ManageEngine
ADSelfService Plus

Streamlining cloud access and improving security with Active Directory-based single sign-on

Streamlining cloud access and improving security with Active Directory-based single sign-on

Moving to the cloud promises organizations greater flexibility, cost savings, and a lot of other benefits. However, it also introduces identity management challenges and concerns about data security. Many recent security breaches have involved some form of credential theft or password cracking. It doesn't help that as the number of cloud apps increases, end users are burdened with remembering a growing number of complex passwords. As a result, they either start using the same password for multiple applications or store their passwords in an unsafe manner.

For IT administrators, there is no respite. They have to securely provision and manage user access to multiple cloud applications, which is cumbersome, error-prone, and takes up valuable time that could have otherwise been spent on more critical tasks.

The real cost of password management

Universally, organizations provide access to IT resources by creating a digital identity for their employees. This digital identity is comprised of a username and password. Now, depending on their role, employees may need access to different applications, with each requiring a unique password. As a result, everyone in the organization—end users, IT admins, and the help desk staff—are affected.

The cost of password management can affect organizations in multiple ways. Not only does each password for every application have to be complex so they're hard to crack, they also have to be changed at regular intervals. Having to frequently change complex passwords makes it even harder for users to remember them, which results in many calls to the IT help desk, and may even cause the user to create a weaker password in the future. Password reset is a costly process that affects employee productivity, increases the help desk's workload, and could result in security breaches if user identity verification is not handled properly during the reset process.

Combating password overhaul with single sign-on

Single sign-on (SSO) is a great solution to deal with having too many passwords. It allows users to remember a single username and password that they can use to access multiple cloud applications from a centralized console. With SSO, you can minimize password security issues, increase productivity, and ease identity management challenges, all while enhancing user experience.

The benefit of Active Directory-based SSO

While SSO simplifies password management and makes it easy for users to access enterprise cloud apps, setting it up is a different story. It requires a central directory that stores credentials for authentication as well as data on their access rights. There are different ways to set up SSO for cloud apps. For example, some SSO vendors require admins create or import users into an entirely new directory that comes built-in with their solution. This may require additional servers and add to the management overhead.

Most organizations already use Active Directory to store and manage users' identities and their access permissions. Doesn't it make sense to use this information for SSO as well? By leveraging Active Directory for SSO, deployment can be quick and the costs associated with infrastructure can be eliminated.

ADSelfService Plus: Seamless, one-click access to cloud apps with AD-based SSO

ADSelfService Plus' SSO feature eliminates the need for multiple user IDs and passwords, streamlines users' login experience, and improves security. It uses Active Directory credentials to verify users' identities, and OU and group-based policies to control access to various cloud applications. Users have to remember only their Windows username and password to access all their enterprise applications. The product doesn't need a separate server or other resources; ADSelfService Plus can be installed on a domain controller, member server, or workstation, or can even be hosted on Microsoft Azure.

ADSelfService Plus supports Active Directory-based SSO for more than 100 cloud applications, including Office 365, G Suite, Salesforce, Dropbox, Slack, and Zoho apps.

