CenTrak Server & Network Requirements

CENTRAK®

Security Solutions Application Server

Supported Operating Systems

Windows Server 2012 R2, 2016, 2019, 2022

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 (minimum 15k RPM) for application components, backups, and log-files on data drive where CenTrak components are installed. Using a dedicated partitioned data drive for CenTrak software is highly recommended.
Network Adapter	Dedicated 1Gbps connection

Network	
Remote Connectivity User account with admin access to server	Remote access via SecureLink for CenTrak personnel to allow unsupervised 24/7 access to all CenTrak servers via a generic admin account for installation, administration, maintenance, and troubleshooting. (Note: user documentation and session recordings provided to any site upon request.) 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 – CenTrak uses SecureLink for access management
Communication Speed	CenTrak products require a high speed connection between endpoints (Timing Controllers, Stars, or Security Controllers) for system synchronization purposes. Due to this necessity specific latency statistics between endpoints (averaged over time, not single point tests) must be maintained; this is typically only sustainable inside private networks. A separation of Core Server applications and system endpoints by any section of public network is not supported. A maximum of 100 milliseconds of latency for completion of round trip communication between the Core server and any endpoints is required to sustain system stability. Stars' reporting events will timeout after 150 ms, at which point the Star will purge the data packet to prioritize the new location information from a subsequent system cycle. Security Controllers are unsynchronized, and thus have a 30 ms maximum latency requirement from their network location to the Core Server. This is mandated by a 45 millisecond reporting event timeout. Upon timeout, the Security controller the data will be dropped in favor of the next location packet. A maximum of 7 milliseconds of network latency is permissible for round trip communication between Timing Controllers and Stars, whether located at a single campus or multiple campuses. Higher latency can cause delays or missed location and sensing events.

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

- Modern web browsers (Microsoft Edge or Google Chrome)
- IIS 7 or above (IIS 8 preferable)
- Microsoft ASP.NET Core 6.0 Runtime - Windows Hosting Bundle
- Microsoft .NET Framework 4.8
- Access to 10 GB of facility Enterprise SQL Server 2016R2, 2017 or 2019 or 2022 Database
- WinRAR 6.0 or above (license provided by CenTrak)
- JavaScript support must be enabled

Internet Protocol Addressing

IP Addresses	**Static**
	Server

Port Configuration

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

Device	Ports	Protocol
Security Solutions Software	8181	TCP
Security Solutions Connector	7171	UDP
SQL Server	1433	TCP
Workstations	80, 443	TCP
Alert Push Connector	9595	TCP
HL7 Connector	9910	TCP

Database Requirements

Supported Operating Systems	Windows Server 2016 or above, 64-bit
Memory	16 GB RAM minimum
Recommended Database Architecture	Recommended 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 CenTrak. If an AlwaysOn setup is being used, the customer will be responsible for set-up. CenTrak requires the Listener IP to configure the application with required account credentials.
Requirements	Access to 10 GB of facility Enterprise SQL Server 2016R2, 2017 or 2019 Database. For CenTrak solutions using databases, it should take a maximum of 10 seconds to perform 10,000 database write operations. Non-expiring service account for DB connectivity (needs to be SQL authentication. Cannot use Windows domain authentication) with 'DBOwner' access to CenTrak database(s) with Read/Write permissions. One database server can support multiple CenTrak Applications in scope, but each Application will require its own unique database which cannot be shared with other applications.

Network Security Configuration

Criteria	Reason
Anti-virus software must exclude scanning and live protection on all CenTrak folders (e.g. D:\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 from being monitored in real time.
Exclude CenTrak folders from network monitoring/firewall software.	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 for 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.
Open all applicable local network ports in firewall software.	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.
Open outbound access to CenTrak Cloud for Connect Pulse™ use (see hostnames and ports below). All TCP connections require inbound traffic (not connection) and no other inbound access is needed. Firewall settings should reference hostnames and not IP addresses as IP addresses are subject to change. If firewall can only reference IP addresses, customer is responsible for monitoring for IP address changes and updating firewall in order to maintain an active connection to the cloud. Proxy settings must be excluded 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 - Port 443 (TCP) ✓ gmsdata.centrak.com - Port 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. Starting with Connect Core versions 5.14 SP23 GA (Pegasus) and 5.15 SP8 GA (Orion), TCP Port 80 for all URLs is not required or used and api.centrak.com (TCP Port 443) is required. Starting with Connect Core versions 5.14-SP23 GA Patch1 (Pegasus) and 5.15 SP8 GA (Orion), TLS 1.2 is supported by default. Prior versions only support TLS 1.0 and 1.1.