

LotusLive™ Engage Security

IBM

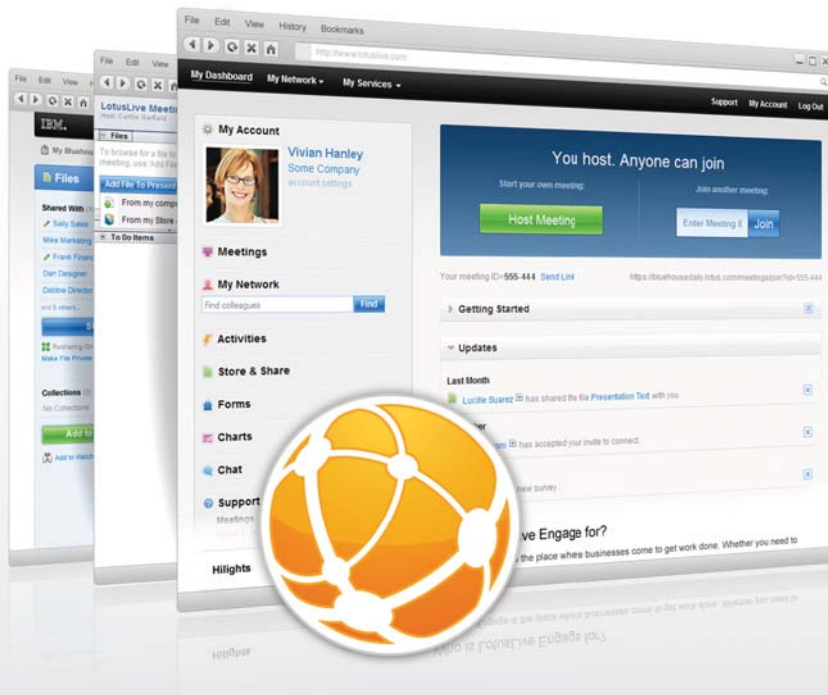
Lotus software

Contents

Introduction	3
Security-rich Infrastructure	4
Policy Enforcement Points Provide Application Security	5
Human Centered Security	8
Future Considerations	9
Conclusion	9



Introduction



LotusLive Engage (<https://www.lotuslive.com/>) provides essential collaboration services, leveraging IBM's unique position as a world-renowned security leader and trusted partner.

Security is a competitive differentiator for LotusLive and LotusLive Engage. Engage's business-ready security is based on a deep understanding of security and privacy best practices, in both IBM and Lotus. Our security controls provide privacy and controlled authorization to sensitive information while enabling business operations. Engage protects our customers' information through governance, tools, technology, techniques, and personnel, each of which we discuss in more detail below.

The LotusLive Engage Security approach is based on three pillars:

- A security-rich infrastructure,
- Policy enforcement points providing application security, and
- Human centered security

These three themes structure our direction, as well as the discussion below.

Security-rich Infrastructure

Physical Infrastructure

LotusLive Engage is deployed in a hardened data center, which provides physical protection to systems and data. The data center is located in Virginia, USA. It uses a myriad of security controls to eliminate or prevent physical access to our systems. Biometric controls are utilized on all physical access points to ensure that only authorized persons have access. CCTV monitoring and recording provides additional protection in the event of an issue. Security officers are on premises 24 hours a day. In addition, the data center utilizes strong fire prevention systems, electrical monitoring systems, earthquake dampers, and solid construction practices to prevent the impact of natural disasters interrupting our services. Power is fed from multiple points in the public power grid and protected with redundant sources.

Systems Infrastructure

Network security is provided by high performance, state-of-the-art firewalls. All client communications are encrypted with 128 bit algorithms, through SSL on HTTP calls, and through RC2 in our Sametime Instant Messaging protocol. System backups leverage 128-bit AES encryption.

