Silverfort | Microsoft

Silverfort Bridging to Entra ID

Extend Entra ID security controls to on-prem resources with Silverfort's bridge, applying access policies across hybrid environments.

Silverfort bridging with Entra ID enables organizations to automatically discover on-prem applications and apply Entra ID security controls to these resources. This enables enterprises to gain real-time protection against identity-based attacks that utilize compromised credentials to access enterprise on-prem or cloud resources.

Bridging legacy resources from AD to Entra ID

Silverfort bridging extends Entra ID security controls and applies Conditional Access policies to any resource and access interface across the on-prem and multi-cloud enterprise environment.

In addition, by bridging authentications of all resources and users, Silverfort empowers organizations to gain better visibility into their users and resources activity. This enables organizations to apply strong modern identity security controls to all resources. By enforcing new security measures with Silverfort, organizations are becoming more proactive against incoming cyber threats such as lateral movement attacks.

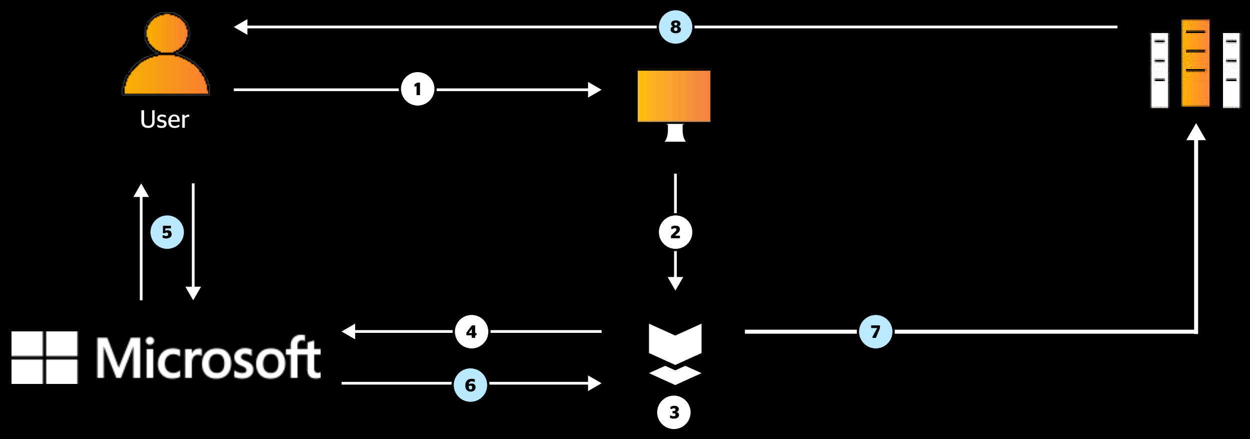
How does Silverfort bridging to Entra ID work

Authentications can be bridged according to their dependencies and usage using Silverfort. Silverfort can seamlessly bridge any type of authentication (legacy apps, command-line tools and more) into Entra ID, as if it were a modern web application. With Silverfort's bridging, an enterprise application object representing the on-prem resource is created in Entra ID automatically.

Entra ID views this object as a SaaS app like any other cloud-based application. In Entra ID, configure an access policy for the application object that can utilize Entra ID's Conditional Access and MFA. By creating and applying the policy to each bridged on-prem resource, organizations will consolidate hybrid resources.

After bridging and configuring authentication and access policies, Silverfort monitors and protects resource access attempts. All bridged applications can now be managed, monitored, and protected in Entra ID.

Enabling the Entra ID 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, trigger MFA, or block.
4. If Silverfort triggers MFA, Silverfort sends the access request to Entra ID.
5. Entra ID evaluates the authentication based on set policy and sends the MFA request to the user.
6. After user's identity verification, Entra ID forwards the verdict to Silverfort.
7. Silverfort accepts the verdict and forwards it to AD.
8. AD sends the response to the user to either allow the authentication or block it.

Key benefits

Unified Policy Enforcement

Secure on-prem environments and resources with Entra ID policies via Silverfort, reducing identity-based risks.

Protect the ‘Unprotectable’

Extend Entra ID MFA and access policies to any resource, including on-prem servers, legacy apps, IT infrastructure, and command-line tools.

Seamless User Experience

Provide users with a consistent and familiar experience when accessing any resource, both on-prem and in the cloud.

Hybrid Attack Protection

Detect and prevent advanced lateral movement attacks that connect between the on-prem and cloud environments.

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.