ManageEngine
ADSelfService Plus

Secure single sign-on
for cloud applications

Secure single sign-on for cloud applications

Traditional on-premises tools used to rule the IT environments of most organizations, but now cloud applications have taken center stage. As organizations continue to adopt cloud applications, each product demanding a complex password, users are faced with too many passwords to remember, resulting in:

- Password fatigue from a mountain of passwords.

- Increased help desk calls due to forgotten passwords and locked out accounts.

- Decreased employee productivity from password-related issues.

- Increased security risks due to weak passwords or end users using the same passwordfor multiple applications.

Although passwords are just strings of characters, they can cause so many issues if not handled properly.

ADSelfService Plus helps unify identities across applications and simplifies the login process using single sign-on (SSO). It allows users to enter a username and password just once, and access multiple cloud applications from a centralized console. With ADSelfService Plus' SSO, you can minimize password security issues, increase productivity, and ease identity management challenges, while also enhancing user experience.

Seamless, one-click access to cloud apps

One of the major benefits of SSO from a user's perspective is convenience. With SSO from ADSelfService Plus, users are no longer required to remember numerous passwords and struggle at the log in screen thinking about which password is for which application. All they have to do is simply log in to ADSelfService Plus once and click on their desired cloud app. The app will open in a new tab and they will be automatically logged in. The list of supported apps is quite exhaustive and includes all critical applications such as Office 365, G Suite, Salesforce, and more.

ManageEngine
ADSelfService Plus

Two-factor authentication for cloud logins

ADSelfService Plus protects access to cloud applications with multifactor authentication.
This is how it works:

