

Syntermed Live™ System(s) Security Overview

- I. The entire Syntermed Live™ system is housed in a private cabinet inside a secure data warehouse facility outside of Atlanta, GA. Access to the physical equipment is regulated by the facility's staff and is limited to Syntermed employees. *All of the information contained in this document is valid for both the commercial and pre-release (beta) environments for Syntermed Live™.*
 - i. Traffic to and from the public IP interface provided by the data warehouse facility is monitored in realtime. Any "out of normal range" traffic is logged and Syntermed is notified immediately based on a urgency structure. Most non-information events trigger an email notification, but emergency events trigger email and phone notifications.
- II. The internal network is protected by Cisco branded firewalls, only allowing data to pass through on a very limited number of TCP/UDP ports as needed to make the Syntermed Live™ application publicly available via the Internet.
- III. Standard syslog functionality is implemented and monitored for all network traffic passing through the public interface of the Cisco firewall. Any traffic reaching "alert" status or higher triggers an email notification.
- IV. The Syntermed Live™ server(s) maintain real-time data redundancy in the form of 3 disk (SCSI 10K RPM) RAID 5 Arrays. Furthermore, all customer data is backed up nightly to a separate network attached storage (NAS) device which also employs a RAID 5 level of real-time redundancy.
- V. The data stored in the Syntermed Live™ system utilizes a Microsoft SQL Server technology back end. Outside access to the SQL Server database(s) is not available without an authenticated passthrough from the web server running Internet Information Services 6 (IIS6).
- VI. Access to data contained in the Syntermed Live™ system is only available via two methods; direct connection to the web interface and through the Master Control Program (MCP) client application. Both of these require a secure Internet connection (SSL over port 443).
 - i. When accessing data through the web interface, a username and password combination must be supplied. The password is configured by the user and must conform to a very high level of complexity (as recommended by the HIPAA guidelines). The Syntermed Live™ system employs a hashing system for password storage; therefore the password is never stored in the system

in a manner that is retrievable by anyone other than user. For added security, all web sessions automatically timeout after 15 minutes.

- ii. When accessing data through the Master Control Program (MCP), the same username and password combination must be supplied (there is an option for MCP to remember these credentials and use them automatically in the future). MCP requires the use of the Microsoft Web Services Extensions 3.0 for added security during file transfer. At the time of installation, MCP is supplied a license, generated by Syntermed from within the Syntermed Live™ system. Another level of security is negotiated based on encrypted information in this license before data can be accessed via MCP.
- III. Access to data contained in the Syntermed Live™ system is managed according to security groups. By default, only members of a security group have access to the data contained within. Access to data outside of a security group is explicitly denied and any and all attempts at data access are audited.
- IV. User account security group membership creation and modification is available only to employees of Syntermed, Inc.
- V. License creation and modification is available only to employees of Syntermed, Inc.