Ping and Microsoft Azure AD

SEAMLESS SECURITY FOR HYBRID IT ENVIRONMENTS
Navigating Your Journey to the Cloud

The race is on to move to the cloud. But getting there often presents challenges. Not every on-premises application has a SaaS substitute, and some on-premises software can’t effectively migrate to a private cloud. As a result, hybrid IT is a reality for almost every large enterprise, where resources are stretched across SaaS, cloud and on-premises data centers.

In this hybrid environment, you still need to provide your users with the ability to authenticate and gain secure access to all of their applications, whether SaaS, on-premises or in any private or public cloud. Yet, many identity and access management (IAM) solutions aren’t able to support hybrid IT well or at scale. The complicated workarounds required to connect disparate environments can delay your cloud strategy, increase risks and costs, and even hurt the user experience.

The combination of Ping Identity + Microsoft Azure AD smooths the way for enterprises operating in hybrid IT environments. It enables secure and seamless access for all of your users to all of their applications, regardless of their authentication route or where applications reside.
The partnership between Ping and Microsoft enables you to connect the Azure AD multi-tenant, cloud-based directory to your hybrid IT enterprise. Our joint solutions focus on seamless and user-friendly security for a hybrid IT environment, where you might have on-premises, private cloud and SaaS applications, many of which are non-Microsoft.

Ping provides solutions that connect your Microsoft and non-Microsoft infrastructures. We make leveraging Office 365 and Azure AD easier, more secure and productive for your enterprise. Whether your user’s journey starts with authenticating via on-premises Active Directory or cloud-based Azure Active Directory, their experience is the same: seamless, secure access to all applications, regardless of where they reside.

To bridge your disparate environments, Ping Identity offers three major integration capabilities with the Microsoft Cloud:

1. PingAccess for Azure AD: for users who authenticate in Azure AD to gain secure access to all of their on-premises or private cloud applications, without the need for a VPN.

2. PingFederate + Office 365: for users who authenticate on-premises and need a federation bridge using Azure AD Connect to securely access Office 365 and applications controlled by Azure AD.

3. PingID for Azure AD & PingID for Active Directory Federation Services (ADFS): for users authenticating either using on-premises Active Directory or Azure AD; provides strong multi-factor authentication (MFA) and contextual authentication policies.
PingAccess for Azure AD

Azure AD provides secure single sign-on (SSO) for thousands of cloud and on-premises web applications, from any device. With PingAccess for Azure AD, you can get secure single sign-on to more on-premises or private cloud applications than with Azure AD alone.

Azure AD provides SSO and secure remote access to on-premises web apps through Application Proxy, a component of Azure AD. Azure AD Application Proxy enables a secure connection to your on-premises applications without the need for a VPN. With Azure AD Application Proxy, you can publish applications—such as SharePoint sites, Outlook Web Access and web-based apps—to make them accessible to your mobile workforce and partners.

Large enterprises can rely on hundreds or even thousands of mission-critical legacy applications. PingAccess for Azure AD can serve as a gateway, enabling SSO to even more of these on-premises apps. By integrating with Application Proxy, PingAccess lets your users use a single, Azure AD-connected identity to access on-premises web apps—without the need for VPN and including those that use header-based authentication or are protected by web access management (WAM) systems.
PingFederate to Office 365 Using Azure AD Connect

With the integration of PingFederate and Azure AD Connect, PingFederate users gain a simple way to federate on-premises Active Directory with Azure AD. This integration enables fast and simple configuration of PingFederate and Azure AD, which in turn provides your users with convenient access to Office 365.

To set up the federation bridge, simply select “Federation with PingFederate” in the User Sign-in section of the Microsoft Azure AD Connect installation wizard. Azure AD Connect handles the configuration and sends a file to PingFederate with the settings needed to federate to Azure AD and Office 365.

Because federation is critical to your enterprise, you need a powerful federation bridge that can enable connections to on-premises applications, SaaS applications and Microsoft Azure applications (like Office 365), while still being able to connect to applications in other virtual clouds. PingFederate + Azure AD Connect simplifies the configuration of federating from on-premises Active Directory to Azure AD, so you can grant employees secure SSO access to their productivity suite, a critical first step in any identity project.
PingID for Azure AD & PingID for ADFS

Authenticating with usernames and passwords alone is outdated and risky, especially for sensitive data and applications. PingID for Azure AD and PingID for ADFS add contextual multi-factor authentication (MFA) to your users login protocol for an added layer of security.

MFA—which requires an additional form of authentication based on something you have (like a mobile device) or something you are (like a fingerprint)—is a proven security measure that can reduce the risk of data breach. PingID is an identity-as-a-service (IDaaS), adaptive MFA solution. It provides contextual MFA that allows you to step up authentication requirements only when warranted and based on policies you define. This allows you to balance security with user experience.

When sensitive data or transactions are involved, your users are becoming more accepting, even welcoming, of additional authentication requirements because of the added peace of mind they experience. PingID’s integration with both Azure AD and ADFS allows you to define and enforce authentication policies that are tailored to your specific requirements. PingID for Azure AD and PingID for ADFS provide support for all of your enterprise use cases, giving you the freedom to apply MFA everywhere it is needed for your employees, partners and customers.
While the push is on to migrate to the cloud, hybrid IT environments are a common reality for large enterprises, at least for the foreseeable future. With your applications spread across SaaS, cloud and on-premises data centers, you need a flexible IAM solution that can bridge these disparate environments. Ping Identity + Microsoft Azure AD provides the security you need and the convenience your users expect.

For more information about how Ping Identity and Microsoft joint solutions can smooth your cloud migration, please contact us.
About Microsoft Azure AD

Microsoft (MSFT) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more. Azure Active Directory (Azure AD) helps you manage user identities and create intelligence-driven access policies to secure your resources. As an integral component of Office 365, Azure and Enterprise Mobility + Security, Azure AD centralizes identity and access management to enable deep security, productivity, and management across devices, data, apps, and infrastructure. Learn more

About Ping Identity

Ping Identity envisions a digital world powered by identity. As the identity security company, we simplify how the world's largest organizations prevent security breaches, increase employee and partner productivity and provide personalized customer experiences. Enterprises choose Ping for our identity expertise, open standards leadership, partnership with companies like Microsoft, Amazon and Google, and collaboration with customers like Boeing, Cisco, GE, Kraft Foods, Walgreens and over half of the Fortune 100. The Ping Identity Platform allows enterprises and their users to securely access cloud, mobile and on-premises applications while managing identity and profile data at scale. Architects and developers have flexible options to enhance and extend their existing applications and environments with multi-factor authentication, single sign-on, access management, API security, directory and data governance capabilities. Visit www.pingidentity.com.