ManageEngine
ADSelfService Plus

Making IT more efficient

with end user self-service password reset, cloud password sync, and cloud single sign-on

www.adselfserviceplus.com

Making IT more efficient with end user self-service password reset, cloud password sync, and cloud single sign-on

Since Windows 2000, organizations who use Windows Active Directory (AD) have been burdened with the need to hire support staff for resetting passwords. Without a portal or solution to allow users to reset their own password, users are forced to call IT for assistance. Now that many organizations are moving to the cloud for some of their services, the issue of password stability and consistency has grown exponentially. With new cloud user accounts and passwords, users are forced to battle with not only their Active Directory user account and password, but all their cloud-based services' user accounts and passwords as well.

The breadth of the issue

Ever since Active Directory was first introduced in 2000, users have been forgetting their passwords. Unfortunately users are often forced to contact IT in order to get their password reset. Many organizations have done cost analysis on how much money is spent on these calls, and the numbers are near $ per call.

Over the past few years, users have been moving to social media and using online services for personal use. The same users that were forced to call IT to reset passwords for their work user account were not required to call IT for their online user accounts. Instead, they were instructed to use their email and cell phone to verify themselves, and after verification they were able to reset their own password.

Not too long ago there were very few cloud services which provided password reset solutions that organizations were comfortable using. Services like those from Zoho, Amazon, Google, and Microsoft were used, but in a limited fashion. Now most organizations take advantage of at least one cloud service and some solely use cloud services. There is no question that the cloud has moved ahead and organizations have taken advantage of the benefits the cloud offers.

Not all good things come without issues, unfortunately. Each cloud application and service has a unique user database and that forces each user to have a unique user account and password. It is a common fact that users have always struggled to keep even a few user accounts and passwords under control, but now many users are struggling to stay on top of them all.

Self-service password reset

For most users, the ability to reset their own password is common place. There are not many cloud services and applications that force users to call a help desk in order for a technician to reset their password for them. For most cloud services this function is not even possible.

On the other hand, on-premises Microsoft Active Directory still does not provide a self-service password reset solution. Today, 18 years after Active Directory was created, there is still no solution for this longtime issue. Users are still forced to call the help desk or submit a ticket so that a delegated IT person can reset their Active Directory password. This has led to security loopholes, inefficiency, and lack of productivity.

If, however, users were able to reset their own password through the Windows logon page, their mobile phone, or a web portal, the entire process would be streamlined.

Figure 1 illustrates what users would see if they had an option to reset their own password on the Windows logon page.

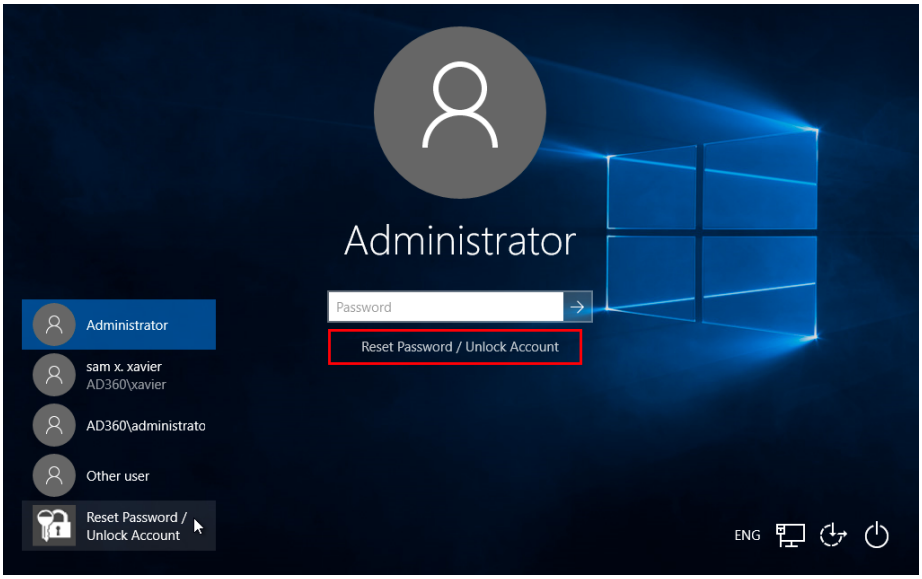

Figure 1. Update to Windows logon page for self-service password reset.

Security is of course a key concern when it comes to users resetting their own Active Directory user account password. This is why self-service password management tools like ADSelfService Plus let administrators determine which level of security and mode of verification end users can use. Figure 2 illustrates the options that ADSelfService Plus provides for verifying users when they attempt to reset their own password.

