ManageEngine
ADSelfService Plus

Synchronizing Office 365 and Azure passwords with Active Directory passwords to help end users

www.adselfserviceplus.com

Enterprises are adopting more and more applications to enhance productivity and improve employees' user experience. Unfortunately, managing the additional passwords that come with vital applications like Office 365 creates multiple issues, including:

- Employee password fatigue from remembering numerous passwords.
- Password-related help desk calls from users who have forgotten their passwords.
- Employees resorting to highly unsafe password retention methods, like using the same password for every app or physically writing down their login information.
- Employees getting locked out of an application after numberous wrong attempts.

Challenges for Office 365 and Azure users

Operation-critical applications like Office 365 and Azure require precise administration and thereby pose several challenges, including:

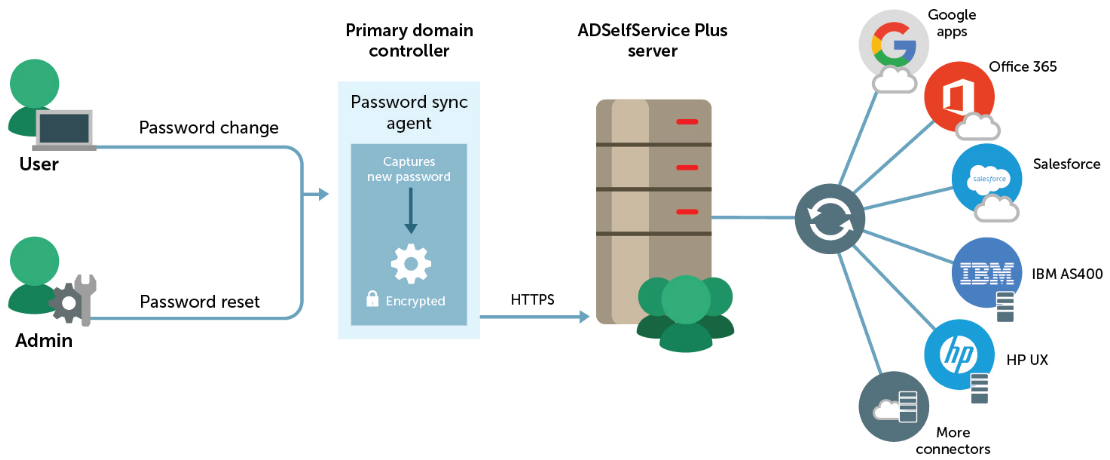
- Managing non-synchronized accounts across applications.
- Inconsistency in the frequency of password change operations. This may seem like a trivial issue at first, but when users change their Office 365 and Azure passwords at different times, its much harder for admins to track password and account expiration.
- Restricting password synchronization privileges based on users' OU or group memberships.

A simple solution

ADSelfService Plus is an integrated Active Directory self-service password management and single sign-on (SSO) solution. It offers password self-service, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and SSO for cloud applications. The solution supports real-time, Active Directory-based password synchronization for Office 365, Azure, and other popular applications to help you avoid the challenges listed above and maintain consistent credentials across all cloud applications.

How it works

ADSelfService Plus' password synchronization feature reflects password change and reset operations to the configured cloud applications in real time. Here's how the application works:



1 If an end user changes their password, the Password Sync Agent captures the new password, encrypts it, and forwards it to ADSelfService Plus' server via HTTPS.

2 ADSelfService Plus then synchronizes the password with all configured cloud applications.

3 A notification email and/or SMS is sent to the end users to let them know that their passwords have been modified.

The entire synchronization process takes less than 30 seconds.

Advantages of using ADSelfService Plus to synchronize passwords

Consistent password policies

Enforce Active Directory-based password policies for cloud applications to prevents employees from using weak passwords.

Group and OU-based access for password synchronization

Restrict password sync operations for specific applications based on user's group or OU membership; that way, employees can only synchronize passwords for the applications they officially use.

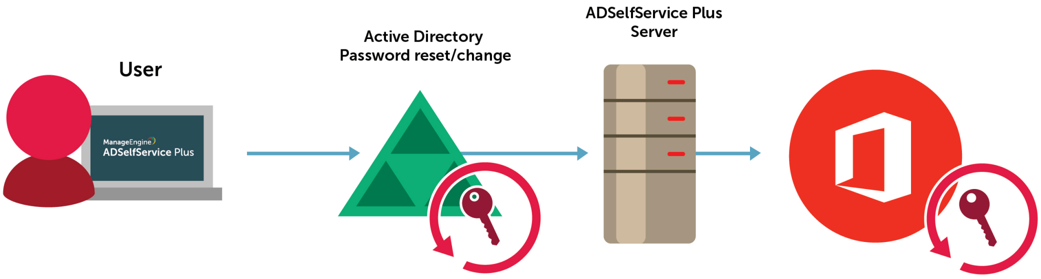
Ability to stop or continue synchronization operations based on Active Directory's operation results

Abort synchronization to other cloud applications if the password operation fails in Active Directory. End users can also include or exclude password sync for their configured cloud applications when they change or reset their passwords from ADSelfService Plus.

Self-service password reset

Even if users forget the one password they use to access all their cloud applications, they can reset their password with ADSelfService Plus without requiring any intervention from the help desk.

Configuring password synchronization for Office 365 and Azure in ADSelfService Plus


User
ManageEngine ADSelfService Plus
Active Directory Password reset/change
ADSelfService Plus Server

Prerequisites

Before you configure password synchronization *for* Office 365 or Azure, you need to install the Windows Azure AD module for Windows PowerShell on the server in which ADSelfService Plus is deployed.

Steps to install Windows Azure AD module:

- Open an elevated PowerShell prompt.
- Execute the following commands:

```
Install-module msonline

Install-module AzureRM
```

Steps to configure Office 365 and Azure accounts with ADSelfService Plus

1. Go to **Configuration > Self-Service > Password Synchronizer.**

2. Click the **Office 365 / Azure** link. You will be taken to the Office 365 / Azure configuration page.

3. Enter the domain name of your Office 365 or Azure account.

4. Enter the username and password of your Office 365 or Azure account.

5. Enter a brief description of the domain.

6. Select the Self-Service Policies by clicking the **plus icon.** Password synchronization will be possible for only those users who fall under the selected self-service policies.

7. Click **Save.**

About ManageEngine ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces. For more information about ADSelfService Plus, visit www.manageengine.com/products/self-service-password.