
Cold Chain Manager™ Application and Data Security

Introduction

Cold Chain Manager is a web-enabled temperature management system for in-transit shipments. Using Cold Chain Manager organizations can create a cold chain knowledge base for compliant record keeping and detailed analysis. Because Cold Chain Manager's is a web application, a user can access the system through a simple browser interface from anywhere in the world. Although the web environment provides convenient access to data, the sensitive data maintained in Cold Chain Manager must be protected.

The following Technical Brief outlines how Cold Chain Manager maintains a secure environment for your cold chain data. In addition, it presents the steps Sensitech takes to ensure Cold Chain Manager's availability.

User Authentication and Privileges

Access to Cold Chain Manager is controlled via Username and Password. Each user must have an active User Profile within Cold Chain Manager. A User Profile is created by a User Administrator and includes general contact information, account expiration date and application privileges.

A valid username or password must be between 6 – 12 alphanumeric characters. When a user attempts to login to the application, the combination of username, password and company name is authenticated against Cold Chain Manager's Membership Database. If any information is incorrect, the user will not be granted access to the system. Repeated failed login attempts (five consecutive attempts) results in the login capability being disabled in that browser session.

A User Profile defines the privileges that a user has available to them in Cold Chain Manager. In addition to controlling who can download TempTale monitors, Search for Data and Manager Users – the User Profile also controls Editing logistics data and Marking shipments as approved.

The User Profile also controls personalization settings such as what time format to display data in and whether to display data in Fahrenheit or Celsius.

Encryption

A User's session in Cold Chain Manager is encrypted using Secure Sockets Layer (SSL) at 128-bit encryption. The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of a message transmission on the Internet. SSL uses the public-and-private key encryption system from RSA Security, which also includes the use of a digital certificate.

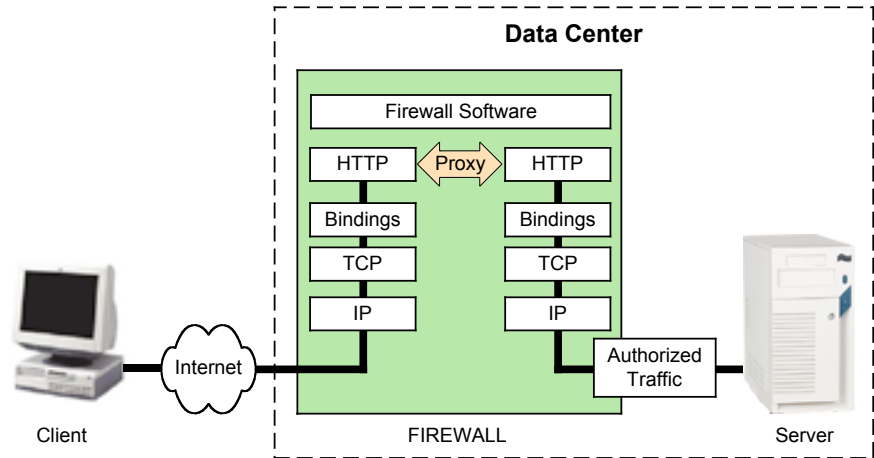
The gold lock in the bottom right corner of the browser is evidence of Cold Chain Manager's SSL protection. Double-clicking the gold lock displays Cold Chain Manager's Certificate. Cold Chain Manager's website is www.sensitechdms.com.

Web Hosting Environment

Cold Chain Manager is maintained in a hardened data center. The data center provides Cold Chain Manager with "Ping, Power, Pipe". "Ping" is provided through multiple points of connectivity to various Internet Exchange Points. This ensures that in the event of a failure at one Internet Exchange Point, Cold Chain Manager will remain live, as data is re-routed across the Internet. "Power" is provided through multiple power grids in the geographical area. This is to avoid downtime if a main power line is damaged or becomes unavailable. In the event of a catastrophic power failure, 2 fully operational diesel generators remain on standby to power the facility for days. "Pipe" ensures that performance impact is minimal during peak usage.

In addition to the login restrictions and authentication checks, all communications with Data Center servers must pass through a firewall. The firewall blocks the flow of unauthorized traffic while allowing authorized (authenticated) traffic to pass. The firewall used with Cold Chain Manager is an *Application-Level Gateway* type. In this design contact between the Data Center server and the client is through a proxy. Consequently, if the firewall is compromised there is no direct access to the Data Center servers. See the Figure below for an example of a typical application-level gateway configuration.

The firewall is certified by the *International Computer Security Association (ICSA)*. ICSA tests firewall products against a set of standardized certification criteria and issues certification to products that pass testing. The tests cover a wide range of functional and assurance requirements, including event logging, administrative functions, administrative authentication, administrative access testing, remote administration, functional testing, block unauthorized traffic, vulnerability testing and denial of service attacks.



Our Data Center also provides 24x7 physical security. All visitors must be pre-registered and have identification to enter the facility. Access to the individual server area is restricted to a small number of employees to ensure equipment and application tampering is prevented. The facility also has robust smoke detection systems, waterless fire suppression systems and temperature control systems.

Monitoring

The Data Center is monitored daily by software that simulates a user opening a web page and viewing their data. The activity is timed and compared to a standard. Slowdowns in performance or unsuccessful attempts to access the site or view a page will send alerts to the Network and Data Center department. Maintenance utilities and anti-virus software are installed on all Data Center servers.

Data Backup

Sensitech performs a daily tape backup of all critical data on each server. The backup tapes are picked up from the facility and stored in a fireproof safe at an undisclosed location. The backup jobs and operating system event logs are monitored on a daily basis to ensure all systems are functioning properly.

System Validation and Quality Assurance

Software and Data Center operating procedures are formally controlled through an engineering change review processes required by Sensitech’s ISO 9001:2000 quality system. Before deploying new Cold Chain Manager releases, updates or service packs at the Data Center, the software is tested in a staging environment (which simulates the Data Center environment) by Sensitech’s Software Development and System Quality Assurance groups. The System Quality Assurance group executes a System Test Plan and verifies that the software meets its functional requirements prior to release.

A full Validation Package for each version of Cold Chain Manager is available upon request. Included in the Cold Chain Manager validation package are the following components:

- Sensitech's Quality Policy
- Software Development Procedures
- Cold Chain Manager Functional Requirement Specifications
- Cold Chain Manager Test Plan and Scripts
- Cold Chain Manager User's Guide
- Client-side Installation Qualification
- Client-side Operational Qualification
- Client-side User Acceptance Test

Disaster Recovery

To ensure a rapid recovery in the event of a catastrophic failure, a comprehensive *Disaster Recovery Plan* is in place. Each server has a documentation package describing, in detail, system IP addresses, system functions, network diagrams and installed system hardware. Each server has a media package containing all of the software necessary to rebuild the server, including; Cold Chain Manager software, operating system, service packs, security updates, option packs, resource kits, server core image, hardware drivers and full system configuration information. In the event of a failure, this level of preparedness ensures a rapid recovery.

About Sensitech

Sensitech is the leading independent provider of cold-chain information and analysis that enable global leaders in food and pharmaceuticals to protect the integrity, freshness and efficacy of their temperature-sensitive products. In the past decade, Sensitech has protected more than \$200 billion of its customers' assets around the globe. The company is based in Beverly, Massachusetts, and has offices in Redmond, Washington, and Fresno, California, with service and distribution offices around the world. For additional information about Sensitech, call 978-927-7033 or visit www.sensitech.com.