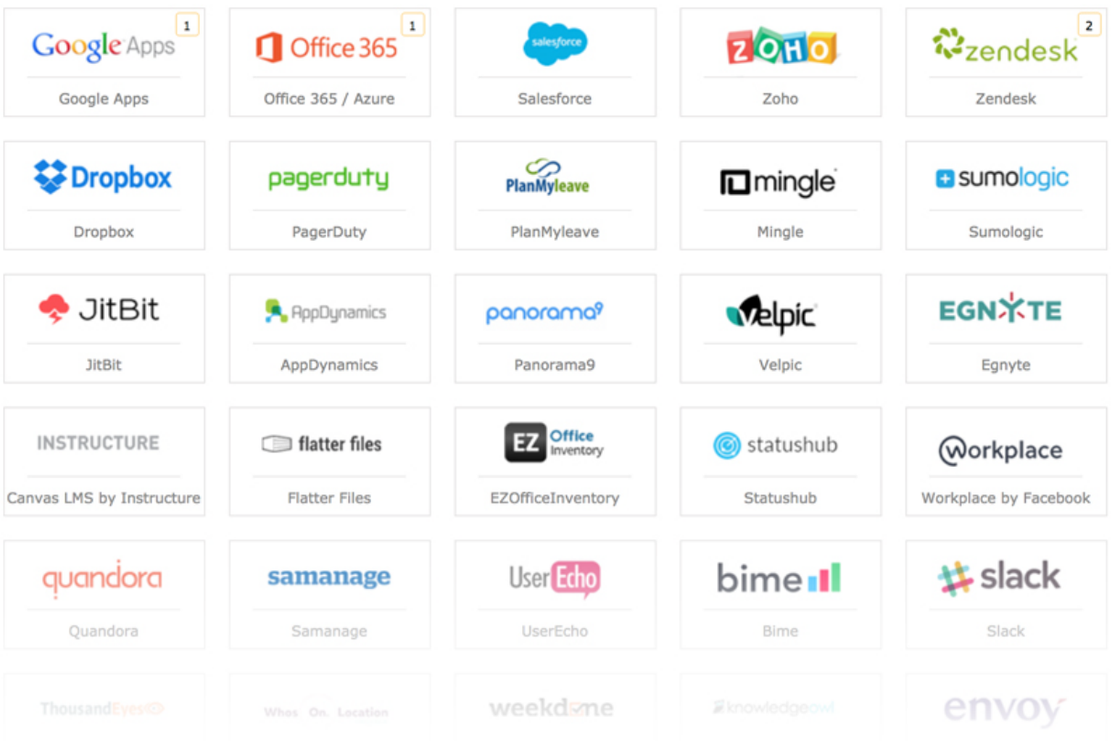

Figure 1: A peek into the list of applications supported by ADSelfService Plus for SSO.

How it works

ADSelfService Plus uses the secure and widely-adopted industry standard Security Assertion Markup Language 2.0 (SAML 2.0) to provide SSO. SAML is an XML-based framework for authentication and authorization between two entities: a service provider and an identity provider. There are two ways users can log into an application or a service using SSO.

- Identity provider (IdP) initiated SSO
- Service provider (SP) initiated SSO

Here, the IdP refers to ADSelfService Plus and the SP refers to the cloud application or service. To initiate SSO, users can begin at either the IdP or the SP.

In IdP-initiated SSO, users are simply required to log in to ADSelfService Plus using their Windows Active Directory domain credentials. Once logged in, users are presented with a dashboard that lists every cloud application they have access to. With just one click, users will be able to access each application without having to enter their username and password again.

In SP-initiated SSO, when users access the cloud application using a link on an intranet, bookmark, or something similar, they will be taken to the login page of the SP. After entering their username or selecting the SAML SSO option, the SP will redirect users to ADSelfService Plus. Users then need to log in to ADSelfService Plus using their Windows domain credentials to be able to access the SP.

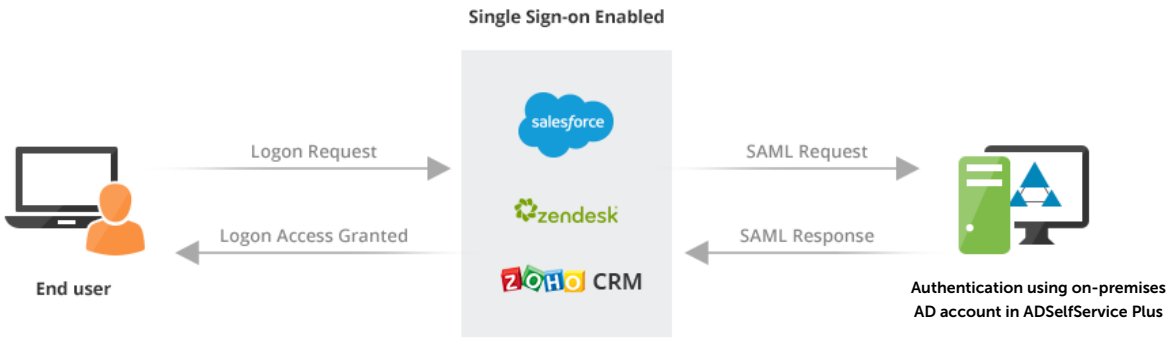

Figure 2: The SSO flow for SP-initiated SSO.

Access control using Active Directory OUs and groups

ADSelfService Plus uses the OU and group-based structure of Active Directory to control access to cloud apps. Administrators can create multiple policies for different types of users based on their role and the apps they need access to.

For example, they can create a policy to provide access to HR applications, such as People HR and BambooHR, only to users in the HR OU. Likewise, a policy for accessing CRM applications, such as Salesforce and SugarCRM, can be created for users in the Sales OU. Similarly, multiple policies can be created to safely provide access to critical business applications to only those users who need them.

