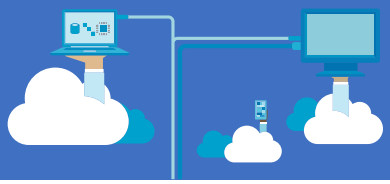
Microsoft Azure

Hybrid Identity

Don't get **Boxed In**

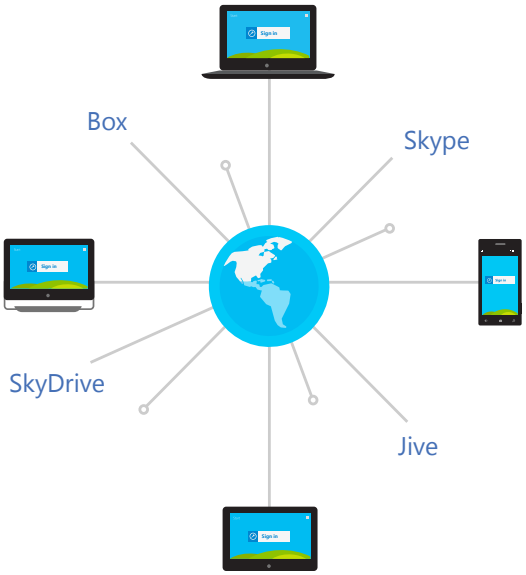
Hybrid Identity



Solving the Enterprise Identity Crisis

Today's enterprise worker expects that they can work from anywhere, through multiple devices, and without any change to the capabilities and tools they have access to. And with the proliferation of cloud services, their needs are getting increasingly more complex as users consume more online applications, such as Office 365 and salesforce.com. So here's the challenge: when planning for identity management in the cloud, how do you satisfy frustrated users who are juggling multiple passwords, unburden overworked IT teams managing individual and group access to resources from many different devices, and thwart attackers from exploiting new ways to gain unauthorized access to your organization's assets?

This is the Enterprise identity crisis, and it is a very real issue facing IT today. In this new mobile first, cloud first world—it is critical to choose a provider that has a comprehensive identity solution that doesn't require you to cobble together offerings from multiple vendors. This solution must also improve access security, combat password sprawl, reduce complexity and service costs, and enhance user productivity, on-premises and off. So how do you know which provider will solve your identity crisis versus add to it?

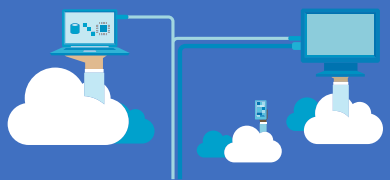


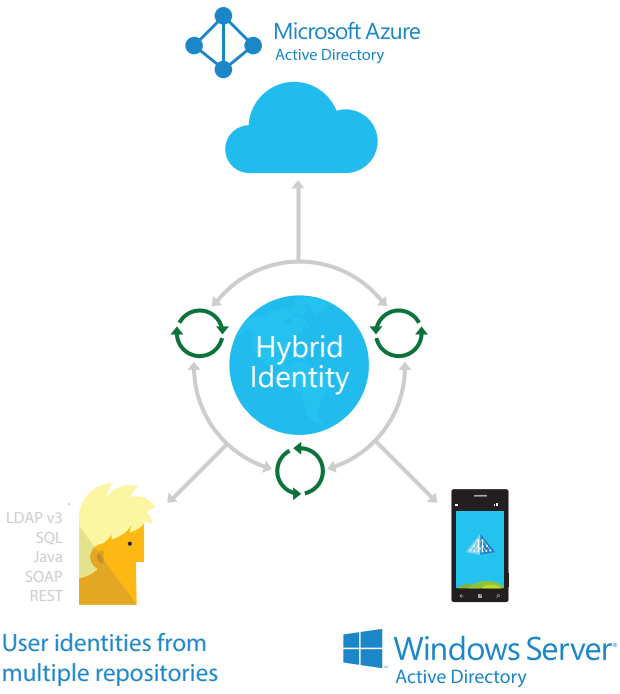
Extending Your Identity Platform to The Cloud

Some cloud services providers, such as Amazon Web Services (AWS), provide identity management for their own services. But they leave it to you to figure out how to unify your on-premises and cloud identity management. With thousands of organizations worldwide using Windows Server Active Directory (AD DS) on-premises, organizations don't want to reinvent identity management or create net new identities for the cloud. With Azure Active Directory (Azure AD) they don't have to.

Azure AD is a comprehensive identity management platform that combines core directory services, identity governance, security, and application access management. It offers a single identity management platform for access control to applications, based on centralized policy and rules, which enables a single identity platform across services, on-premises and in the cloud, and clouds outside the IT landscape.

