The Intralinks Multi-Tenant SaaS Platform

Our Security Model and Practices Explained

Version 1.0

January 2015

Executive Summary

Intralinks is a trusted global leader for providing secure enterprise content collaboration solutions. Our platform offers customers the ability to easily work with anyone, anytime and anywhere. Our customers can share documents and files securely, allowing them to complete their tasks quickly and efficiently. We support the secure, compliant, and auditable exchange of critical information, from any device or machine.

Interested in learning about our enterprise class-security? Then please read on. This guide describes how we enforce best practices around the safe and legal collection, processing, and leveraging of data. Not only do we ensure client data are highly secured and protected — we do it seamlessly, without sacrificing high availability and performance for our end users.

Content

Our Security Pillars

At Intralinks, we rely on a robust security model that stands on four pillars: application, infrastructure, personnel and process. Combined, these pillars provide secure cloud-based content collaboration services that stand among the best in the industry.

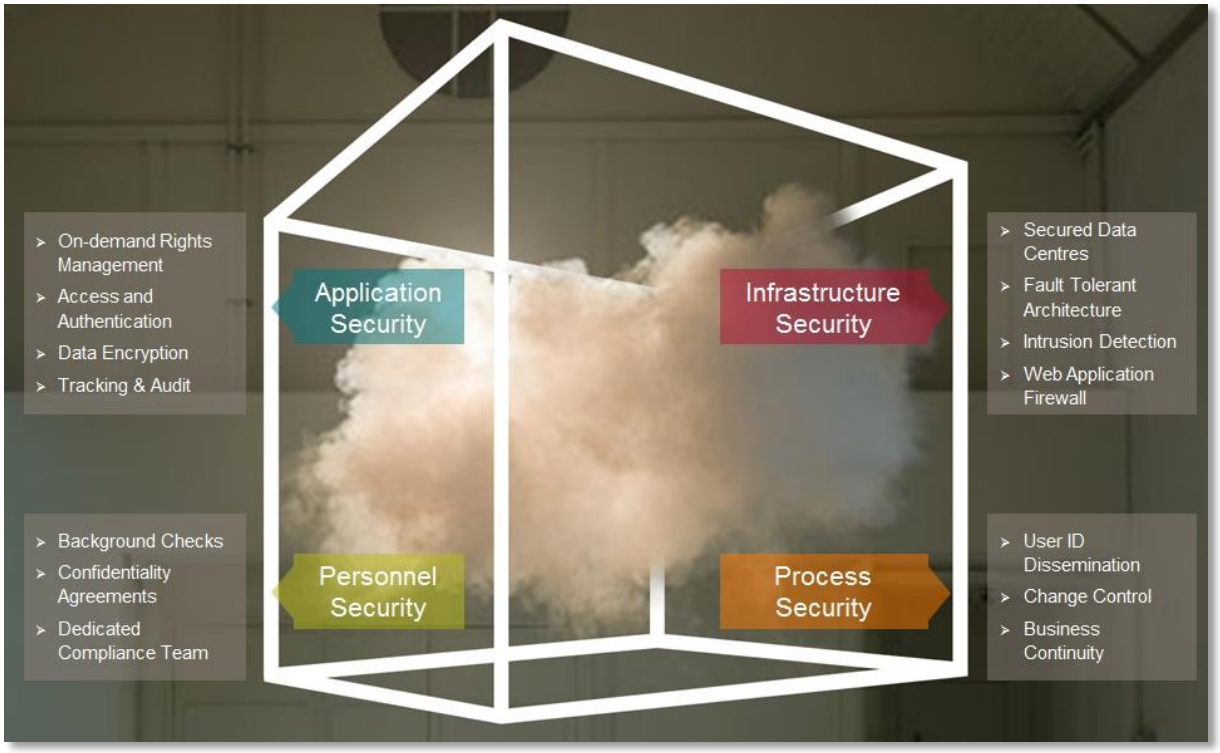


Figure 1: Intralinks Pillars of Security

We take information security very seriously. During the past 18 years, we've built a solid reputation for our systems' secure content management capabilities. The Intralinks Platform's security services provide extensive document control and auditability.

Specific security related capabilities and policies include:

- A granular access management framework, with access defined by user, role, and document types
- The ability to delegate administration to appropriate users
- Seamlessly integrated plug-in free information rights management (IRM) capabilities
- Multi-tier encryption key management
- Customer managed encryption keys
- 256-bit encryption, at rest and in transit
- Annual SOC2 Levell II certification, conducted by a Big Four auditing firm
- Multi-factor authentication in conjunction with RSA Adaptive Authentication services
- Periodic network penetration and vulnerability testing

- Mandated background checks for all Intralinks staff
- Redundant geographically distributed data centers in the U.S. and United Kingdom

These capabilities and best practices allow our customers to work with confidence: they know the security of their documents and content will satisfy the most rigorous assessment and audit criteria.

Client Data

Document and Content Management

Our solution supports secure document management and collaboration, enabling a company to conduct its mission critical projects and tasks. All content is manageable within the Intralinks Platform, making the solution an ideal location for both ad-hoc file sharing and inter-enterprise collaboration.

We do more than just provide a secure location for documents. In fact, our solution manages the full content lifecycle. We enable document creation, publication, indexing, and virus scanning. Users leverage our full workflow controls to create and publish documents, perform audits, process tasks (using streamlined controls), and securely distribute the content to appropriate audiences.

