ManageEngine
ADSelfService Plus

Single sign-on
and how it helps meet regulatory **compliance.**

Table of contents

Introduction ---- 3

Streamline application access with Enterprise Single Sign-On ---- 4

The major business drivers for SSO ---- 4

The major benefits of SSO ---- 4

The compliance benefits of SSO ---- 5

Reaping the benefits of SSO with ManageEngine ADSelfService Plus ---- 6

Granular policy enforcement ---- 6

Authenticate user identities with two-factor authentication (2FA) ---- 6

Secure, one-click access to all corporate applications ---- 7

Introduction

Today's IT teams are leveraging all facets of cloud and on-premises services to gain countless benefits—reduced IT expenses, improved user productivity, and access to applications/resources from anywhere, at any time. Based on the level of sensitive information involved, most applications will have different levels of password policy complexity requirements; these constitute what is considered a valid password, often requiring a combination of uppercase letters, lowercase letters, and numbers. On top of this, every department has teams and sub-teams that each manage a subset of applications, increasing the number password policies that need to be enforced across the enterprise.

"I enjoy creating and remembering strong passwords for all the 30 different applications I use," said no employee ever. Expecting employees to remember a separate username and password for every application they use is simply unrealistic and often results in a huge volume of password reset calls for the IT team.

Wouldn't it be great if employees could securely log in to all their corporate apps using just one set of credentials? *Single Sign-On (SSO)* ensures just this. It offers the security that your organization needs and provides the streamlined application access that your employees want.

Streamline application access with single sign-on

SSO eliminates the need for individual passwords for each user account, replacing this mix of passwords with a single set of corporate credentials. Your users can sign in with just one set of credentials to access all of their applications and services.

The major business drivers for SSO

In every organization, the major business drivers for SSO are:

Password mismanagement: Users need a simplified process to access multiple applications such as Office 365, G Suite, and Salesforce. With SSO, you can eliminate the use of weak passwords due to password fatigue and liberate your IT team from password-related help desk calls.

Secure authentication: You need to secure enterprise applications with a second factor of authentication. If you've already invested in an authentication technique like SMS/email one-time passwords (OTPs), hardware tokens, or Fingerprint Authenticator, you can leverage them to strengthen access to *all* applications.

Compliance: Organizations must comply with various regulations such as HIPAA, SOX, and PCI DSS. Failure to comply can result in hefty fines and other negative repercussions like losing the trust of your customers.

Identity management: Organizations need an efficient enterprise-wide identity management system, the first step of which is deploying an SSO solution.

The average employee has to manage **191 passwords**[1].

The major benefits of SSO

Cost savings: SSO reduces the total number of inbound password reset calls from employees and frees up help desk teams to work on other tasks that require attention. According to Forrester, many large organizations spend over $1 million[2] each year for password-related support calls, and often, costs continue to increase. Regardless of your organization's size, eliminating a large percent of help desk calls would mean significant savings.

Improved security: SSO uses identity standards like SAML 2.0, OAuth, SCIM, and OpenID Connect for the secure transmission of user access and provisioning information. It does this by using signed assertions instead of storing usernames and passwords. If your IT team manages user access manually, there's a chance that there are active user accounts belonging to users who no longer work for your enterprise. At best, this could increase your IT expenses; at worst, it could pose serious trouble during compliance audits.

Enhanced user experience: By providing secure, one-click access to users' apps, SSO eliminates the need to complete redundant sign-on attempts across applications. A seamless sign-on experience enhances the user experience of customers, employees, and partners.

43 percent of consumers would pay more for convenience according to a study by PwC research[3].

The compliance benefits of SSO

Deploying SSO can help you meet specific criteria associated with various regulations, including:

Sarbanes-Oxley (SOX), Section 404: SOX requires that IT controls are documented and organizations prove that adequate measures are in place to protect data. SSO helps with meeting SOX's requirements around data access.

Health Insurance Portability and Accountability Act (HIPAA): HIPAA requires effective authentication of users who are accessing electronic records or who require audit controls to track activity and access. SSO, combined with multi-factor authentication (MFA), can help comply with these requirements.

Payment Card Industry Data Security Standard (PCI DSS), Section 8.1: PCI DSS requires organizations to assign unique IDs to all employees with computer access and ensure proper user identification mechanism for users. When you integrate your SSO solution with Active Directory, you gain central control of identities and automated sync of Active Directory group membership. This includes automatically revoking access to terminated users and removing inactive user accounts within a specific time. It ensures that resources (credit card data) are made available for users with appropriate authorization. Combine that with MFA to completely secure the resources that PCI DSS requires.

