Silverfort

Silverfort Authenticator for Microsoft Teams

Extend on-prem authentication flows into Microsoft Teams for enhanced security and user experience

Use the Microsoft Teams app as an alternative to the Silverfort Desktop Application for Identity Bridge flows, with Silverfort Authenticator. With our Teams integration, enterprises can use our SSO bridging functionality to receive real-time alerts for all authentication requests in their hybrid environment, without installing the Silverfort desktop application on their workstations.

In addition to Identity Bridge flows, Silverfort Authenticator for Microsoft Teams supports FIDO2 tokens, One-Time Password (OTP) authentication, and Just-in-Time (JIT) access notifications for Privilege Access Security users. These capabilities allow end users to receive and approve access request directly within Microsoft Teams, reducing dependency on the Silverfort Desktop Application while maintaining strong identity security posture across authentication methods.

Bridging authentication flows with Microsoft Teams

Extend authentication flows into your existing environments and enforce strong identity security controls with the Silverfort Authenticator for Microsoft Teams. By enabling Teams for Identity Bridge flows, you can simplify the Silverfort's deployment process and scale protection to every end user without needing to install agents. You can also utilize the Silverfort Authenticator application for Microsoft Teams to receive notifications from FIDO and OTP tokens, and if you enforce JIT policies for privileged accounts within your environment, you can gain JIT access through the chat in Microsoft Teams. With enhanced authentication flows through Silverfort, your end users can get efficient, streamlined access to any resource, as defined by your access policies.

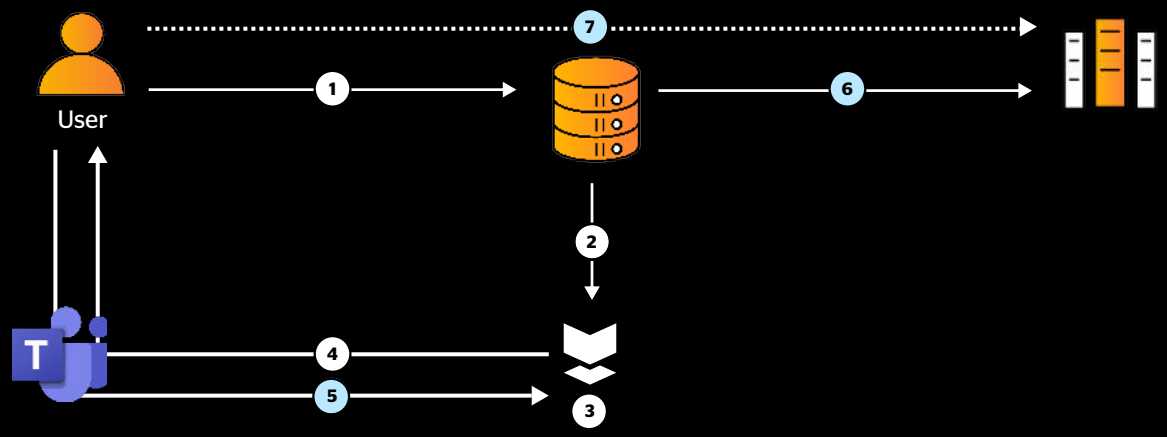
How does Silverfort Authenticator for Microsoft Teams work?

Silverfort seamlessly extends any type of authentication request and approval by embedding Identity Bridge flows, FIDO2, OTP and JIT authentications directly into Microsoft Teams' environment. Once the Silverfort Authenticator application is downloaded from the Microsoft Teams App Store, end users can install it individually or admins can use bulk deployment tools to extend it to the entire organization. During the installation, Silverfort automatically pairs with the application for a streamlined onboarding process.

When an Identity Bridge policy is triggered, the Silverfort app in Teams opens a browser to initiate the SSO request to verify the user's identity. The user can approve or deny the authentication request directly in Teams. Once the user has accepted the request, the bridge session is established, and the user gains secure access to a specific resource within your environment.

When FIDO2 or OTP-based policies are triggered, the Teams app displays a corresponding prompt for users to validate their identity with the configured method. Similarly, Privileged accounts operating under JIT policies will receive a Teams-based request to verify access at the time of need. These authentication events are securely processed within the Microsoft Teams chat interface, using Silverfort's centralized policy enforcement engine.

How does Teams Identity Bridge work?



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 policy, Silverfort opens a browser via MS Teams to initiate the SSO request to verify the user's identity.
5. The user accepts their identity:
   - **for Identity Bridge**, the user signs in via the configured IdP
   - **for FIDO2 or OTP**, the user authenticates using the respective method
   - **for privileged accounts with JIT access**, the user provides a valid reason for access and completes preliminary MFA.
6. Silverfort informs AD that the user can be trusted to access the resource.
7. AD returns the response to the unaware client/server and grants the user access.

Key benefits

Seamless user experience

Provide users with a consistent experience by enabling secure authentication directly within the Microsoft Teams interface.

Streamlined deployment

Simplify installation and configuration with an agent-free solution that supports both individual and bulk deployments.

Enhanced security

Protect resources with secure Identity Bridge flows, FIDO2 and OTP authentication, and gain JIT access for privileged accounts with JIT notification. Safeguard against identity-based threats across 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.