ManageEngine
ADSelfService Plus

5 hacks that'll help SMBs bolster password security in 2021

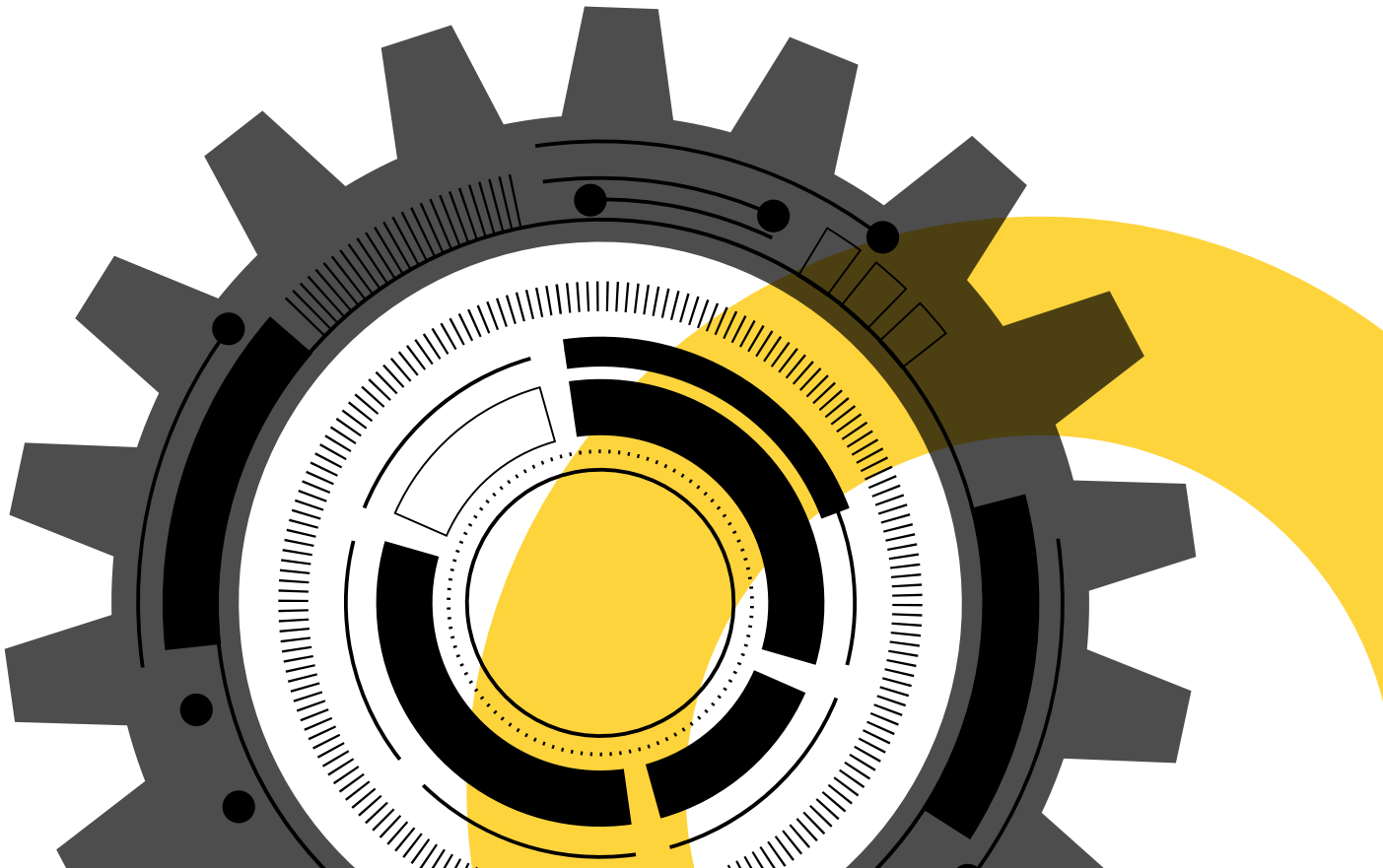
Introduction

Cybercriminals don't discriminate based on the size of a business. Back in 2019, long before the pandemic sent cyberattack rates soaring, 66 percent of the small and medium businesses (SMBs) surveyed by Ponemon Institute said they had experienced at least one cyberattack in the past twelve months. And 47 percent of those cyberattacks were caused by compromised employee passwords[1].