Reaping the benefits of SSO with ADSelfService Plus

ADSelfService Plus is an integrated self-service password management and single sign-on solution. It helps reduce password reset calls, ensures network security during self-service operations, and simplifies user access to enterprise applications including Office 365, Salesforce, and G Suite.

Let's take a closer look at the features ADSelfService Plus has to offer that can help your organization reap the benefits of SSO.

Granular policy enforcement

ADSelfService Plus uses the OU and group-based structure of Active Directory to control access to cloud apps. You can create multiple policies for different types of users based on their role and the apps they need access to. For example, you can create a policy to provide access to HR applications, like Zoho People, only to users in the HR OU. Likewise, you can create a policy for accessing CRM applications, such as Salesforce and SugarCRM, for users in the Sales OU. You can create multiple policies to safely provide access to critical business applications only to users who need them.

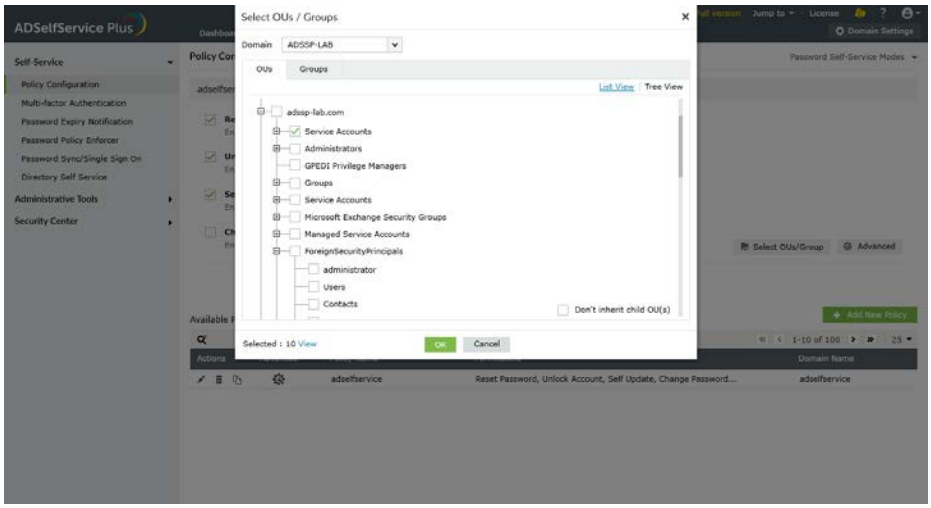

Figure 1: **Policy-based access control via OUs and groups.**

Authenticate user identities with two-factor authentication (2FA)

ADSelfService Plus supports 2FA. When enabled, 2FA requires employees to prove their identity via a second factor of authentication in addition to their Active Directory domain credentials before they can gain access to their cloud apps. You can configure ADSelfService Plus to use Active Directory's mail and mobile attributes to send a one-time passcode that users have to enter to successfully prove their identities and gain access to their cloud apps.

In addition to SMS and email verification, ADSelfService Plus also supports Duo Security, RSA SecurID, Biometrics, Security Questions, QR code, TOTP authentication, RADIUS, and Google/Microsoft Authenticator for authenticating users during login.

