Documentation for Sumo Logic apps and integrations.

This category has documentation for Sumo Logic apps. Several of the guides below are partner-specific: Amazon and AWS, Microsoft and Azure, and Google. The rest of the app content is organized by functionality. Please also see the Solutions page.

Apps help you get started gaining insights from your data source by providing example searches and dashboards for common use cases. They are customized with your source configurations and populated in a folder selected by you. Feel free to edit them to get the results you want.

To determine if an app is supported by your pricing plan, please visit this page.

Sumo Logic supports a wide variety of data sources. To interact with other Sumo Logic users, post feedback, or ask a question, visit the Sumo Logic Community Apps and Integrations Forum.

- Amazon and AWS
Amazon Aurora MySQL ULM
- Amazon Aurora PostgreSQL ULM
- Amazon CloudFront
- Amazon DynamoDB
- Amazon EKS - Control Plane
- Amazon Elasticache
- Amazon Elastic Container Service (ECS)
- Amazon GuardDuty
- Amazon Inspector
- Amazon Inspector App - Classic
- Amazon Kinesis - Streams
- Amazon Network Load Balancer
- Amazon RDS
- Amazon Redshift ULM
- Amazon Route 53 Resolver Security
- Amazon S3 Audit App
- Amazon Security Quick Start
- Amazon SES
- Amazon SNS
- Amazon SQS
- Amazon VPC Flow Logs
- AWS API Gateway
- AWS Application Load Balancer
- AWS Classic Load Balancer
- AWS CloudTrail
- AWS Config
- AWS EC2
- AWS Elastic Load Balancer - Application
- AWS Elastic Load Balancing
- AWS Elastic Load Balancing - Classic
- AWS Elastic Load Balancing Metrics
- AWS Lambda
- AWS Network Firewall
- AWS Security Hub
- AWS WAF
- CIS AWS Foundations Benchmark App
Global Intelligence for Amazon GuardDuty
- Global Intelligence for AWS CloudTrail SecOps
- Global Intelligence for AWS CloudTrail DevOps
- Host Metrics (EC2)
- PCI Compliance for Amazon VPC Flow Logs
- PCI Compliance for AWS CloudTrail App
- Threat Intel for AWS

- Microsoft and Azure

Docs for Sumo apps for Microsoft and Microsoft Azure.
- Active Directory JSON
- Active Directory Legacy
- Azure Active Directory
- Azure Audit
- Azure Integration using ARM - FAQs
- Azure Kubernetes Service (AKS) - Control Plane
- Azure Network Watcher
- Azure SQL
- Azure Web Apps
- IIS 7
- IIS 10 (Legacy)
- Microsoft Office 365
- Microsoft SQL Server
- Microsoft Teams App
- PCI Compliance for Windows Legacy
- PCI Compliance for Windows JSON
- Windows JSON
- Windows Legacy
- Windows Performance

- Google

Docs for Sumo apps for Google.

- Google App Engine
- Google BigQuery
- Google Cloud Audit
- Google Cloud Firewall
- Google Cloud Functions
- Google Cloud IAM
- Google Cloud Load Balancing
- Google Cloud SQL
- Google Cloud Storage
- Google Cloud VPC
- Google Compute Engine
- Google Kubernetes Engine (GKE) - Control Plane
- Google Workspace
Docs for Sumo apps for platforms and tools that support software development processes.

- Artifactory
- Bitbucket
- GitHub
- GitLab
- Jenkins
- JFrog Xray
- Jira
- Jira Cloud
- JMX
- Puppet
• **Containers and Orchestration**

  Docs for Sumo apps for container management and orchestration tools.
  - ActiveMQ
  - Kafka
  - Kubernetes
  - Kubernetes Control Plane
  - RabbitMQ
  - VMware

• **Databases**

  Docs for Sumo apps for database servers.
- Cassandra
- Couchbase
- Elasticsearch
- MariaDB
- Memcached
- MongoDB
- MongoDB Atlas
- MySQL
- Oracle
- PostgreSQL
- Redis

- Hosts and Operating Systems

Docs for Sumo apps for hosts and Linux.

- Host and Process Metrics
- Host Metrics
- Linux
- Linux Performance
- **PCI Compliance**

  Docs for Sumo apps for PCI Compliance.

- **SAAS and Cloud Apps**

  Docs for Sumo apps for SAAS and Cloud applications.

  - Acquia
  - Akamai Cloud Monitor
  - Box
  - Fastly
  - Istio
  - Opsgenie
  - PagerDuty V2
  - PagerDuty V3
  - Salesforce
- **1Password**

  1Password is a secure and convenient password manager for documents, credit card information, and addresses.

  - Collect Logs for 1Password
  - Install the 1Password App and View the Dashboards
• **SAML**

Docs for Sumo apps for SAML.

- Okta
- OneLogin

• **Security and Threat Detection**

Docs for Sumo apps for Security and Threat Detection.

- Akamai Security Events
- Barracuda WAF
- Carbon Black Cloud
- Cisco ASA
- Cisco Meraki
- CloudPassage Halo
CrowdStrike Falcon Endpoint Protection
- Cylance
- Duo Security
- Evident.io Evident Security Platform
- F5 - BIG-IP LTM
- Imperva - Incapsula Web Application Firewall
- Netskope
- Observable Networks
- Palo Alto Networks 6
- Palo Alto Networks 8
- Palo Alto Networks 9
- Threat Intel Quick Analysis
- Trend Micro Deep Security
- Twistlock
- VMware Carbon Black
- Zscaler Internet Access
- Zscaler Private Access
- Zscaler Web Security

• Web Servers

Docs for Sumo apps for web servers.

- Apache
- Apache Tomcat
• Apps for Sumo

Docs for apps that help you monitor your Sumo Logic org.

• Audit App
• CSE App
• Data Volume App
• Data Volume App - Legacy
• Enterprise Audit Apps
• Enterprise Search Audit App
• Infrequent Data Tier
• PCI Compliance through Professional Services
• Security Analytics App

• Cloud Security Monitoring and Analytics

This page provides documentation access for all five data source apps that Sumo provides

• Amazon GuardDuty - Cloud Security Monitoring and Analytics
• Amazon VPC Flow - Cloud Security Monitoring and Analytics
• AWS CloudTrail - Cloud Security Monitoring and Analytics
• AWS Security Hub - Cloud Security Monitoring and Analytics
• AWS WAF - Cloud Security Monitoring and Analytics
• Linux - Cloud Security Monitoring and Analytics
• Palo Alto Firewall 9 - Cloud Security Monitoring and Analytics
• UEBA App
• Windows - Cloud Security Monitoring and Analytics

• Partner Ecosystem Apps

Partner Ecosystem Apps Documentation- Third-party Sumo Logic apps for Alcide kAudit, Aqua Security, Aria Packet Intelligence App, Armory, Auth0, Barracuda CloudGen Firewall, CircleCI, CloudFlare, Code42, StackRox, CheckPoint, Cybereason, and Nucleon.

• Partner Integrations