CenTrak Server & Network Requirements

Security Solutions Application Server

Supported Operating Systems
Windows Server 2008 R2, 2012 R2, 2016, 2019

Minimum Hardware Requirements	
Server can be a Virtual Machine or Physical Server	
Processor	Dedicated Quad Core Processor running at 2.75 GHz or higher Virtualized systems should have at least the 4 cores dedicated, and not shared, across other software applications.
Memory	16 GB RAM minimum
Hard Drive	500 GB local disk space for application components, backups, and log-files Minimum 15k RPM
Network Adapter	Dedicated 1Gbps connection

Network	
Remote Connectivity User account with admin access to server	Remote access process for CenTrak personnel to access the CenTrak server for installation, administration, maintenance and troubleshooting. Local access to server from within facility network. – E.g. RDP access from CenTrak laptop while onsite – Web browser access to server with supported web based applications
Communication Speed	Maximum of 7 milliseconds round trip communication for all wired nodes (server, star, timing controller and security controller).

CenTrak products do not support the Connect Core Software to be used over public internet connections due to uncontrollable latency issues. CenTrak's Location and Sensing Services should always meet the timing constraints of the system specifications over averaged time, not single point tests, which is typically not possible outside of private networks.

Required Applications

- Microsoft Internet Explorer 9 (or above) or Google Chrome
- JavaScript support must be enabled
- Adobe Reader
- WinRAR 3.0 or above (license to be acquired by customer)
- Microsoft .NET Framework 4.0 or above
- Internet Explorer with ActiveX control or Google Chrome with IE Tab browser extension by Black Fish Software (link)
- IIS 7 or above (IIS 8 preferable)
- Access to 10 GB of facility Enterprise SQL Server 2016R2, 2017 or 2019 Database

Note: For CenTrak solutions using databases, it should take a maximum of 10 seconds to perform 10,000 database write operations.

CenTrak Server & Network Requirements

CENTRAK®

Internet Protocol Addressing

IP Addresses	Static
	Server

Port Configuration

The following Ports need to be opened for the CenTrak RTLS Server.

Device	Ports	Protocol
SQL Server	1433	TCP
Workstations	80	TCP
Alert Push Connector	9595	TCP
HL7 Connector	9910	TCP

Network Security Configuration

Criteria	Reason
Need to configure anti-virus software to exclude scanning and live protection on all CenTrak folders (e.g. C:\CenTrak, "C:\Program Files\CenTrak")	CenTrak software continuously writes data to storage. Due to the format of the file and consistency of the writing, anti-virus and other security software will monitor and block these writes. The entire folder will need to be excluded from both periodic scanning and being monitored in real time.
Need to exclude network monitoring / firewall software from all CenTrak folders	CenTrak software makes many network connections with the various CenTrak hardware deployed. Network monitoring software will intercept network communications and scan for signatures. This process slows down the ability of CenTrak to provide locations and alerts in real time, and in some cases, CenTrak software is completely shut down due to the intrusive security measures.
Need to open all ports in Firewall for the local network access	CenTrak software will communicate using UDP and TCP through several different ports to CenTrak hardware. Therefore, the CenTrak server should be able to communicate to any CenTrak hardware inside the network. If there are any restrictions on internal (within the network) communication, exceptions need to be provided to CenTrak server to be able to communicate to all CenTrak hardware.
Connect Pulse™ access: outbound access to the following URLs need to be open from the CenTrak server. All TCP connections require inbound traffic (not connection). No other inbound access needed. Firewall settings should reference hostnames and not IP addresses as IP addresses are subject to change. Exclude the proxy settings for the Pulse sites and ports. In HTTP/HTTPS calls, the firewall / proxy server should not modify the request headers and should support authentication headers. ✓ gms.centrak.com - Ports 80, 443 (TCP) ✓ gmsdata.centrak.com - Ports 80, 443 (TCP) ✓ gmsrtdata.centrak.com - Port 10309 (TCP) ✓ api.centrak.com - Port 443 (TCP)	Transfer log files for maintenance and access in CenTrak Connect Pulse Portal. Proxy servers tend to block files from being transferred. Pulse needs the RTLS equipment log files to be uploaded from the on-site server to the Pulse cloud server.

Contact Us: www.centrak.com | marketing@centrak.com | 800-515-2928