LIFE™ SERVICES

Frequently Asked Questions

Services

What is LIFE™ Services?

LIFE™ Services, offered by Vertiv™, provides increased uptime and operational efficiency through continuous monitoring, expert analysis, and proactive response. Detailed parametric data is continuously captured with advanced technology embedded in select critical systems. The data is transmitted safely and efficiently to an authorized remote service center staffed with remote system engineers. Should an operating anomaly or alarm condition arise, the engineer performs an immediate analysis and initiates an appropriate response to have the critical system quickly, safely, and accurately restored to its proper operating condition.

1. 24x7 continuous remote monitoring

2. Expert analysis and diagnosis

3. Quick, safe, and accurate response

How is LIFE™ Services different than monitoring via a building management system?

The key advantage of LIFE™ Services is having remote system engineers monitor, analyze, and respond to critical system alarm messages and operating anomalies. These experts receive specialized training and have access to extensive tools to aid in optimizing the health of critical systems. The end result is increased uptime and operating efficiency.

Who is monitoring the critical systems and where?

Remote system engineers located in remote service centers monitor, analyze, and respond as necessary to optimize the health of the critical systems. At present we have remote service centers around the world to manage critical systems in each of the major regions: Americas, Asia Pacific, Europe, Middle East and Africa.

Is critical system data available to review?

Yes, critical system data is analyzed and summarized in a trend and analysis report that is provided for review quarterly. This report includes details regarding the operating condition and any alarm conditions that were present during the period under review.

Is the service available for non-Vertiv critical systems?

No, LIFE™ Services is currently only available for select Vertiv critical systems.

Which equipment is enabled for the service?

Please contact your sales representatives for the most recent list of enabled critical systems. The list of supported critical systems continues to be expanded.

Is a maintenance contract required to have LIFE™ Services?

Yes, having a maintenance contract on the critical system ensures that any required on-site action can be quickly coordinated and taken in the event of a critical alarm or detection of an operating anomaly.

What is required to activate the service?

Please either refer to quick start guide or contact your sales representative to initiate the activation process. A physical Ethernet RJ45 connection (CAT 5, 5e, 6) with access to the internet is required for each critical system.

Connectivity

How is the data transmitted?

Hypertext Transfer Protocol (HTTP) is used as an encapsulating protocol to transmit data between the enabled critical systems and the remote service center. All communication is initiated by the equipment beginning with a request to communicate with the authorized server. Upon successful validation of the request, data is transmitted and then the connection is closed. There are three primary message types:

- Emergency – Occurs in case of a condition which requires service

- Routine – Occurs on a scheduled interval (usually every 24 hours)

- Manual – Occurs when activated from the critical system

Are other critical systems or devices on the network accessible via the connection?

No, only the critical systems that have been activated will transmit data. The communication technology is such that the equipment initiates the transmission of data. Any critical system that does not have the technology is not accessible. The same is true for critical systems with the technology in a disabled state.

Is a static IP address required?

No, a dynamic IP address assigned via Dynamic Host Configuration Protocol (DHCP) is sufficient.

Does communication work through a firewall?

Yes, given that internet traffic (Outbound to TCP port 80) is allowed through the firewall.

Which network ports are required?

Outbound connections to TCP port 80 are required.

What will be the network traffic?

100 kb/equipment per file transfer.

Does communication work through a proxy?

Yes, the communication technology includes the proper settings to accommodate a proxy server with null and basic authentication methods.

Data/Control

What type of data is collected?

Critical system alarms, events, operating parameters, and identification data are collected and transmitted to authorized remote service centers. The alarm and status messages contain vital information regarding the state of the critical system and are used to initiate a rapid incident response. The select operating parameters are a source for detailed diagnosis and trending analysis to ensure an appropriate response that optimizes the health of the critical system. The unit serial number is used to identify the unit. No customer contact information is transmitted.

Is a remote system engineer able to turn off the critical system remotely?

No, critical systems cannot be controlled remotely.

Where is the data stored?

The data is stored in the state-of-the-art Vertiv global data center located in the United States. A backup of the data is maintained for disaster recovery and is stored in a failover facility also located in the United States.

Who has access to the data?

Authorized remote system engineers and managers have access to the data collected from the critical systems. User identification and passwords are used to control access to the analysis tools and the data.