

# LIS Integrity Services

## Overview:

Through collaboration with customers, C4 determines which devices in the IT environment to remotely monitor and manage. We implement policies on all managed devices. In addition to our standard policies, we have developed many software-specific laboratory information system (LIS) policies to ensure customer success. Alerts are tracked in C4's customer relations management system for reporting purposes, and emailed in real-time to approved client recipients.

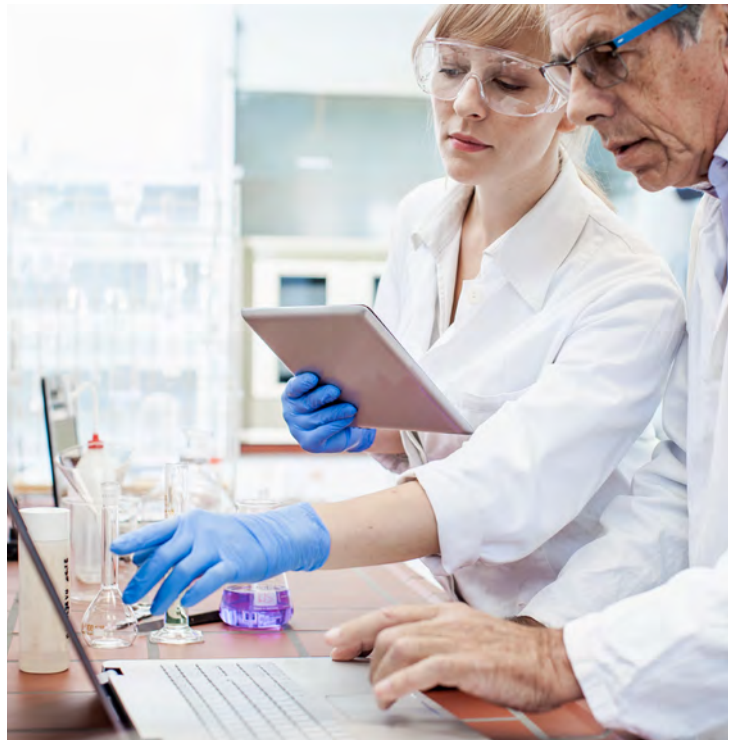
Each month clients receive the following reports based upon their listed monitors:

- Executive Summary—Represents capability of the network to perform to standards, including disk and memory capacity, and overall network health
- Device Activity—Shows the amount of time C4 has worked on all managed devices by task
- Device Health—Displays overall health of the devices under C4 management

## Specific Monitor Alerts:

Based on a customer IT environment and the brand and version of LIS software being used, C4 creates many specific alerts as part of LIS Integrity Services. The monitoring scenario may include many or all of the following types of alerts:

- General / non-LIS software based:
  - C4\_StandardWindowsWorkstation: details of assigned workstations, including desktops, laptops, surface devices
  - C4\_StandardWindowsServer: details of assigned Windows servers
- LIS software brand-specific:
  - C4\_TomcatServer: details of assigned monitored Tomcat Servers
  - C4\_DatabaseServer: details of assigned monitored Software Database Servers
  - C4\_InterfaceClient: including instrument interfaces, provides details of assigned monitored Software Interface Clients
  - C4\_InstrumentInterfaceClient: details of assigned monitored Software Instrument Interface Clients
  - C4\_PrintServer: details of assigned Software Printer Servers





## Alert Metrics:

Depending on the nature of the device being monitored, different metrics are tracked. Some are common throughout all alerts and others are specific to certain types. They include but are not limited to:

- Common metrics:
  - Priority level
  - Response status
  - Ticket created
- Performance metrics:
  - CPU – varies from overall use and uptime, to percentage within time limits
  - Memory and disk space – percentages, use within time frames
  - Downtime – critical extended stop times, device off-line
- Capacity metrics:
  - File size percentages of critical directories
  - Usage of critical directories
  - Amount of targeted codes in user and event logs
- Specific device scenario metrics (examples, more possible):
  - Metrics for versions of Tomcat, Apache and Nginx
  - Application, error and hang
  - System reboot and event log / application windows errors
  - Tracked application memory consumption
  - Application errors related to PDF creation and print spoolers