Passwords, especially those that give access to an organization's Active Directory (AD), are a prime target for cybercriminals. Once a hacker compromises an organization's AD, they can alter security policies, escalate privileges, or even execute a ransomware attack. The possibilities are endless. SMBs have to ensure that passwords—their first line of defense—is as secure as possible.

This guide elaborates on the obstacles SMBs face when it comes to strengthening password management and discusses solutions to overcome them.

Unique password management challenges SMBs face



Handling password reset-related help desk tickets is harder and costlier for SMBs

According to Forrester Research[2], the average help desk labor cost of a single password reset is $70. Though the cost will vary depending on the size of your organization and the average hourly wages of your employees, you know password reset requests are a costly affair on any given day.

Employee productivity costs at SMBs are also likely to be higher in comparison to enterprises, because SMBs often have a smaller IT team, which means each password reset request will likely take longer to resolve than at an enterprise.

At an SMB, the personnel who resolve the help desk issues might be the ones who have to take care of network stability issues, perform server audits, or ensure backups jobs are running smoothly without any hiccups.

Password reset requests chip away at the time needed to take care of business-critical IT tasks. SMBs looking to make the best out of their already constrained resources can't afford to take password resets lightly.

Password resuse is rampant in SMBs

At 47 percent of SMBs, employees continue to reuse passwords, reveals a recent study by Devolutions. It's not coincidence that the Verizon's 2020 Data Breach Investigation report[3] found that over 52 percent of data breaches involving small businesses were due to credential theft.

People reuse passwords because they find it taxing to remember different passwords for all the various devices and applications they use daily. Password reuse should be taken seriously because, when a reused password is compromised, all the accounts associated with it are also compromised.

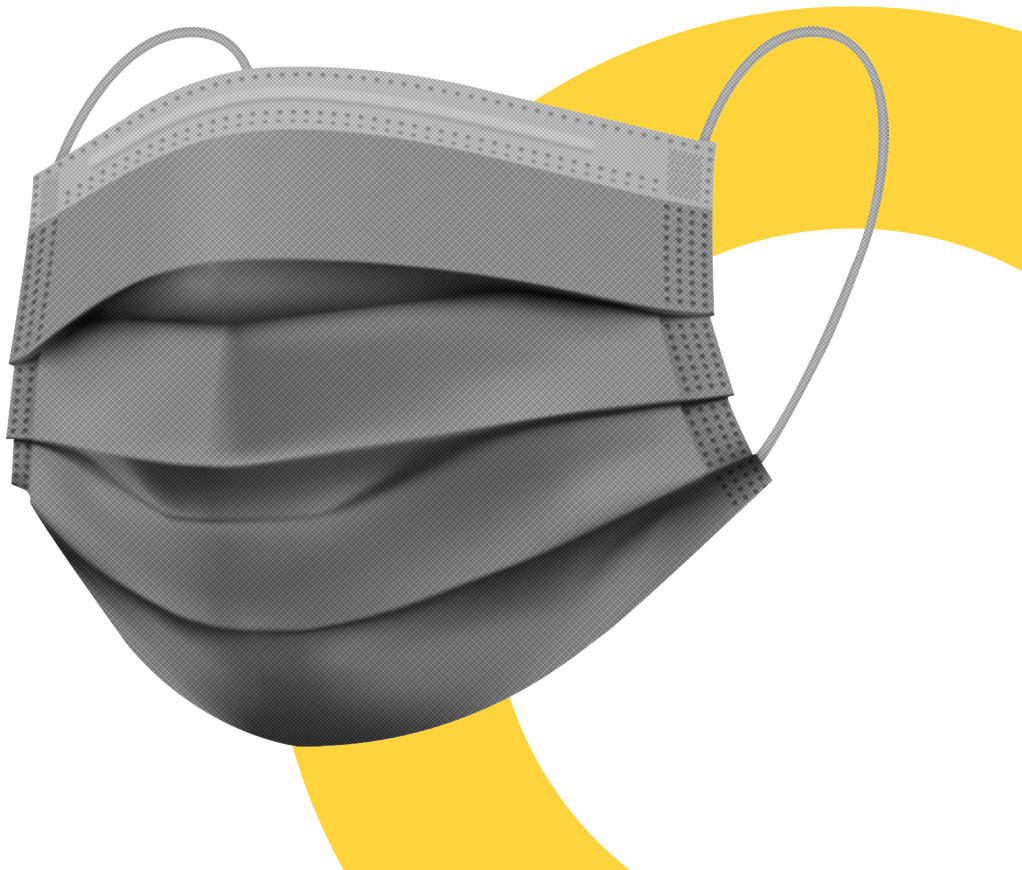
How damaging can password reuse be? Here's an example: in 2016, a reused password led to the theft of more than 60 million user credentials. Need we say more? The solution to stopping password reuse is requiring unique passwords for each account or service. But ironically, the solution itself leads us to the next headache SMBs face.

