LR Associates, inc.
Secure Internet Solutions

Helping people profit from changing trends

SHARESYNC FROM LR Associates, Inc.:

DETAILS ON SECURITY FEATURES

ShareSync from LR Associates, Inc. is an enterprise-class backup and file sharing service. It's a complete file management solution that gives employees access to always up-to-date files from virtually any device and allows them to securely share files and folders inside and outside the company. ShareSync also fully protects and preserves data with real-time backup and point-in-time restore capabilities.

ShareSync's data protection features enable business managers to:

- Assure compliance with security best practices
- Get full visibility over end-user activity with Audit Log and Admin File Management features
- Minimize potential downtime from data loss events with real-time backup and restore capabilities
- Utilize remote wipe capabilities in case of lost or stolen devices
- Keep content safe with at-rest and in-transit encryption
- Assure reliability with a 99.999% financially backed uptime guarantee
- Leverage enterprise-class datacenters with redundant storage clusters and connections to multiple Internet providers
- Protect content integrity with features that guard against accidental deletion or version conflict
- Keep content in the right hands with permissions and access that are strictly controlled and easily amended

This paper provides detailed information about ShareSync's security features.

Encryption

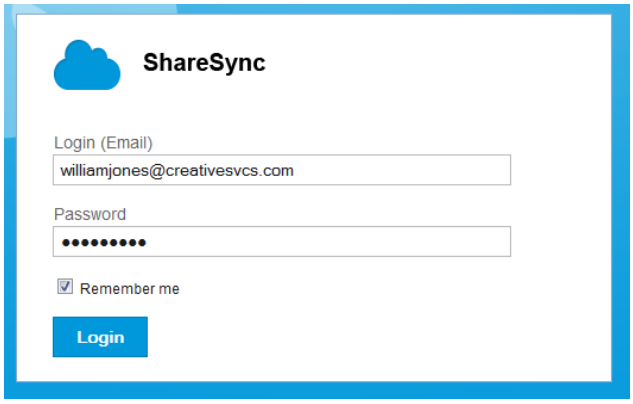
ShareSync data is encrypted both when it's at rest as well as when it's in transit. At-rest data is encrypted with 256-bit AES encryption, while in-transit data is encrypted using 256-bit SSL/HTTPS encryption. Additionally, ShareSync generates a unique encryption key for every account, creating an even greater degree of protection through data isolation.

The following chart compares ShareSync's encryption features to other providers:

	ShareSync	Carbonite Pro	CrashPlan for Business	Mozy Pro	File Servers	Box for Business	Dropbox for Business	OneDrive for Business
In-transit encryption	✔	✔	✔	✔	✘	✔	✔	✔
At-rest encryption with unique account-level encryption key	✔	✘	✔	✔	✘	✘	✘	✘

Password Protection

Each time a user activates a new ShareSync device or accesses ShareSync from the web, they must login using their username and password.

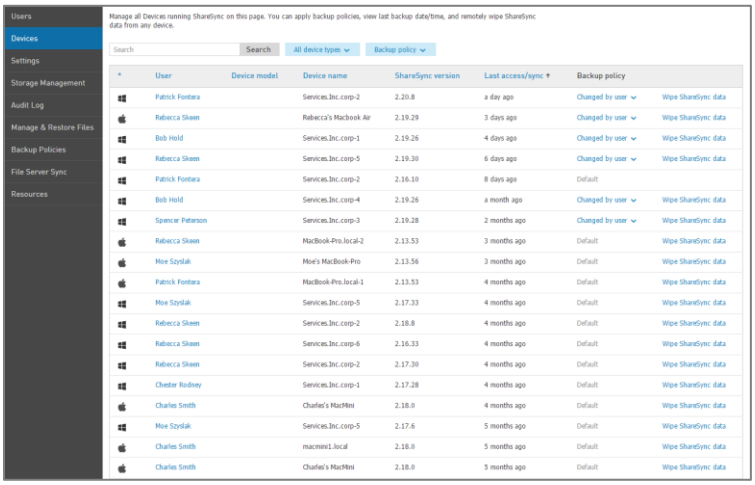


ShareSync password policies are imported from Active Directory and utilize "strong" parameters, helping to eliminate the possibility that external parties will guess passwords. This Active Directory integration requires users to use the same password for ShareSync that are used for other cloud services from LR Associates, Inc.. Because there are no additional passwords to remember, it reduces the possibility that they will write their password down where others might see it.

