

Gain End-to-End Visibility Across Your Environment with Silverfort

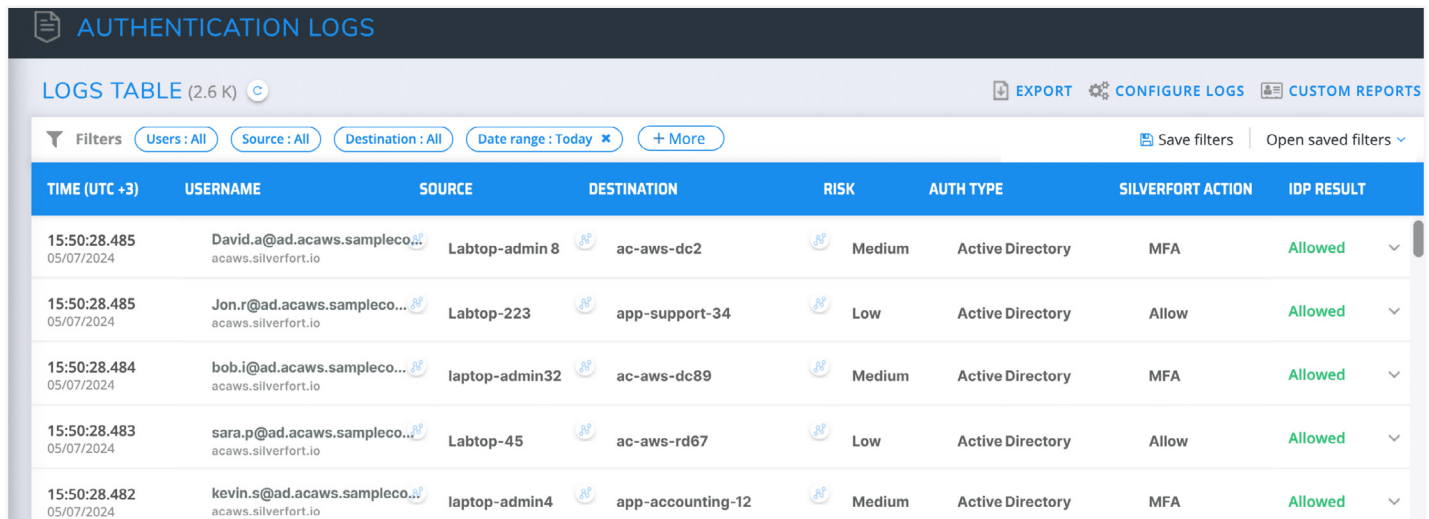
Real-time visibility into all identity traffic and authentication activities in one place

Security starts with visibility. If you don't have full visibility across your environments, you are essentially operating in the dark. Without clear insight into user and authentication activity, access permissions, risky identities, authorized applications, and the potential identity security risks in your organization, you cannot make informed decisions. As a result, you could be leaving critical identity security gaps without even being aware of them.

Complete Visibility of User Activity & Authentication

The moment Silverfort is deployed into your environment, it will detect and monitor all user accounts and offer real-time insights into their activity and associated risks, providing instant benefit to your security operations.

Silverfort's native integration with Active Directory enables it to log every authentication request. This allows you to gain a unified view of all activity across all users and resources within your organization. As each user is detected, their details are displayed in the Log screen by username, risk level assigned by Silverfort, authentication type, Silverfort's action, and the IdP result.



The screenshot shows the 'AUTHENTICATION LOGS' interface. At the top, there's a 'LOGS TABLE (2.6 K)' header with options for 'EXPORT', 'CONFIGURE LOGS', and 'CUSTOM REPORTS'. Below the header is a filter bar with 'Filters' and buttons for 'Users: All', 'Source: All', 'Destination: All', 'Date range: Today', and '+ More'. There are also 'Save filters' and 'Open saved filters' options. The main table has columns: TIME (UTC +3), USERNAME, SOURCE, DESTINATION, RISK, AUTH TYPE, SILVERFORT ACTION, and IDP RESULT. The table contains five rows of log entries.

