COMPARISON

Specops uReset
vs. Microsoft Entra (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 MICROSOFT ENTRA SELF-SERVICE PASSWORD RESET WORKS

Microsoft Entra (Azure AD) Self-Service Password Reset can be used to change, unlock or reset passwords from Entra ID (Azure AD) and write them back to on-premises Active Directory. This functionality is only available for hybrid implementations, e.g. have synchronized on-premises Active Directory to Entra ID with a P1/P2 or Microsoft 365 Business Premium license. Note for Education plans this is included in A3/A5 licenses.

Although the platform has made some advancements, the solution falls short in a few areas:

1. MFA options are lacking
2. No support to update locally cached credentials for remote users
3. No password policy rules display
4. Lacks a dedicated service desk interface

MFA options are lacking

Limited options including no third-party identity provider support

Entra ID (Azure AD) MFA options are limited for securing password resets. While more MFA options are available for other Entra ID use cases, the only MFA options Microsoft offers for the password reset scenario are:

- SMS
- Voice call
- Push notification via Microsoft Authenticator
- TOTP via apps like Google or Microsoft Authenticator
- Security questions (not available for admin users)

These limited options mean organizations who have invested in a 3rd party identity provider like Okta, Duo, Ping or hardware tokens like Yubikey are unable to remove the end user enrollment burden by extending their investment to the Entra ID password reset scenario. These limited options also mean that users without their own devices are left with security questions only for MFA.

Specops uReset offers a flexible MFA platform with 20 forms of authentication including 3rd party providers like Okta, Duo, Ping, Symantec VIP, and Yubikey. uReset caters to organizations with different user types; offering MFA options like Trusted Network Location and Manager Identification for users without devices of their own.

Security questions are questionable

With Microsoft Entra (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. Microsoft Entra also lacks a lockout threshold to answering questions incorrectly.

Organizations with users without their own devices often turn to security questions as a "better than nothing" MFA option. Where necessary, Specops uReset can help 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 Costs

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

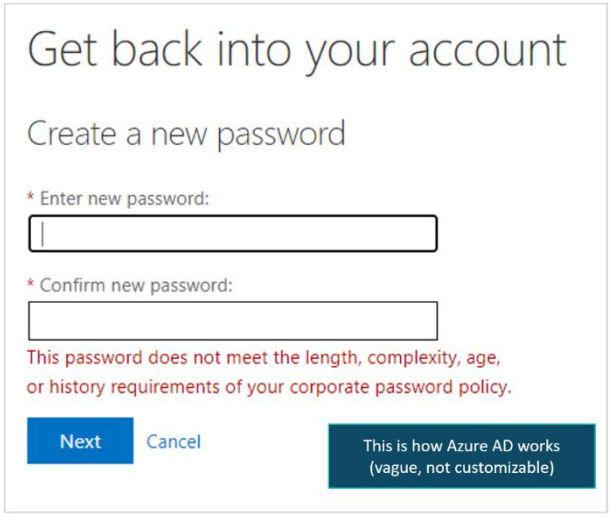
Microsoft Entra (Azure AD) Self-Service Password Reset has no mechanism for updating the cached credential when line of sight to a domain controller is lost, likely driving a big increase in calls to the service desk for organizations with any remote users relying on Microsoft Entra Self-Service Password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

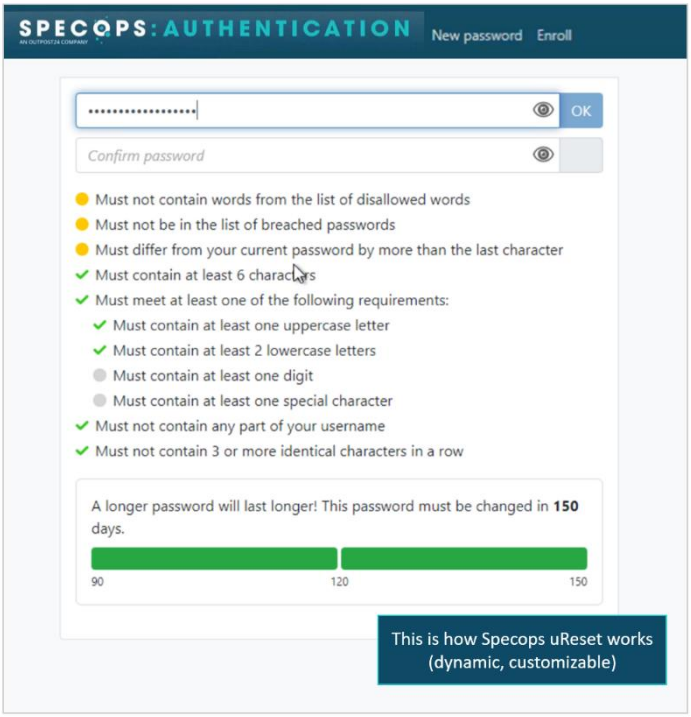
Specops uReset supports updating locally cached credentials, with or without a connection to the domain controller. This is an important and common use case for the majority of our customers, as end-users are increasingly working full-time or part-time remote.

No password policy rules display

Microsoft Entra (Azure AD) Self-Service Password Reset does not give users any feedback to assist them while setting a compliant password. The interface provides vague feedback and only after the new password is submitted. This can lead to users failing multiple times to reset their password, 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.





Lacks a dedicated service desk interface

While a self-service password reset solution should reduce calls to the service desk, there is no eliminating all service desk calls. The passwords reset by users themselves via a secure MFA-powered solution are vulnerable if the service desk reset call is not itself secured. Microsoft Entra (Azure AD) Self-Service Password Reset does not offer a dedicated service desk interface to verified caller's identities for password resets, changes or account unlocks, leaving this use case open for social engineering attack.

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.

Our Technology Partners

Our Technology partnerships ensure that organizations can confidently extend the value of their existing investments and systems to optimize password security– whether that's extending existing multi-factor authentication investments or extending Microsoft Active Directory functionality. Read more.