

Splunk Cloud Integration



Splunk Cloud is a widely used, cost-effective data and analytics platform that helps organizations centralize logs, monitor security events, and gain operational insights. However, Saviynt currently does not offer a prebuilt Saviynt Exchange connector or native integration for Splunk Cloud.

This lack of an out-of-the-box integration limits customers from seamlessly forwarding Saviynt security logs, identity events, and analytics data to Splunk Cloud for centralized monitoring, correlation, and reporting. As a result, customers face challenges in achieving unified visibility across their identity governance environment and wider security ecosystem.

Customer Value

With this solution, customers can enable a smooth and secure integration between Saviynt and Splunk Cloud. This allows organizations to centralize their Saviynt logs and identity events within Splunk Cloud, unlocking improved monitoring and analytics capabilities.

The solution empowers customers to:

- Consolidate Saviynt data into Splunk Cloud for unified security visibility
- Leverage Splunk dashboards, alerts, and analytics for identity-related insights
- Strengthen compliance by maintaining centralized audit and activity logs
- Improve incident detection and response through correlation with other security data
- Reduce manual efforts by automating the log forwarding and monitoring process

Overall, the integration helps customers enhance their security posture and operational efficiency by combining Saviynt's identity intelligence with Splunk Cloud's powerful analytics platform.

Solution Benefits

Customers can integrate Saviynt with Splunk Cloud using the connection template developed by Macnica.

This integration delivers several key advantages that enhance security operations, compliance management, and overall identity governance efficiency.

Centralized Visibility of Provisioning Activities

The integration enables Splunk Cloud to ingest Saviynt's provisioning logs, offering a consolidated view of account creation, updates, and deprovisioning activities. This unified visibility improves monitoring accuracy and simplifies troubleshooting across identity workflows.

Values

- Centralized view of Saviynt provisioning logs
- Easier monitoring
- Faster troubleshooting
- Detects access and account anomalies
- Identifies unusual patterns
- Helps reduce security risks
- Better compliance visibility
- Clear audit trails
- Easier reporting
- Faster incident response
- Quick detection of unauthorized access
- Reduces impact of security issues
- Improved operational efficiency
- Automated data flow
- Less manual effort

Benefits

Centralized Visibility of Provisioning Activities:

- Splunk Cloud ingests Saviynt provisioning logs for unified monitoring
- Provides a consolidated view of account creation, updates, and deprovisioning
- Enhances troubleshooting by centralizing identity workflow data

Real-Time Detection of Anomalies in Account Imports

By analyzing imported account and entitlement data, Saviynt can automatically identify unusual patterns - such as abrupt privilege escalations, inactive or orphaned accounts, or mismatches in expected access. This helps organizations detect security risks early and take proactive action.

Compliance and Audit Transparency

All Saviynt provisioning and access import events are logged and correlated within Splunk Cloud, creating a comprehensive audit trail.

This simplifies compliance reporting and ensures full traceability of identity lifecycle operations, supporting regulatory and internal audit requirements.

Faster Incident Response for Access Issues

With Saviynt access data synchronized into Splunk Cloud, security teams gain immediate insight into unauthorized, suspicious, or excessive permissions. This accelerates response times and reduces the likelihood of security incidents or data exposure.

Operational Efficiency Through Automation

The automated transfer of Saviynt logs and identity data to Splunk Cloud eliminates manual data extraction and reduces operational overhead. Organizations benefit from timely, accurate, and consistent visibility into identity and access management activities.

Benefits

Real-Time Detection of Access and Account Anomalies:

- Analyzes imported account and entitlement data in Saviynt
- Detects unusual access patterns such as privilege escalation or orphaned accounts
- Helps prevent security risks through early anomaly identification

Compliance and Audit Transparency:

- Captures all provisioning and access import events in a centralized audit trail
- Supports regulatory and internal audit needs with complete traceability
- Simplifies reporting by correlating Saviynt identity data within Splunk Cloud

The Saviynt Identity Platform

Identity Security for AI. AI for Identity Security.™



Next Step

- View the extensive library of integrations at <https://saviynt.com/integrations> to see detailed information and implementation guides designed to help you get the most

About Partner

Macnica provides a broad range of solutions to resolve customer issues based on our technical planning prowess and our sourcing capability for cutting edge technology on a global scale.

About Saviynt

Saviynt's AI-powered identity platform manages and governs human and non-human access to all of an organization's applications, data, and business processes. Customers trust Saviynt to safeguard their digital assets, drive operational efficiency, and reduce compliance costs. Built for the AI age, Saviynt is today helping organizations safely accelerate their deployment and usage of AI. Saviynt is recognized as the leader in identity security, with solutions that protect and empower the world's leading brands, Fortune 500 companies and government institutions. For more information, please visit www.saviynt.com.



Headquarters
1301 E El Segundo Blvd,
Suite D El Segundo, CA 90245
United States

310.641.1664
info@saviynt.com
www.saviynt.com