

## Alfresco in the Cloud Security

At Alfresco we know that choosing a solution to store your business critical data is never easy, and often the biggest concern is security. Around 7 million users trust document management that manages over 3 billion pieces of data.

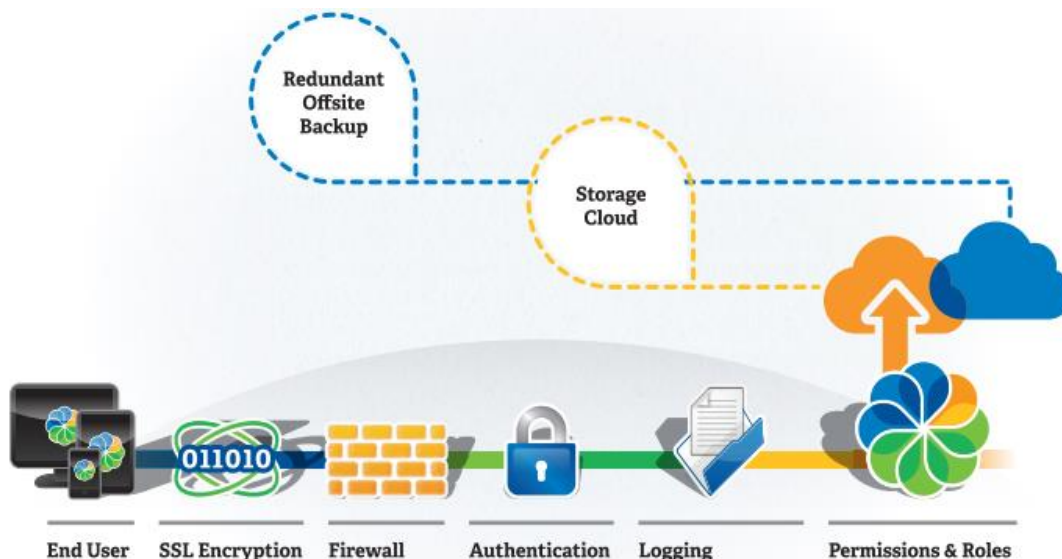
### Application Security

There are a number of security features within the application that gives Alfresco in the cloud multi-level security coverage.

- ⊕ Authentication  
Using strong password combinations users must authenticate before they can access data within the platform. There is no anonymous access.
- ⊕ File Permissions and Sharing  
All files uploaded can be shared or marked private as appropriate. This can be done on a per-user or per-site basis. Summary notifications can be configured.
- ⊕ Encryption on transfers and rest  
Ability to use the platform from anywhere on any device, all transfers are made with AES 256 SSL encryption.
- ⊕ Trashcan  
All deleted files are moved to a trashcan. If a file is deleted in error it can easily be retrieved. Files in the trash do not expire, and can be retrieved until manually deleted from the trashcan.
- ⊕ Administrative Audit Trail  
A full audit trail allows monitoring of file and user activities as granular as per session. Logs are accurately time stamped and stored with originating IP addresses allowing investigation of incidents.
- ⊕ Mobile Application Storage  
Data can be stored exclusively in the cloud, so that if a device is lost or stolen, no data is lost with the device.

### Hosting

Alfresco in the cloud is hosted in the Amazon Web Services (AWS) infrastructure taking advantage of their market leading technologies such as Elastic Load Balancer (ELB) and Simple Storage Services (S3).



alfresco.com | Americas +1 888 317 3395 | UK +44 (0)1628 876 600



Websites displaying the McAfee SECURE™ are tested and certified daily to pass an intensive security scan. McAfee tests for personal information access, links to dangerous sites, phishing, and other online dangers.



Amazon Web Services has been ranked as the #1 in cloud infrastructure with some of the world's most popular online services. Alfresco has chosen Amazon as a hosting provider to take advantage of their highly reliable, and scalable platform to provide a superior service.



Amazon Simple Storage Service is storage for the internet, which is based on the same infrastructure as Amazon's global network of websites. Amazon S3 buckets provide scalability, availability and an unlimited amount of storage making data stored quickly accessible perfect for online ECM platforms such as Alfresco.



## Hosting & Infrastructure

### Multiple Level Firewalls

Our architecture is configured with multi-layer firewall security. Each firewall is independent and from different suppliers to ensure efficient coverage. Some operate at the application level while others do so at the transport layer, thus preventing multiple forms of attack.

### Intrusion Detection

Network and host intrusion adds an additional level of security, with particular focus on all points of ingress. Rule sets powering the detection engines are updated continuously. Alerts are sent to 24/7 security staff.

### Application Penetration Testing

Alfresco in the cloud is subject to regular penetration testing by a respected, third party security consultancy. In the event of a problem being discovered, fixes are rapidly rolled into development and applied once the correct quality assurance is established.

### Regular Environment Vulnerability Scans

In-house security staff undertake regular vulnerability scans of the whole cloud environment. Any weaknesses exposed are remedied in short order.

### Physical Security & Environmental Controls

Amazon Web Services take physical security of their infrastructure very seriously. You can review Amazon's security measures by visiting <http://aws.amazon.com/security>

### n-Tier Segmented Architecture

In order to provide the best coverage, Alfresco's cloud architecture is segmented into different trust zones approximating to the typical tiers of an n-tier environment. This allows for fine-grained access control to each tier and makes containment of any attack much more effective.

## Data Protection

Alfresco utilizes the Amazon Simple Storage Service (S3) that provides scalability, high availability, and low latency storage – ideal for enterprise content management.

### Data Storage

Currently data for networks that are part of Alfresco in the cloud is stored within SafeHarbor certified AWS S3 buckets based in the USA.

### Data Retention

Data is retained until deleted by the administrator of the network. In the event of account closure all data will be removed.

### Data Encryption

All data stored as part of the Alfresco in the cloud service is encrypted using AES 256 SSL.

### Backup and Disaster Recovery

S3 is designed to provide 99.99% durability and 99.99% availability for all data stored. In addition to this backup and disaster recovery Alfresco replicate the encrypted data storage to multiple datacenters.

## About Alfresco

Alfresco helps teams share, manage and retain content across the extended enterprise with simplicity that end users love and smarts that IT can endorse. Alfresco enables organizations in more than 180 countries to collaborate more effectively, improve business process efficiency and ensure information governance across cloud, mobile, hybrid and on-premise environments, Alfresco is smart enterprise content made easy.

## Data Privacy

Alfresco takes privacy seriously in order to protect our customers data. You can review our full privacy policy on our website [alfresco.com/privacy](http://alfresco.com/privacy)

Alfresco operates a global business and has several corporate entities established around the world. Alfresco Software Limited, a UK company, is the company responsible for all of the Alfresco customer transactions. Therefore, it is the company responsible for ensuring compliance of all the Alfresco companies with data protection standards. Being a UK company, Alfresco complies with EU and UK data protection standards and it has chosen to enter model processor contracts with each of its non-EU affiliates to ensure their compliance with EU data protection standards. This compliance method is an alternative to Safe Harbor certification. Alfresco also holds its non-EU vendors to EU data protection standards by ensuring that they are Safe Harbor certified.

## Certifications

In order to ensure we are providing the best service our hosting partner Amazon Web Services and Alfresco maintain a number of certifications to provide piece of mind.

Currently Amazon Web Services are accredited to several security standards including SAS70 Type II, SSAE SOC1, ISAE3402 and ISO270001.

Independently Alfresco is working towards SSAE SCO2 and ISAE3000, which are the emerging standard by which SaaS organizations are judged.