We support file distribution combined with stakeholder or workgroup alerts. This ensures appropriate stakeholders are immediately identified, and notified of document arrivals, along with edits and changes, and any pending tasks. Customers can choose to receive alerts via email or directly to their desktop.

Also, the client can select any channel for end users to receive notifications. The notification message templates are configurable and can support customizable content, offer links to the documents/task list, and provide notes detailing the pending action requirements.

Transmission of End-User Files

Below, Figure 2 shows our application-level file processing.

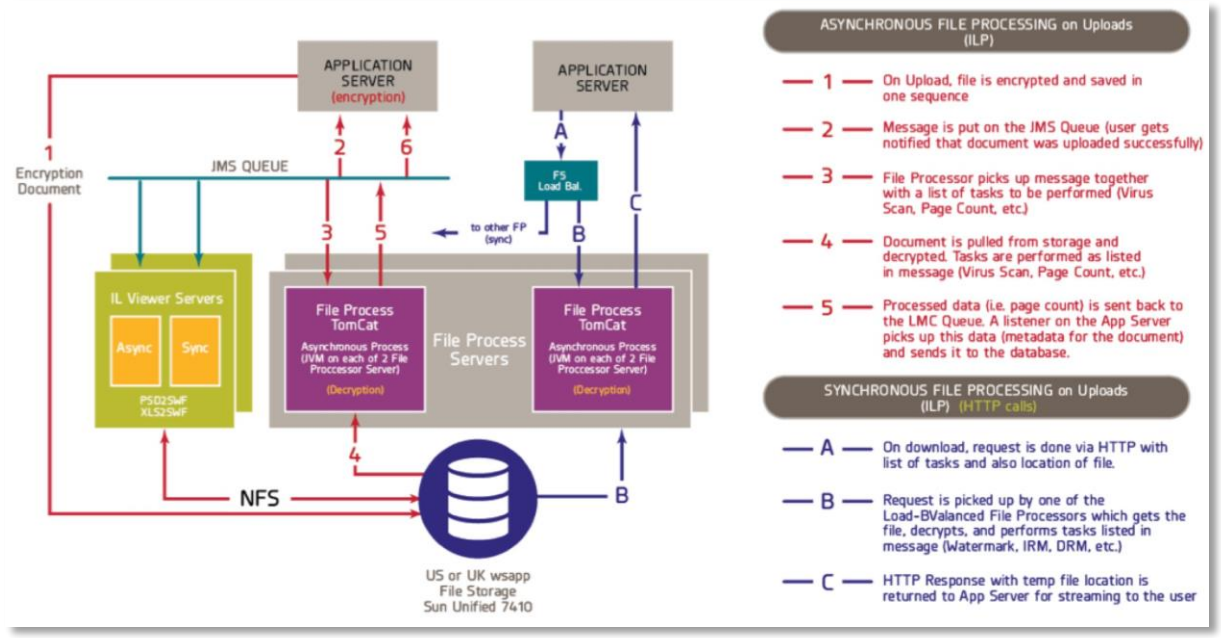


Figure 2: Technical View of the File Processing

Document Upload

The Intralinks Platform can host any file type. To upload files, users can leverage Intralinks Designer, a browser interface, as well as Intralinks Drive, a Microsoft® Windows desktop-based tool. Before any document is uploaded, we scan it for viruses. If a document is infected, the solution replaces it with a placeholder and alerts the owner of the Exchange.

Document Download

When an end user requests a file download, a processing server locates and then retrieves the specified file. The server then decrypts the file, and then applies a watermark or PDF protection. The file leaves the application server and enters another server, which, using an SSL accelerator to boost speed, performs SSL encryption and decryption functions. The file is then streamed to the requestor. After the download is complete, the system immediately and permanently purges the file from the temporary processing directory.

Data Encryption Process

We employ multiple techniques to ensure client content is protected at rest and in transit. The system relies on a multi-layer key management system, detailed below.

Data In-Transit

The end user's browser connects to the Intralinks data center via an encrypted transport channel. By default, the channel deploys Transport Layer Security (TLS), using 2048-bit RSA keys, and the 256-bit Advanced Encryption Standard (AES) packet encryption. Extended validation certificates handle server identity and encryption.

Data At-Rest

All client data stored on disk remains encrypted. On upload, all documents are encrypted via the 256-bit Rijndael AES standard, with each file receiving its own unique key combination. To extend the protection, the solution also uses a master encryption key to encrypt the individual file keys. Master key protection involves a mix of technical and physical controls, including:

- The separation of duties between system and database administrators
- The breakup in pieces of the master key, and each key piece is stored on a separate machine
- No one has access to all the machines that store the master key segments

Our security architecture prevents the application layer from accessing the master key or data encryption keys. Instead, the application layer leverages key IDs, and encryption services handle all cryptographic functions.

