Silverfort | FaceSign

Bridging on-prem authentication with FaceSign

Require live proof-of-human verification for on-prem and legacy access with Silverfort's bridge, applying step-up policies across hybrid environments

Silverfort's FaceSign Bridge enables organizations to require a FaceSign verification session as a step-up action for on-prem and legacy resources. Enterprises gain a real-time check at the point of access that confirms a live human is present and assesses deepfake and coercion signals. FaceSign does not establish that the person owns the account. Silverfort continues to authenticate the account and decides when the session is required, so teams can target it to the users, groups, and resources that matter most, such as privileged accounts and sensitive servers.

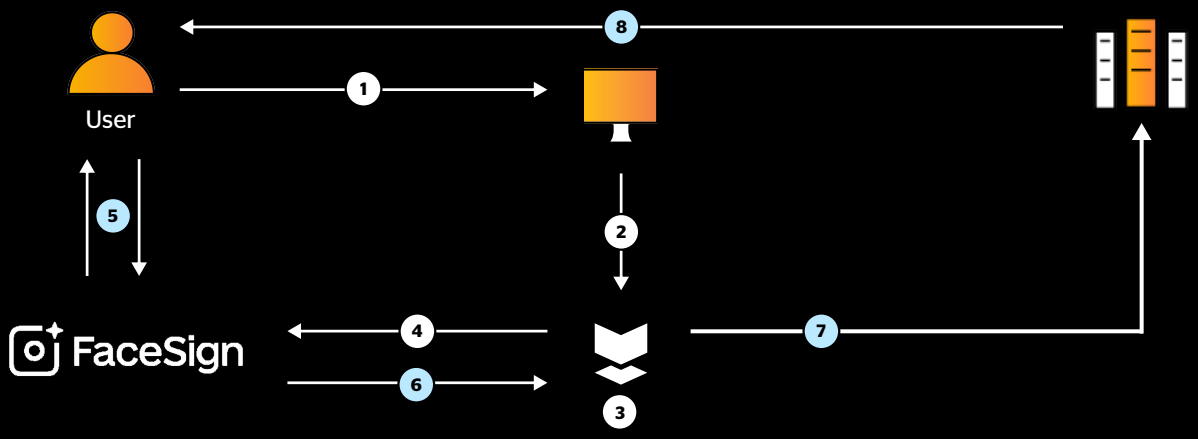
Bridging legacy resources

Silverfort bridges on-prem and legacy authentication into FaceSign by registering FaceSign as a SAML identity provider in the Silverfort Admin Console. Customers then create a policy for each resource they want to protect and select FaceSign as the step-up action. When a policy requires step-up, Silverfort redirects the user to FaceSign. When the session completes, FaceSign returns a signed response, and Silverfort applies the policy decision. A missing or incomplete response is never treated as a success.

How does Silverfort's FaceSign bridge work

Silverfort acts as a SAML Service Provider (SP) and connects legacy authentication protocols like Kerberos, NTLM, and LDAPS to FaceSign through the Silverfort Bridge. Admins define step-up policies for these bridged resources that require a FaceSign session. By applying a policy to each on-prem resource, organizations decide where the session is required. When a policy requires step-up, Silverfort redirects the user to FaceSign and applies the policy decision based on the signed response.

Enabling the FaceSign bridge



1. User initiates an authentication to on-prem resources (to Active Directory) and sends Active Directory (AD) a request to access the resource.
2. AD forwards the request to Silverfort.
3. Silverfort evaluates the authentication and decides whether to allow, require a FaceSign step-up, or block.
4. If the policy requires FaceSign, Silverfort redirects the user to the FaceSign session.
5. FaceSign checks liveness, asks whether the person is signing in by choice, and assesses deepfake and coercion signals.
6. A passing check returns a signed SAML success response. A completed non-pass can return a signed denial. Interrupted or unavailable flows may yield no usable response.
7. Silverfort matches the response to the original request, applies the policy decision, and forwards it to AD.
8. AD sends the response to the user to either allow the authentication or block it.

Key benefits

Targeted Policy Enforcement
Apply FaceSign verification where it matters most, scoped by Silverfort policy to specific users, groups, and resources.

Protect the 'Unprotectable'
Bring live proof-of-human verification to on-prem, legacy, and hybrid resources that sit outside modern web authentication.

Short, Browser-Based Session
Users complete a short video interaction in a browser with internet, camera, and microphone access.

Coercion Risk Signals
FaceSign assesses behavioral signals that may indicate pressure or coaching. These signals are advisory; a pass does not prove that coercion is absent.

About Silverfort

Silverfort secures every dimension of identity—human, machine, and AI—across on-prem, cloud, and hybrid environments. We are the first to deliver an end-to-end Identity Security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline and at runtime to stop lateral movement, ransomware, and other identity threats.