ManageEngine
ADSelfService Plus

# Active Directory based password synchronization

www.adselfserviceplus.com

## Real-time password synchronization for cloud applications

More and more enterprises are making the move to the cloud, which puts the applications that run on the cloud at the crux of these enterprises' IT environments. Though the cloud offers it's fair share of advantages, managing passwords for each of these cloud apps can become a burden, resulting in:

- Password fatigue from remembering numerous passwords.
- Password-related help desk calls.
- Employees resorting to highly unsafe password retention methods, like using the same password for every app or physically writing them down.

## Challenges for Salesforce users

Business critical applications like Salesforce products require precise administration and thereby pose several challenges, including:

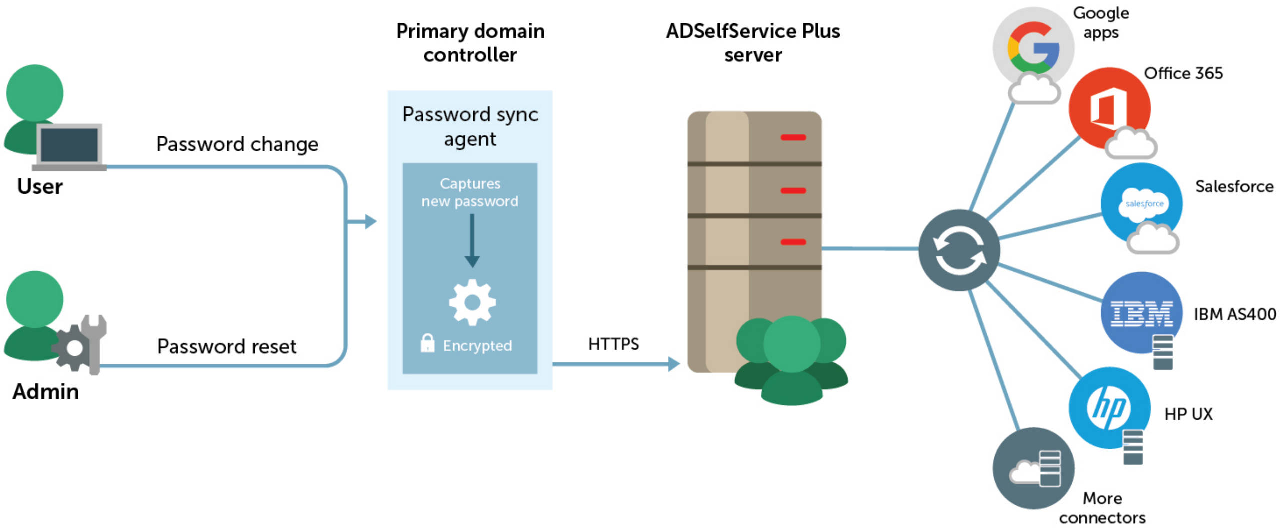
- Managing non-synchronized accounts across applications.
- Delays caused by password hassles, which can lose you a prospective client or business deal.
- Additional infrastructure required to effectively manage user account details.
- Inconsistency in the frequency of password change operations. This may seem like a trivial issue at first, but when the magnitude of change operations comes to light, it takes a toll on the IT support staff.

## A simple solution

ADSelfService Plus supports real-time Active Directory-based password synchronization for Salesforce and other popular applications to help you avoid these types of issues and maintain consistent credentials across all cloud applications.

## How it works

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



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

2 ADSelfService Plus then synchronizes the password for all the 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 process—from start to completion of synchronization between all applications—takes less than 30 seconds.

## Advantages of using ADSelfService Plus to synchronize passwords

### Consistent password policies

By using ADSelfService Plus for password sync, administrators have the option to enforce Active Directory-based password policies from within the application. This prevents employees from using weak passwords for cloud applications.

### Group and OU-based access for password synchronization

ADSelfService Plus also acts as a directory synchronization tool for passwords. With ADSelfService Plus, admins can restrict password sync operations to certain applications for specific users by providing access based on groups or organizational units. This way, employees can only synchronize passwords for the applications that they officially use.

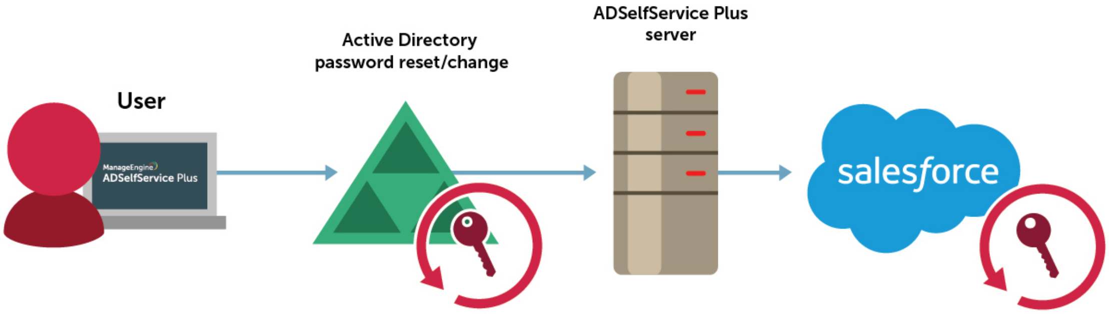
### Ability to revert or proceed synchronization operations based on Active Directory's operation results

Administrators have the ability to abort synchronization to other cloud applications if the password operation fails within Active Directory. Although this isn't a mandatory setting, administrators can save effort spent on these types of password-related issues by utilizing this setting. Moreover, end users also have the ability to include or exclude password synchronization for their cloud applications when they perform password resets or changes.

### 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.

## How to configure password synchronization for Salesforce in ADSelfService Plus



Many enterprises use Saleforce as their customer relationship management (CRM) software. Here's how to configure password synchronization for Salesforce to maintain a consistent experience:

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

2. Click Salesforce. You will be presented with the Salesforce configuration page.

3. Enter the domain name, username, password, and security token of your Salesforce account.

> **Steps to get the security token:**
>
> a. Log in to your Salesforce admin account.
>
> b. Navigate to <Your Login Name> (located at the top right corner) > My Settings > Personal > Reset My Security Token.
>
> c. In the page that opens, click Reset Security Token.
>
> d. The new security token will be sent to the email address in your Salesforce personal settings.

4. Enter the Client ID and Client Secret of the ADSelfService Plus app from your Salesforce account.

> **Steps to get the Client ID and Client Secret:**
>
> a. Log in to your Salesforce admin account.
>
> b. Navigate to Setup > Build > Create > Apps > Connected Apps and click the ADSelfService Plus app you created.
>
> c. Here, you'll be able to see the Consumer Key (which is the Client ID) and the Consumer Secret (which is the Client Secret).
>
> **Note:** Follow the steps found here to create a custom app for ADSelfService Plus.

5. Click the Plus icon to select the self-service policies. Password synchronization will be possible for only those users who fall under the selected self-service policies.

6. Click Save.

## About ManageEngine ADSelfService Plus:

ADSelfService Plus is an integrated Active Directory self-service password management and single sign-on solution. It offers password self-service, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and single sign-on for cloud applications. ADSelfService Plus supports IT help desks by reducing password reset tickets and spares end users the frustration caused by computer downtime.

Want to learn more? Click here to try out a free, 30-day trial of ADSelfService Plus.