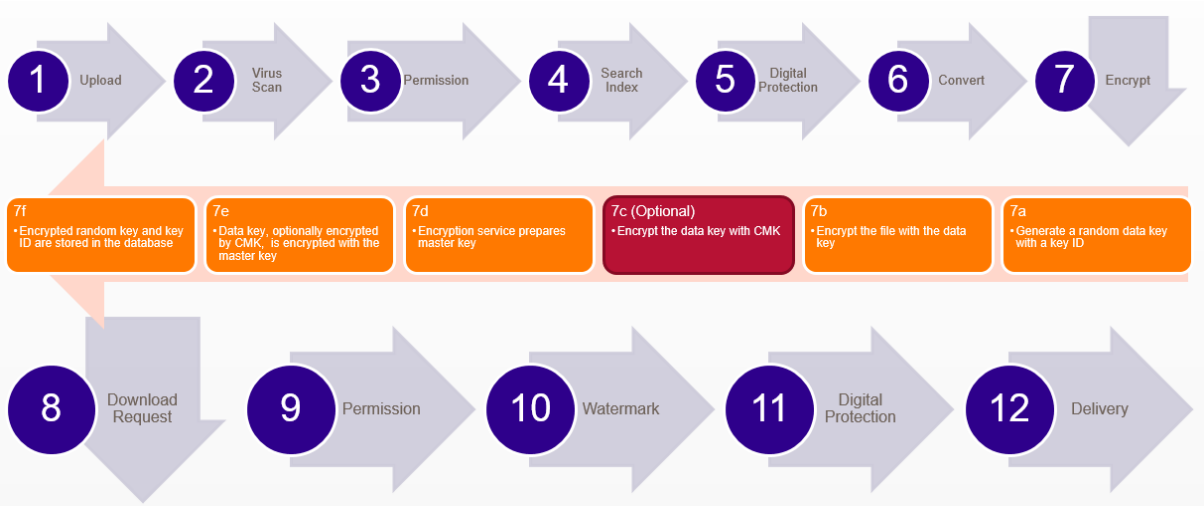


Figure 3: Intralinks' Encryption Process

Customer Managed Encryption Keys

Customer Managed Keys (CMK) give enterprises the ability to maintain security and privacy over their hosted content without disrupting business information sharing with customers and partners.

Key elements of the Intralinks CMK solution include:

- A dedicated partition of a SafeNet™ HSM device, which is hosted in our secure data center, to generate and host each customer's own encryption keys

- Full customer control of these keys, with the ability to rotate, revoke or renew keys at any time, for any reason, without depending on Intralinks staff;
- An additional step in the key management process — this means customer keys will encrypt data keys of customer information first, and key rotation won't force unnecessary data re-encryption.

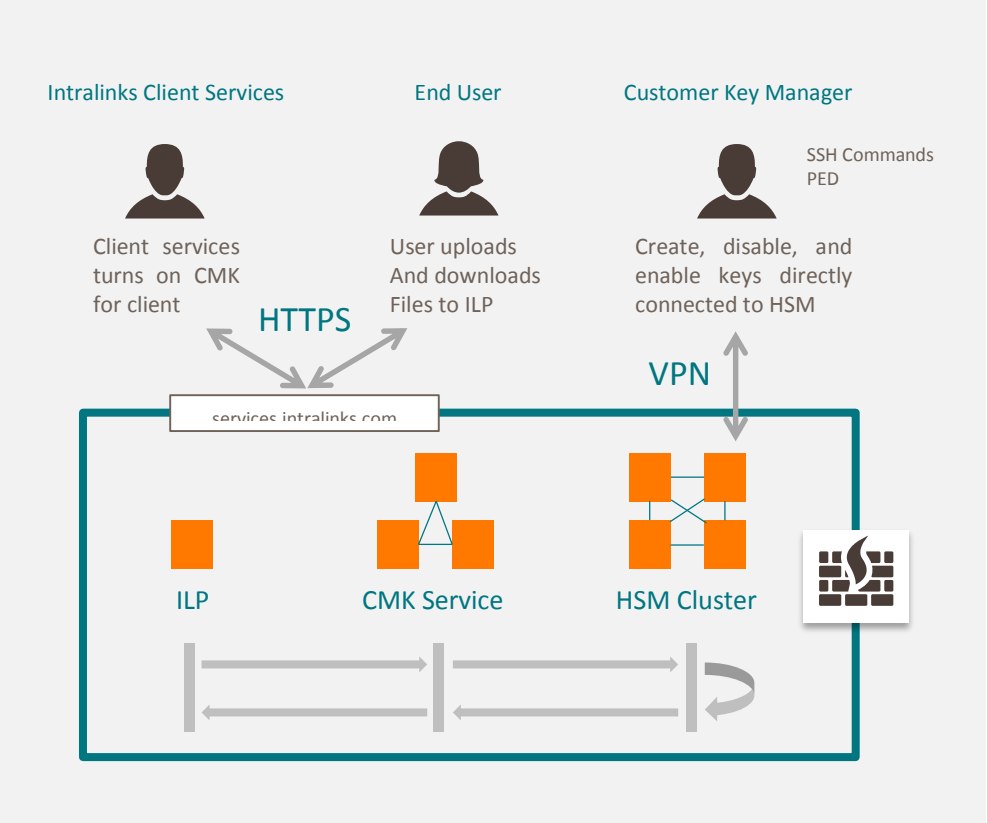


Figure 4: CMK Process Flow

Data In Use - Protection via Information Rights Management

Protection follows the granting of a permission. Once a group has permission to view a document, a publisher can set the group's protection level. Different groups can have varying protection levels for the same document. The protection levels for Office and PDF documents are as follows:

- **Open**: Users are free to view, download, and print the document with no restrictions
- **Protect**: Users may view and print document but can't download or save it on their own machines; typically, publishers will apply watermarks to prevent users from leaking a printed document
- **View only**: A user may view the document but can neither save it locally nor print it

No plug-ins are required to review protected documents. On the other hand, users have the choice of accessing protected documents within the Intralinks Viewer (Figure 5). Our Viewer is a 100% web tool that requires no local installation, and it doesn't cache documents or permit screen capture.