For mobile devices, an additional layer of security can be added by configuring a passcode that must be entered each time the app is launched.

Device Management

Using the ShareSync Control Panel, administrators can view and manage all the ShareSync devices enabled on their account. Each time a new device is configured by an end user, the administrator is notified, and all users' devices are catalogued in the Control Panel.

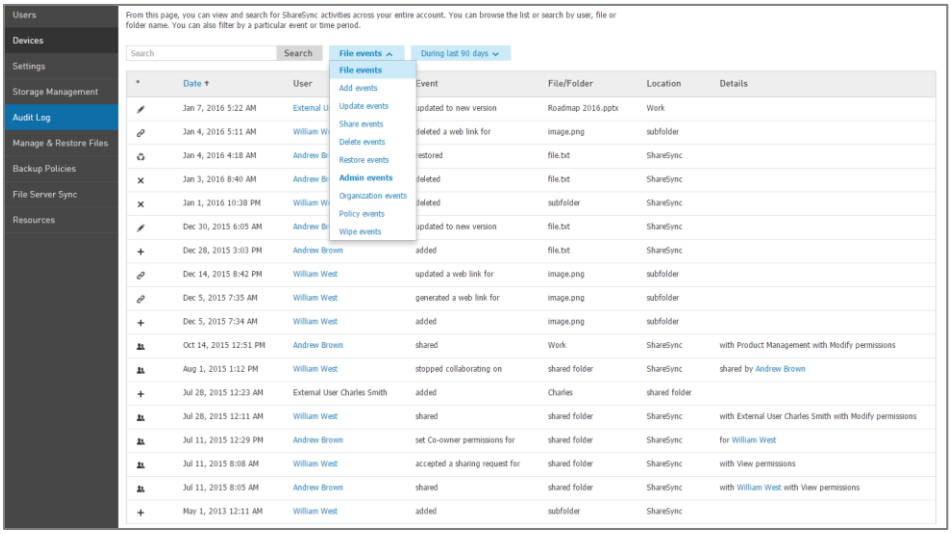


Remote wipe

ShareSync is one of just a few file management solutions that allows administrators to wipe data remotely from any device. In case of a lost or stolen laptop, tablet, or mobile phone, or when facing a personnel issue, corporate data can generally be quickly removed, helping to minimize potential data leakage.

	ShareSync	Carbonite Pro	CrashPlan for Business	Mozy Pro	File Servers	Box for Business	Dropbox for Business	OneDrive for Business
Device management with remote wipe	✔	✘	✔	✔	✘	✘	✔	Mobile devices only

Audit Log



The Audit Log is a ShareSync Control Panel feature that allows administrators to view all the ShareSync activities on their account. Whenever files or folders are added, updated, shared, or deleted, the event is logged and available for tracking and auditing purposes, providing a greater level of administrative control over ShareSync. There are multiple ways to use the Audit Log:

- Browse by event type
- Search by user, file name, or folder name
- Filter by event type or date range

Admin File Management

ShareSync's Admin File Management feature lets account owners exert administrative control over all end user files and folders. Once account owners enable this feature through the control panel, they can manage all ShareSync content across the environment.

Admin File Management increases the ability for administrators to monitor and manage end user content. Using Admin File Management, account owners can:

- View and adjust sharing permissions
- Add, delete or restore files
- Search for specific files within a user's ShareSync folder and file structure

This feature needs to be explicitly enabled for each admin. All admin actions are tracked in the audit log.

