Silverfort

Silverfort for Windows Logon

Silverfort for Windows Logon enables organizations to enforce MFA on any Windows machine without deploying additional infrastructure. By integrating directly at the authentication protocol level, Silverfort applies MFA in real time both domain-based authentications and local account authentications on endpoints, whether on a physical device, a virtual machine or offline system. The result is an identity protection layer across all Windows access points that strengthens identity security posture and simplifies operational management for security teams.

What is Silverfort for Windows Logon?

Silverfort secures Windows Login, Remote Desktop Protocol (RDP), and User Elevated Credentials (UAC) to allow authorized users to authenticate to the domain of their local AD or Entra ID. Silverfort also protects local accounts, enabling organizations to secure both domain and local Windows logins consistently across servers and end-user devices.

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. This includes applying access-based controls to local and domain accounts and enforcing MFA for local accounts when they are bound to their corresponding AD identities. Using Silverfort's risk-based and location-based policies, organizations now can deploy adaptive policies on the device layer to stop any malicious activity or identity attacks.

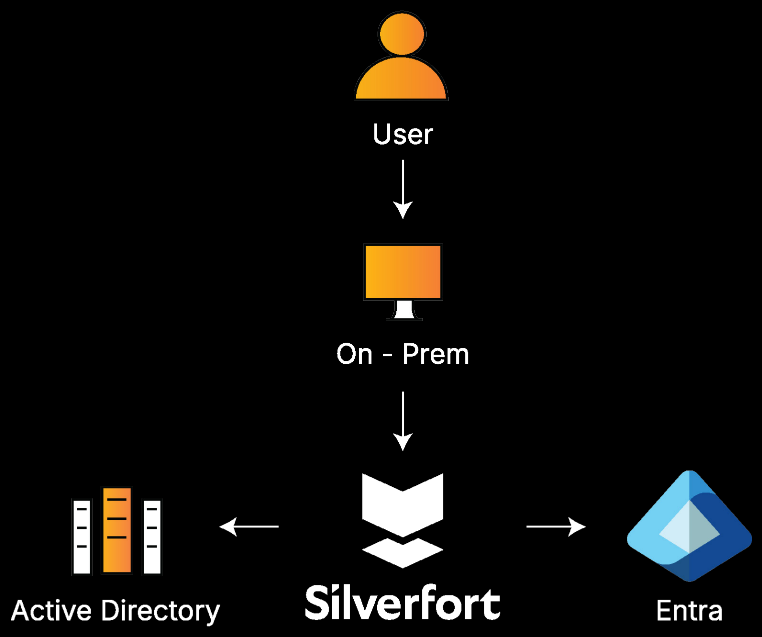
How does Silverfort for Windows Logon work?

By evaluating authentication requests with the Silverfort policy engine, Silverfort can trigger MFA push notifications for online devices and supports OTP or FIDO2 tokens for offline devices. This applies to both domain and local account logins, with MFA supported for local accounts through AD binding. 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.

By deploying security policies on the device layer, Silverfort can help prevent identity-based attacks, including compromised credentials, brute force, phishing, and lateral movement attempts involving unmanaged local admin accounts.

Silverfort also supports full MFA protection enforcement in air-gapped environments by leveraging its on-prem Desktop Messaging Service (DMS) instead of the cloud-based messaging layer. This includes MFA support for both domain and local accounts, enabling policy-based authentication with OTP or FIDO2 tokens on devices that never connect to the internet. It ensures strong identity security posture even in highly sensitive or isolated networks as OT or critical infrastructure.

How does Silverfort for Windows Logon work?



Key benefits

Adaptive policy engine

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

Local account protection

Discover, manage, and protect local accounts; apply access-based policies and enforce MFA protection via AD binding.

Real-Time risk analysis

Evaluate the risk of each access attempt based on the user's full context and activity.

Offline and air-gapped support

Enforce MFA in disconnected or air-gapped environments using OTP or FIDO2, with no reliance on internet access.

Geo fencing

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

Detailed audit trail

Monitor, audit and report on all desktop authentication activity.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.