Managing users and authentication with on-premises Active Directory for O365

Many organizations are making the move to cloud, specifically to Office 365 (O365). Recognized as the most popular business productivity software, O365 offers many benefits to today's mobile workforce. Its users reap all the benefits of a cloud service – freed up internal resources, and easy access to updates with minimal maintenance – while its administrators face the inevitable complications of hybrid identities.

With the creation of a tenant in Azure AD, O365 introduces new user management and authentication processes for IT. To optimize user account management, and avoid administrative redundancies, organizations can connect their existing on-premises Active Directory to O365 – a process also known as directory synchronization.

This report compares Microsoft's out-of-the-box tools, with third party tools, for on-premises solutions for managing users and authentication for O365.

How do you want to manage users?

On-premises management of O365 comes with complexities – despite what tools you use. Many of the complications relate to the current state of your Active Directory environment. Before getting started with your migration, you will need to do some, or in some cases, a lot of preliminary work to ensure that all the attributes you want to synchronize with Azure AD are handled properly. Microsoft offers some guidance, and a free tool (IdFix) to help. Unfortunately, it is not all encompassing, and will require scripting to pin point errors outside of its scope.

Microsoft solution (Azure AD Connect)

Many organizations will use Azure AD Connect, Microsoft's free tool, to synchronize and provision users to O365. Organizations with a well-maintained Active Directory, using the default settings in Azure AD Connect, will likely have a straightforward experience. Organizations intending to use advanced features can run in to complex scenarios. Some of the difficulty comes from setting up scheduled sync cycles, and can result in delays between when a change is made in Active Directory, and when the change appears in Azure AD. Further, depending on the number of affected users, the set up can be time consuming, and the resulting errors may be difficult to troubleshoot. To find and remediate those errors, PowerShell scripting may be required.

Third-party tools

You can also achieve synchronization with third-party tools such as Specops Authentication for O365. The solution automatically creates users in O365, and updates users during authentication using Group Policy settings, without the need for complex sync cycles. A light agent is installed in Active Directory to obtain user and group membership information. When a user logs in to O365, their account is created and the appropriate license is assigned. Remember, not all third party tools are created equal. Other tools may require you to duplicate user and group data to their own cloud directory or to recreate security groups before synchronizing to O365.

How do you want users to authenticate to O365?

O365 is a valuable target for hackers, so just a username and password will not be sufficient for securing its data. A layered method, like multi-factor authentication (MFA), is best practice for O365 authentication.

Microsoft solution (Azure MFA)

Azure MFA is Microsoft's two-step verification solution. It is included with Office 365 for Business, Azure Active Directory Premium plans and Enterprise Mobility + Security plans. Azure MFA supports phone-based MFA (phone call, text message, mobile app notification), using the password as the first authentication factor. By default, authentication options beyond phone-based factors are not supported. This poses a usability and operational challenge when a user does not have their device with them.

Physical or virtual smart cards can also be used when authenticating to O365, however several requirements must first be met, including Active Directory Federation Services (ADFS) configuration, and Azure MFA server.

Third-party tools

Specops Authentication for O365 uses a powerful multi-factor authentication engine that can replace the password during login. Alternatively, you can strengthen passwords and combine them with stronger authentication factors to move beyond a single point of vulnerability. With out-of-the-box support for 15+ identity providers, including Apple Touch/Face ID, Google/Android Fingerprint, Duo Security, Symantec VIP, Social SaaS, and various authenticator mobile apps, users always have a secure way to access important resources.

Summary

The adoption of O365 creates user management and authentication challenges. A centralized approach that leverages the on-premises Active Directory can circumvent common issues, specifically those related to data replication. If you want to manage Active Directory on-premises for O365 with increased security and minus the extra administration time, consider evaluating a third-party provider.

Start a free trial of Specops Authentication for O365!