SPECOPS SECURE ACCESS

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

MFA FOR WINDOWS LOGON, RDP AND VPN

with SPECOPS SECURE ACCESS

Specops Secure Access adds an important MFA layer to Windows logon, RDP and VPN connections, helping organizations better secure hybrid environments and fulfill compliance and cybersecurity insurance requirements. With flexible MFA options that include an offline mode, Secure Access ensures that organizations can enable their users securely authenticate at logon, through RDP and/or VPN whether they are connected to the network or not.

Enrolling with Specops Secure Access is simple. Users will be guided through enrollment upon their first authentication attempt via the Client. MFA enrollment options consist of Yubikey, Duo Security, the included Specops:ID app, and SMS. Offline enrollment is available with OTP authenticators. If you are using Specops Secure Access with any other Specops Authentication products, you can extend user enrollments from Specops Secure Access to secure password resets and encryption key recovery.

Feature Highlights

FEATURES	SPECOPS SECURE ACCESS
MFA at the Windows logon	Yes
MFA for RDP connections	Yes
MFA for VPN connections (RADIUS)	Yes
Customizable “remember me” settings to reduce the number of MFA prompts a user experiences at logon/unlock, VPN or RDP	Yes
OOTB authentication with Duo Security, Yubikey	Yes
Push notification without existing 3rd party identity service	Yes, with the included Specops:ID mobile app
Biometrics authentication	Yes, with the included Specops:ID mobile app
Offline support	Yes, with OTP authenticator
Protects both layers of logon – Active Directory password and flexible 2FA options	Yes, with Specops Password Policy

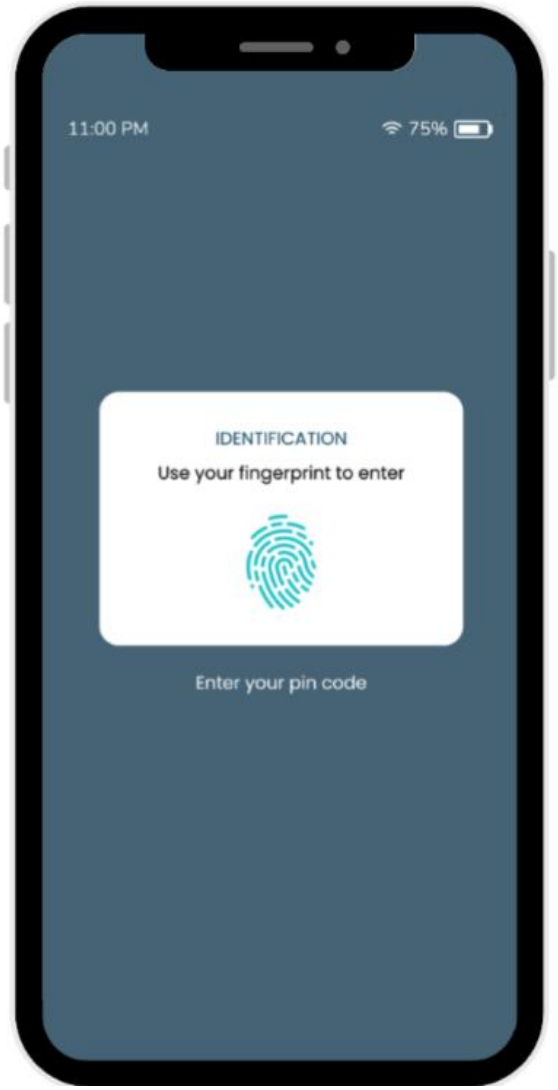
Passwords Are Attacked 1287 times per minute (Microsoft)
Microsoft observed 1287 password attacks per minute in 2022. The best defense against such volume of attacks is a layered one.

What does it look like?

End user experience at Windows Logon

With the Specops Client installed and configured for Secure Access, users are forced to identify themselves with a second factor after having typed their Windows username and password on Windows login screen. Once that second authentication is completed, the end user will be logged in as usual.

End user experience for VPN or RDP



An end user gets a prompt to authenticate for VPN or RDP via the Specops:ID mobile app.

Organizations with users accessing their network remotely using a VPN, or accessing computers via a Remote Desktop Gateway (RDGW), can protect their users by adding a second factor for those logins.

The VPN server or Remote Desktop Gateway can, using RADIUS, be configured to call Microsoft NPS (Network Policy Server) with Specops NPS companion installed and configured, which enables the use of Secure Access.

Get a Demo of Specops Secure Access

Interested in seeing how Specops Secure Access can work in your environment? Click here to set up a demo or trial today.

Customers Love Specops Software

“Great Product.”

"Outstanding. Support was fantastic and extremely quick to respond. The product itself is exactly as advertised."

Our Technology Partners

Our Technology partnerships ensure 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.