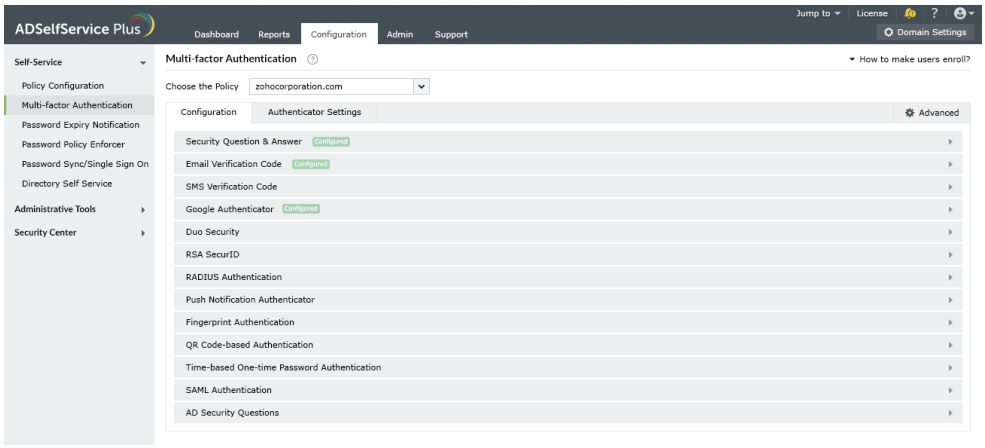

Figure 2. Self-service password reset security verification options.

Password sync with cloud apps

Users struggle to keep all their user accounts organized, separated, and secured. Users are known to write down passwords when they are overwhelmed with too many passwords. Ideally, users should have their passwords synchronized with their Active Directory user account password. This will ensure that users have one password for all systems and they only need to change their password in Active Directory, which will then be pushed out to all their cloud applications and services.

Since on-premises Active Directory is still the core of most corporate networks, it only makes sense for password synchronization to stem from this database. Therefore, no matter how the user updates their password (IT staff resets, user changes using Windows, or using a self-service password reset solution), it will be synchronized with all appropriate cloud applications and services.

Unfortunately, Microsoft does not provide a solution that will help users in this situation.

ADSelfService Plus, on the other hand, offers a simple cloud password sync solution. With support for over 10 of the most common cloud applications, synchronizing the password from Active Directory is easy and seamless for the user. Figure 3 illustrates which cloud applications are supported for password synchronization.

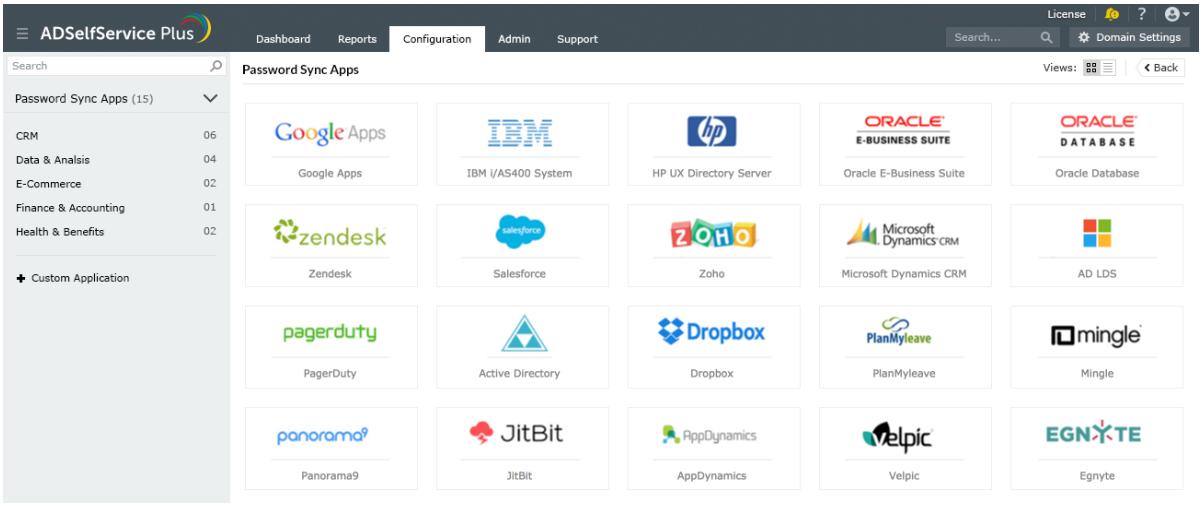

Figure 3. Cloud applications supported by ADSelfService Plus for password sync.