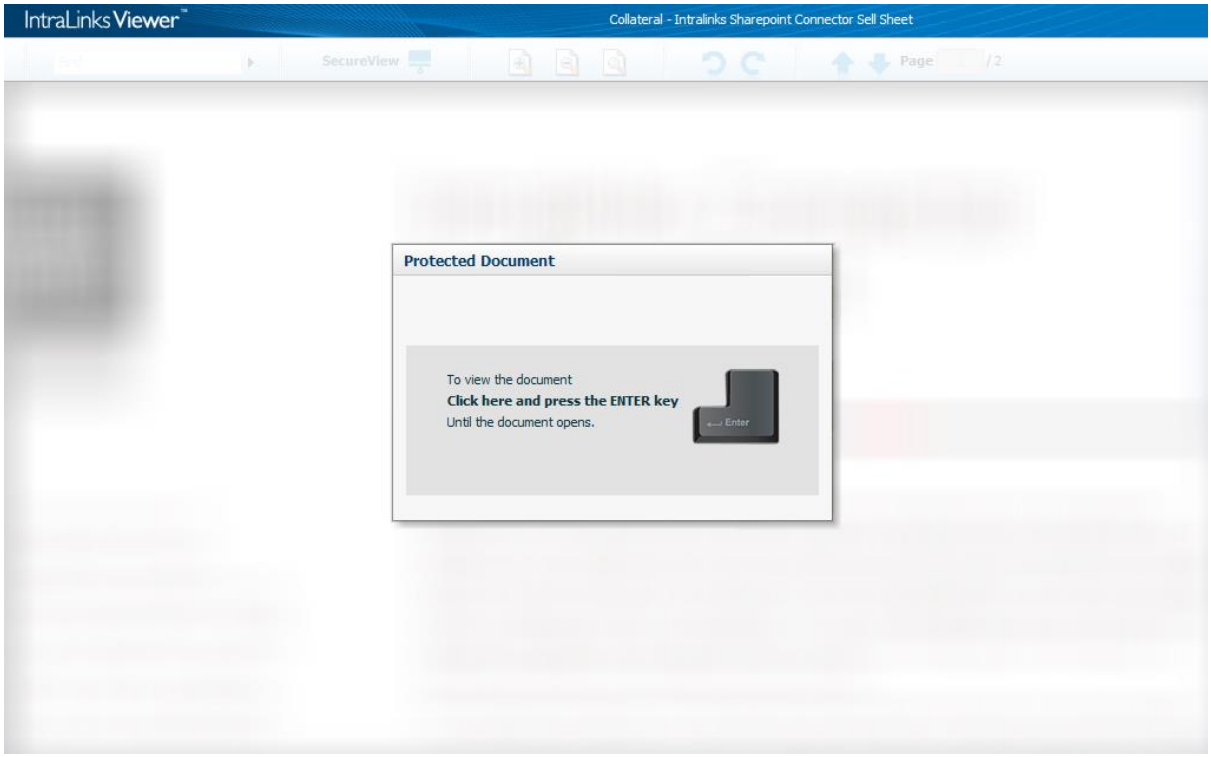


Figure 5: Intralinks Viewer

Watermarking

The Intralinks system can watermark protected documents to mitigate the risks of leaking sensitive and confidential documents. This capability involves embedding a watermark containing the user's credentials, the download date, and a time stamp, along with other identifying criteria (like custom term or project name). The watermarks will be visible in the printed versions of document — this means any leaked document will present enough clues so the source of the leak can be quickly traced.

Figure 6: Intralinks Dynamic Document Watermarking

Client Data Isolation

We logically separate out clients' information the same way a bank separates its accounts and transactions. This is done at the row-level within a database table. Each customer Exchange is assigned a unique ID used for all access and authorization decisions — files and users are associated with a particular Exchange ID. The Exchanges are segregated at the application and database layers.

Our service has a role- and-permission-based security model. All user interaction is via the service's applications, without the user ever accessing the underlying servers or network infrastructure. The client's Exchange coordinator controls the creation and allocation of Exchanges to their Exchange managers. The Exchange managers are, in turn, responsible for all administrative controls within an Exchange. This includes adding/removing users, assigning roles, adding/deleting documents, and granting users document permissions.

Our service presents users with only the Exchanges to which they are permitted access (as granted by the client's own designated Exchange managers). All access to client data is logged and audit-ready. Clients have the option to block Intralinks personnel from accessing their exchanges.

Final Disposition

Once an end user file is deleted from an Exchange, the system marks it in the database as removed. It thus becomes unavailable unless the "save deleted documents" function was activated for the Exchange the document resided in.

It requires 60 days for us to delete files from the user accessible Intralinks applications after they have been marked for elimination.

Files are erased during a standard weekly purging, after which backup data remains on location-specific storage tapes for a standard 30-day retention period. At the end of 30 days, we clear the tapes for reuse and the existing data on them cannot be restored. These backups are for disaster recovery purposes only.

