

Service Description

The SaaS-version of Logpoint SIEM is a cloud service with a SaaS operational model that provides capabilities of Logpoint SIEM+SOAR.

The service can be accessed in two ways:

- Via Web UI on <https://..logpoint.cloud/> – by the end users of the service.
- Via Logpoint Cloud Connector Appliance deployed on Customer premises.

Capabilities

The SaaS-version of Logpoint SIEM provides the following capabilities:

- Via on-premise Cloud Connector Appliance:
 - Collection of log information from a variety of log sources
 - Normalization of log information into events
 - Enrichment of collected events with information from a variety of enrichment sources, both static and dynamic
- Via Web UI:
 - Dashboards for continuous monitoring
 - Alerts for automatic detection of threats
 - Search and Search templates for data analysis, investigation, and threat hunting.
 - Reporting
 - Incident management
 - Case management
 - Automation of investigations and response

between the Cloud Connector Appliance and the Web UI.

- Enrichment information is not shared between on-premises instance and web UI, which means that:
 - Static enrichment sources (CSV, TXT) must be replicated by the user
 - GeoIP and TI enrichment sources must be configured on Cloud Connector Appliance and the Web UI.
 - Certain enrichment sources such as IP2Host, AD or ODBC cannot be used in the Web UI.
- Logpoint SOAR Investigation and Response integrations are limited to publicly-accessible services.
- Logpoint Director is not supported by Logpoint Cloud Connector Appliance or Logpoint Converged SIEM service.

Compatibility

- The SaaS-version of Logpoint SIEM is compatible with the content and plugins released for Logpoint SIEM 7.0.
- Logpoint Cloud Connector Plugin may only be installed on a full Logpoint SIEM 7.0 installation and cannot be installed on a Logpoint Collector (LPC) instance.
- Only username-password authentication is supported in the Logpoint Converged SIEM Web UI.

Supported Regions

The SaaS-version of Logpoint SIEM is supported in the following geographical locations:

- US (Oregon)
- EU (Ireland)

As part of the Logpoint SIEM service, the Customer must select a region where Logpoint SIEM service will be activated. Logpoint will store and process the submitted data in the selected region according to [Logpoint Data Processing Addendum](#).

email for communication regarding the service. Logpoint will use the provided contact information for the following purposes:

- Notifications about changes in service status such as degraded operation, incidents, or outages.
- Notifications about changes to the service, such as changes to the capabilities, service level agreements and terms of service.
- Notifications of Maintenance Windows.

As part of the Logpoint SIEM service, the customer can use Logpoint ServiceDesk for technical support, reporting incidents, and service requests.

Service Level Agreement

This Service Level Agreement defines the Logpoint SIEM service policy and Logpoint's commitment to service availability.

Shared Responsibility

By using Logpoint SIEM service, the Customer agrees to the Shared Responsibility model of service availability.

As part of Shared Responsibility model, Logpoint takes the following responsibility:

- Ensure availability of Logpoint SIEM Web UI, targeting communicated Service Level Agreement.
- Monitor the on-premises Logpoint Cloud Connector Appliance instance via Logpoint Support Connection to ensure a smooth collection of log information into Logpoint SIEM service.
- Provide support to the customer regarding data collection on-premises.
- Provide support to the customer regarding Logpoint SIEM Web UI.
- Notify the customer in case of changes to the service status, capabilities, service level agreements and terms of service.



architecture and Cloud Connector Appliance instances.

- Configure log collection, normalization, and enrichment according to the agreed number of devices and/or company employees.
- Ensure the security of all license and credential files issued by Logpoint in connection with the service.
- Ensure proper capacity and Internet connection bandwidth for the Cloud Connector Appliance instance to ensure smooth collection and transmission of the logs.
- Ensure Support Connection is always enabled on the Cloud Connector Appliance instance for Logpoint Support to provision monitoring and support services.
- Follow the user manuals and recommendations from Logpoint Support when configuring and using Logpoint Converged SIEM and Cloud Connector Appliance.
- Configure detection, monitoring, and reporting content according to best practices and recommendations from Logpoint.

