CenTrak Server & Network Requirements

Activate, Environmental Monitoring & Hand Hygiene Compliance Monitoring Application Server

Supported Operating Systems

Windows Server 2016 or above, Standard Edition or above, 64-bit

Minimum Hardware Requirements	
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 local disk space Fast disk I/O for more responsive performance
Network Adapter	Dedicated 1Gbps connection
Number of Application Servers Needed	One for each CenTrak application in scope
File System Compatibility Note	Must be NTFS (not ReFS or others) format

Network	
Remote Connectivity	Remote access via SecureLink Gatekeeper or Nexus connection for CenTrak personnel to access the server for file transfer, installation, administration, maintenance and troubleshooting user account with admin access to server.
Communication Speed	Maximum of 10mS round trip communication to Core Server and the Application Database
SMTP Server	Access to facility SMTP server for email delivery, including support for sending emails outside of the network.

Required Applications

For both clients and server:

- A modern browser is required (released post 2018): Microsoft 11 or Edge Browser, Mozilla Firefox, Google Chrome are supported
- JavaScript support must be enabled

For application servers only:

- Microsoft .NET Framework 4.6 or above - for Environmental Monitoring and Activate application server only
- Microsoft .NET Framework 3.5 - for Hand Hygiene Compliance application server only
- SQL Server Management Studio

CenTrak Server & Network Requirements

Internet Protocol Addressing	
IP Addresses	Server requires a static IP address

Port Configuration

The following Ports need to be opened for the servers.

Device	Ports	Protocol
External Applications	7166 to 7270	UDP
Internal Web Browser	80, 443	TCP

Cisco Wi-Fi Locating

If Cisco Wi-Fi locating is in scope, access credentials to Cisco MSE/CMX to obtain location hierarchy information (building and floor names) and floor plan images.

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.
Connect Pulse™ API access: outbound and inbound access to the following URL need to be open from the CenTrak server. gms.centrak.com - Port 80, Port 443 api.centrak.com - Port 443	Retrieve tag and infrastructure health information for display in the application. Share certain metadata to Connect Pulse for assistance with device maintenance in Pulse. Retrieve tag and infrastructure health information for display in the application. Share certain metadata to Connect Pulse for assistance with device maintenance in Pulse. Retrieve map configuration details.
Rollbar product access: outbound and inbound access to the following URL need to be open from the CenTrak server. api.rollbar.com - Port 443	CenTrak software uses the Rollbar cloud platform for automated application error/exception monitoring to improve uptime and issue resolution within the application.
Cetani external notification access: outbound and inbound access to the following URL need to be open from the CenTrak server. notify.cetani.com - Port 443	CenTrak software uses an optional external SMS and phone calling notification service. Use of this service is dependent on scope of project.
TLS Requirements: Enable TLS 1.2 Enable TLS 1.0 - for Hand Hygiene Compliance application server only	Database server utilizes TLS 1.2 when communicating to/from the application server. If the server is for the Hand Hygiene Compliance application, 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