

SecurCommander™

Integrated Command and Control Software for Physical Data Security

SecurCommander is an intuitive graphical interface that forms the command, control, monitoring and reporting platform for the Fiber SenSys **SecurLAN™** product suite. **SecurLAN** products provide physical, layer one security for critical data networks by co-locating a fiber optic sensor cable to detect motion and vibration on the protected data runs. This enables the **SecurLAN** system to sense attempts to tap or compromise the data within the network. Once an attempt is detected, the **SecurLAN** system can shut off the data so that it can no longer be compromised.



- **Command**
- **Control**
- **Monitor**
- **Report**

SecurCommander provides annunciation for all data runs that are alarmed and guides the operator through an embedded standard operation procedure ensuring consistent processes can be applied. Additionally, it allows for reporting and management of security sensors.

SecurLAN products including **SecurCommander** comply with the Committee on National Security Systems Instruction (CNSSI) No. 7003 which provides guidance and standards for Protected Distribution Systems (PDS).

SecurCommander is designed to operate on a computer system with the following specifications:

System Requirements	
Operating system	Windows® 10 Professional, Windows Server 2016, or Windows Server 2019
Supporting software	Microsoft .NET framework 4.6.1 and Microsoft SQL Server
Hard disk	Minimum: 1 TB Recommended: 2 TB in RAID 1
Processor	Minimum: 64 Bit 1.4 GHz Recommended: 64 GHz 2 GHz or faster Core i7 64-bit processor or equivalent
RAM	16 GB

Windows® is a registered trademark of Microsoft Corporation.

SecurCommander Features and Benefits	
Web-based	Accessible through standard internet browsers utilizing secure website Hyper Text Transfer Protocol Secure (HTTPS) technology. Multiple simultaneous browser instances can be open from multiple computers on the SecurCommander network.
Role Based Access Control (RBAC)	Utilizes role-based access control (RBAC); allows access based on administrator assigned user roles within the organization.
Device Management	Manages fiber optic sensors monitoring the data runs and optical cut-off switches. Provides administrative control of SecurCommander for assembling devices in groups based on the protected areas.
Zone Management	Segmentation by zones for discreet monitoring; i.e., a single room, a specific hallway, or a section of the data run.
Zone-Specific SOP	Zone-based handling depending on the user-set Standard Operating Procedure (SOP) requirements. As an example, if an alarm occurs in an executive office, the SOP might require that the secretary first be called before a response team be deployed.
Case Management	Case management includes a process of identifying, recording, analyzing, monitoring and resolving events such as alarms, tests, or equipment failures. It includes the collection of data for the adherence to the SOP and related communications.
Zone Monitoring	Zone Status: view zones according to status; i.e., all in alarm or all not. Cases: view disposition of zones by cases based on user-set parameters.
Reports	Utilizing a SQL database with advanced reporting capabilities and features, SecurCommander provides the flexibility to view data, patterns, and information.
Notifications	Alarm notifications: zone-based notification for alarms or fault conditions. Case notifications: programmable notification of case generation can be key to ensuring the SOP is followed. Notifications can be delivered via email messages, SMS messages, report of notifications, or the triggering of remote relays. Status alerts by parameters; i.e., case generation date can be enabled for follow up.
Multi-level base maps	An unlimited number of maps can be associated with each site. Maps allow the user to “drill down” to the needed level of detail or change the views of a site. For instance, a geographical map associated with a site could toggle to a schematic wiring diagram for additional details.
Custom integration	Flexible management capabilities allow additional FSI devices and third-party devices to be included in the system. Based on site requirements, this could include two-dimensional LIDAR sensors protecting the ceiling of the Secure Compartment Information Facility (SCIF) or a camera monitoring a seldom-used hallway.
Rx/Tx SNMP Traps	SNMP traps provide network equipment fault notification. When SecurCommander detects an error or a change, a notification to one or more trap receivers is sent. SNMP traps contain information such as: <ul style="list-style-type: none"> • Time, source, and version of the event • Severity, agent, and event OID (ID of a specific event) • Event message/description or “bindings”

For more information, contact us at
info@fibersensys.com
Tel: +1(503) 692-4430
Toll free (US) +1(800) 641-8150

