ManageEngine
ADSelfService Plus

The benefits of synchronizing G Suite and Active Directory passwords

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

- End user password fatigue from having to remember additional 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.

Challenges for G Suite users

Operation-critical applications like G Suite require precise administration; otherwise, you might run into several challenges, including:

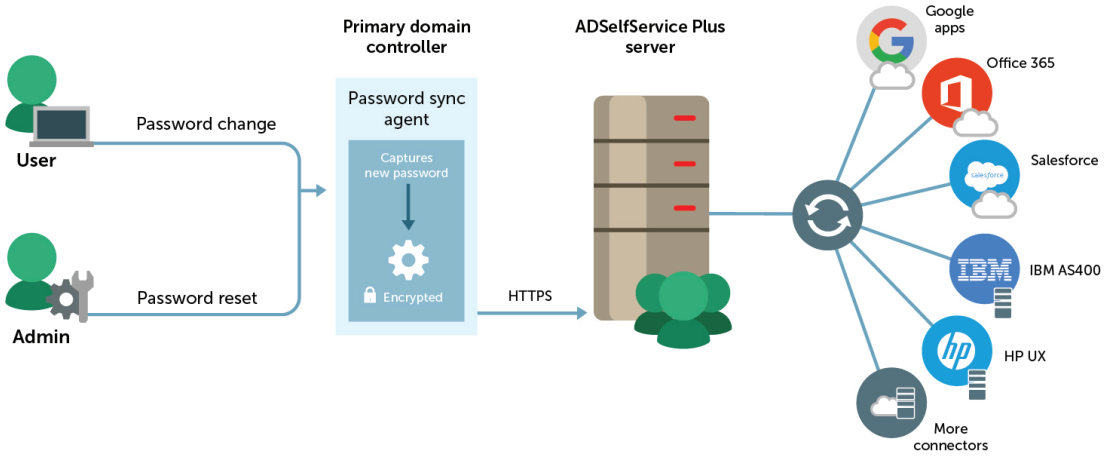
- Managing non-synchronized accounts across applications.
- Inconsistency in the frequency of password change operations. This may seem like a trivial issue at first, but when users change their G Suite passwords at different times, it's much harder for admins to track password and account expiration.
- Restricting access to password synchronization 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. With real-time, Active Directory-based password synchronization for G Suite and other popular applications, ADSelfService Plus helps 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 in your 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 user letting them know that their password has 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 prevent employees from using weak passwords.

Group and OU-based access for password synchronization

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

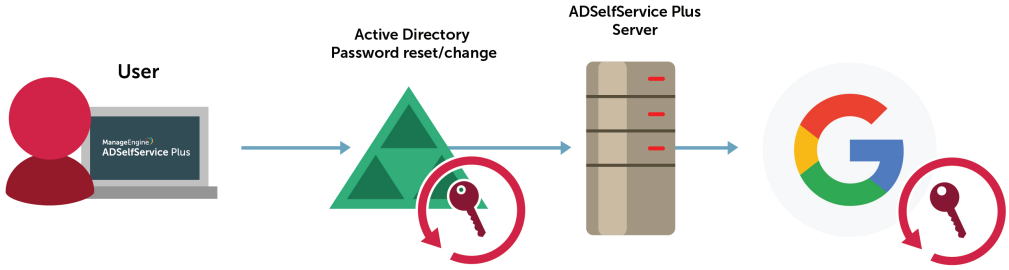
Ability to stop or continue syncing passwords based on Active Directory's operation results

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

Self-service password reset

Even if users forget the 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 G Suite in ADSelfService Plus



Many enterprises use G suite for keeping their organizations up and running. Here's how to configure password synchronization to maintain a consistent experience for users:

Enable API access in G Suite

Before you can configure password synchronization between G Suite and ADSelfService Plus, you have to enable Domain Admin API access in G Suite.

1. Go to the Google API Dashboard.
2. Log on using your G Suite administrator account.
3. Create a new project named **ADSelfService Plus.**
4. In the left pane, click **Library**. Under G Suite APIs, locate **Admin SDK** and turn it on.
5. In the left pane, click **Credentials.**
6. On the right-hand side, click **Create Credentials** and select **Service Account Key.**
7. Click the drop-down menu under Service account and select **New service account.**
8. Enter a name for the service account and provide the service account with the role of project owner.

9. Set the key type as P12 and click **Create.** You will now receive a P12 file. Save this file to your computer and click **Close.**
10. Click on **Manage service accounts.**
11. Click on the options next to the service account you created, and select **Edit.**
12. Mark the checkbox next to Enable G Suite Domain-wide Delegation, enter a name in the Product name for the consent screen text box, and click **Save.**
13. Click on **View Client ID** under the options column and copy the value from the client ID field.
14. The service account email should match the one listed in the Service account field.

Delegate domain-wide authority to your service account

The service account you created needs to be given access to the G Suite domain's user data that you want to access.

1. Go to your G Suite domain's Admin console.
2. Select **Security** from the list of controls.
3. Select **Advanced settings** from the list of options.
4. Select **Manage API client access** in the Authentication section.
5. In the Client name field, enter the service account's **Client ID** that you copied earlier.
6. In the One or More API Scopes field, enter the list of scopes that your application should be granted access to. For example, if you need domain-wide access to users, groups, and organizational units, enter:
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.group
   - https://www.googleapis.com/auth/admin.directory.orgunit
7. Click the **Authorize** button.

Your service account now has domain-wide access to the Google Admin SDK Directory API for all users in your domain.

Configure G Suite password synchronization in ADSelfService Plus

1. Log in to **ADSelfService Plus** with administrator credentials.
2. Go to **Configuration > Self-Service > Password Synchronizer.**
3. Click the **G Suite** link. In the G Suite configuration page that opens, select **Password Synchronizer** as the **Module** from the drop-down list.
4. Enter the **domain name** (e.g. adselfserviceplus.com) of your G Suite domain.
5. Enter the **User Name** (e.g. demo@adselfserviceplus.com) of your G Suite admin account.
6. Enter the **Service Account Email** (e.g. 428499212222-9csoom2llko9292ro21rhm411214lkrh@developer.gserviceaccount.com), you created earlier in G Suite.
7. Select the relevant **P12 key file** of your G Suite admin account.
8. Enter a brief **description** of the configuration.
9. Select **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.
10. Click **Save.**