REUSE PLASTICS, NOT PASSWORDS!

Employees at SMBs aren't immune to password fatigue

SMBs with over 250 employees use close to 100 different SaaS applications, and the ones with less than 50 employees use 25-50 different applications, a recent survey says[4]. When employees are tasked with remembering "strong" passwords for numerous applications, they'll often resort to easier but unsecure ways of storing passwords—like random slips of paper or spreadsheets. More than 40 percent of IT professionals surveyed for a report[5] said that they often rely on sticky notes for password management.

Password fatigue creates a vicious cycle that looks like this: employees find it tedious to remember hundreds of passwords for all the resources they need access to. So, they create easy to remember passwords and record them in easy to remember places like on a piece of paper, or in their favorite note taking app, or in a spreadsheet. Those who are lazy create simple passwords, and often even decide to reuse them! Weak and reused passwords mean the employees of your organization are easy pickings for attackers.



Ensuring employees follow password best practices is hard for SMBs

In a recent survey, 34 percent of the SMBs said that they relied on strong passwords to secure their data[6]. This shows that there is considerable awareness about the importance of strong passwords. However, 54 percent of SMBs reported that they lack visibility into the password practices of their employees, and with close to 50 percent admitting that they have no policy governing employee password use, it is clear that SMBs are unable to manage passwords in their organizations[7].

Besides using weak or reused passwords, employees might be sharing passwords with colleagues, and in some cases even with people outside the company, setting the stage for insider attacks. Insider attacks are tricky to detect and resolve because the attack is carried out from someone's account who has legitimate access to the systems and applications.

