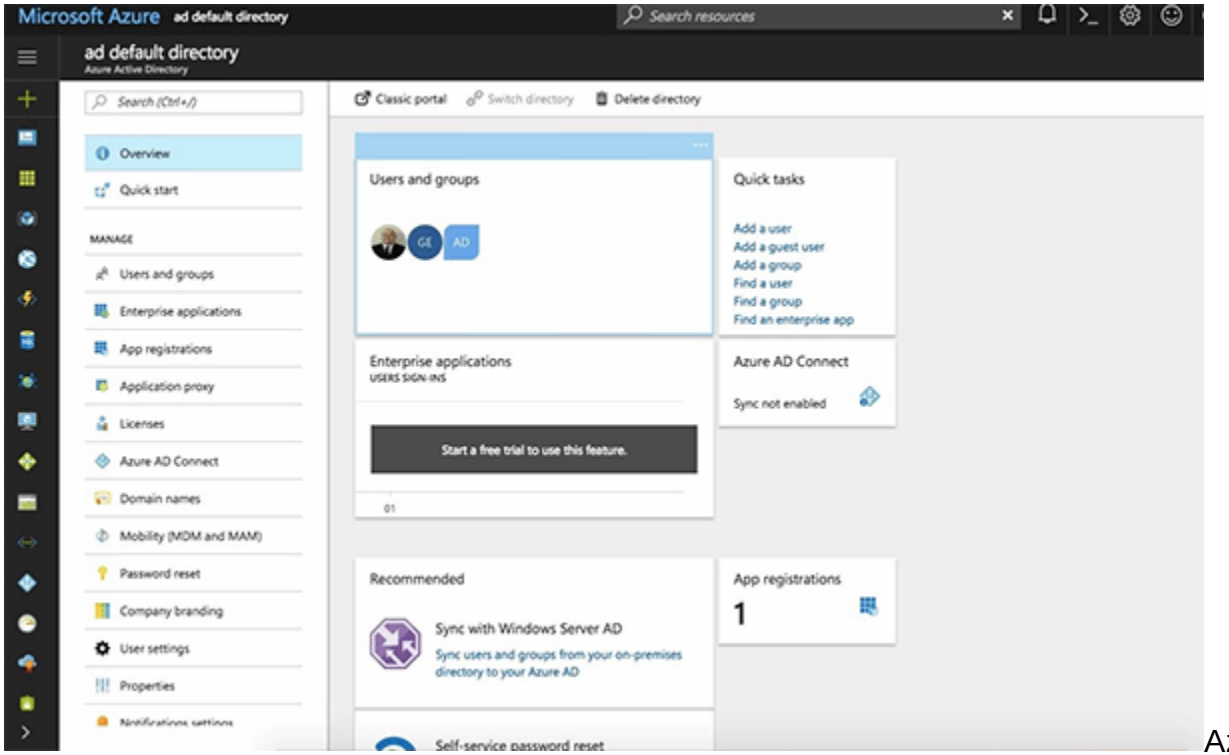
Most Windows administrators use classic AD to manage users, profiles, Group Policy Objects and other relationships. Bandwidth and interoperability are rarely an issue on premises. The cloud is a whole different proposition. Servers and services in the cloud have different needs and requirements than in-house deployments. Azure Active Directory extends classic AD into the cloud environment, rather than replacing AD with a cloud version. Active Directory has a treelike structure of organization, but Azure AD is essentially a flat exported version.

Azure Active Directory vs. on-premises AD

The public cloud is as device-agnostic as possible, which means it isn't designed to look after computers and Group Policy Objects. Azure doesn't need the heavy feature set of on-premises AD; it requires only that authenticated user accounts, groups and security information carry forward into the cloud. This is where administrators use Azure Active Directory.

How to use Azure Active Directory differently than classic AD

Azure Active Directory is a web-based system that manages and authenticates users against web services. It works with web-hosted, custom-built applications, as well as integrated third-party web services and applications. Microsoft's term for this list is the *portfolio*. Look for ways to use Azure Active Directory as an easily managed, extensible identity services front end to web services, platform-as-a-service offerings and other products.



Azure Active Directory can also manage identity and application provisioning on Windows devices:

The enterprise Windows 10 systems have a configuration option for on premises or Azure Active Directory. Don't expect it to apply Group Policy Objects, however.

Azure Active Directory even has its own PowerShell extensions to manage and configure users.

How to use Azure Active Directory in an enterprise

Azure Active Directory's setup suits companies with BYOD programs. Azure Active Directory connects Microsoft- and Android-based user devices, as a truly web-first affair. Once authenticated, the user can consume applications from the Azure system portfolio as dictated by the administrator. As the Azure Active Directory framework grows, its portfolio supports more applications. While end users download and consume apps easily, administrators retain a certain amount of control over local system configuration regarding apps.

Administrators can control the application sign-in for a web service from the portfolio. They can let the user specify username and password, choose to store preconfigured values or use federated services, such as Active Directory Federation Services (ADFS). Azure Active Directory passes these settings down upon app install.

Administrators can set up and release an application for users via a wizard interface in Azure Active Directory. They specify groups or individual users and can add users from other Azure Active Directory-enabled companies. In large environments, administrators commonly add these users so that Azure domains can authenticate with each other via ADFS without divulging any secrets. Multifactor authentication is also available on Azure Active Directory.

How to use Azure Active Directory differently than classic AD

There's no direct cost to use a basic Azure Active Directory setup. Anyone can sign up for an Azure account and explore Active Directory.

A premium version offers better reporting on users, infrastructure and systems, as well as the ability to customize page layout and branding for the users (consumers).

Microsoft offers a free trial with $200 worth of credit.

Administrators should take advantage of the in-app authentication feature. This enables you to validate Office 365 license statuses and management, authenticate users seamlessly to OneDrive and SharePoint and set up other pathways.

Use Azure Active Directory with Azure Active Directory Connect, a Microsoft tool that ties on premises to cloud. It helps prevent pesky authentication prompts or nasty hacks around them. An organization installs Azure AD Connect on the on-premises AD controller to extend authentication across both private and public cloud.

Administrators with a simple Active Directory setup, with a single domain and forest, will find it easy to extend into Azure.