Microsoft Azure

Azure Active Directory Conversation Guide

Conversation Starters

- What are your top security concerns and priorities?
- What resources (apps or data) do you share with partners and customers, and how do you manage access and security?
- In what way has identity and access management become more complex and/or costly?
- How many identity management solutions are you using?
- How do you provision and manage apps for remote employees?
- What cloud services are you using—and what is your cloud roadmap?
- How do you give employees the right access while keeping hackers at bay?

Azure Active Directory overview & benefits

Azure Active Directory (Azure AD) is a cloud-based identity and access management service that enables employees to sign in and access internal and external resources including on-premises and cloud apps. Organizations can:

Safeguard business information with multi-factor authentication and role-based access across devices, apps, servers, and more.

Securely connect your workforce to the apps they need from almost any location and device.

Simplify access and identity management across your organization with one platform.

Objections and Responses

"I'm already using Active Directory—why do I need a cloud-based solution?"
If you're using cloud services, supporting remote employees, or collaborating with external users like customers or partners, then you can benefit from Azure AD. Microsoft introduced Active Directory Domain Services in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user. **Azure AD takes this approach to the next level by providing organizations with an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises. For example, vendors, contractors, and partners can get secure access to in-house resources with Azure AD B2B collaboration.**

"I don't need another identity management solution to manage."
You can integrate your on-premises Active Directory and other directories with Azure AD through Azure AD Connect and use one identity to access any app. Azure AD already works with thousands of pre-integrated apps like Microsoft 365, SAP Concur, Box, and Workday—and you can also add your own custom apps.

"I like the idea of simpler management, but I'm worried about security."
Azure AD helps protect users, apps, and device in almost any location. For example, multi-factor authentication gives you an additional layer of authentication protection to provide a significant barrier against cybercrime. Safeguards also include conditional access policies based on location, application sensitivity, device state, and user or sign-in risk.

"I need to control costs—this isn't the best time for adopting new technology."
You get great value for your money with Azure AD, including single-sign on, multifactor authentication, password self-service, integration with a wide range of SaaS Apps, and the ability to enforce conditional access for users. **And, if you are an existing Microsoft 365 Business Premium customer you already have access to Azure AD Premium P1.**

Azure AD helps keep IT overhead low with self-service capabilities like password resets. In addition, Azure AD is a great foundation for future implementation of cloud services or device upgrades. For instance, Azure AD is built into Windows 10 and Windows 11. These devices are connected and protected the moment you join them to Azure AD, and you can also take advantage of Windows Autopilot for zero-touch provisioning.

Microsoft Azure

Azure Active Directory – Solution in a Box

Azure Active Directory

Virtual Network

VPN Gateway

Azure Active Directory

Connect all apps and users to Azure Active Directory for secure single sign-on from almost anywhere.

Azure Active Directory (Azure AD), now part of Microsoft Entra, is an identity service that provides single sign-on, multifactor authentication, and conditional access to guard against 99.9% of cybersecurity attacks. Organizations can:

- Provide single sign-on, including integrated cloud apps.
- Enforce multi-factor authentication.
- Secure cloud resources for hybrid workstyles
- Automate user provisioning and enable self-service password reset

Pricing estimate for SMB customer infrastructure

Based on Azure pricing for 50-person Azure Active Directory with supporting infrastructure.[1]

Deliver great value

Significantly improve your customer experience for less than $200.

1. See the table below for estimated costs.
2. Watch the Azure Pricing and Packaging Webinar for an in-depth discussion of Azure pricing principles
3. Test out your specific customer environment with the pricing calculator.*

Pricing calculator

Azure Pricing and Packaging Webinar

*You can optimize costs with Azure Reserved Instances

Note: Azure AD P1 comes with Microsoft 365 Business Premium (M365 BP). This is Microsoft's recommended purchase option. Customers without M365 BP can purchase Azure AD P1 separately.

Service type	Region	Description	Estimated monthly cost	Estimated upfront cost
Azure Active Directory P1	East US	50 users Premium P1, 0 users Premium P2, Standard tier, 730 directory objects, User forest hours {5, Resource forest hours {7}.	$0 Without M365 BP: $309.75	$0.00
Virtual Network		100 GB data transfer	$4.00	$0.00
VPN Gateway	East US	VPN Gateways, Basic VPN tier, 730 gateway hours, 10 S2S tunnels, 128 P2S tunnels, 0 GB, Inter-VNET outbound VPN gateway type	$26.28	$0.00
If you need a cloud domain controller for legacy applications, group policies, etc. add the following VM to your solution. Estimates do not include Domain Controller.				
Virtual Machines - Domain Controller	East US	1 D2s v4 (2 vCPUs, 8 GB RAM) x 730 Hours; Windows – (OS Only); Pay as you go; 0 managed disks – S4	$137.24	$0.00
		Estimated Total Monthly Cost with Microsoft 365 BP **Without Microsoft 365 Business Premium**	**$177.27** **$477.27**	**$0.00**

1. All costs are assumptions based on estimates from the Azure Pricing calculator and are not a guarantee of pricing for purchase. Prices may change based on region, working hours, and other variables. Because prices are subject to change, please use the Azure pricing calculator for your own estimate.