Apps and Integrations

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 Redis ULM
- Amazon Elastic Container Service (ECS)
- Amazon GuardDuty
- Amazon Inspector App
- Amazon Kinesis - Streams
- Amazon RDS Metrics
- Amazon Redshift ULM
- Amazon S3 Audit
- Amazon Security Quick Start
- Amazon SES
- Amazon SNS
- Amazon SQS
- Amazon VPC Flow Logs
- AWS CloudTrail
- AWS Config
- AWS Elastic Load Balancer - Application
- AWS Elastic Load Balancing
- AWS Elastic Load Balancing - Classic
- AWS Elastic Load Balancing Metrics
- AWS Elastic Load Balancing ULM - Application
- AWS Elastic Load Balancing ULM - Classic
- AWS Lambda
- AWS Lambda ULM
- 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
- PCI Compliance for Amazon VPC Flow Logs
PCI Compliance for AWS CloudTrail App

- Threat Intel for AWS

- **Microsoft and 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
  - Microsoft Office 365
  - Microsoft SQL Server
  - PCI Compliance for Windows
  - 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
- G Suite
• App Development

Docs for Sumo apps for platforms and tools that support software development processes.

- Artifactory
- Atlassian
- Bitbucket
- GitHub
- Jenkins
- JFrog Xray
- Jira
- Jira Cloud
- JMX
- Puppet
- Varnish
• Containers and Orchestration

Docs for Sumo apps for container management and orchestration tools.

◦ Kubernetes
◦ Kubernetes Control Plane
◦ VMware
◦ VMware ULM

• Databases

Docs for Sumo apps for database servers.

◦ MongoDB
• Hosts and Operating Systems

Docs for Sumo apps for hosts and Linux.

• Host Metrics
• Linux
• Linux Performance
• PCI Compliance

Docs for Sumo apps for PCI Compliance.

◦ Choosing Between PCI Compliance Apps and PCI Compliance Professional Services App

• SAAS and Cloud Apps

Docs for Sumo apps for SAAS and Cloud applications.

◦ Acquia
◦ Akamai Cloud Monitor
◦ Box
◦ Fastly
◦ Istio
◦ Opsgenie
◦ PagerDuty V1
◦ PagerDuty V2
Salesforce
  ◦ Slack
  ◦ Zoom

- SAML

Docs for Sumo apps for SAML.
  ◦ Okta
  ◦ OneLogin

- Security and Threat Detection

Docs for Sumo apps for Security and Threat Detection.
  ◦ Barracuda WAF
  ◦ Carbon Black
  ◦ Cisco ASA
• Cisco Meraki
• CloudPassage Halo
• CrowdStrike Falcon
• 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
• Zscaler Web Security

• Web Servers

Docs for Sumo apps for web servers.

• Apache
• Apache Tomcat
• Nginx Ingress ULM
• Apps for Sumo

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

- Audit App
- Data Volume App
- Enterprise Audit Apps
- Enterprise Search Audit App
- Infrequent Data Tier
- PCI Compliance
- Security Analytics App

• Partner Ecosystem Apps

Partner Ecosystem Apps Documentation
• Partner Integrations

Integrations created and supported by Sumo Logic Partners.