

Security Overview

Enterprise-Class Secure Mobile File Sharing

Overview	3
End to End Security	4
File Sharing Security Features	5
Storage	7
Encryption	8
Audit Trail	9
Accellion Public Cloud – Amazon EC2	10
Accellion 3 rd Party Auditing	11

Overview

More than 1,700 Enterprise corporations and government agencies and 11 million enterprise users have chosen Accellion for securely sharing files and collaborating with colleagues, partners and vendors across organizational boundaries and across devices. Ensuring enterprise data security is a top priority for corporations and government agencies and is reflected throughout the Accellion Secure Mobile File Sharing solution, in our processes, procedures and product design.

This document provides an overview of the Accellion security features designed to ensure protection of your enterprise data.

End to End Security

One of the best ways to understand the multiple levels of security of the Accellion Secure Mobile File Sharing solution is to follow the path of a file from desktop, laptop, or mobile device through the Accellion system as users collaborate and share files. We have created a secure mobile file sharing system that allows organizations to protect their Enterprise content throughout the file sharing process.

Account Access and Authentication

Starting with login to an Accellion account, let's take a look at the security features of the Accellion Secure Mobile File Sharing Solution.

Log-in Security Features

Robust and Flexible Password Policies

IT Administrators can create configurable password policies:

- Password strength (number of characters, number of numeric character(s) between 0-9, number of special characters, number of upper and lower case characters)
- Password resets (a configurable time period)
- Password re-use restrictions
- Notifications after a configurable number of failed attempts
- Overall maximum session duration

Single Sign-on

Accellion offers Active Directory/multi-LDAP integration for Enterprise accounts. This gives IT Administrators centralized control and management over user accounts.

Accellion supports single sign-on through SAML (Secure Assertion Markup Language) 2.0. SAML is an industry standard protocol for exchanging authentication and authorization information between different security domains. Enterprises can implement multi-factor authentication and then seamlessly exchange authentication information with Accellion through SAML integration.

Accellion also provides single sign-on via Kerberos.

For information on Accellion single sign-on integrations, contact support@accellion.com.

File Sharing Security Features

After logging into the Accellion solution, users can quickly create secure workspaces, upload files, share files, add comments, subscribe to notifications, synchronize files, and send files to stakeholders internal and external to the organization.

All files on an Accellion system are encrypted in transit and at rest. Data in transit is encrypted with TDES (168 bits) or AES (128/256 bits) depending on the web browser. Accellion uses AES encryption for data at rest.

Accellion has optional anti-virus software, provided by F-secure, to scan files on upload and download. When a file containing a virus is uploaded to Accellion it will be quarantined.

Flexible and Robust Secure Workspace Permissions

IT Administrators can control access to Enterprise content across the organization.

File Tracking – Workspace managers can view activity logs to see who has accessed the workspace, downloaded, uploaded, and deleted files, and who has added comments, etc.

Notifications – Managers and contributors in a secure workspace can subscribe to notifications to receive emails when workspace members add files or make comments to files in their workspace.

Workspaces – IT Administrators can set workspace and file expiration dates for their organization. Workspace managers can also set workspace and file expirations within the parameters set by IT.

Secure Links – Users can easily share files by sending stakeholders a secure link to a file in their Accellion secure workspace. Users can decide that: 1) the file can be downloaded by only the recipient of the email, 2) the recipient can forward the file to others, or 3) all authenticated users can download the file. Users can set file link expiration dates and can automatically get return receipts when files are downloaded.

Collaboration - Secure workspaces are designed to be shared with internal and external stakeholders. Workspace managers can manage users in their workspace and assign to them specified user roles depending on business requirements.

Secure File Synchronization Security Features

Accellion provides robust, secure, and flexible file synchronization, including kitedrive continuous sync and workspace on-demand sync. Administrators have the ability to enable sync for their organization.

Furthermore, they can specify if they want users to have access to kitedrive and/or workspace sync.

Once workspace sync is enabled, users with manager privileges can enable and disable sync for their individual workspaces.

Specific Accellion file synchronization security features:

- Accellion supports end-user authentication to the kitedrive sync client through LDAP and SAML.
- Kitedrive sync never stores or sends passwords in the clear.
- Kitedrive session authentication is done through OAuth.
- Kitedrive works in conjunction with data leak protection (DLP) solutions to ensure that file synchronization is based on corporate policies for the protection of intellectual property.
- IT Administrators can view kitedrive activity logs and track which files are being synchronized.