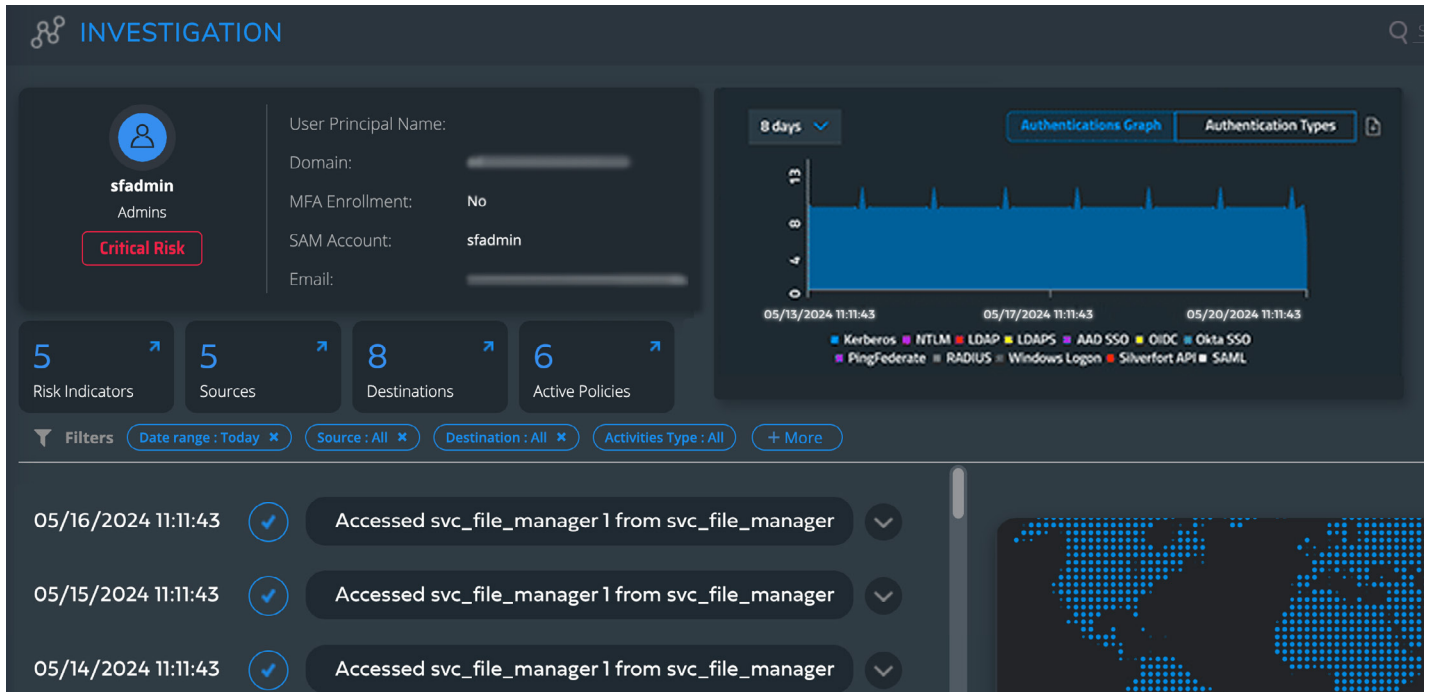
TIME (UTC +3)	USERNAME	SOURCE	DESTINATION	RISK	AUTH TYPE	SILVERFORT ACTION	IDP RESULT
15:50:28.485 05/07/2024	David.a@ad.acaws.sampleco... acaws.silverfort.io	Labtop-admin 8	ac-aws-dc2	Medium	Active Directory	MFA	Allowed
15:50:28.485 05/07/2024	Jon.r@ad.acaws.sampleco... acaws.silverfort.io	Labtop-223	app-support-34	Low	Active Directory	Allow	Allowed
15:50:28.484 05/07/2024	bob.i@ad.acaws.sampleco... acaws.silverfort.io	laptop-admin32	ac-aws-dc89	Medium	Active Directory	MFA	Allowed
15:50:28.483 05/07/2024	sara.p@ad.acaws.sampleco... acaws.silverfort.io	Labtop-45	ac-aws-rd67	Low	Active Directory	Allow	Allowed
15:50:28.482 05/07/2024	kevin.s@ad.acaws.sampleco... acaws.silverfort.io	laptop-admin4	app-accounting-12	Medium	Active Directory	MFA	Allowed

Silverfort's authentication logs screen provides full visibility into all user logs, authentication activity, and risk indicators.

