CenTrak Server & Network Requirements

Activate, Environmental Monitoring & Hand Hygiene Compliance Monitoring Database Server

Supported Operating Systems

Windows Server 2016 or above, 64-bit

Recommended Database Architecture

We recommend databases be placed on a separate, existing customer-managed Microsoft SQL Server cluster (with MS SQL Server 2016 or above). This will leverage existing customer best practices, including resource monitoring and requisition, automated log backups, etc.

In addition, both database backups and transaction-log backups should be configured by the customer on a dedicated SQL Server instance that is created/provided to us- not doing that may result in a future application crash due to filling up the transaction log drive)

Minimum Hardware Requirements - If Recommended Database Architecture cannot be met

Server can be a Virtual Machine or Physical Server

Processor	Minimum six (6) cores, physical or virtual 2.4 GHz minimum clock speed per core
Memory	24 GB RAM minimum
Hard Drive	100 GB SSD-backed local disk space, fast disk I/O needed
Network Adapter	Dedicated 1Gbps connection
Database	Microsoft SQL Server 2016 or above, 64-bit, Standard License or above 10 GB starting size (additional storage may be required to support growth) **SQL Express is not supported**
DB Connectivity	**Non-expiring** service account for DB connectivity (can use either SQL authentication or Windows domain authentication) with 'DBOwner' access to CenTrak database(s) If using Windows domain authentication, the service account must also have "local log on as" as well as file system modification rights on the application server(s)
Number of DB Servers Needed	One database server can support all CenTrak Applications in scope (Activate, EM, and/or HHC)

CenTrak Server & Network Requirements

Database Administration		
CenTrak is not responsible for Database Administration. The customer/partner should assume this role, which includes but is not limited to configuring the DB recovery mode, scheduling database and transaction log backups, periodically recalculating index statistics, etc. Some CenTrak applications can automatically remove old historical data to prevent excess database growth and slow application performance. Recommended historical data retention should be discussed as part of project implementation.		
Network		
Remote Connectivity User account with admin access to server	Remote via SecureLink Gatekeeper or Nexus connection process for CenTrak personnel to access the databases and/or database server for file transfer, installation, administration, maintenance and troubleshooting	
Communication Speed	Maximum of 10mS round trip communication	
Internet Protocol Addressing		
IP Addresses	Server requires a static IP address	
Access Rights		
Normal operating and troubleshooting activities can use an account with Database Owner rights on all application databases.		
Port Configuration		
The following Ports need to be opened		
Device	**Ports**	**Protocol**
Application Server	1433	TCP
Network Security Configuration		
Criteria	**Reason**	
Need to configure Anti-Virus software - to exclude scanning and live protection on all CenTrak folders	CenTrak Software continuously writes data to storage. Due to the format of the file and consistency of the writing, Antivirus and other Security software monitors and blocks these writes. The entire folder will need to be excluded from both scanning periodically 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. So CenTrak server should be able to communicate to any CenTrak hardware inside the network. If there is 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.	
TLS Requirements: Enable TLS 1.2 Enable TLS 1.0 - when a Hand Hygiene Compliance application server is in scope	Database server utilizes TLS 1.2 when communicating to/from the application server. When a Hand Hygiene Compliance application server is in scope, TLS 1.0 is also required. The Hand Hygiene Compliance application will migrate to TLS 1.2 in a future version.	

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