SPECOPS SOFTWARE

uReset vs. Azure AD Self-Service Password Reset

ABOUT SPECOPS Specops Software is the leading provider of password management and authentication solutions. Specops protects your business data by blocking weak passwords and securing user authentication. Every day thousands of organizations use Specops Software to protect business data. For more information, please visit specopssoft.com

HOW AZURE AD SELF-SERVICE PASSWORD RESET WORKS

Microsoft's Azure AD Self-Service Password Reset solution can be used to change, unlock or reset passwords from Azure AD and write them back to on-premises Active Directory. This functionality is only available to organizations that have a hybrid implementation, e.g. have synchronized on-premises Active Directory to Azure AD and have a P1/P2 or Office 365 Business license. Note for Education plans this is included in A3/A5 licenses.

Although Microsoft has made some advancements, the solution falls short when considering the user experience and security in a few areas:

1) MFA options is all or nothing

2) Security question implementation is questionable

3) No support to update locally cached credentials for remote users

4) No password policy rules display

5) Lacks a dedicated service desk interface

MFA options and platform are lacking

Azure AD Self-Service Password Reset offers MFA options but the problem with the platform is that MFA is an all-or-nothing choice. Azure AD Self-Service Password Reset does not offer admins the ability to require additional or stronger authentication factors for more privileged or sensitive users, leaving IT departments with the choice of increasing the burden on every user or sacrificing security.

Specops uReset offers a robust MFA platform with more than 20 forms of authentication out-of-the-box that integrates seamlessly with organizations' Active Directory structures, offering the ability to require different authentication factors for different GPOs. uReset MFA enrollments can also be seamlessly extended to support other high-risk use cases including self-service encryption key recovery and service desk assisted password resets/changes.

Security questions are questionable

With Azure AD Self-Service Password Reset, all security questions are displayed to the user at the same time and answers are not obfuscated. This creates a perfect scenario for over-the-shoulder surfing or for an attacker to social engineer the answers to all of the questions. Azure AD also lacks a lockout threshold to answering questions incorrectly.

A lot of the security industry has moved beyond questions and answers as a form of authentication because of the threat of social engineering or brute force attacks. However, should your organization still require them, Specops uReset can help you implement them with more security features – like not displaying them all at once, obfuscating answers end-users are typing, and custom lockout settings for failed answers.

No support for updating locally cached credentials

Remote users can cause a big increase in calls to the IT service desk. Locally cached credentials are what allow users to authenticate when a connection to the domain controller cannot be made. However, if a user resets or changes their password without a tool that can update that credential locally, conflicts arise and the user can get locked out.

Password Reset Calls Drive Service Desk Cost and Burden

The Gartner Group estimates 40% of calls to the service desk are related to passwords. Forrester Research estimates each call can cost organizations upwards of $70.

Azure AD Self-Service Password Reset has no mechanism for updating the cached credential when line of sight to a domain controller is lost, likely driving a big increase in calls to the service desk for organizations with any remote users relying on Azure AD Self-Service Password Reset.

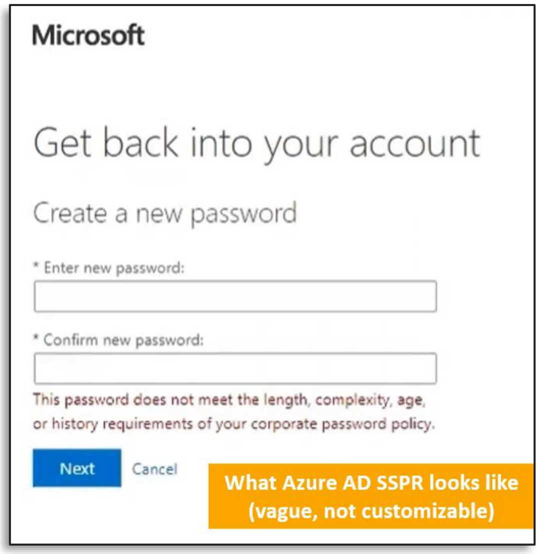
Specops uReset supports updating locally cached credentials, with or without a connection to the domain controller. This is an important and common use case for the majority of our customers, as end-users are increasingly working full-time or part-time remote.

