Silverfort for Entra ID Sign-In Logs

Silverfort offers a native integration with Entra ID (formerly Azure AD), enabling Silverfort to help aggregate logs from on-prem and Entra ID, including access requests to applications and resources.

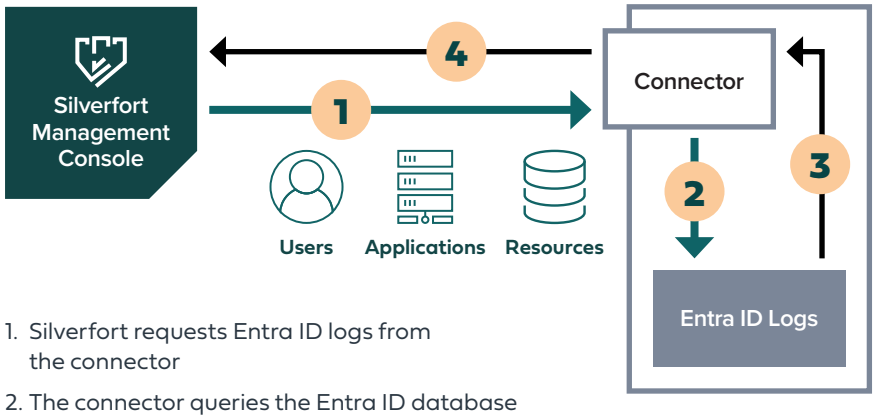
Full Context Into Each Sign In

Silverfort's ability to analyze Entra ID sign-in logs enables Microsoft customers to gain complete visibility into all their Entra ID authentication traffic. By enabling Silverfort to analyze all Entra ID sign-in logs, joint customers are empowered with Entra ID authentication risk indicators and advanced risk analysis of all user logs both in Entra ID and on-prem Active Directory, all in the convenience of a single platform. Now organizations can have complete visibility and full context into every access request across their hybrid environment.

How Silverfort Integrates with Entra ID for Unified Identity Protection

Silverfort seamlessly integrates with Entra ID to provide unified identity protection across on-prem, cloud, and edge environments. It does this by integrating with multiple Microsoft capabilities such as analyzing sign-in logs to protect customers' identity infrastructure. For example, Silverfort can prompt a user to sign in through Entra ID and protect authentications from other identity providers and directories with Azure MFA and Entra ID conditional access. With this integration, organizations have the ability to have complete visibility into all sign-ins to all on-prem and cloud resources in Entra ID.

How Silverfort for Entra ID Sign-In Logs Works



1. Silverfort requests Entra ID logs from the connector
2. The connector queries the Entra ID database
3. The Entra ID database sends the logs to the connector
4. The connector sends the logs to Silverfort

KEY BENEFITS

Actionable Threat Detection
Get concrete alerts of identity threats such as lateral movement, Pass the Hash, Kerberos, and more

Automated Risk Analysis
Leverage Silverfort to allow the correlation of data to calculate the risk of each user and resource in the environment

Optimized Investigation
Accelerate investigation time with granular forensic data on users, protocols, machines, and apps

Consistent Logs Experience
Context into all identity-based data in a single console

Security-Focused Insights
Automate all security data and logs with enriched and in-depth details of each sign in request