How ADSelfService Plus can help you overcome these challenges

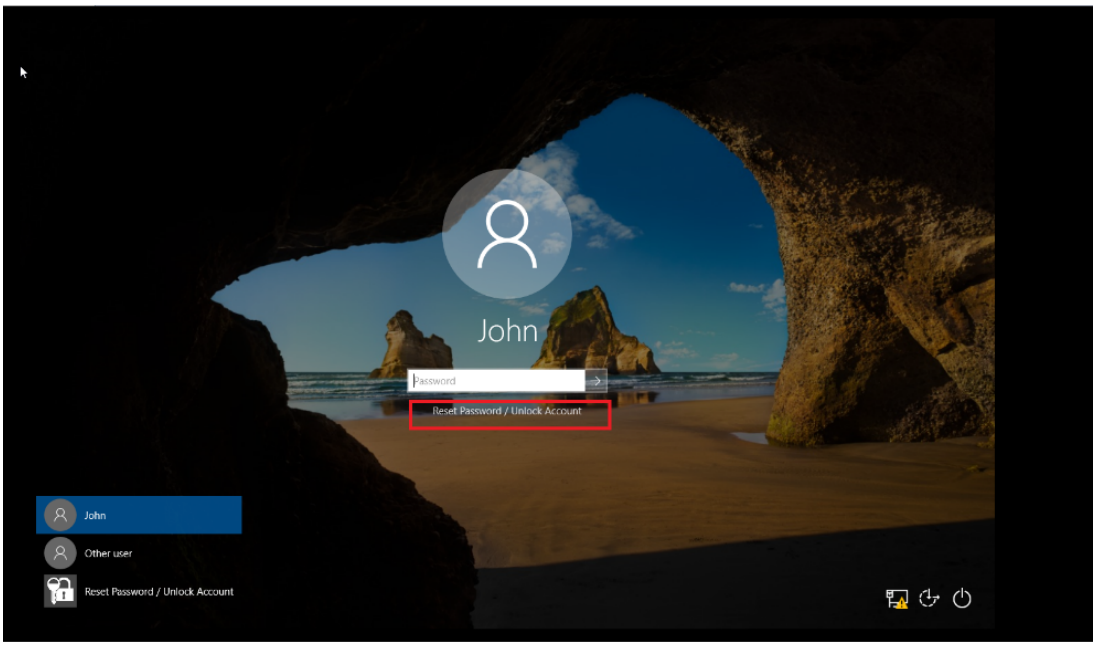
ManageEngine ADSelfService Plus is an integrated self-service password management and single sign-on (SSO) solution.

With ADSelfService Plus you can:

- Enable self-service password reset and account unlock for your users.
- Restrict users from reusing old passwords during password reset.
- Enforce strong custom password policies.
- Set up SSO for your applications.
- Enable multi-factor authentication (MFA) for workstations, applications, and self-service features.

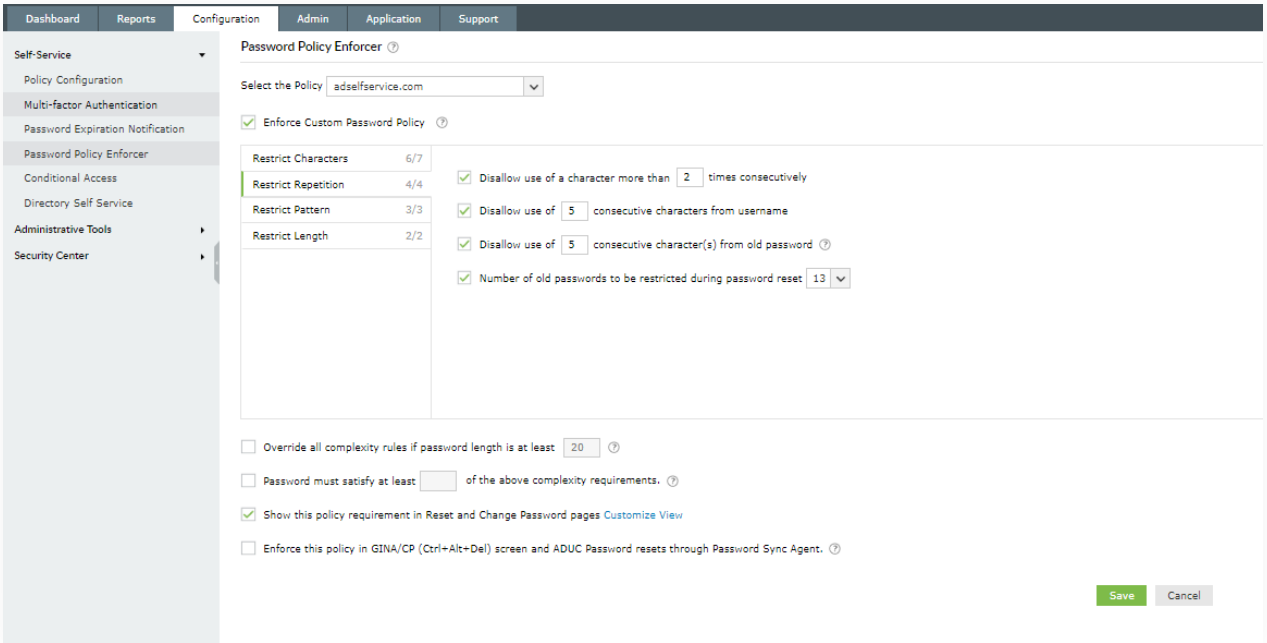
Enable self-service password reset and account unlock for your users

