SPECOPS SECURE SERVICE DESK

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 SECURE SERVICE DESK

Employee password resets continue to drive a big volume of service desk tickets. Aside from draining IT resources, they also introduce a security vulnerability to your organization. Can your service desk verify that a user is really who they say they are before handing over a new password to an attacker posing as one of your users?

User verification at the service desk primarily often relies on knowledge-based questions using static Active Directory information that is vulnerable to targeted attacks, such as employee ID.

Specops Secure Service Desk increases security with stronger authentication methods that minimize the risk for user impersonation. Identity verification options range from mobile or email verification codes, to commercial authentication providers such as Duo Security, Okta, Symantec VIP, PingID and YubiKey. These authentication options are paired with technical enforcement of the ID verification, blocking agents from proceeding with the caller's request until authentication through the platform is completed.

48% of organizations do not enforce user verification for calls to the service desk

Source: The Weak Password Report

Feature Highlights

FEATURES	OTHER SOLUTIONS	SPECOPS SECURE SERVICE DESK
OOTB 3rd party identify services e.g. Duo Security, Okta, Symantec VIP, PingID	Some support but lacking	Yes, plus several other ID options to support non-mobile users
Service desk interface for user verification	Yes	Yes (plus secure logins for service desk agents)
Service desk assisted password resets	No	Yes (and can force users to change password at next logon)
User verification enforcement (agent cannot proceed without first verifying)	No (agent not forced to authenticate identity before proceeding to help caller)	Yes

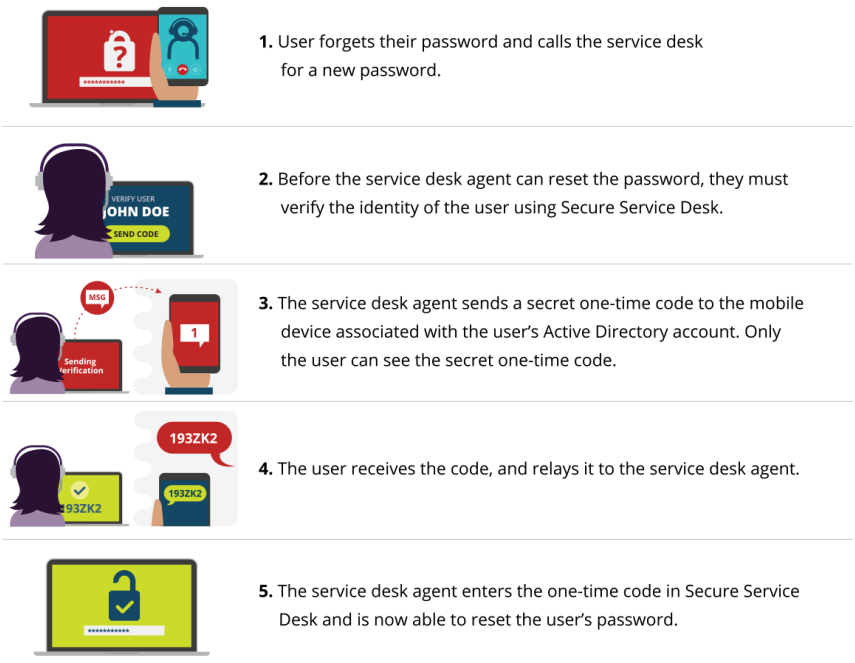
FEATURES	OTHER SOLUTIONS	SPECOPS SECURE SERVICE DESK
User verification tracking	Yes (but detail is lacking)	Yes (details who was verified, for what use case, and by whom)
API for user verification	Some	Yes (allows user verification with 3rd party systems with any of the 15+ enrolled ID services)

The 2023 MGM ransomware attack, which cost the company over $100 million, was a result of missing ID verification at the service desk.

Read more about this attack.

How does it work?

Specops Secure Service Desk 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.



1. User forgets their password and calls the service desk for a new password.

2. Before the service desk agent can reset the password, they must verify the identity of the user using Secure Service Desk.