Mobile Access Security Features

Mobile users can securely access their Accellion accounts through mobile browsers or the Accellion Mobile Apps for iPad, iPhone, Android and BlackBerry devices.

Accellion Mobile Apps support authentication through LDAP, ensuring that only authorized users gain access to secure workspaces. Files saved on the mobile device are stored in a secure container with 256-bit AES encryption. Files shared with others via email are sent via the SSL protocol. Files downloaded to the device are password protected and encrypted while at rest. Users choose a six digit passphrase to access encrypted files downloaded to the mobile device using Accellion Mobile Apps.

With Accellion, administrators can centrally manage and control mobile access to corporate resources. They can enable or disable mobile access. They can select Edit or View access for users depending on security requirements. For users with View only access, Accellion offers server side viewing, enabling users to securely view content without the ability to download files. They can set expiration dates on files accessed through mobile devices. They can whitelist applications that are allowed to open files from Accellion. They can immediately disable an Accellion account if a phone is lost or stolen. They have access to workspace activity logs ensuring data security and compliance. There are five Admin configurable PIN settings- Always ask, Never ask, for local files, Idle timeout and Max PIN attempts.

In conjunction with MDM solutions such as MobileIron, BoxTone and Good, IT Administrators can also ensure that only authorized apps are downloaded, users have the latest software updates, and users are not using excessive bandwidth. And, if phones are lost or stolen, they can be remotely wiped using MDM solutions to protect corporate data from getting into the wrong hands. Lastly, with application technology partners such as Mocana organizations can not only secure confidential files on the device but also secure the application data.

Kitepoint Security Features

Kitepoint provides secure mobile access to enterprise content stored in Microsoft SharePoint® and other enterprise content stores – anytime, anywhere, without a VPN. With Accellion, organizations control every aspect of their deployment. Kitepoint leverages the existing enterprise infrastructure rather

than replicating content out to external file stores, simplifying and supporting corporate information management, compliance and security policies.

- Each kitepoint enterprise connect management system (ECM) connector securely communicates through the firewall to Accellion using HTTPS and a secure Web Socket connection.
- Kitepoint authenticates users against enterprise Active Directory server - only authenticated users can access content.
- Kitepoint respects existing users, groups and roles in place around content - kitepoint does not change any access controls or user permissions.
- Kitepoint maintains existing information hierarchy - documents continue to exist in the relevant context in which they were published.
- Kitepoint maintains "Document of Record" - users have access to the most current copy of the document stored in SharePoint; Back-end policy systems such as Digital Leak Protection (DLP) and Records Management (RM) are not compromised by duplicating the content to other systems.
- Accellion provides complete logs of all transactions on content stored in the ECM systems. Logs can be downloaded and exported to third-party reporting and audit systems.
- IT Administrators can centrally provision users and manage security policies including access rights for auditing, reporting and demonstrating compliance. The system can also be configured so users cannot access highly-secure ECM sites via mobile devices.

Storage

Files uploaded to Accellion are stored either in the private cloud (on-premise using VMware, Citrix XenServer, or Microsoft Hyper-V), Accellion public cloud (Amazon EC2), or in a hybrid cloud depending on the deployment option you choose for your organization. Accellion also gives you the ability to leverage NFS/ EMC Atmos storage with your Accellion on-premise deployment.

Private Cloud

Accellion supports private cloud on-premise deployment in VMware, Citrix XenServer, or Microsoft Hyper-V environments. Private clouds help organizations ensure the availability, integrity and confidentiality of their information. Located inside a company's firewall, private clouds are owned and

controlled by IT allowing information to be solely controlled by enterprises rather than managed by third party cloud providers.

Public Cloud

Accellion provides single and multi-tenant storage in Amazon's EC2 public cloud. Amazon security details are available in a later section of this document.

Mix of Public and Private Cloud

Accellion Mobile File Sharing offers the only true hybrid deployment model. Organizations can mix and match public and private cloud (on-premise via virtual machine) deployments. Data can be segregated between private (on-premise) and public cloud servers. Note that automatic synchronization of local and online files is not supported.

Using Accellion, organizations can utilize a private cloud environment for specific locations or regions (for example, European or Canadian data can be separated from US data), while other offices can use the public cloud (such as those in the US). Administrators can set up rules restricting the movement of data. For example, they can specify that all files uploaded in a particular country or region, stay in that region. Organizations can also segregate the data that users access in one location between the public and private cloud. Rules can be created by which external users access a public cloud and internal users access a private cloud. In that case internal users (marked as LDAP users) trying to authenticate on the DMZ controller will receive a "Please login via VPN" message. External users authenticate on the DMZ controller using passwords specific to Accellion.