Authentication and Authorization

Authentication

Adaptive Authentication

Intralinks has integrated with RSA® Adaptive Authentication service that provides risk-based authentication functionality for web-based applications. Adaptive Authentication quietly reviews user activity and conducts a risk assessment of each action, and then rates that action according to a predefined risk score. If the user's action qualifies as high risk (or if it violates company policy), the system challenges the user. This approach increases security, but doesn't interfere with regular user tasks.

How it works:

RSA Adaptive Authentication verifies a user's identity by comparing the profiles of his or her activity with an existing profile pattern. This approach requires the creation of a profile from data the RSA system gathers. The RSA system does this during an initial period, where it monitors and records the technical parameters of the user's computers and behavior.

Adaptive Authentication stores data about the registration and usage of the end user's laptops and other devices — in effect, creating a "fingerprint" for each machine when it initiates requests for services. Device fingerprinting enables strong authentication processes without having to upgrade the user's hardware or buying a new hardware token. Device fingerprint information includes the user's:

- Browser type, version, etc.
- Screen display (width, height, color scheme, etc.)
- Installed software — this includes software versions of commonly installed programs such as media and flash players, Java, and the like
- System time zone settings
- Regional and language settings

The system feeds both the unique user parameter data and the device fingerprint information into the RSA Risk Engine. This performs an assessment and creates a user profile. The system then monitors the device information; it sees if the user data matches the fingerprint, or if a new request breaks the usual behavior pattern. If so, the system will assign the user a higher risk score and report that. It may

also present additional verification challenges to the user. Managers can configure the risk engine's rules to emphasize different types of parameters, such as: the IP address ranges, typical time of access, days since last logon, and so on.

Additionally, the risk engine takes feeds from the eFraudNetwork — the RSA database for sharing and disseminating information on fraudulent activity. It proactively identifies and tracks fraudster profiles, patterns, and behavior across 65-plus countries. This is relevant to our customers because the database contains profiles of parties that were already caught attacking other systems. We will recognize these hackers even if the hackers present valid user IDs and passwords when logging on.

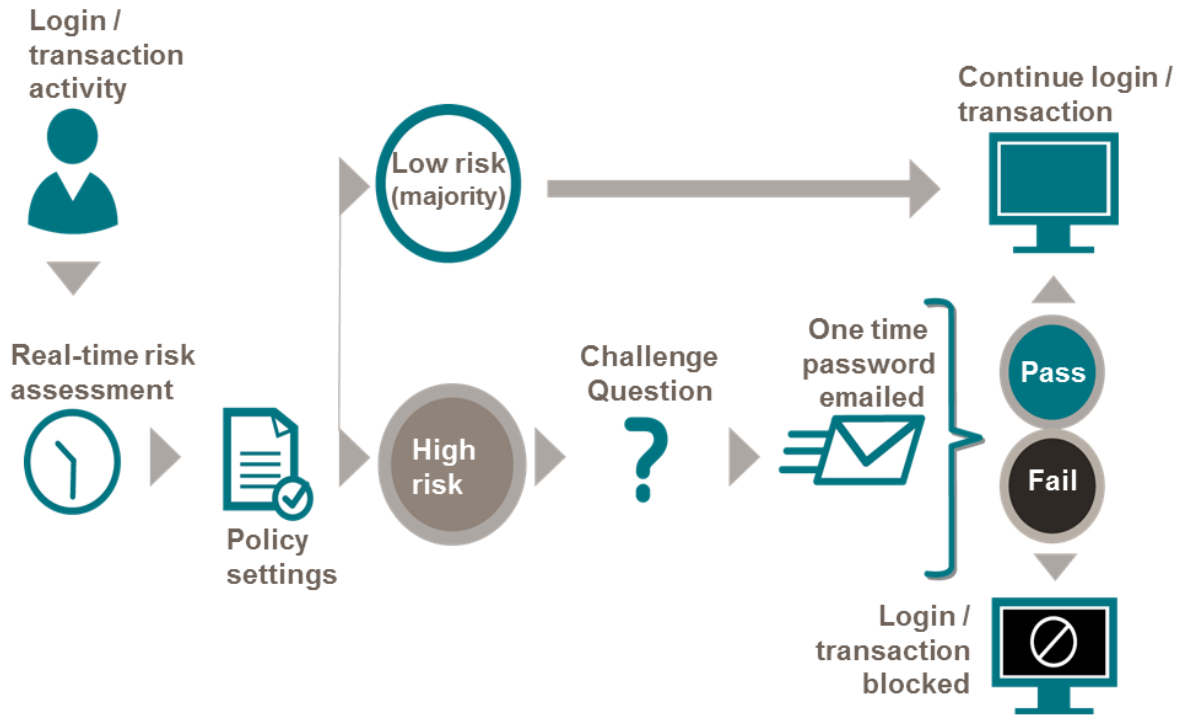


Figure 7: Intralinks MFA

Two-Factor Authentication

We allow managers to apply forced second-factor options for authentication. In this way, users logging on to an Exchange must provide additional information before being authenticated. There are six different security options available to Exchange managers; the verifying information is segregated by sensitivity, with appropriate protections.

