KNIGHT SECURITY SYSTEMS
HONOR, INTEGRITY, SERVICE

Sentry System Health Monitoring Technical Requirements

QUICK OVERVIEW

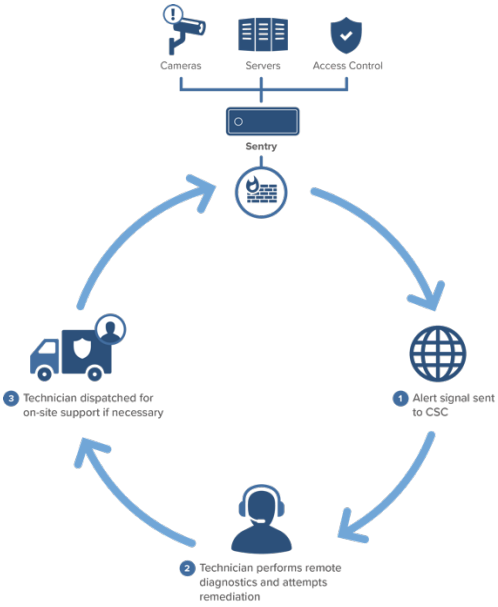
The System Health Monitoring (SHM) provided by Knight Security Systems is enabled by Knight Sentry™, a purpose built appliance developed and patented by Knight Security Systems. The architecture of Sentry SHM requires a Sentry appliance to be directly connected to the local network supporting the devices that are being monitored. All SHM data is communicated to the KSS Client Support Center (CSC) for diagnosis, remediation, and response actions. To protect the security of the SHM data in transit, Sentry uses a 256-bit encryption TLS connection back to our CSC.

NETWORK CONNECTIONS AND PORT REQUIREMENTS

Each Sentry appliance requires a physical connection to the network containing the devices to be monitored and a statically assigned IP address. Also required is outbound communication access to the CSC via the fully qualified domain names **https://ss0.knightsecurity.com** and **https://support.knightsecurity.com** on both TCP ports 22 and 443. Additionally, a Domain Name System (DNS) server is required for Sentry to resolve its connection back to the CSC. System Health Monitoring does not require access on any ports for inbound access (port forwarding).

AIR-GAPPED/ISOLATED SECURITY NETWORKS

Sentry incorporates dual network interfaces in its design making it possible to reside on multiple networks simultaneously. This allows isolated security networks to be monitored from one interface and the Sentry appliance to report alert data back to the CSC on the other interface.



EVENT LIFE CYCLE

When an event occurs, such as a camera losing network connectivity, an alert is generated by the Sentry appliance according to the parameters set for that specific camera. The alert information is securely communicated to the CSC. After receiving an alert, CSC technical personnel may begin a remote root cause analysis and remediation action utilizing the communication channel initially established by the outbound alert. To perform these actions, the CSC personnel will generally employ the remote support platform by Bomgar and have access to all devices monitored by the Sentry appliance. No additional permissions or settings are required to enable this access, and all remote sessions are recorded and archived. For scenarios where remote remediation is not possible or successful, the CSC will engage a regional office service team to provide on-site remediation of the detected issue.

For more information on System Health Monitoring, please contact your Knight Security Systems Account Manager or contact us at Support@KnightSecurity.com.