3. The service desk agent sends a secret one-time code to the mobile device associated with the user's Active Directory account. Only the user can see the secret one-time code.

4. The user receives the code, and relays it to the service desk agent.

5. The service desk agent enters the one-time code in Secure Service Desk and is now able to reset the user's password.

What does it look like?

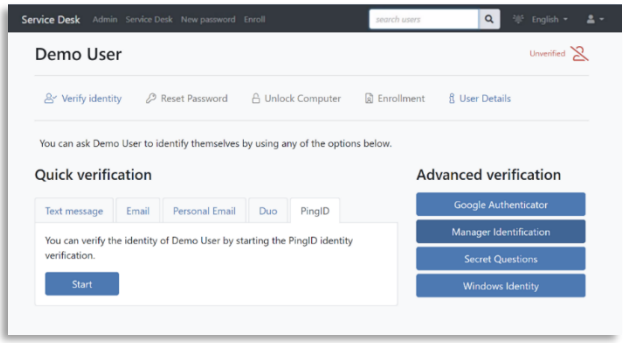
The solution interface allows service desk agents to view user details and perform the following actions:

1. Manage user enrollments
2. Reset Active Directory passwords
3. Recovery encryption keys for lockouts triggered by BitLocker or Symantec Endpoint Encryption.

Service desk agent view

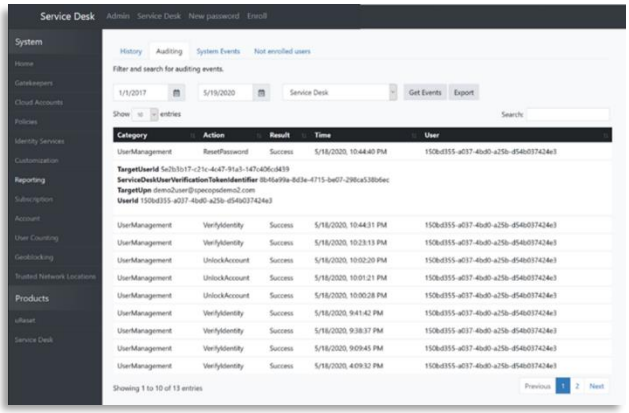
The above actions can be secured by enabling user verification enforcement.

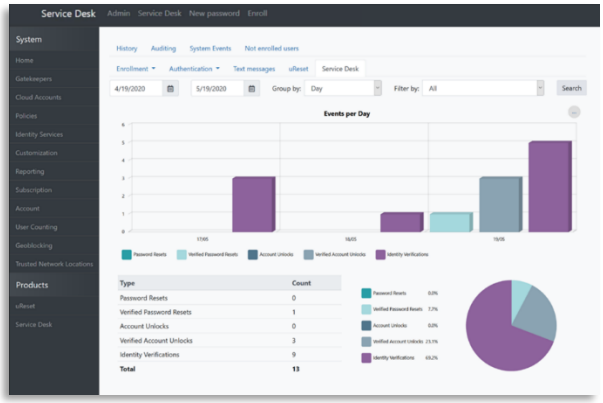
When this feature is turned on, the agent will need to successfully verify the user's identity before being able to complete any of these high-risk actions.



Admin reporting view

User verification can be tracked within the solution via detailed audit logs.





The solution also provides a reporting dashboard that reflects verification data across multiple uses cases. This data can also be exported to JSON or XSLX for further processing.

What people are saying

Delivers on its promise

"Specops Secure Service Desk delivers on its promise. It helps organizations enforce secure user verification through stronger authentication methods."

- Techgenix review by Nuno Mota, Microsoft Exchange, MVP

Exponentially more difficult for an attacker

"It provides the means for service desk technicians to effectively verify the identity of a supposed end user who requests a password reset. This should make it exponentially more difficult for an attacker looking to perform a social engineering or other type of attack to steal credentials."

- 4sysops review by Brandon Lee, Senior Editor at Virtualizationhowto.com

See a demo of Specops Secure Service Desk

Interested in seeing how Specops Secure Service Desk can work for your organizations?

Click here to set up a demo or trial today.

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.