

Bridging On-Prem Authentication with Okta

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

Silverfort's Okta Bridge enables organizations to implement Okta web SSO flows to on-prem applications within their Okta environment and apply 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. Silverfort bridge allows organizations to extend authentications with Okta, enabling better visibility into their users' and resources' activities across web and on-prem applications.

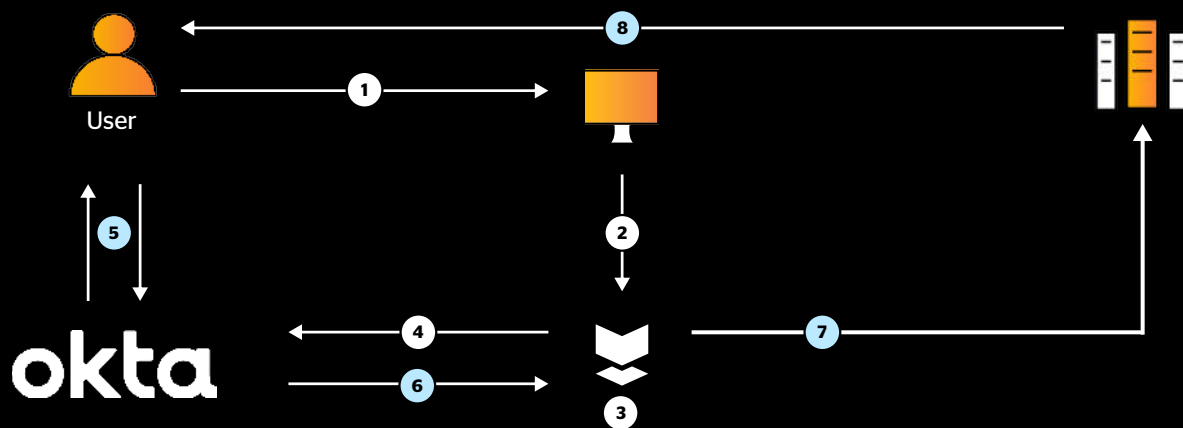
Bridging legacy resources

Okta's security controls can be extended using Silverfort bridging, while access policies can be applied to any resource on-prem or in multi-cloud environments. This enables organizations to apply strong modern identity security controls to all resources. By enforcing new security measures with Silverfort, organizations can take proactive measures against incoming cyber threats such as lateral movement attacks.

How does Silverfort's Okta bridge work

Silverfort can seamlessly bridge any type of application authentication (legacy apps, command-line tools, and more) into Okta as if it were a modern web application. With Silverfort's Okta bridge, customers can create applications representing the on-prem resource in Okta. Okta views this object as a SaaS app like any other cloud-based application. In Okta, configure an access policy for the application object that can utilize Okta Adaptive Authentication and MFA. By creating and applying the policy to each bridged on-prem resource, organizations will consolidate hybrid resources. Once the authentication and access policies have been configured, Silverfort monitors and protects attempts to access resources. All bridged applications can now be managed, monitored, and protected in Okta.

Enabling the Okta 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 Okta.
- 5** Okta evaluates the authentication based on set policy and sends the MFA request to the user.
- 6** After user's identity verification, Okta 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 Okta policies via Silverfort, reducing identity-based risks.



Seamless User Experience

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



Protect the 'Unprotectable'

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



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.