The options include:

1. One-factor security that doesn't leverage the risk engine
2. All high-risk users must answer a security question; after three failed attempts to answer, these users will be issued a single-use password
3. All high-risk users must answer a security question; after three failed attempts, the user is locked out and must call Client Services to gain entrance to the system
4. All high-risk users must use a one-time password

5. All users must answer a security question every time they access an Exchange
6. All users must apply a single-use password every time they access an Exchange

The system requires no additional downloads or registration to leverage these additional security capabilities. There may be cases when an Exchange's security setting (or a high-risk user) requires an additional challenge. If so, a pop-up will instruct the user to enter the additional factor (a challenge question/answer or the one-time password, sent automatically to the user's email account). Because any given Exchange may be configured differently for security, users who access multiple Exchanges may find their interactions vary considerably. Some Exchanges may require no additional security measures; other Exchanges may be configured to demand additional factors each time a user enters them.

User Authorization

Password Reset Process

If an end user incorrectly enters a password three consecutive times, the system automatically locks that account. The solution also automatically issues a message to the registered email address of the end user associated with the account. The message announces the account is frozen and contains a password reset link.

Unauthorized Access

The Intralinks solution is architected into compartments with varying protections. The primary compartment offers access to the Intralinks Hub. The Hub serves as a home page which displays all Exchanges a user can access. Only Exchange owners or users with the Exchange Manager+ role have the authority to grant third parties access to Exchanges. If a user can't access an Exchange, that user can contact Intralinks support for help. Support will first verify the user's information to confirm the user has an actual live account. If not, the support staff member will immediately end the call and log it. If the user has a valid account, support will restrict all discussion to the Exchanges associated with that account. If the caller asks about an unlisted Exchange, the agent will be unable to locate it. The agent will inform the user the Exchange isn't associated with the user account. The agent will not confirm or deny if the Exchange is live and will not look for or discuss such an unknown Exchange. (Further conversation with the end user could enable a social engineering attack.)

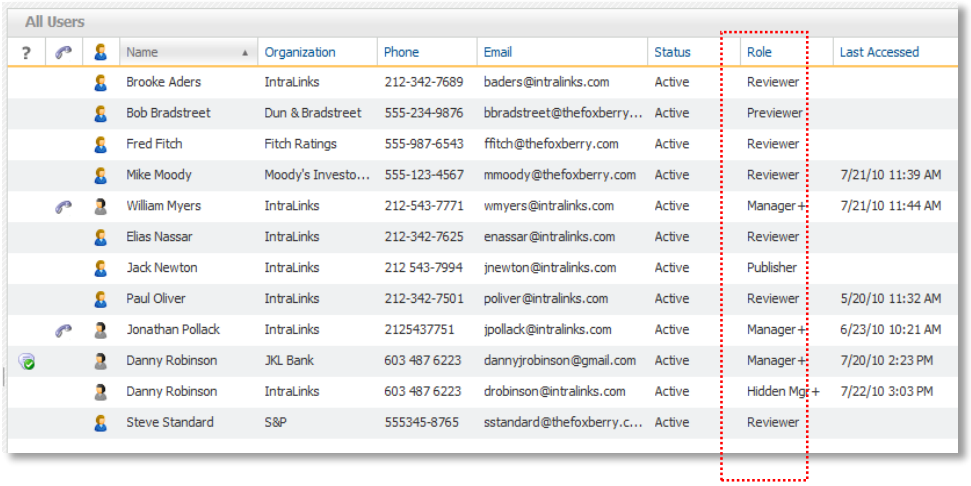
Permission Assignment

The Intralinks solution's primary security wall employs a hierarchical role-based system. With this, specific parties are assigned particular functions — such as adding users or posting documents. There are a variety of roles for the deal team members, including: potential buyers, advisors, book-runners, and arrangers.

When a user is assigned a role, the system determines that user's overall level of document access and the granularity of visibility into the other participants in the Exchange. For example, a firm's executive team may have open access to all documents and participants. Other users in the Exchange may be permitted to read a limited set of documents and have a limited snapshot of the other team members.

Any given Exchange will support nine different end-user roles, which are variants of three basic user personas: manager, publisher and reviewer. A user's permissions during the different phases of a transaction are also linked to these roles. For example, the project support team may have Manager+

roles. (Such a role gives the user the widest set of controls for adding or updating documents and groups.) Subject matter experts (SMEs) may have publisher roles but with limited access to view and post certain documents.



Name	Organization	Phone	Email	Status	Role	Last Accessed
Brooke Aders	IntraLinks	212-342-7689	baders@intralinks.com	Active	Reviewer	
Bob Bradstreet	Dun & Bradstreet	555-234-9876	bbradstreet@thefoxberry...	Active	Previewer	
Fred Fitch	Fitch Ratings	555-987-6543	ffitch@thefoxberry.com	Active	Reviewer	
Mike Moody	Moody's Investo...	555-123-4567	mmoody@thefoxberry.com	Active	Reviewer	7/21/10 11:39 AM
William Myers	IntraLinks	212-543-7771	wmyers@intralinks.com	Active	Manager+	7/21/10 11:44 AM
Elias Nassar	IntraLinks	212-342-7625	enassar@intralinks.com	Active	Reviewer	
Jack Newton	IntraLinks	212 543-7994	jnewton@intralinks.com	Active	Publisher	
Paul Oliver	IntraLinks	212-342-7501	poliver@intralinks.com	Active	Reviewer	5/20/10 11:32 AM
Jonathan Pollack	IntraLinks	2125437751	jpollack@intralinks.com	Active	Manager+	6/23/10 10:21 AM
Danny Robinson	JKL Bank	603 487 6223	dannyjrobinson@gmail.com	Active	Manager+	7/20/10 2:23 PM
Danny Robinson	IntraLinks	603 487 6223	drobinson@intralinks.com	Active	Hidden Mgr+	7/22/10 3:03 PM
Steve Standard	S&P	555345-8765	sstandard@thefoxberry.c...	Active	Reviewer	

