

SPECOPS URESET Datasheet

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.

SPECOPS URESET

Datasheet

Specops uReset lifts the burden from the IT service desk by enabling end users to address common tasks related to password management including forgotten passwords, locked out Active Directory accounts, and password resets and changes. The solution goes beyond the traditional identity verification methods, and revolutionizes self-service with flexible authentication prior to resets. With a powerful multi-factor authentication engine, uReset ensures that users always have a secure way to reset their password, from any location, device, or browser.

Enrolling with uReset is simple. Guide users to their enrollment using configurable reminders and notifications. To guarantee adoption, use the pre-enrollment options (3rd party ID services like Okta or Duo, AD attributes and more) to register users before roll out. If you are using uReset with any other Specops Authentication products, you can extend user enrollments to secure service desk assisted password resets and encryption key recovery. Additionally, if you are using Specops uReset with Specops Password Policy (with Breached Password Protection validation) users will not be allowed to select a weak password during the password creation process.

FEATURES	SPECOPS URESET	AZURE AD SELF-SERVICE PASSWORD RESET
OOTB 3 rd party identify services e.g. Duo Security, Okta, Symantec VIP, PingID	Yes	Yes
Updates locally cached credentials (remote)	Yes	No
Enrollment notification	Yes (Email, SMS, balloon tip)	Yes (Email)
Helpdesk interface	Yes, with Secure Service Desk	No
Reporting	Yes	Yes
Compromised password protection validation	Yes, blocks over 2 billion known compromised passwords	No, allows use of leaked password based on scoring algorithm
Dynamic password policy display	Yes	No, users receive vague guidance



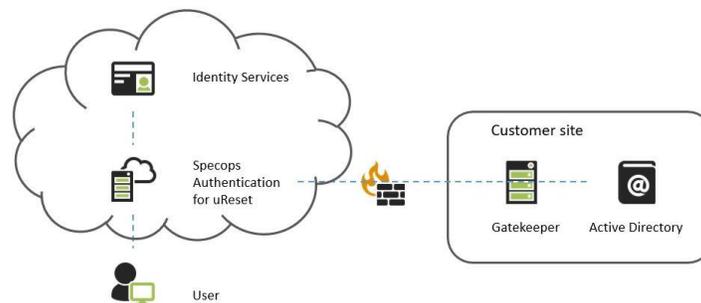
Password Reset Calls Drive Service Desk Cost and Burden

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.

How does it work?

Specops uReset is natively integrated with Active Directory. Configuration of the system is done using Group Policy, without introducing added complexity to your environment. This means that no external database is required to store password related information. User data is stored directly in Group Policy user objects, minimizing security risk while ensuring inherent real-time password provisioning.

uReset consists of the following components and does not require any additional resources in your environment. The authentication backend, web, and identity services are hosted in the cloud.

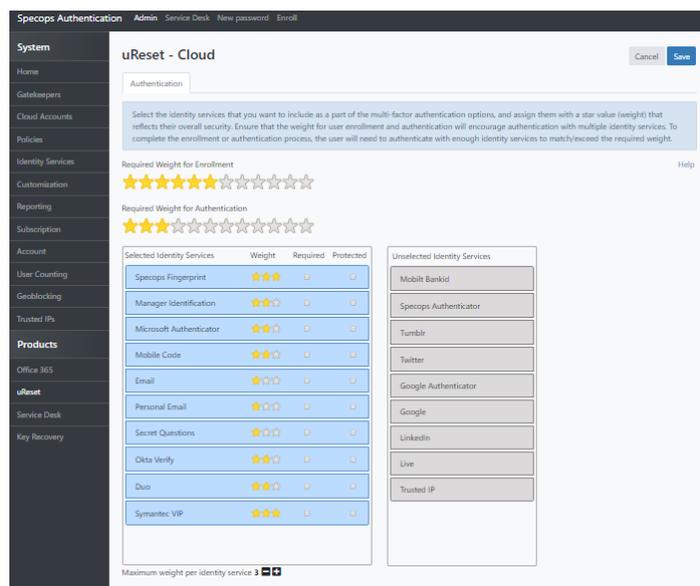


What does it look like?

uReset enhances login security by extending multi-factor authentication to self-service password reset. There are 20+ identity services available to ensure that you can select the best options for your users.

However, since not all identity services are equally secure, administrators can assign each identity service a trust value, based on their perceived level of security.

The trust assignment is managed via stars, as shown in the administrator view to the right.



What does it look like for end users?

Specops uReset uses a dynamic and customizable 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.

uReset customers using Specops Password Policy can also display length-based password aging and compromised password check feedback.

Why customers choose Specops

Very simple to use

“It’s very simple to use, I would say. You just have a link on the first page of your computer, click that one, open the authenticator in your phone, get a code, put it in, and then you write a new password, and then you’re up and running again.”

- [Case study](#) from Thomas Lundvall, Manager R&D Sweden Mechanics at Cargotec

Super End-User Friendly

“But most importantly the system has proven to be super end user friendly, especially around authentication with all the options such as Twitter and Fingerprint authentication to name a few. Our users get it, it’s quick, and secure.”

- [Case study](#) from Eric Tanner, Service Desk Manager at Medical College of Wisconsin

Quickly reset insecure passwords after a ransomware attack

When a group of hackers used weak passwords to carry out a ransomware attack on the municipality of Kalix in Sweden, the municipality worked with IT consultants and security experts to complete system upgrades.

- Read how uReset was an essential part of their recovery process in [their case study](#).

Get a Demo of Specops uReset

Interested in seeing how Specops uReset can work in your environment? [Click here](#) to set up a demo or trial today.