Additionally, you can filter users' logs according to account type or risk indicator, as detected and assigned by Silverfort's risk engine. Silverfort supports a wide range of risk indicators, including NTLMv1, kerberoasting, brute force, MFA bombing, abnormal MFA activity, failed authentications, and many others. By filtering by risk indicator, you will gain complete visibility and insights into your risky users so you can begin the remediation process.

Investigate Quickly and Efficiently

You can gain more actionable insights by analyzing the details of a user's logs authentication activity, and risk indicators. These details provide a more granular understanding of each user and their authentication activity.



Silverfort's user investigation screen provides a detailed review of the authentication activities of a selected user to display their access requests in your environment.

Identity Security Posture Management

Silverfort provides an identity inventory of your environment in the Insights screen of the console, including users, resources, risky users, and more.



Silverfort's Insights screen offers insights into users, servers, applications, and devices protected by Silverfort.

Silverfort displays the types of users and resources in your environment as well as any weaknesses in your security that adversaries could abuse to launch identity threats. Among these are shadow admins, admin users with SPNs, accounts with passwords that do not expire, and many more. With actionable insights into the security posture of your environment, you will be able to resolve many security issues, making it significantly more difficult for threat actors to gain access to your network.

Visibility and Monitoring of Service Accounts

Silverfort identifies all service accounts based on the repetitive behavior that sets them apart from human users. Silverfort categorizes all detected service accounts into three main types: machine-to-machine (M2M) accounts, hybrid accounts, and scanners. Silverfort also supports Group Managed Service Accounts (gMSA) and offers a filter that allows you to see every gMSA in your system. Each gMSA will be detected and treated the same as any service account.

Protection	Service account	Sources	Destinations	Authentications	Risk	Baseline change	Info
<input checked="" type="checkbox"/>	svc_file_manager	6	8	250.1K	High	Last 7 days	🔒 ...
<input checked="" type="checkbox"/>	svc_healthmgmt-1	2	6	167.8K	Critical	Over a month	🔒 ...
<input type="checkbox"/>	svc-PLAN	1	3	98.7K	Medium	Over a month	🔒 ...
<input checked="" type="checkbox"/>	SQL Server Agent	1	4	25.6K	Medium	Last 14 days	🔒 ...
<input type="checkbox"/>	svc-jenkins	2	3	19.5K	Low	Over a month	🔒 ...

Silverfort's Service Accounts screen displays the service account name, source, destination, number of authentications, risk score, baseline change and account info.

Once all migrated service accounts have been detected, you can monitor service account activity and associated risks. Silverfort provides real-time insights and visibility into all service account details and behavior, and continually monitors and audits their use. This allows Silverfort to assess the risk of every authentication attempt and detect any suspicious behaviors or anomalies.

Investigation details for **svc_file_manager** (Users):

- User Principal Name: svc_file_manager
- Domain: svc_file_manager
- MFA Enrollment: No, has 10 MFA values
- SAM Account: svc_file_manager
- Email: svc_file_manager@svc_file_manager.com

Member of: Amit-AD-Users, Domain Users, Remote Desktop group

Summary: 5 Risk Indicators, 6 Sources, 8 Destinations, 6 Active Policies, 0 Cloud Applications, 0 AAD Roles

Filters: Date range: Today, Source: All, Destination: All, Activities Type: All, +More

Recent Activities:

- 05/15/2024 11:11:43 Accessed svc_file_manager 1 from svc_file_manager
- 05/16/2024 11:11:43 Accessed svc_file_manager 1 from svc_file_manager
- 05/17/2024 11:11:43 Accessed svc_file_manager 1 from svc_file_manager
- 05/18/2024 11:11:43 Accessed svc_file_manager 1 from svc_file_manager
- 05/19/2024 11:11:43 Accessed svc_file_manager 1 from svc_file_manager

Silverfort's investigation screen shows insights into a specific service account's activity.