Figure 8: Intralinks Individual User Roles

User Roles

Our powerful permission system governs access to each document in an Exchange. When a document is published, the project support team (which will include someone with Manager+ credentials) determines which users can see or update that document. Those users can access the document while the permissions remain in place, but at any time a manager can change permissions — revoking or adding access for individuals or entire groups. There is a permissions copying feature in the system that allows the project support team to quickly replicate the permissions of other system groups.

Backup and Business Continuity

Data Backup

On-Site and Off-Site Backups

Intralinks' hosting provider, SunGard, performs daily backups and maintains a backup tape set onsite, in a fireproof cabinet. Iron Mountain provides offsite storage for the backup sets.

Server-Based Contingency

In addition, Intralinks ensures that the client data are replicated from the primary data center to the backup site, in real time. In case the primary data center fails, the mirror site can go live quickly to ensure business continuity for clients.

Data Control

During backup, the system spreads the encrypted data across multiple tapes; the tape index is stored on another tape, rendering each individual tape useless. Our backup tapes are solely dedicated to our clients.

Backup Testing

We test our backup procedures twice annually.

Backup Schedule

The backups are as follows:

- Incremental tape backups are scheduled whenever the database is updated; these backups can be scheduled daily; the backup data is retained at an off-site location for 30 days
- Cumulative incremental backups are triggered by new or changed data entered in between full backups; they are scheduled bi-weekly and the data retained off-site for 90 days
- Full backups of the entire database are conducted bi-weekly, during weeks opposite of the cumulative incremental tape backups; the data is retained off-site for 90 days
- Full backups are conducted once per quarter; the data is retained off-site for 180 days

Off-Site Storage

The staff removes tapes from the library and places them in secured containers (with professional security personnel) for transportation to a facility maintained by Iron Mountain, SunGard's off-site storage vendor.

Real-Time Replication and Business Continuity

We designed our service to be highly available, secure, and fast. To support those objectives, we maintain two instances of our application at each data center. Our application infrastructure is identical in both data centers to support real time data replication between them.

Data Center – High Availability

We operate two North American data centers and two U.K.-based ones. All four data centers are in a standard high availability configuration, and each one runs an Oracle exaData server to provide optimal local redundancy. The data centers are configured for full system redundancy to eliminate single points of failure. SunGard operates the data centers, using the most current secure hosting technologies.

The co-primary data centers are staffed with expert engineers who variously specialize in all the technologies the application suite leverages. Senior engineers and management are available 24/7.

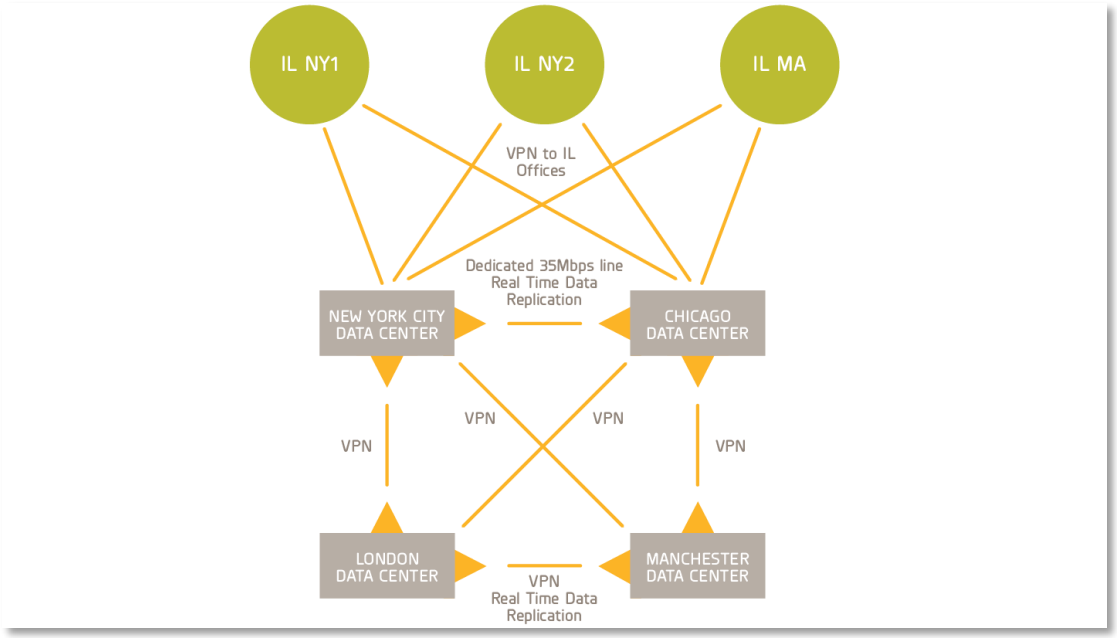


Figure 9: Intralinks Data Center HA configuration

Compliance and Auditing

Intralinks complies with all applicable local laws and regulations related to the performance of its services, including but not limited to, as applicable, the European Data Protection Directive 95/46/EC (the "Directive"), the German Federal Data Protection Act (Bundesdatenschutzgesetz), the Personal Data (Privacy) Ordinance (Cap 486 of the Laws of Hong Kong), the U.S. Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act and United States' state data privacy and data protection laws and related implementing regulations.

