Silverfort for Windows Login

Identity-based attacks that utilize compromised credentials to access enterprise resources are increasing in volume, sophistication and impact.

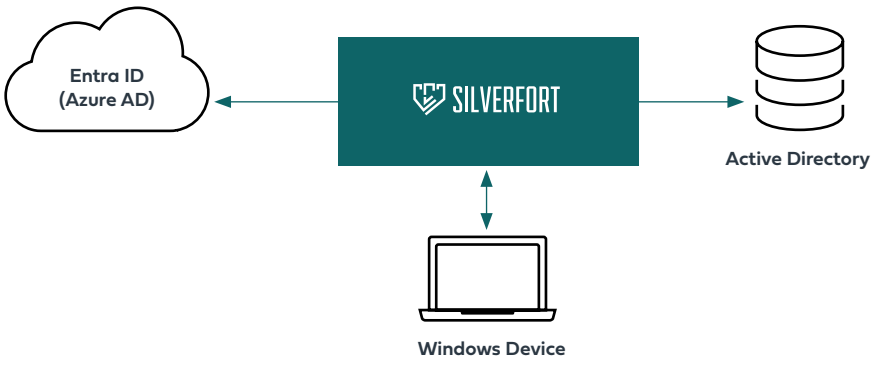
Organizations need to take appropriate measures to secure internal and remote networks and relying only on usernames and passwords to secure users' accounts is no longer an option. To help further address these identity protection challenges, Silverfort provides a multi-factor authentication (MFA) protection layer for login to Windows desktops and servers.

Silverfort Securing User and Device Access

Silverfort secures Windows login, Remote Desktop Protocol (RDP), User Elevated Credentials (UAC) to authorized users to authenticate to the domain of their local AD or Entra ID. This allows organizations to better secure their Windows server environments and enduser Windows machines logins. Silverfort is the only solution that integrates MFA with a policy engine that allows organizations to apply different conditional access policies for their users when logging into a Windows device. Utilizing Silverfort's risk-based and location-based policies, organizations now have the opportunity to deploy adaptive policies on the device layer to stop any malicious activity or incoming attacks.

Logging in to Windows with Silverfort

The Silverfort for Windows Login feature provides control access and risk analysis for all Windows endpoints. Silverfort supports both online and offline devices by evaluating authentication requests with the Silverfort policy engine and receiving MFA push notifications or leveraging OTP or FIDO2 tokens for offline devices. When a user attempts to login into their windows device, the Silverfort credential provider checks whether a policy should be applied, and whether to allow or block access or require MFA to the user. By deploying security policies on the device layer, Silverfort empowers organizations to prevent identity-based attacks such as stolen credentials, phishing and more.



KEY BENEFITS

Adaptive Policy Engine
Easily apply various conditional policies to protect against malicious activity and incoming attacks.

Offline Support
Secure access using OTP for users who don't have network connectivity.

Geo Fencing
Implement location based policies that explicitly allow or deny certain countries.

Real-Time Risk Analysis
Evaluate the risk of each access attempt based on the user's full context and activity.

Detailed Audit Trail
Monitor, audit and report on all desktop authentication activity.