Single sign-on

With users resetting their own password, only to then be synced with cloud applications directly out of Active Directory, the next step is to round out end users' self-service password features by providing a single sign-on (SSO) environment. Single sign-on requires users log on one time to Active Directory, which then provides them with seamless access to their cloud applications without additional logons.

Microsoft provides a robust SSO solution that supports most cloud applications, including Microsoft's own Azure and Office 365 environments. The tragic issue with their solution is its complex configuration. Microsoft's SSO solution has three options:

- Federated Single Sign-On
- Password-based Single Sign-On
- Existing Single Sign-On

Each of these options has its advantages and disadvantages, but they all require substantial setup and additional technologies to be integrated with on-premises Active Directory and Azure.

ADSelfService Plus provides a very robust and exhaustive single sign-on environment with over 100 cloud applications supported. Figure 4 shows a partial listing of the supported cloud applications that can perform single sign-on with on-premises Active Directory.

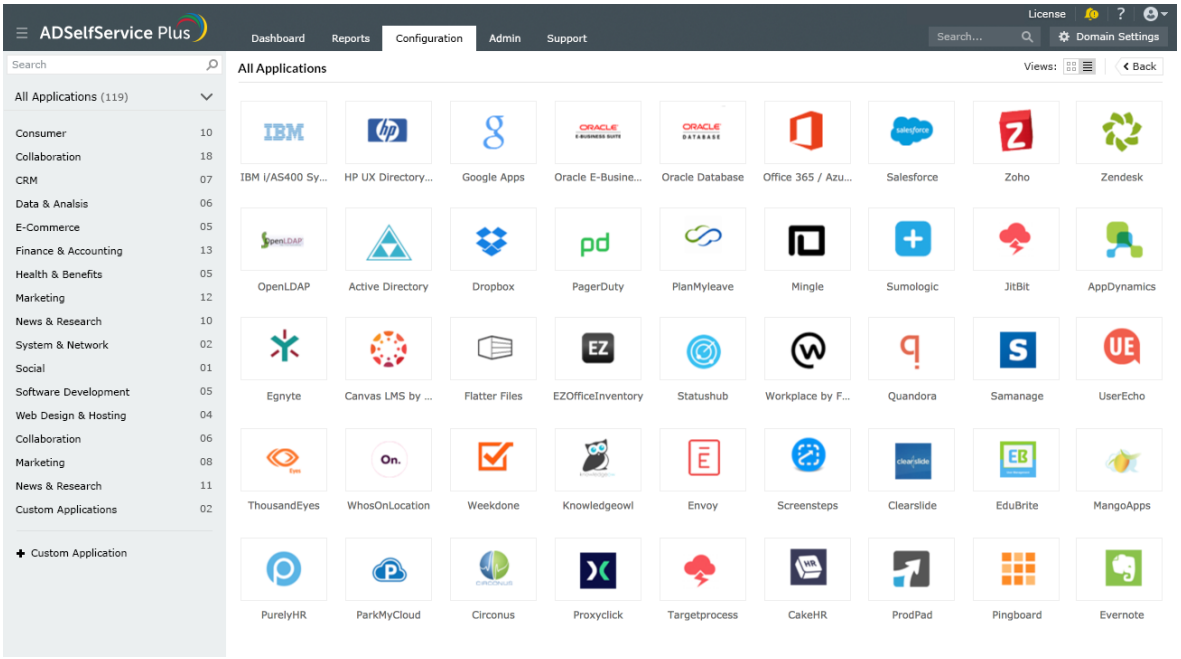

Figure 4. Supported single sign-on cloud applications in ADSelfService Plus.

The biggest benefit of using ADSelfService Plus is that it not only provides SSO, but it also ensures that users have a single username and password, due to its powerful password sync technology.

Summary

Microsoft's solutions for end-user password management and password use are not mature. Solutions like ADSelfService Plus are designed to handle self-service password reset, password synchronization, and SSO as their primary functions. Thus, ADSelfService Plus will surpass any solution provided by Microsoft due to the limitations of Microsoft's existing solutions and Microsoft's overall focus on developing solutions outside of password management.

ADSelfService Plus can be downloaded, installed, configured, and in use in under an hour. Unfortunately, Microsoft's solutions for password technologies are clumsy, difficult to install, hard to configure, and time-consuming to implement. To see how easy and robust ADSelfService Plus is for your environment, download it today here.