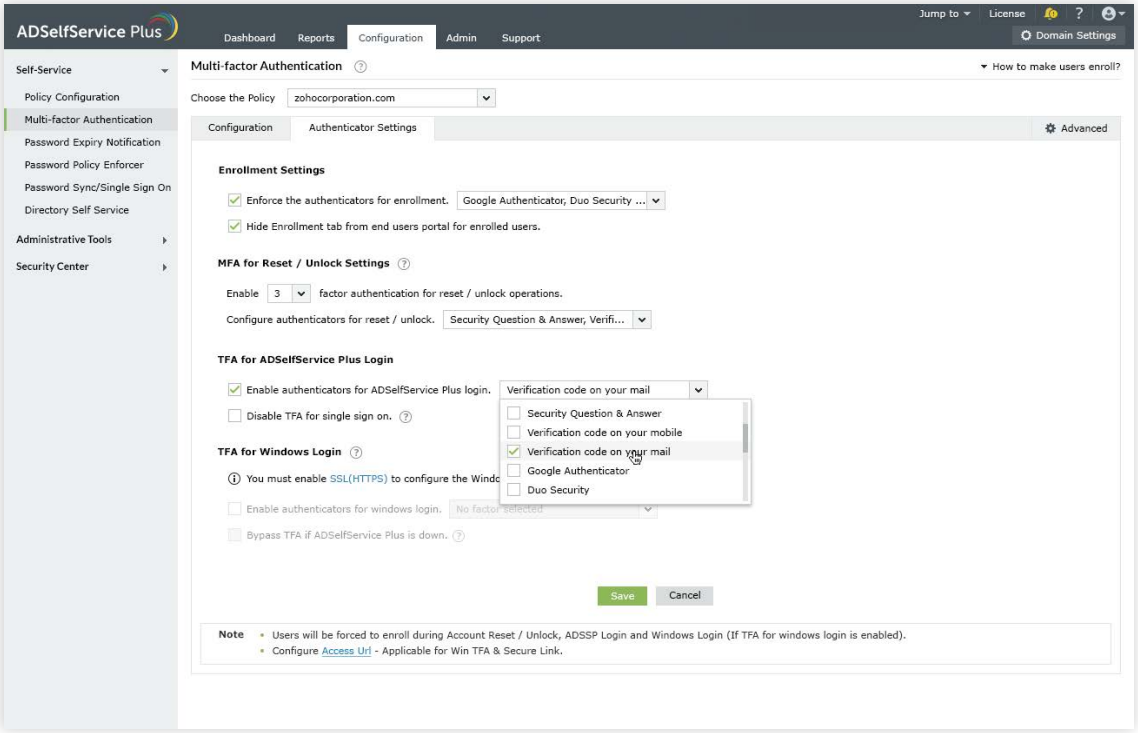

Figure 2: **SSO and MFA.**

The average cost of a data breach in 2018 was **$3.86 million**[4].

Secure, one-click access to all corporate applications

Users only need to log in to ADSelfService Plus using their Active Directory domain credentials. Once logged in, they're presented with a dashboard that lists every cloud application they have access to. With just one click, users can access each application without having to re-enter their username and password.

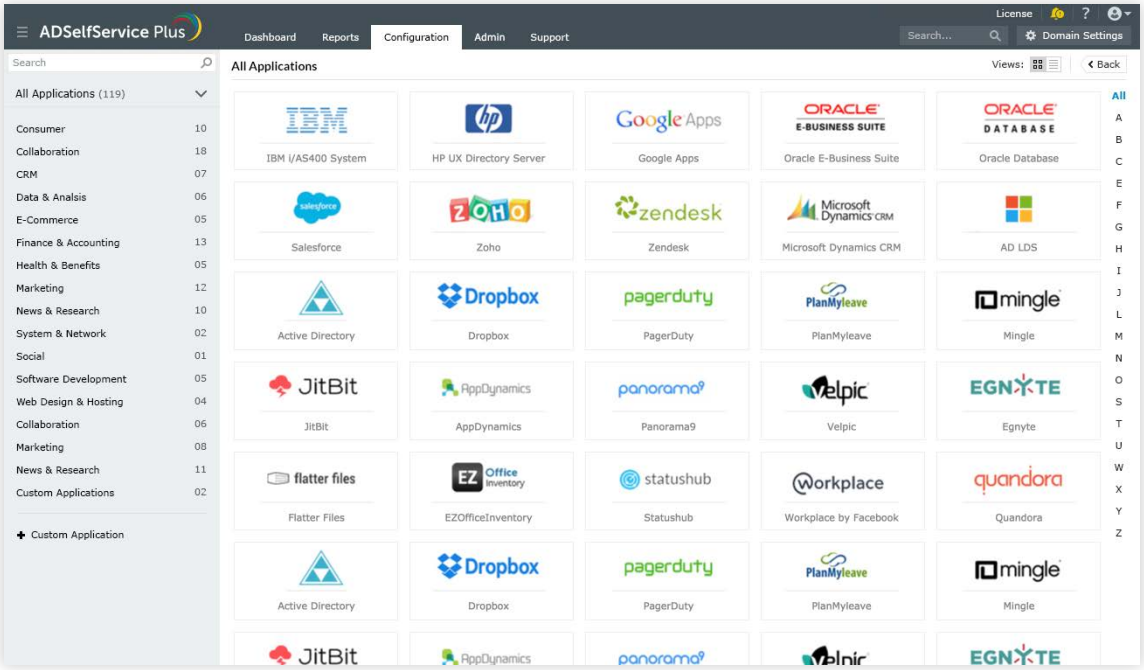

Figure 3: **SSO app catalog.**

Endnotes

1. 8 truths about the threats – and opportunities – of employee passwords.
2. Best Practices: Selecting, Deploying, and Managing Enterprise Password Managers Solutions reduce the risk of breaches from Compromised Credentials.
3. Experience is everything: Here's how to get it right, PwC.
4. 2018 Cost of Data Breach Study: Impact of Business Continuity Management.