

# Security Data Sheet

Version 1.3

## White Springs

Mercia House  
51 The Green  
South Bar  
Banbury  
Oxfordshire OX16 9AB UK

**t** +44 1295 210230  
**f** +44 1295 201232  
**e** [info@whitesprings.co.uk](mailto:info@whitesprings.co.uk)  
**w** [www.whitesprings.co.uk](http://www.whitesprings.co.uk)

## White Springs

425 Market Street  
Suite 2200  
San Francisco  
CA 94105  
United States

**t** 415-955-2785  
**f** 415-397-6309  
**e** [info@whitesprings.co.uk](mailto:info@whitesprings.co.uk)  
**w** [www.whitesprings.co.uk](http://www.whitesprings.co.uk)

## SECURITY DETAILS

---

### Physical Security

White Spring's main production equipment is based in Kentucky (USA) and managed by Maximum ASP, a specialist hosting organization. A second location is based in Birmingham (UK) and managed by UK Solutions Limited.

Each provides 24-hour physical security, palm print identification systems, redundant electrical generators, redundant data center air conditioners, and other backup equipment designed to keep servers continually up and running.

### Perimeter Defense

The network perimeter is protected by multiple firewalls and monitored by intrusion detection systems – all sourced from industry-leading security vendors. In addition, firewall logs are monitored and analyzed to proactively identify security threats. White Springs also contracts with a third-party security firm that proactively monitors our security configurations for changes, vulnerabilities, and errors and regularly conducts vulnerability threat assessments including penetration tests.

### Data Encryption

White Springs leverages strong encryption products to protect customer data and communications, including 128-bit Verisign SSL Certification. For example, for browser-based products, the lock icon in the browser indicates that data is fully shielded from access while in transit.

### User Authentication

Users access White Springs products only with a valid username and password combination which is encrypted via SSL while in transmission. Users are prevented from choosing weak or obvious passwords. For browser-based products, an encrypted session ID cookie is used to uniquely identify each user. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

## **Application Security**

Our robust application security model prevents one White Springs customer from accessing another's data. This security model is reapplied with every request and enforced for the entire duration of a user session.

## **Internal Systems Security**

Inside of the perimeter firewalls, the systems are safeguarded by network address translation, port redirection, IP masquerading, non-routable IP addressing schemes, and more. The specific details of these features are proprietary.

## **Operating System Security**

White Springs enforces tight operating system-level security by using a minimal number of access points to all production servers. We protect all operating system accounts with strong passwords, and production servers do not share a master password database. All operating systems are maintained at recommended patch levels for security and are hardened by disabling and/or removing any unnecessary users, protocols, and processes.

## **Database Security**

Whenever possible, database access is controlled at the operating system and database connection level for additional security.

## **Server Management Security**

All data entered into the White Springs applications by a customer is encrypted within the database and owned by that customer. White Springs employees do not have direct access to the White Springs production equipment, except where necessary for system management, maintenance, monitoring, and backups.

## **Reliability and Backup**

All networking components, SSL accelerators, load balancers, Web servers, and application servers are configured in a redundant configuration. All customer data is stored on a primary database server that is clustered with a backup database server for redundancy. All customer data is stored on carrier-class disk storage using RAID disks and multiple data paths. All customer data, up to the last committed transaction, is automatically backed up to a primary tape library on a nightly basis. Backup tapes are immediately cloned to verify their integrity, and the clones are moved to secure, fire-resistant off-site storage on a regular basis.

## **Disaster Recovery**

White Springs uses two separate locations - USA and UK - with required hardware, software and Internet connectivity, providing geographically remote disaster recovery facilities in the event one of our production facilities were to be rendered unavailable.