Splunk Cloud Administration Managed Services

The Splunk Cloud Administration Managed Service provides ongoing operational administration, platform support, and managed assistance for Splunk Cloud environments. The service ensures Splunk Cloud deployments remain stable, secure, performant, and well governed, while allowing organisations to adapt data ingestion, searches, content, and configurations within clearly defined operational boundaries.

Service Overview

Delivered by certified Splunk specialists, the service provides business-as-usual administration, proactive maintenance, and technical assurance for Splunk Cloud environments, including premium applications and Edge Hub deployments. It enables customers to maximise value from Splunk while removing the day-to-day operational burden of platform management and retaining access to controlled levels of optimisation and change support.

Platform Administration & Management

- Ongoing administration of Splunk Cloud environments
- Monitoring of platform availability, health, performance, and capacity
- Configuration management aligned to Splunk best practice
- Licence usage, ingestion, and capacity oversight
- Coordination and oversight of Splunk Cloud upgrades and updates
- Performance investigation and optimisation recommendations
- Liaison with Splunk vendor support, including case creation, tracking, and resolution

Data Ingestion, Index & Search Management

- Monitoring of data feeds to ensure expected and continuous data ingestion
- Index management, including creation, modification, and maintenance
- Support for onboarding new data sources using existing architectures and approved patterns
- Forwarder management and configuration updates
- Support for data normalisation and ingestion optimisation within agreed scope
- Monitoring and optimisation of scheduled searches and workloads
- Troubleshooting of search performance and SPL-related issues

Where activity exceeds routine operational change, work will be delivered under separate project or enablement services.

Content & Knowledge Object Support

- Creation, modification, and maintenance of knowledge objects
- Support for searches, reports, and dashboards
- Content optimisation to improve performance, usability, and operational insight

Large-scale content development, solution design, or use-case implementation is delivered separately under published enablement or professional services.

Application & App Management

- Installation of standard Splunk applications
- Upgrading and maintenance of standard Splunk apps
- Configuration of app content to ensure correct operation and accessibility

User & Access Management

- Creation, modification, and removal of user accounts
- Administration of role-based access control (RBAC), roles, and permissions
- User access troubleshooting, including authentication and authorisation issues

Support, Incident & Change Management

- Platform-level incident investigation and technical troubleshooting
- Defined response and resolution targets aligned to incident severity
- Coordination of changes in accordance with customer change-management processes
- Proactive monitoring and alerting for platform and performance issues
- Clear escalation paths and service-desk integration

Documentation, Reporting & Assurance

- Maintenance of operational documentation and service records
- Regular service reporting covering platform health, usage, and incidents
- Service reviews with recommendations for optimisation and operational improvement
- Knowledge transfer and operational handover support where required

What the Service Delivers

- Stable and well-managed Splunk Cloud environments
- Reliable data ingestion, search, and content operation
- Controlled support for evolving data sources, searches, and dashboards
- Reduced operational risk and unplanned disruption
- Consistent application of security and access controls
- Ongoing access to specialist Splunk expertise within defined service boundaries

How the Service Is Used

This service is used by organisations operating Splunk Cloud that require ongoing administration, operational support, and controlled platform change, but do not wish to retain dedicated Splunk specialists internally. It may also be used to supplement internal teams during periods of increased demand, platform evolution, or organisational change, while maintaining a clear separation between business-as-usual administration and project-based delivery.

Delivery & Commercial Model

- Delivered as an ongoing managed service
- Scalable based on platform size, data volumes, and usage patterns
- Delivered by SFIA v8-aligned Splunk specialists
- Clear operational boundaries, responsibilities, and assumptions
- Routine activities delivered within agreed monthly service parameters
- Suitable for G-Cloud Lot 3 (Cloud Support) procurements

Relationship to Other Services

The Splunk Cloud Administration Managed Service complements Splunk Health Check & Assessment Services, Splunk Data Platform Enablement Services, and wider Cyber, Observability, and AIOps offerings. It provides the operational foundation required to sustain value from Splunk Cloud over time while enabling more advanced outcomes to be delivered through separate specialist services.