Silverfort Bridging to Entra ID

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

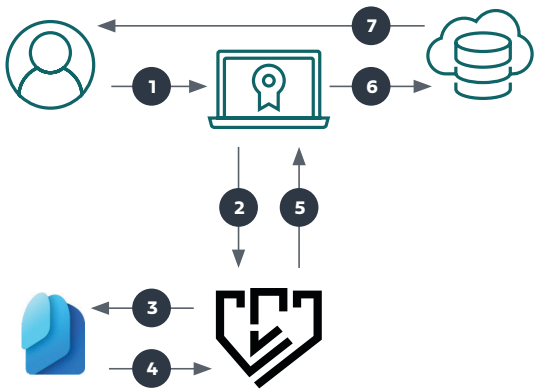
Authentications can be bridged according to their dependencies and usage using Silverfort. Silverfort can seamlessly bridge any type of authentication (legacy apps, command-line tools and more) into Entra ID, as if it were a modern web application. With Silverfort's bridging, an enterprise application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

How Does Entra ID Bridging Work?

1. The user sends the Active Directory (AD) a request to access resources
2. AD forwards the request to Silverfort
3. Silverfort translates the access request and forwards it to Entra ID
4. Entra ID evaluates the authentication based on its policy and forwards its verdict to Silverfort
5. Silverfort accepts the verdict and forwards it to AD
6. AD grants or denies access based on the Entra ID's verdict
7. Now all the applications and resources are in Entra ID



*A similar flow would apply upon attempting to access any other resource – the only change is the respective directory.

KEY BENEFITS

Discover All Applications and Resources

Simply discover all applications and resources in your hybrid environment, whether on-prem or cloud.

Bridge On-Prem Resources to Entra ID

Automatically discover on-prem applications and apply Entra ID security controls to these resources.

Protect the 'Unprotectable'

Extend Azure 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 traverse between the on-prem and cloud environment.