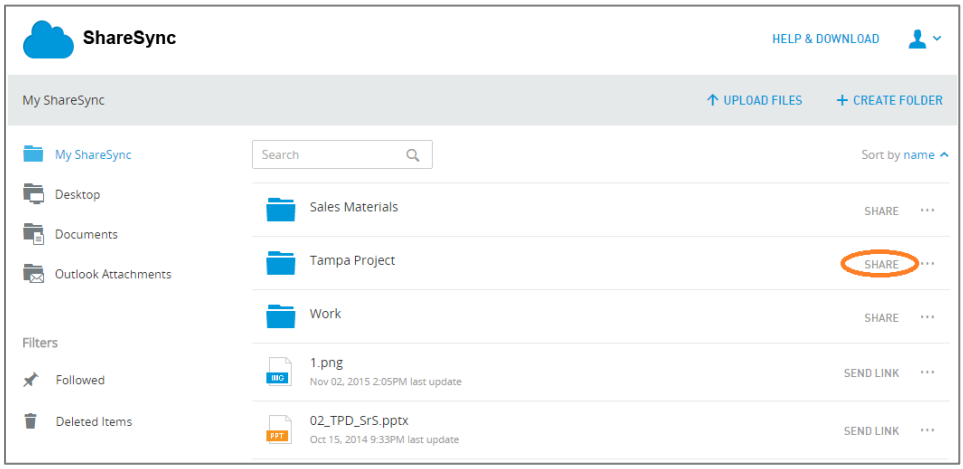
	ShareSync	Carbonite Pro	CrashPlan for Business	Mozy Pro	File Servers	Box for Business	Dropbox for Business	OneDrive for Business
Admin File Management (manage content, shares, restores)	✔	✘	✘	✘	✔	✘	✔	✘

User control over sharing permissions

When a user shares a ShareSync folder, he or she can set permissions for each collaborator independently. The configurable sharing permissions are "Co-Owner," "Modify" or "View-only".

- "Co-Owner" permissions give others full control to modify, delete, or re-share content
- "Modify" permissions allow others to view, modify and delete content but not share it
- "View-only" permissions only enables others to download the files

Permissions can be set differently for each collaborator. And sub-folders can be shared with different collaborators. Permission levels can be changed or revoked at any time.



Permissions:	Co-owner	Modify	View
Download	✓	✓	✓
Add	✓	✓	
Edit	✓	✓	
Delete	✓	✓	
Restore deleted files	✓	✓	
Restore by date	✓		
Permanently delete	✓		
Re-share	✓		
Send link	✓		

Sharing web links

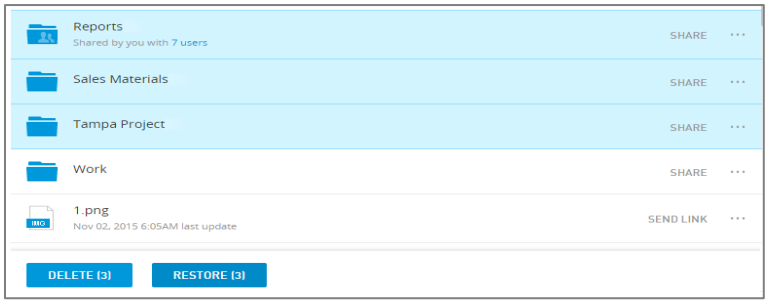
Web links allow users to share individual files with users both inside and outside of the company. Links can be generated for a single file, which gives access to just that file, or an entire folder, which gives access to all files in the folder. For additional security, web links can be protected with passwords.

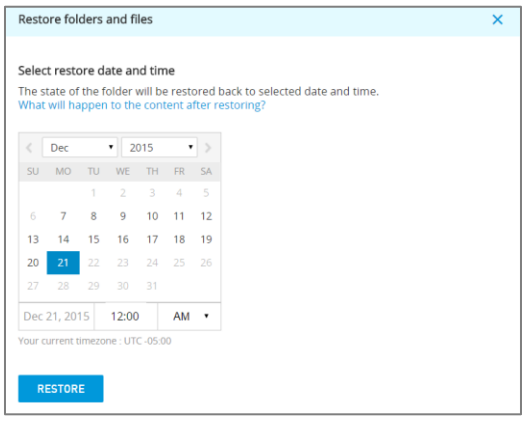
external collaborators

Administrators can configure external sharing policies to allow users to easily share with individuals or organizations outside the company, for example vendors or business partners. External ShareSync users can edit files, sync files, and access all content in the folders that have been shared with them. This is a useful feature for collaborating on files and folders with another company on an ongoing basis.