With a mixed public and private cloud deployment, data can be replicated, but the public and private cloud data are not commingled.

Data replication can be precisely controlled. Administrators can replicate only certain instances or all instances of Accellion data and can decide to replicate only certain file types.

Additional Storage

Accellion supports integration of NFS/ EMC Atmos storage with Accellion on-premise deployment. Accellion currently supports EMC Atmos storage by mounting it as an NFS disk. EMC Atmos storage can be utilized in all Accellion virtualized and physical hardware deployments.

Encryption

In virtualized (VM) and cloud deployments, by default, files are stored within the Accellion system on an encrypted partition using AES 128-bit encryption. Additionally, each file can be encrypted with a unique key. The file encryption key is not stored on the server, so even if the server is compromised, the decryption keys for stored files cannot be obtained from the compromised server. Data is also encrypted in transit using SSL/HTTPS.

Accellion's security mechanisms guard against malicious access:

- File names are de-referenced when stored on Accellion to ensure that files are inaccessible.
- Files may be stored encrypted for added security.
- Data can be accessed only through the file URL embedded in the email.
- Each URL call is authenticated individually.

Restricted Admin Access to Content

IT Administrators do not have access to files once they are uploaded to the Accellion system. However, they can view the list of files and delete, replicate, and set life cycle rules on these files. Administrators can also view reports and logs in relation to file access events.

Audit Trail

As an Enterprise-class mobile file sharing solution, Accellion automatically logs all file and user activities in the application. The audit log provides administrators insight into what is being done in the system, which users are accessing files, what files are being uploaded, and how the system is working overall. Audit trails and comprehensive file tracking help enterprise organizations demonstrate compliance with industry and government regulations. Audit logs are date/time stamped and tracked by user, email address, IP address, and action taken. Administrators can sort by these attributes and also export the audit log either as a CSV file or to a Syslog server. Administrators determine how long logs are stored on Accellion.

Data Loss Prevention

Accellion Mobile File Sharing supports integration with commercially available DLP solutions via the ICAP protocol. The Accellion DLP module enables organizations to not only secure the sharing of files but also monitor and analyze the contents of file sharing, and filter file sharing based on corporate policy, for protection of IP and compliance requirements.

Tested solutions include DLP products from Symantec (Vontu), RSA, Fidelis, Palisades, Websense, and Code Green Networks.

Global Settings

Accellion Mobile File Sharing is designed for enterprise organizations and is deployed and centrally managed by IT. Administrators have the ability to centrally manage users across the globe through an Admin Console. They can set restrictions globally on user accounts, including:

- Who can create workspaces or upload files
- How long files are retained in the system
- Who can use Accellion Mobile Apps and whether users have View or Edit permission
- How many versions of a file are retained
- How long after files are deleted or expired can files be recovered
- Whether users can delete files

Data Retention

IT Administrators can set file and workspace life cycle rules and as well as select how long deleted and expired files are retained in the Accellion system. Organizations can have files stay in the trash from 1 to 180 days.

FIPS 140-2 Level 1

Accellion offers a FIPS 140-2 Level 1 certified module in its secure file sharing solution for both on-premise and off-premise, virtual, cloud and hosted deployments. For Accellion mobile applications, organizations can take advantage of FIPS 140-2 Level 1 certified modules provided by technology partners such as Good and Mocana.

Accellion Public Cloud – Amazon EC2

The Accellion Hosted Cloud Service enables organizations to rapidly implement mobile file sharing to quickly scale resources and teams and manage peaks in usage. Accellion offers both single and multi-tenant public cloud deployment options through Amazon EC2.

Reports and Certifications

Amazon Web Services (AWS) has completed multiple **SAS70 Type II** audits, and now publishes a Service Organization Controls 1 (SOC 1) report, published under both the **SSAE 16** and the **ISAE 3402** professional standards. AWS has also achieved **ISO 27001** certification, and has been successfully validated as a Level 1 service provider under the Payment Card Industry (**PCI**) Data Security Standard (**DSS**). (*Amazon, 2011*)

Physical Security

AWS datacenters are housed in nondescript facilities. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. (*Amazon, 2011*)

Data Privacy

AWS enables users to encrypt their personal or business data within the AWS cloud and publishes backup and redundancy procedures for services so that customers can gain greater understanding of how their data flows throughout AWS. *(Amazon, 2012)*

Accellion 3rd Party Auditing

Accellion products undergo regular 3rd party security audits. For more information, please contact Accellion.