Hybrid Identity





AWS's Identity and Access Management (IAM), only provides access management for AWS specific solutions, compared to Azure AD which provides organizations one comprehensive solution, for all of these scenarios:

- Maintaining one repository for all on-premises and cloud identities
- Managing access to applications on different clouds including Azure, AWS, and salesforce.com
- Single Sign-On (SSO) access to thousands of cloud-based and on-premises applications
- Monitoring and Reporting with advanced machine-learning based analytics
- Protecting access to enterprise applications by using multiple authentication layers and conditional access policies
- Personalizing access and self-service capabilities
- Publishing on-premises applications to external users through Azure AD

Azure Active Directory enables organizations to efficiently sync user accounts from their on-premises directories, which simplifies configuring SSO. To make SSO set up easier, Azure has pre-integrated popular cloud apps in an application gallery, regardless of the where the application is hosted!

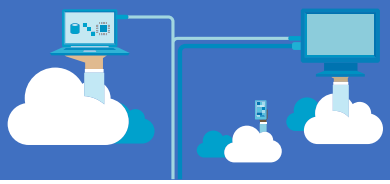
In addition, the Azure Management Portal simplifies managing identities and apps. Enabling custom and purchased LOB apps for SSO, and assigning them to the appropriate users and groups is straightforward. And when an administrator assigns access to pre-integrated SaaS applications by using the Azure Portal, users can see shortcuts to these apps on a single personalized web page that is hosted on Azure.

With the Azure AD identity management solution, administrators can manage a growing number of users and SaaS apps that live on other clouds from the same console with the same processes. Compare this to using AWS IAM, which offers only identity for AWS services and does not address other cloud services, or on-premises applications. With providers like AWS, you only add to your identity crisis versus solving it with Azure AD.

"Convenience is essential to our users. They want to get into their applications and get their work done as quickly as possible. They can do that more easily with Azure Active Directory."

Toon Dillen, IT Manager, Dillen Bouwteam

Source



That's one great value of operating the Azure Active Directory identity management solution: administrators can manage a growing number of users and SaaS apps that live on other clouds from the same console with the same processes. Compare this capability to AWS IAM, which offers only identity for AWS services and does not address any other cloud service.

Capability	Azure AD	AWS IAM
Single sign-on	✓	
User self-service support	✓	
Manage user access to any cloud app	✓	
Synchronize user identity on-premises and in the cloud	✓	

The Value of Cloud-Based Identity Management

Cloud identity management should simplify IT not make it more complex. For example, Azure Active Directory enables IT to minimize support efforts through enabling self-service for employees, delegating tasks such as password reset, and creating and managing their own groups for collaboration and access to resources, whether they are on-premises or in the cloud. And being able to control how SaaS apps are created, published, and used is a great productivity enhancement for both IT and end users.

What about security? Azure Multi-Factor Authentication provides a second level of authentication that helps prevent unauthorized access to both on-premises and cloud applications. Achieve further protection by using security monitoring, alerts, and advanced machine learning-based reports that identify inconsistent access patterns, such as unknown source logins, multiple failed logins, logins from multiple geographies and even logins from possibly infected devices. These reports provide insights to improve access security and respond to potential threats.

Azure Hybrid Identity Offers Superior Value

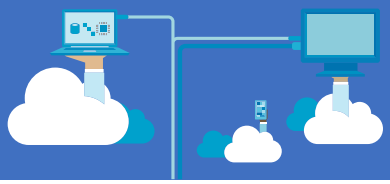
Microsoft brings decades of on-premises identity management experience to the cloud through Azure AD—combining core directory services, advanced identity governance, security, and application access management. It offers an identity management platform to deliver access control to applications, based on centralized policy and rules that enables a single identity platform that can be used across services, on-premises, and in the cloud.

"For physicians, every second counts. If they need to get into an application right away to view an x-ray, for example, they can do that quickly and securely with Azure Multi-Factor Authentication."

Mike Baran, System Director, Technology, Presence Health

Source

Hybrid Identity



Azure AD offers native hybrid identity management capabilities that AWS fails to provide:

- Single sign-on to applications in any public cloud and on-premises
- User self-service support for password and group management
- Comprehensive management of user access to cloud apps
- Advanced machine-learning based security reports

Your users and management are asking you to find a way to connect and synchronize their on-premises identity management system with numerous cloud applications in a seamless way, talk with various protocols, and scale globally—all with improved security. Why get boxed-in with AWS when Azure AD enables you to authenticate users wherever they are from any device in a way that integrates simply with their existing identities. Choose a cloud provider that solves your identity crisis with Azure AD.

To learn more, please visit:

Comparing Microsoft Azure and Amazon Web Services
http://azure.microsoft.com/en-us/campaigns/azure-vs-aws/

Hybrid identity management
http://www.microsoft.com/en-us/server-cloud/solutions/identity-management.aspx

What is Azure Active Directory?
http://azure.microsoft.com/en-us/services/active-directory/

Cloud identity and access management
http://azure.microsoft.com/en-us/documentation/infographics/cloud-identity-and-access/