Definitions

- The monthly Uptime Percentage is calculated by subtracting from 100% the percentage of minutes in the Monthly Period where the service was not in the state of Availability as described by the service.
- Service Credit Percentage is the percentage of the service costs prorated to the Monthly Period where the SLA is applied.
- The monthly Period is from the 1st of a calendar month until the 1st of the following calendar month.

Commitment

Logpoint commits to the following levels of service availability:

- Web UI: 99% uptime within every month, except for Maintenance Windows and disaster events. Availability is measured as Logpoint Web UI's ability to respond to requests.



Monthly Uptime Percentage	Service Credit Percentage
Less than 99% but more than 95%	10%
Less than 95%	25%

Our internal Service Level Objectives are significantly higher than the communicated commitments, and Logpoint works towards raising the SLA commitments.

Logpoint service objectives for Service Requests and Support are governed by Logpoint Support Service Level Agreement.

Example on calculation

In Oct 2022, the customer experienced an outage of Logpoint UI, so the customer couldn't log in and perform investigations for 2 hours on a particular Monday – and 4 hours on the following Tuesday.

Total Time = 31 (days) * 24 (hours) * 60 (minutes) = 44640 (minutes)

Confirmed Outage Time = 720 (minutes)

Monthly Uptime (October) = $(1 - 720 / 44640) * 100\% = 98.39\%$

Eligible credit = 10% of the Monthly Price.

Service Credit

If LogPoint does not meet a Monthly Uptime Commitment, the Customer has the right to claim a Service Credit. For LogPoint to consider a claim, the Customer must submit the claim by emailing LogPoint at saas-billing@logpoint.com and citing the applicable invoice number the Service Credit is claimed against. The Service Credit shall be deemed waived unless LogPoint receives the foregoing email request claiming a Service Credit within 14 days of the end of the Applicable Monthly Period.

If LogPoint determines that a Service Credit is owed to the Customer, LogPoint will apply such Service Credit to any future payment of fees occurring. Service Credits will not entitle the Customer to any refund or other payment from LogPoint. The customer may not unilaterally offset its fees for any availability issues.

Exclusions from the Service Level Agreement

The service availability SLA does not apply to the service issues:

- Due to factors outside Logpoint's reasonable control, including network, Internet, or other access or availability problems beyond the demarcation point of Logpoint.
- That result from the Customer's inability to comply with responsibilities defined in the Shared Responsibility section of this document.
- That result from Customer's unauthorized access, customization of the service, fault in or absence of Customer's input.
- That result from the Customer's overburdening of the service or failure to properly configure system components, modify its use as advised by Logpoint, or comply with the official documentation.
- That result from the provision of Support, including maintenance operations (see Maintenance Windows section) and any actions arising out of Support as requested or performed by the Customer.
- That result from any additional components outside of the Logpoint services scope.
- That appears in the service component or instance defined as "beta," "preview," or "non-production" by Customer's agreement and/or official documentation.

Maintenance Windows



notified via Technical Contact communication at least two weeks before the activity.

In rare cases of Unplanned Maintenance, where urgent action is needed to maintain stability and continuity of the service, Logpoint will notify the Technical Contact about the time and nature of the maintenance operations to be performed and their impact on the service.

Disaster Recovery

Events that are not under the control of Logpoint and impact Logpoint's ability to operate Logpoint Cloud service for more than one customer are qualified as disaster events. These events may include natural disasters, technological failures, or human actions, either malicious or erroneous.

Logpoint takes reasonable measures to ensure recovery in case of disasters that affect a single availability zone with the following objectives:

- Recovery Time Objective: 24 hours
- Recovery Point Objective: 24 hours

Logpoint works continuously on our disaster recovery measures to improve the objectives and enable recovery across geographical locations.

Compliance

Logpoint is committed to following best practices and obtaining certifications according to SOC2 or equivalent, GDPR and ISO 27001.