No password policy rules display

When resetting/changing passwords with Azure AD Self-Service Password Reset, users are not presented with any password policy rules to assist them in setting a compliant password. Users are only notified after the fact with very generic feedback as to why their password change/reset failed. This can create a situation where a user fails multiple times to reset or change their password successfully, negatively impacting their experience and ultimately leading to calls to the service desk.

Specops uReset uses a dynamic password policy rules display to guide users with real-time feedback as they are typing in their new password. This allows users to self-correct before submitting the new password and ultimately reduce calls to the service desk.

End-user feedback comparison



Get back into your account

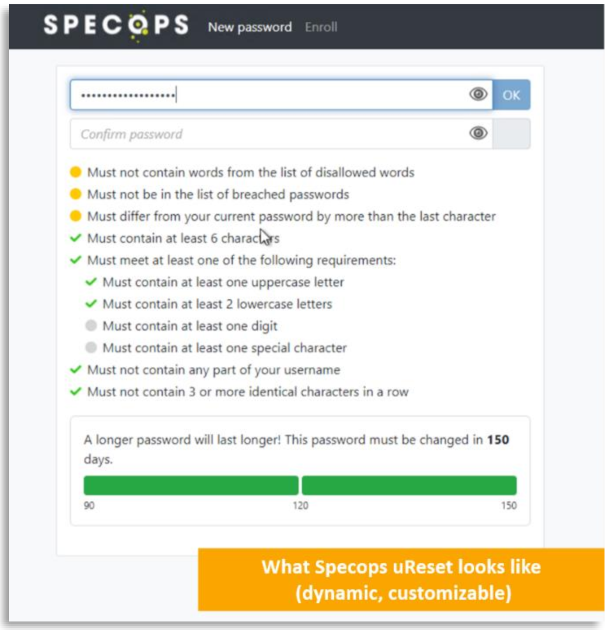
Create a new password

* Enter new password:

* Confirm new password:

This password does not meet the length, complexity, age, or history requirements of your corporate password policy.

What Azure AD SSPR looks like (vague, not customizable)



Confirm password

- ● Must not contain words from the list of disallowed words
- ● Must not be in the list of breached passwords
- ● Must differ from your current password by more than the last character
- ✓ Must contain at least 6 characters
- ✓ Must meet at least one of the following requirements:
  - ✓ Must contain at least one uppercase letter
  - ✓ Must contain at least 2 lowercase letters
  - ○ Must contain at least one digit
  - ○ Must contain at least one special character
- ✓ Must not contain any part of your username
- ✓ Must not contain 3 or more identical characters in a row

A longer password will last longer! This password must be changed in **150** days.

What Specops uReset looks like (dynamic, customizable)

Lacks a dedicated service desk interface

Yes, the point of a self-service password reset solution is to deflect password reset calls from the service desk. However, due to conditioning or due to the solution's inability to update cached credentials, some users will continue to call the help desk. Azure AD Self-Service Password Reset does not offer a dedicated service desk interface to facilitate password resets, changes or account unlocks.

Half of all data breaches involve a malicious or criminal attack with social engineering making up a large percentage of these (Ponemon, 2019). The IT service desk is a prime target for social engineering, so user verification is imperative. Specops offers a companion product to uReset, Secure Service Desk, which enables service desk staff to verify user's identities utilizing the authentication factors they've enrolled with before proceeding to reset or change their passwords.

About Specops uReset

Specops uReset is a self-service password management solution that enables organizations to lift the burden of password reset calls from their IT service desk.

With Specops uReset, users can reset their passwords and update their locally cached credential from anywhere and from any device. End-users can initiate the password reset process from any browser, their mobile device, or right from the Windows logon screen on their workstations. The solution is a part of a robust multi-factor authentication platform that also supports secure user verification for encryption key recovery as well as different authentication requirements for different Group Policy Objects.

To see how Specops uReset can lift the burden from your IT department and increase password security, click here.