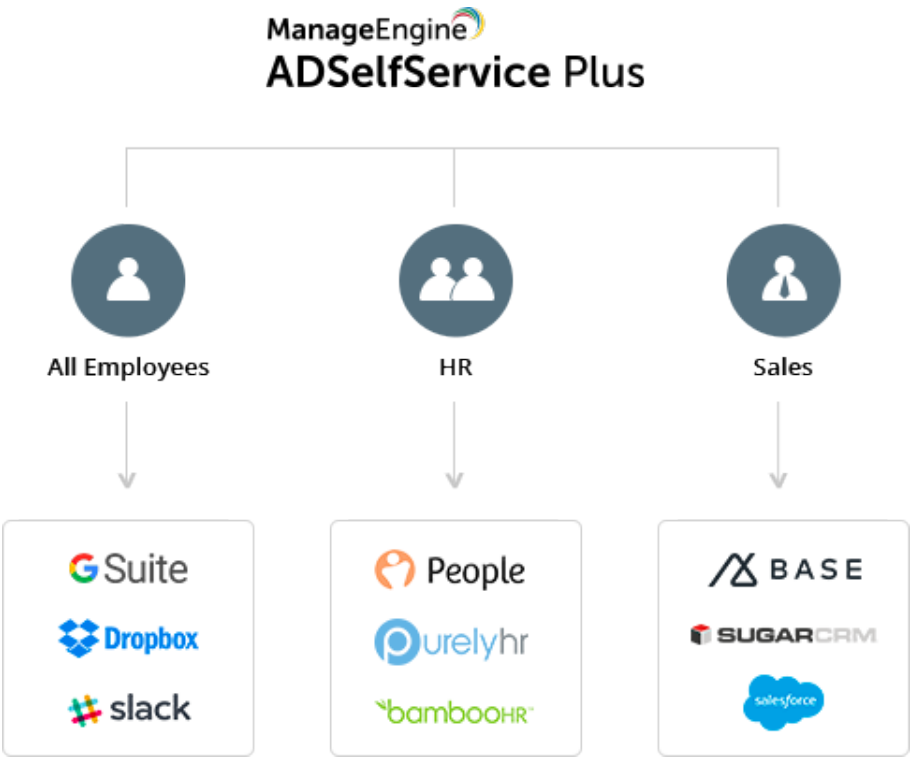

Figure 3: How ADSelfService Plus controls access based on users' roles using OU/group structure in AD.

Implementing multi-factor authentication (MFA) using the mobile and mail attributes in AD

ADSelfService Plus supports multi-factor authentication, which, in addition to the Active Directory domain credentials, requires users to go through a second authentication factor to gain access to their cloud apps for heightened security. ADSelfService Plus can be configured to use the mail and mobile attributes present in Active Directory to send a one-time passcode, which users have to enter to successfully prove their identity and gain access to their cloud apps.

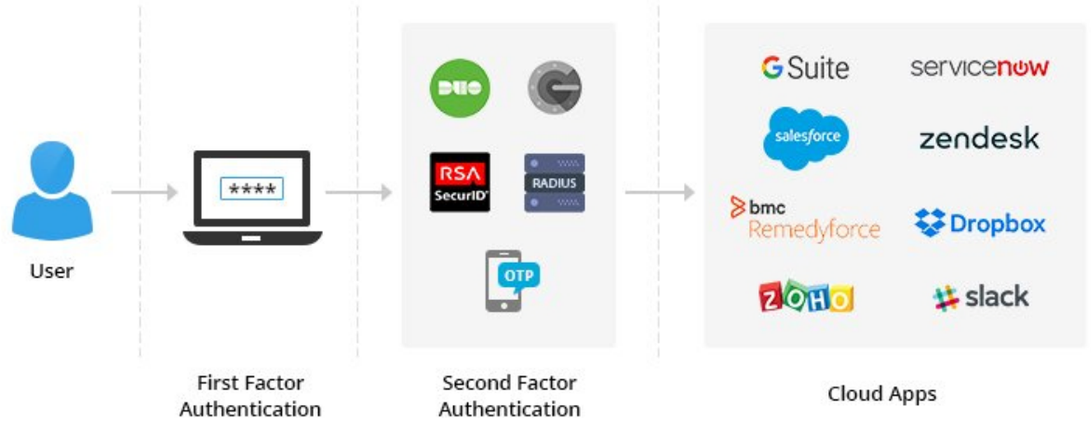

Figure 4: Illustrates the MFA process during SSO login.

In addition to SMS and email verification, ADSelfService Plus also supports Duo Security, RSA SecurID, RADIUS, Google Authenticator, and YubiKey Authenticator for authenticating users during login.

Summary

SSO is a straightforward, sensible approach to curb the burden of password management on end users, IT admins, and the help desk while improving the security of cloud apps. With ADSelfService Plus, organizations can deploy SSO quickly and realize return on investment in terms of increased productivity, reduced password-related help desk tickets, and improved security within days, all without making a severe dent in their IT budget.

In addition to SSO, ADSelfService Plus provides a comprehensive set of password management features including self-service password reset, granular password policy enforcement, password expiration notifications, and real-time password synchronization.

Get started with a free trial

Get started with ADSelfService Plus right away. Download a free 30-day trial here. For small businesses with less than 50 users, the application is completely free without any restriction.