With ADSelfService Plus, IT admins can enable local and remote users to reset their AD and cloud account passwords without IT's assistance from anywhere, at anytime. Users can perform password reset and account unlock from their workstation logon screens, mobile devices, and web browsers. Moreover, the solution auto-updates the cached credentials in the machines of remote users who connect to work via a virtual private network (VPN) or use the Remote Desktop Protocol (RDP). Additionally, IT admins can also leverage ADSelfService Plus' adaptive authentication feature to analyze user risk before enabling them to access the self-service features.



Restrict users from reusing old passwords during password reset

With ADSelfService Plus' password history check feature, IT admins can ensure that users can't reuse any of their past 24 AD passwords.

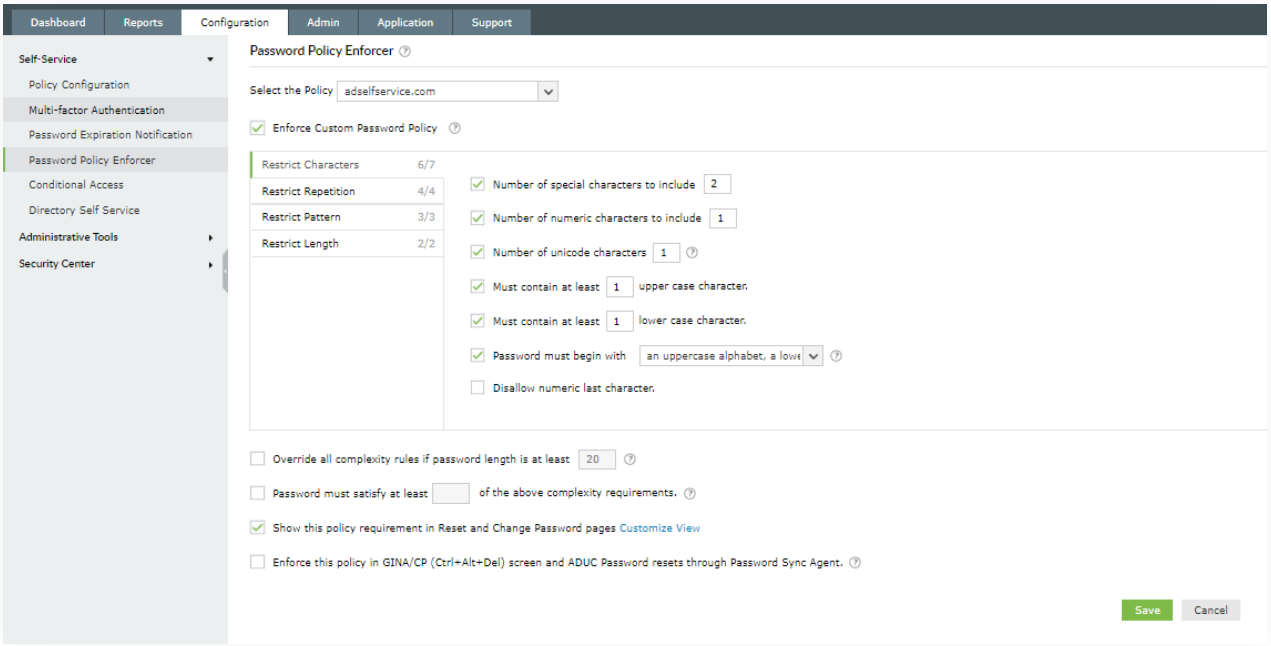


Enforce strong custom password policies

It isn't always easy to get users to follow password best practices, like setting long and complex passwords, skipping passwords that are common dictionary words, and avoiding already compromised passwords. That's where ADSelfService will help.