First factor authentication

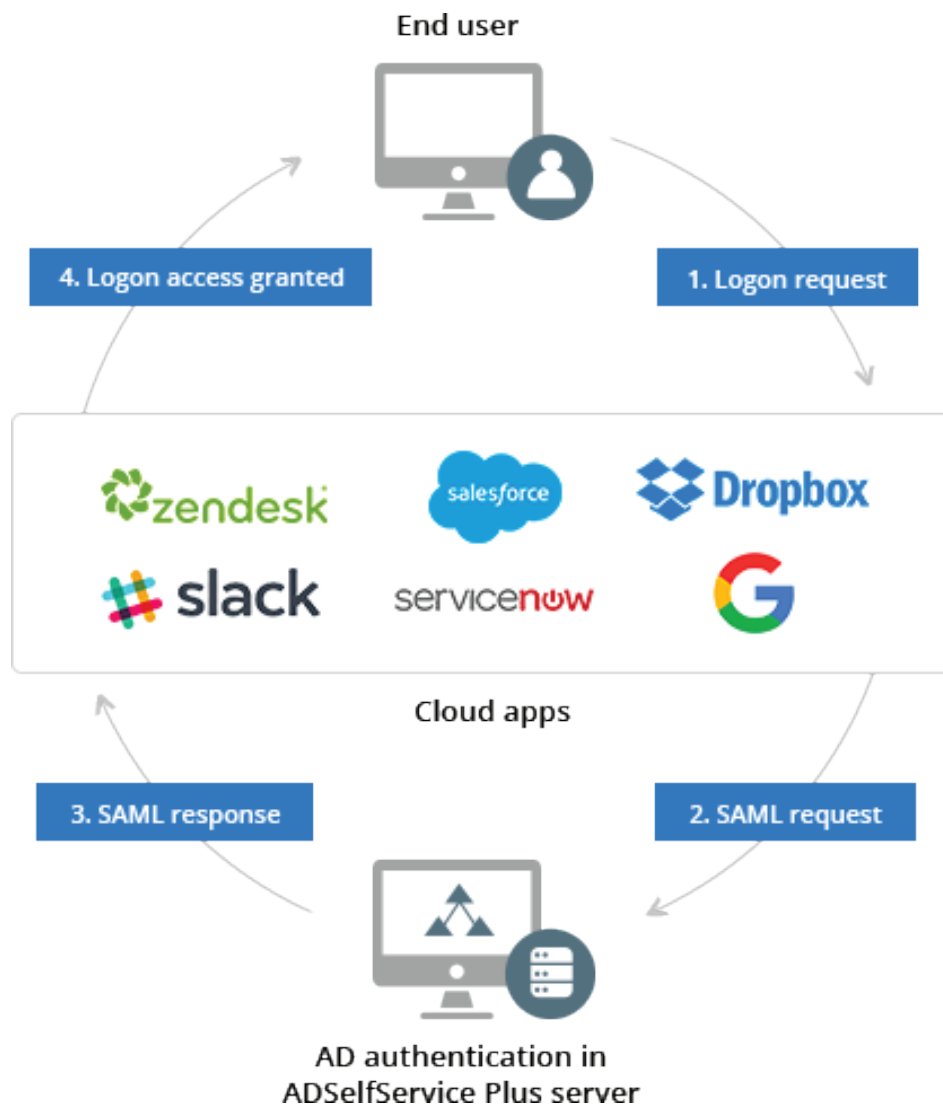**Second factor authentication**
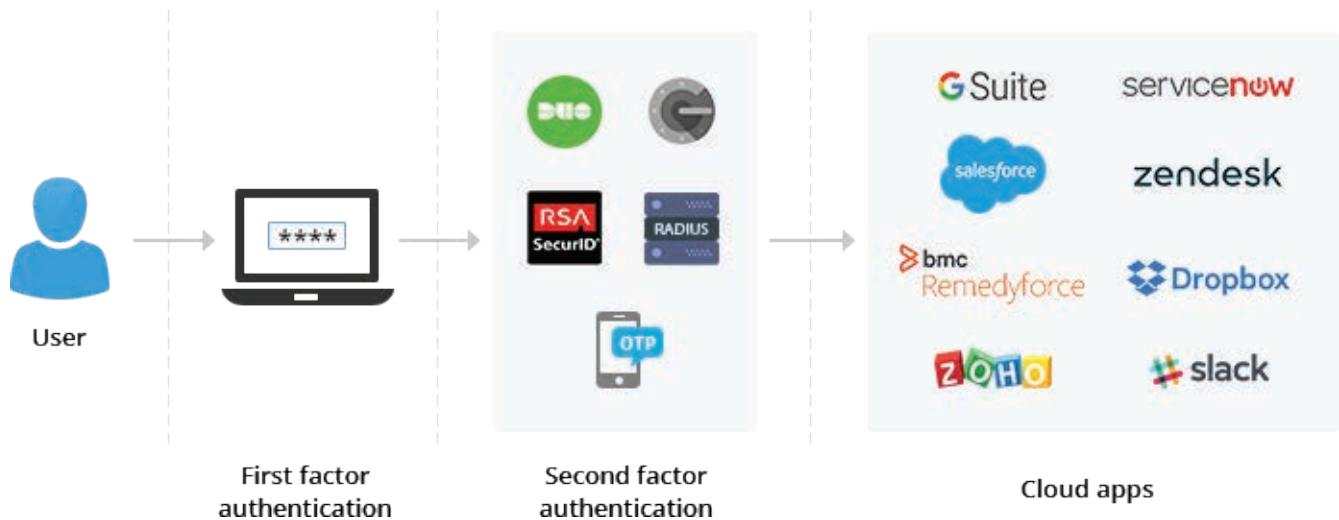
Cloud apps

- When SSO is enabled, users must first log in to ADSelfService Plus using their Windows Active Directory domain credentials to prove their identity before they can access any cloud applications.

- Next, users must authenticate themselves using a second authentication factor as chosen by you, the admin.

- Once successfully logged in, users can access cloud applications from the Applications tab. All they need to do is click on an application's icon to open it in a new tab. Best of all, the user is automatically logged in to the application.

- Even if users try to access an SSO-enabled cloud application by directly entering its URL in a browser, they will be redirected to the ADSelfService Plus login page for authentication.

ADSelfService Plus supports SMS and email one-time passcode (OTP) verification, Duo Security, RSA SecurID, RADIUS, and Google Authenticator for verifying users' identities.

