



## SAManage and Data Security:

Security of our service and your data is our top priority, and this FAQ would outline the practices we have in place to ensure your data security. SAManage servers are hosted in a **secured SAS70 certified** Tier4 class A DataCenter, which is the highest standard in data center security. We have taken numerous security actions from the access to our datacenter to the security of the service layer itself. This means that physical access to the SAManage servers is restricted to authorized operators - no other personnel can access our hosting area. Our service is protected by the latest security systems and is monitored 24x7 by certified network security teams.



## How we keep your data secured:

We work very hard to assure you that:

- 1. Your data is private** - your personal information is never transferred or sold to anyone.
- 2. Your data is secured** - no one can access your information at SAManage.
- 3. Your data is yours** - you can always take it with you. Download your data in multiple convenient formats, or if you decide to leave the service, you can permanently remove it from our servers.

## How we maintain your privacy:

SAManage keeps your data private and does not disclose your privacy. We limit the information collected to the minimum required to provide an easy to use and valuable service to you. Please read our complete Privacy Policy available at <http://www.SAManage.com/privacy.html> for further information.

## State of the art security practices:

We are working every day to make our service more secure and up to date with the latest security technology. Here is how we do it:

- 1. Data Center Security** - our servers are hosted at a secured Tier4 SAS 70 certified data center, protected by biometrics scanners and 24x7 security guards. This means that only authorized personal can access the data centers and physically access the cages where our servers are hosted.
- 2. Network Security** - SAManage is using the latest firewall protection, intrusion detection systems, SSL encryption, and proprietary security products across all segments of our network. We are working with 3rd party service providers to constantly test the network for security breaches.



**3. Backup** - all customer data is continually backed up to local disk as the first level of data protection. Backups are transmitted to our secured Disaster Recovery site on a daily basis as the second level of data protection.

**4. Disaster Recovery** - we have implemented a disaster recovery plan designed to allow us to resume service delivery from a secondary data center with minimum service disruption. Based on using Amazon EC2 and S3 infrastructure as our secondary data center, our data is replicated to Amazon periodically so we can resume service delivery using the Amazon infrastructure if needed.

**5. Certifications** - we are constantly working with third parties to test the service and receive third party certification for our security practices.

**6. Application Access** - SAManage protects customer data by ensuring that only authorized users can access it using their username and password. Account Administrators can assign security rules that define which users in their company or partners have access to the data based on user's roles.

**7. Data Encryption** - all data is encrypted in transfer and all access to the service is governed by strict password security policies. All passwords are stored in MD5 hash format, which means they cannot be reversed to the original password and are not readable. The usage of the SAManage service available at [www.samanage.com](http://www.samanage.com) is protected by 256bit SSL encryption.

**8. Monitoring and logging** - our service is continually monitored for security violations attempts and our team receives immediate notification on such violations. Our service generates certain logs and audit data that is reviewed to detect any security violations. We implement various 3rd party scanning technologies to monitor the service against existing and new threats.

## Security of our agent

The agent operates like many other beacon software that runs in your network and connects to a server on the internet, including Windows Update service, Adobe Acrobat Reader or the Java runtime environment. The agent only connects to the SAManage server and no communication is initiated with other destinations. In addition, the agent does not receive requests from any device, internal or external to your network, but only initiate outbound requests. This approach ensures that no other service can exploit the agent or use the information it gathers.