With respect to the processing of any personal data by Intralinks, Intralinks implements appropriate technical and organizational measures to protect personal data supplied to it by clients against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing in accordance with Article 17 of the Directive. In addition, Intralinks will only process personal data where Intralinks is acting on a client's instructions, or otherwise where required or permitted pursuant to applicable law or regulations.

When processing personal data, Intralinks acts only as a "data processor."

Intralinks will, to the extent permitted by applicable law, promptly notify the other party upon receiving a request from any third party or regulatory authority for access to data provided by clients to Intralinks.

- Intralinks will notify a client as soon as reasonably practicable upon becoming aware of any unauthorized access to or acquisition, use, loss, destruction, compromise, or disclosure of data supplied by or on behalf of that client to Intralinks
- You can find a copy of Intralinks' data privacy policy here: http://intralinks.com/privacy

This is also compliant with §11 (Auftragsdatenverarbeitung) of the German Federal Data Protection Act (Bundesdatenschutzgesetz).

Safe Harbor

While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union.

In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce, in consultation with the European Commission, developed a "Safe Harbor" framework. The decision by U.S. organizations to enter the U.S.-EU Safe Harbor program is entirely voluntary. Organizations that decide to participate in the U.S.-EU Safe Harbor program must comply with the U.S.-EU Safe Harbor Framework's requirements and publicly declare that they do so.

Intralinks adheres to the EU "Safe Harbor" scheme requirements with respect to protection of structured data processed and maintained for clients in Europe. Intralinks' commitment to protecting the confidentiality of client data is reflected in our service contracts and internal confidentiality and security policies.

Certification status is current http://safeharbor.export.gov/companyinfo.aspx?id=24318

Intralinks' current Safe Harbor certification specifically covers personal information (such as contact information) that we collect from our customers within the managed services portal. It does not apply to data that our customers collect and store on their systems within our data centers.

The European Commission's Directive on Data Protection went into effect in October of 1998, and would prohibit the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection.

US Patriot Act

Intralinks must comply with U.S. law. Intralinks has, to date, not been subject to a demand for information under the Patriot Act. However, if Intralinks were to receive such demand, to protect the legitimate interests of its clients and comply with its service agreements, Intralinks would take the following actions:

1) Notify the client (to the extent permitted by law) of any request for disclosure of information
2) Challenge (to the extent legally allowed) any "gag order" to suppress such notification
3) Cooperate with the client to challenge the disclosure of the client's information
4) Cooperate to exhaust all avenues of appeal should an order of disclosure be entered
5) Turn over only that information which is legally required to be disclosed

There has been much debate about the Patriot Act. As a practical matter, however, it will be the rare exception where the government will insist on receiving records without there being a full opportunity to challenge the government request. Despite the expanded powers of the government under new enactments, the practical effect on ordinary businesses has not been great. It is fair to say that U.S. law protects business records from disclosure much as it has for the past 60 years.

Some background information about the law: The Patriot Act amended a number of pre-existing federal laws and made it easier, in some cases, for the government to obtain information connected to investigations of international terrorism and clandestine intelligence. However, in almost all cases, the law allows a demand for information to be challenged in court. Further, in most cases, the recipient of a demand for information (Intralinks) has the right to notify the subject of the demand (our client). Rarely,

the law (specifically the Foreign Intelligence Surveillance Act (FISA) prohibits notification of the demand. (Between 2001 and 2005, only 35 FISA orders were issued.)

Most demands for information under the Patriot Act have taken the form of so-called National Security Letters. These letters apply only to specific types of businesses and types of information (specifically, "electronic communication transactional records"). These letters may be challenged in court on the basis that the recipient, or information sought, falls outside the scope of the law, or that the request is unreasonable, oppressive, or otherwise unlawful. A court may prohibit notification of an NSL request if the government certifies that notification may result in "danger to national security."

The information contained herein does not constitute legal advice and the accuracy of the information is not guaranteed. Companies should consult with their own legal advisors regarding data privacy laws and regulations.

Audit History

We provide an audit history of all activity within an Exchange. The audit trail allows the client to see which user accessed which document (the ID of the file rather than the content), at what time, and on what date. Currently, this audit trail is based and backed-up in the U.S., and is permanently deleted within 30 days of the Exchange's deletion.

Client Audits and Penetration Tests

More than 170 clients have performed independent audits and/or due diligence on our security operations. These were to verify that our operational controls, procedures, and technology meet their stringent security standards. Multiple clients have conducted tests, including network penetration tests and application vulnerability tests.

In addition, we have been subject to dozens of successful audits from pharmaceutical companies for 21 CFR Part 11 compliance (a set of guidelines from the U.S. Food and Drug Administration).

We contract with independent third parties for periodic network penetration and application vulnerability testing of our core platform. In general, our service undergoes network penetration testing bi-annually. We subscribe to a managed security service that conducts continuous application vulnerability testing of production environments.