CenTrak Server & Network Requirements

Connect Core™ High Availability Linux Server

Supported Operating Systems
Ubuntu 20.04 LTS

Minimum Hardware Requirements	
Servers are required to be a Virtual Machine.	
Processor	Dedicated Dual Core Processor running at 2 GHz or higher Virtualized systems should have at least the 2 cores dedicated and not shared across other software applications.
Memory	2 GB RAM minimum
Hard Drive requirements	8 GB minimum local disk space for application components
Network Adapter	Dedicated 1Gbps connection
Number of Machines Needed	2
Architecture	If virtualized, each server can be nested inside of the physical or virtual Windows server so long as the Master Linux server is nested inside of the Master Windows server and the Backup Linux server is nested inside of the Backup Windows server. If Linux servers are nested within the Windows servers, the requirement for dedicated resources is no longer a requirement.
Number of Linux Servers Needed	Two total servers needed (one for Active and one for Backup) CenTrak will deliver an OVA file for installation. OVA file contains a local account used by CenTrak user access and services.
Network	
Remote Connectivity	Remote access via SSH for CenTrak personnel to access the CenTrak server for installation, administration, maintenance and troubleshooting.
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 our RTLS Platform Software to be used over public internet connections, due to uncontrollable latency issues. CenTrak Real-Time Locating should always meet the timing constraints of our system specifications over averaged time, not single point tests, which is typically not possible outside of private networks.	

CenTrak Server & Network Requirements

Internet Protocol Addressing

IP Addresses	Static
	Linux Servers (Master & Backup), Floating Virtual IP (for VRRP)

Windows Server IP addresses, Linux Serer IP Addresses, and the Virtual IP Address must be within same subnet.

Port Configuration

The following Ports need to be opened for the Linux Servers.

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 Spaces	10309	TCP
Aruba ALE	7117, 7779, 443	UDP, TCP
External Applications	7170 to 7270	UDP
Security Solutions Server	8181	TCP
Security Solutions SQL Server	1433	TCP
Between Linux Servers & Windows Servers	8500, 3031, 7071, 80	TCP

CenTrak Server & Network Requirements

Network Security Configuration	
Criteria	**Reason**
Need to configure anti-virus software to exclude scanning and live protection on all CenTrak folders: ✓ /etc/nginx ✓ /home/ha_service ✓ /etc/keepalived	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