CenTrak Server & Network Requirements

Connect Core$^{\text{TM}}$ 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 for application components, backups, and log-files Minimum 15k RPM
Network Adapter	Dedicated 1Gbps connection
Network	
Remote Connectivity	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 – CenTrak uses SecureLink for access management
Communication Speed	Maximum of 7 milliseconds round trip communication between Timing Controllers (primary and secondary) and between Timing Controllers (primary and secondary) and their assigned Stars. Higher latency can cause delays or missed location and sensing events due to time synchronization requirements. Maximum 100 milliseconds round trip communication from Stars and Timing Controllers to Server. Higher latency can cause delays of the server receiving locating and sensing events from Stars. Event timeout is 150 ms, at which time the Star will retry for 3 more seconds before the packet is dropped. Maximum 30 milliseconds round trip communication from Security Controller to Server. Higher latency can cause delays of the server receiving events from Security Controllers. Event timeout is 45 ms, at which time the Security Controller will retry for 3 more seconds before the packet is dropped.

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 6.0 or above (license to be acquired by customer)
- Microsoft .Net Framework 4.7.2 or above
- Microsoft Visual C++ 2022 Redistributable

Required Applications Minimum Requirements

	Win RAR	.NET	MS Visual C++	Windows Server	HTTP/HTTPS
5.15					
SP8	3.0 or higher	4.0 or higher	2010 Visual C++ Redistributable Pkg (32 bit)	2012 R2, 2016, 2019	HTTP
SP9	3.0 or higher	4.0 or higher	2010 Visual C++ Redistributable Pkg (32 bit)	2012 R2, 2016, 2019	HTTP
SP10	3.0 or higher	4.0 or higher	2010 Visual C++ Redistributable Pkg (32 bit)	2012 R2, 2016, 2019	HTTP/HTTPS*
SP11	6.0 or higher	4.7.2 or higher	2022 Visual C++ Redistributable Pkg (32 bit)	2012 R2, 2016, 2019, 2022	HTTP/HTTPS*
SP12	6.0 or higher	4.7.2 or higher	2022 Visual C++ Redistributable Pkg (32 bit)	2012 R2, 2016, 2019, 2022	HTTP/HTTPS*
5.14					
SP23	3.0 or higher	4.0 or higher	2010 Visual C++ Redistributable Pkg (32 bit)	2012 R2, 2016, 2019	HTTP
SP24	3.0 or higher	4.0 or higher	2010 Visual C++ Redistributable Pkg (32 bit)	2012 R2, 2016, 2019	HTTP
SP25	3.0 or higher	4.0 or higher	2010 Visual C++ Redistributable Pkg (32 bit)	2012 R2, 2016, 2019	HTTP/HTTPS*
SP26	6.0 or higher	4.7.2 or higher	2022 Visual C++ Redistributable Pkg (32 bit)	2012 R2, 2016, 2019, 2022	HTTP/HTTPS*
SP27	6.0 or higher	4.7.2 or higher	2022 Visual C++ Redistributable Pkg (32 bit)	2012 R2, 2016, 2019, 2022	HTTP/HTTPS*

*HTTPS is the primary and preferred connection. System will default to HTTPS but fall back to HTTP if Firewall setting block HTTPS (Port 443). HTTP will no longer be supported in future releases.

Internet Protocol Addressing

	Static	DHCP or Static
IP Addresses	Server Timing Controller	Stars Security Controllers

Supported Devices

Device Type	Tags - Qty. 18000 Virtual Walls and Monitors - Qty. 4094 Hand Hygiene Sensors - Qty. 3000	LF Exciters - Qty. 500 Stars - Qty. 750

For systems which plan to exceed any of the above device quantities, please contract CenTrak. Please supply which device type will be exceeded, the total quantity of the device type and current server system hardware specifications for review.

Port Configuration

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

Device	Ports	Protocol
Star	7070, 4747, 6128, 3030, 5051, 5050, 5580	UDP, TCP
Wi-Fi Associating Devices	5757	UDP
Cisco MSE or CMX	9292, 4567, 443	UDP, TCP
Cisco DNA Space or Juniper/MIST	10309	TCP
Aruba ALE	7117, 7779, 443	UDP, TCP
External Applications	7166 to 7270	UDP
Security Solutions Server	8181	TCP
Security Solutions SQL Server	1433	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 HTTPS calls, the firewall / proxy server should not modify the request headers and should support authentication headers. **US-Based Pulse** ✓ gms.centrak.com - Port 443 (TCP) ✓ gmsdata.centrak.com - Port 443 (TCP) ✓ gmsrtdata.centrak.com - Port 10309 (TCP) ✓ api.centrak.com - Port 443 (TCP) **AU-Based Pulse** ✓ connectpulse.centrak.com.au - Port 443 (TCP) ✓ augmsrtdata.centrak.com - Port 10309 (TCP) **EU-Based Pulse** ✓ eupulse.centrak.com - Port 443 (TCP) ✓ eupulsedata.centrak.com - Port 443 (TCP) ✓ eupulsertdata.centrak.com - Port 6379 (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.