Azure Active Directory, Identity and Access Management, and Windows 10

Jack Madden, TechTarget

WHITE PAPER

Table of Contents

Microsoft Azure Active Directory serves several roles: It's an identity and access management service; it's a cloud-based directory; it can be used to enroll devices into other management systems; and it provides integrated identity management in Windows 10.

Why identity and access management, and what's different now?

Identity and access management (IAM) concepts have been around for years. But more recently the rise of cloud services, SaaS applications, mobile devices, BYOD, and general consumerization of IT trends have made IAM crucial for end user computing.

One of the first and most important functions of IAM services is to provide identity federation and enable single sign on, allowing users to use one

SPONSORED BY

Microsoft

TechTarget Custom Media

A TECHTARGET WHITE PAPER

username and password across multiple applications that reside both within and outside of corporate networks.

Instead of authenticating to individual cloud services with unique credentials, users instead can authenticate to an IAM service. The IAM service (acting as what's known as an identity provider) can use a federation protocol to pass information about the user to other applications (referred to as service providers). IAM services can also in turn use other sources to authenticate users. (An example of this scenario would be using on-premises Active Directory, exposed via Active Directory Federation Services, in conjunction with a cloud-based IAM service.)

Common protocols for federation include SAML, OpenID, OAuth, and WS-Fed. For applications don't support any protocols, IAM services can resort to storing and automatically filling passwords.

Since authentication happens only with one service, advanced authentication techniques like multi factor authentication only have to be set up once.

The benefits—both for security and user convenience—are obvious. With only one password to remember, users are much less likely to resort to unsafe practices.

The other important role of IAM services is access management. IT can use policies to determine which users are allowed to access different applications, and under what circumstances. An IAM platform can also disable a user's access to all applications, instantly—another significant security benefit over having unique credentials for each application.

IAM services can also be used to automatically provision user accounts or modify user attributes in applications, making it easier to adopt SaaS applications. Some identity protocols have specifications to support provisioning, however many provisioning integrations are custom built.

Setting up federations for multiple applications—especially in light of rapid SaaS adoption and the landscape of multiple evolving standards—is not easy. Today many companies are turning to vendors that provide identity and access management as a service. These vendors can take care of maintaining integrations and setting up new ones.

IAM services have a lot of visibility into user behavior—they can see which users are accessing different services, where and when they're doing it, and often from what device. This provides an opportunity to apply policies and analyze usage, further increasing security.

Azure Active Directory as an IAM

All of the attributes of identity and access management services discussed so far are present in Microsoft Azure AD.

Azure AD supports multiple federation protocols, including SAML, WS-Fed, OAuth, and OpenID Connect. Azure AD provides password management for applications that don't support any protocols (Microsoft calls it "password single sign on"), and the SCIM protocol for account provisioning. Azure AD also acts as the built-in identity and access management system for Microsoft's SaaS products, including Office 365, Intune, and OneDrive.

Like any IAM service, integrating support for third-party applications is a constantly evolving process. Microsoft provides the Azure Active Directory Marketplace as a catalogue of current integrations.

Most companies will also have a significant number of on-premises applications, and to manage these, Azure AD has an on-premises application proxy. Remote users can access on-premises applications

over the internet without a VPN by using a reverse proxy. The IAM infrastructure of Azure AD provides all the same opportunities to create access policies.

Almost all companies already have existing on-premises user databases in Active Directory, and companies don't want to set up an entirely new, separate user database in their IAM service. For this reason, Microsoft provides Azure Active Directory Connect, a tool to sync users, groups, and attributes to Azure AD. Azure AD Connect replaces several previous tools, including DirSync and Azure AD Sync.

One of the more important implementation decisions is where authentication will happen. Azure AD Connect can sync password hashes from on-premises Active Directory, so that users can authenticate to both services with the same credentials.

However, some companies prefer to continue to authenticate users with their existing on-premises Active Directory. User identities can be federated to Azure AD via Active Directory Federation Services.

Azure AD can use policies to make automatic conditional access decisions when users attempt to access applications. Policies can block, allow, or require multi factor authentication based on application, user group, and user location.

Access to Azure AD itself can require multi factor authentication, and can also be blocked or allowed by device registration status, device management status, or device health status (for Windows 10).

Azure Active Directory and devices

Azure AD can play a significant role with devices, enabling IT to enroll them into management platforms and create richer access policies for applications.

Azure AD can become aware of iOS, Android, Windows Phone, and Windows 7, 8, and 8.1 devices using the Azure AD Device Registration service. Registering a device installs a certificate on it and creates a record of it in Azure AD. The certificate can be used as a factor to authenticate without having to enter other credentials, or as a second factor alongside other credentials. (Device Registration is also sometimes referred to as Workplace Join.)

Device Registration does not actually give Azure AD any direct control over a device—there's no scripting, no Group Policy, nor any other management tools. This is one of the primary differences between Azure AD and Domain-joined Windows computers with on-premises Active Directory.

Instead, Azure AD can use conditional access policies to require that devices are enrolled in a mobile device management (MDM) platform before they're allowed to access applications through Azure AD.

Azure Active Directory and Windows 10

Windows 10 and Azure AD is a special case. Like other mobile devices and previous versions of Windows, Windows 10 can be registered with the Azure AD Device Registration service, and conditional access policies can require MDM enrollment. However, in Windows 10 device registration is called Azure AD Join, and it enables several additional features.

Azure AD is integrated directly into Windows 10, so that users can use their Azure AD credentials to sign in to devices, and then receive access to cloud and on-premises applications (enabled by the Azure AD IAM infrastructure). Azure AD can also roam settings (such as wallpapers, Start Menu layout, and Wi-Fi settings) across corporate Azure AD-joined Windows 10 devices.

Azure AD is also used to enable a process for provisioning new corporate devices called the "out of box experience." Employees can buy a new device off the shelf from a retail outlet, and then the device can be joined to Azure AD during the setup process and automatically enrolled in MDM over the internet. This process is powerful enough to turn most off the shelf devices into enterprise machines without the need to re-image them or even bring them onto a corporate network. (Azure AD join requires at least Windows 10 Pro, however.)

On personally-own devices, users can sign in to Azure AD through Settings. (To the user, this is referred to as adding a work or school account.)

MDM enrollment can be required as part of this process, and users will receive single sign on access to enterprise apps through Azure AD.

Domain-joined devices that are managed through Group Policy, System Center Configuration Manager, or other client management tools can also be joined to Azure AD for all of the same benefits.

Conclusion

As devices, mobility, and SaaS proliferate, IAM services will become an essential part of end user computing.