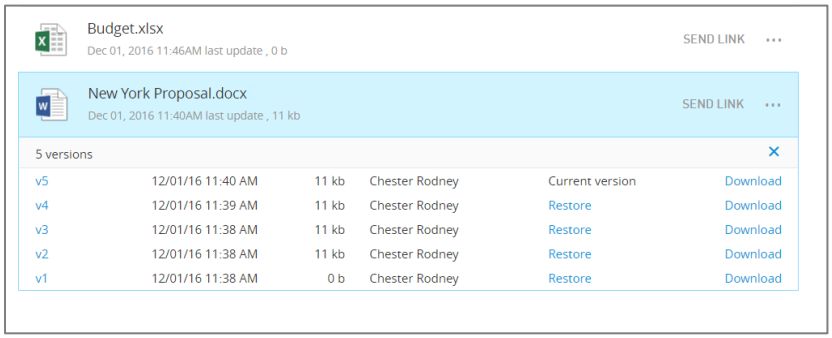
External ShareSync users are able to access the complete set of ShareSync features and functionality. Administrators can track external user activity in the audit log and control data with remote wipe.

DATA PROTECTION





ShareSync was designed with a high level of data protection, to help reduce the chances of files being accidentally deleted, and to help provide simplify the process to restore and recover files in the case of a data loss event.



Files can be rolled back to specific earlier versions or to a specific point in time. Files can be rolled back individually or multiple files and folders can be rolled back in a mass restore capability. Files can be restored by either end users or by administrators through the Admin File Management functionality.

From a service architecture perspective, every ShareSync file is replicated to redundant storage clusters to help minimize the risk of data loss. Additionally, each user's data is fully isolated from every other user's data.

In the unlikely event of a service outage, users can still access all their locally-synced data.

ShareSync co-editing features help to prevent file overwrites and conflicts. File versioning allows users to easily restore previous versions of all files stored in ShareSync.

If a file is deleted, it is moved to a recycle bin, where it can be restored. Administrators can restore deleted files and prevent permanent deletions.

Infrastructure

ShareSync is backed by a 99.999% uptime guarantee. No other file backup and file sharing solution offers a comparable uptime guarantee.

	ShareSync	Carbonite Pro	CrashPlan for Business	Mozy Pro	File Servers	Box for Business	Dropbox for Business	OneDrive for Business
99.999% uptime SLA	✔	✘	✘	✘	✘	✘	✘	✘

ShareSync is delivered through a data infrastructure comprised of:

- Multi-tenant platforms secured with redundant firewalls, multiple Intrusion Prevention Systems
- Facilities with dedicated, full-time certified security personnel and rigorous physical security measures

Compliance

ShareSync takes strict security measures to reach regulatory compliance across industry and vertical-specific standards.

Data Privacy, Integrity and Security Standards

- **SOC 2 Type II** - ShareSync has a SOC 2 Type II audit report from an independent auditor who has validated that, in their opinion, our controls and processes were effective in assuring security during the evaluation period. ShareSync is audited company-wide, not just at the datacenter level. Additionally, while some service providers may only choose to be audited against one or two of the five trust service principles (security, availability, processing integrity, confidentiality and privacy), ShareSync has been audited against all five.
- **SSAE 16 Type II-audited datacenters** – ShareSync datacenters are audited to the SSAE 16 Type II standard, which validates the provider's commitment to the trust principles of security, availability, processing integrity, confidentiality, and privacy.

- **US-EU & US-Swiss Safe Harbor** - ShareSync is registered with the US Department of Commerce as compliant with US-EU and US-Swiss Safe Harbor frameworks, which were created to bridge the gap between US and EU/Swiss data protection and privacy standards. All our EU and US customers benefit from this level of protection.**PCI Data Security Standards (PCI DSS) -** The payment processing system utilized by ShareSync has passed the strict testing procedures necessary to be compliant with the PCI Data Security Standards (PCI DSS). This helps ensure that your payment information will not be accessed by unauthorized parties or shared with unscrupulous vendors.

- **HIPAA** - The Health Insurance Portability and Accountability Act mandates a set of regulations protecting the privacy and security of patients' confidential health information, including when and with whom that information can be shared.

•

	ShareSync	Carbonite Pro	CrashPlan for Business	Mozy Pro	File Servers	Box for Business	Dropbox for Business	OneDrive for Business
HIPAA compliance	✔	✘	✔	✔	✘	✘	✔	✔

Conclusion

These security features make ShareSync a highly-secure, highly-reliable file backup and file sharing solution. For more information about ShareSync's security features—or to request a live product demonstration— contact LR Associates, Inc..