ManageEngine
ADSelfService Plus
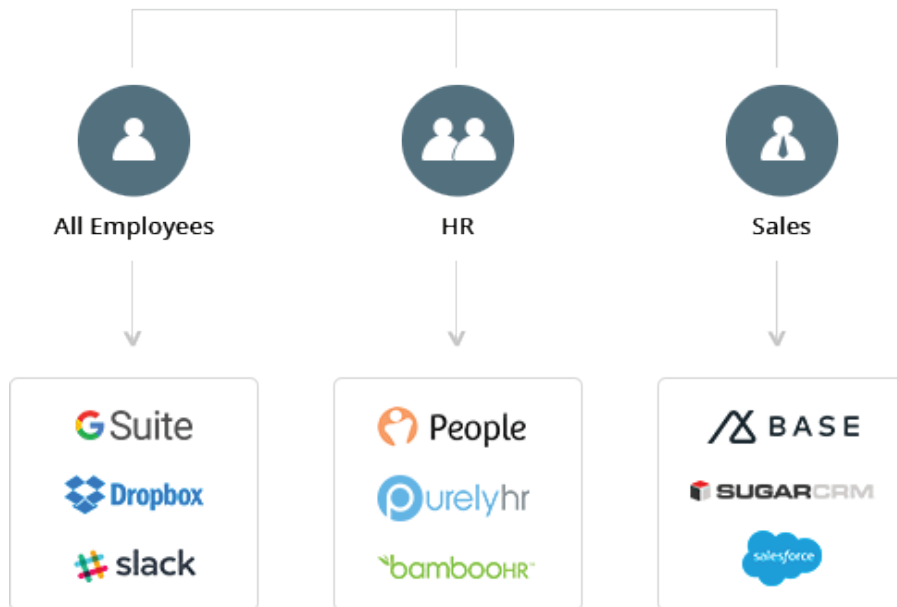
Leverage Active Directory identities

ADSelfService Plus' SSO feature integrates your users' cloud accounts with their Active Directory (AD) account so they can enjoy a consistent logon process across apps. ADSelfService Plus uses the SAML protocol to communicate with your users' cloud applications and provide SSO capabilities. End users can easily access all their cloud accounts with just their Windows domain password.

End user

4. Logon access granted

1. Logon request

zendesk   salesforce   Dropbox

slack   servicenow   G

Cloud apps

3. SAML response

2. SAML request

AD authentication in
ADSelfService Plus server

Fine-grained security policy for access control

In ADSelfService Plus, you can create fine-grained security policies to restrict access to cloud applications based on Active Directory organizational units (OUs) and groups. These policies determine who gets access to what cloud applications.

ManageEngine
ADSelfService Plus

ManageEngine
ADSelfService Plus

All Employees | HR | Sales

G Suite | **People** | **BASE**
Dropbox | **urelyhr** | **SUGARCRM**
slack | **bambooHR** | **salesforce**

For example, you can create and enforce a policy that provides access to your company's HR applications, such as People HR and BambooHR, only to users in the HR OU. Likewise, you can create a policy that provides access to CRM applications, such as Salesforce and SugarCRM, only to users in the Sales OU. You can create multiple policies and safely provide access to critical business applications to only those users who need them.

Self-service password reset

ADSelfService Plus also supports self-service password reset and self-service account unlock for Active Directory. Even if users have to remember just their Windows password for SSO, passwords can be forgotten for various reasons. With ADSelfService Plus, users can securely reset their Windows domain password on their own and continue to log in to cloud applications without seeking help desk intervention.

Get started right away

If you already have Active Directory, you can easily implement SSO for cloud apps in your organization using ADSelfService Plus. Download a free 30-day trial here. And if you are a small business with less than 50 users, then you can use the application for free without any restrictions.

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.

For more information,

please visit www.manageengine.com/products/self-service-password.

ManageEngine
ADSelfService Plus

Tech Support
support@adselfserviceplus.com

Direct Dialing
+1-408-916-9890

US:
+1 888 720 9500

$ Get Quote   ± Download