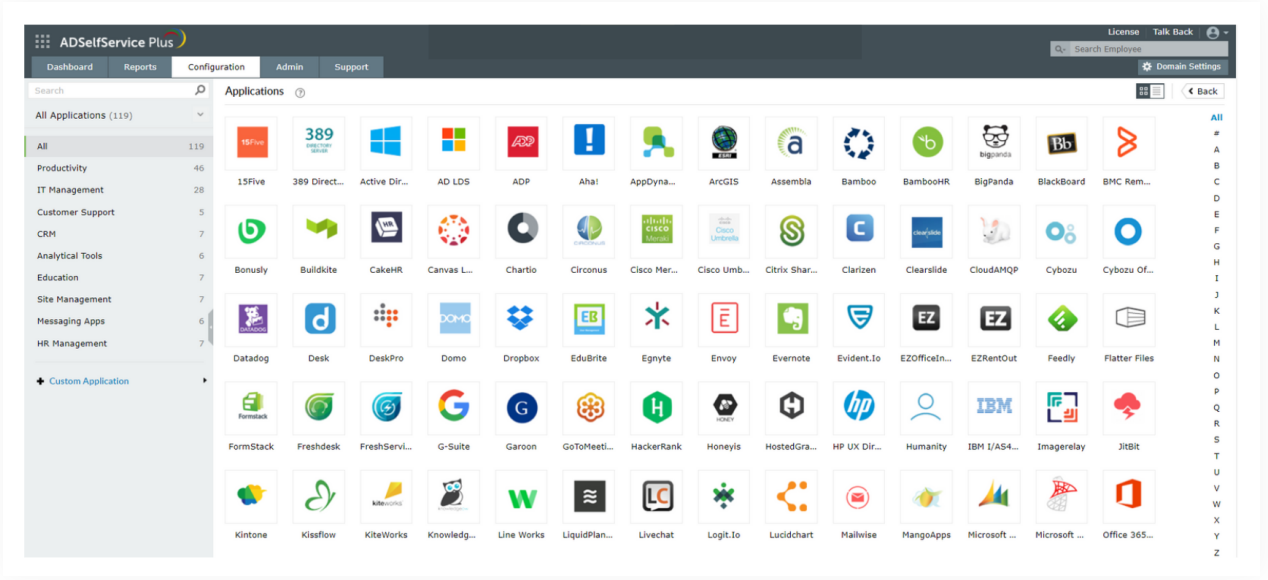
With ADSelfService Plus' password policy enforcer, IT admins can ensure one or more of these rules are followed when the password is set:

- Meets a minimum length
- Includes both upper and lower case letters
- Includes special characters
- Includes numbers
- Requires that the password begin with either a letter, a number, or a special character
- Blocks dictionary words, or patterns that are easy to crack
- Create a custom list of weak passwords which new password resets will be checked against
- Prevent the use of breached passwords through an integration with the "Have I been Pwned?" service that checks passwords against a continuously updated list of compromised passwords



Set up SSO for your applications

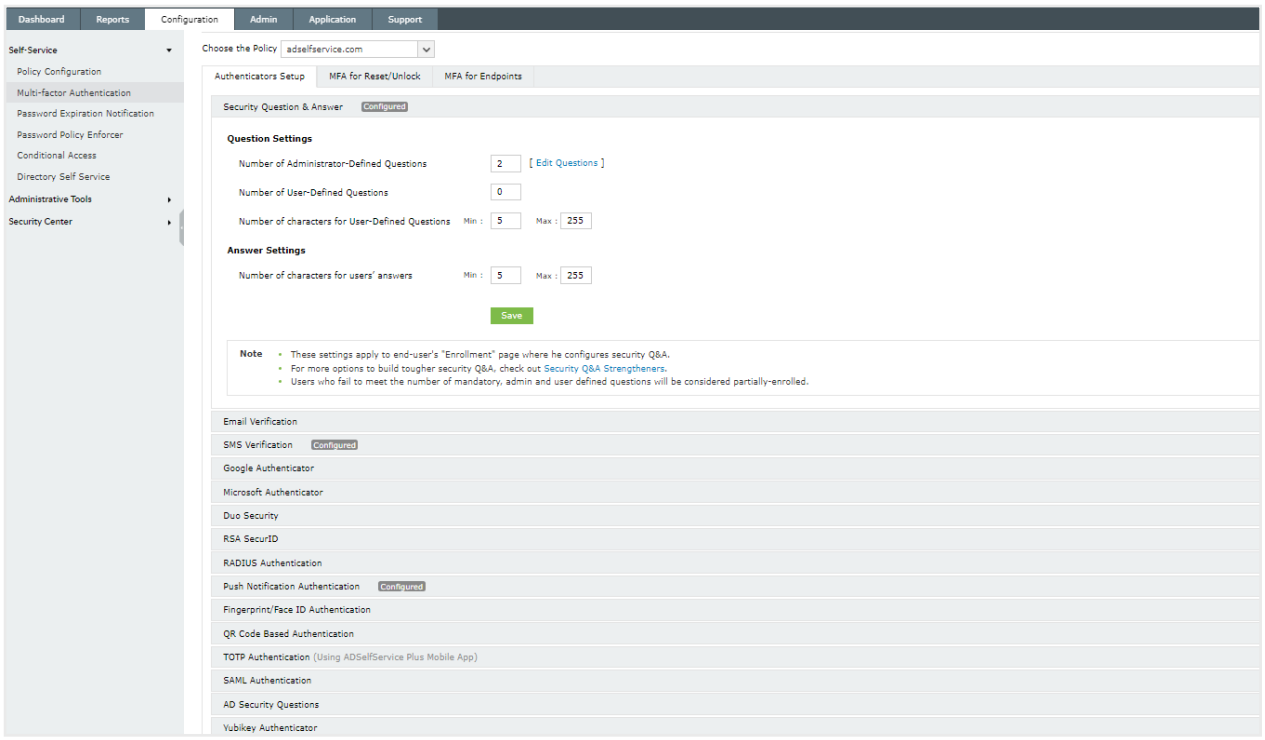
With SSO, IT admins can enable users to manage access to all applications with one click. ADSelfService Plus shows the user all the applications they have access to in a single dashboard. Access to applications can be secured using MFA. Additionally, IT admins can decide who has access to which applications by creating policies based on AD organizational units (OUs) and groups.



Enable MFA for workstations, applications, and self-service features

Passwords, the most common authentication factor used to verify identity, is the most vulnerable one too, because users tend to set easy to remember passwords, and are likely to use the same weak password for other devices and services. MFA provides an extra layer of security, as it involves verification of an additional factor that the user owns, like a smartphone, or the user is, like a fingerprint or any other biometric attribute. With MFA, even if the password is compromised, the attacker can't complete the heist, as they don't have access to the additional factor.

ADSelfService Plus supports over 15 authentication techniques, including YubiKey authentication, biometrics, and RSA SecurID. With ADSelfService Plus' MFA options, IT admins can secure local and remote access of the organization's Windows, Mac, and Linux endpoints, safeguard access to SSO-enabled applications, and ensure users can use the self-service password reset or account unlock features only after their identity is verified.



About ADSelfService Plus

ADSelfService Plus is a web-based self-service password management and single sign-on solution. It offers password self-service, MFA for endpoints, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and single sign-on for applications. ADSelfService Plus also offers both Android and iOS mobile apps to facilitate self-service for end users anywhere, at any time. ADSelfService Plus supports IT help desks by reducing password reset tickets, and spares end users the frustration caused by computer downtime.

$ Get Quote Download

Footnotes

1. 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses Report, Ponemon Institute
2. Best Practices: Selecting, Deploying, And Managing Enterprise Password Managers, Forrester Research
3. Verizon's 2020 Data Breach Investigation Report (DBIR)
4. Survey conducted by technology service agency 99 Firms
5. The Manifest 2020 Small Business Survey
6. 2020 State of Password and Authentication Security Behaviors Report
7. 2018 State of Cybersecurity in Small and Medium-Sized Businesses Report, Ponemon Institute