Real time Antivirus support services provide on demand scanning capabilities for the LotusLive environment. IBM uses a robust commercial AV product which is deployed not only on the system servers but within the application to provide immediate real time scanning on file storage and sharing.

People and Processes

IBM Online Collaboration Services has a dedicated security organization that provides clear security management activities surrounding the network, infrastructure, applications, and supporting services. It is responsible for the delivery of security capabilities as well as the specification and design of security architecture and compliance management technologies and processes. It defines the security development and testing activities in the organization, and delivers much of the security functionality in LotusLive.

All personnel roles across LotusLive and their access authorizations are recorded in a Separation of Duty matrix. These include system developers, operators, customer support personnel, and other stake holders.

LotusLive is covered by numerous security assurance activities throughout its entire lifecycle. IBM performs quarterly security configuration reviews of all systems and infrastructure. Periodic vulnerability scanning is performed on the network and servers, and there are regular independent application and infrastructure reviews. Rational AppScan testing checks for common web exposures such as cross site scripting, cross site request forgery, and SQL injection. Manual ethical hacking supplements the expertise in the AppScan tool set, targeting the unique application and infrastructure configuration in LotusLive.

IBM compliance programs are deployed throughout the delivery environment. IBM's approach to compliance is multi-layered, with periodic compliance programs that address all elements of the service environment. The system development lifecycle includes code reviews, code control, and accountability. Programs have been established to enable application and infrastructure reviews at the corporate level. Business process based reviews are conducted through the project cycles. IBM compliance programs mandate periodic self assessments and production scanning and reporting of compliance posture. Privacy reviews help to ensure customer data protection. IBM's comprehensive policies on privacy and client data protection can be found at <http://www.ibm.com/privacy/us/en/>.

IBM ensures that the data center and operational processes are consistent with SAS70 Type II controls testing. IBM enforces that all third party services providers are SAS70 Type II certified. IBM is planning SAS70 Type II certification of the service delivery environment.

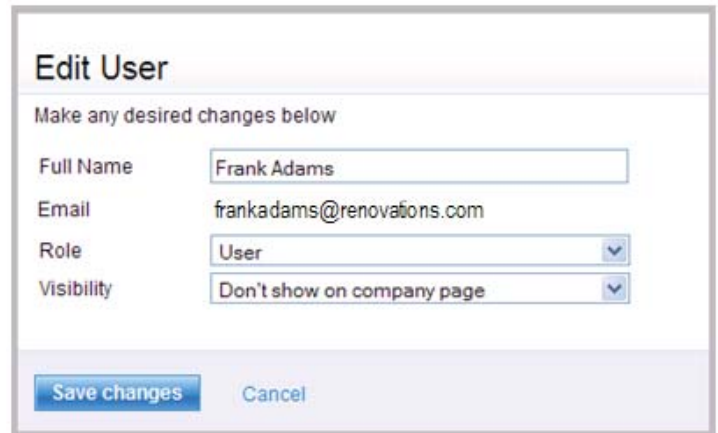
Policy Enforcement Points Provide Application Security

Policy enforcement points in the application, middleware, and infrastructure allow the business customer to better secure their collaboration within and across their organizational boundaries.

LotusLive authentication policy is provided by the widely utilized IBM Tivoli Access Manager software, which provides single sign-on for registered users to all LotusLive components and authenticates those users to each other. Unregistered (and unauthenticated) users may join meetings.

Application level policies are built on the notion of the business organization as an information boundary. Different controls and policies apply within and across organizational boundaries. A directory of subscribers within a specific LotusLive registered organization is available to all the members of that organization (but only to them). This allows every member of the organization to see the names, LotusLive roles, job titles, photos, and email address of every other member of their organization.

Controls are available to both the individual and the organization's administrator to provide security and privacy for identity and personal information of employees in a business social networking context. Individuals or their administrator can opt-out of their information being show to users outside of the organization, through the company's externally facing company page, or through the LotusLive search feature.



Edit User

Make any desired changes below

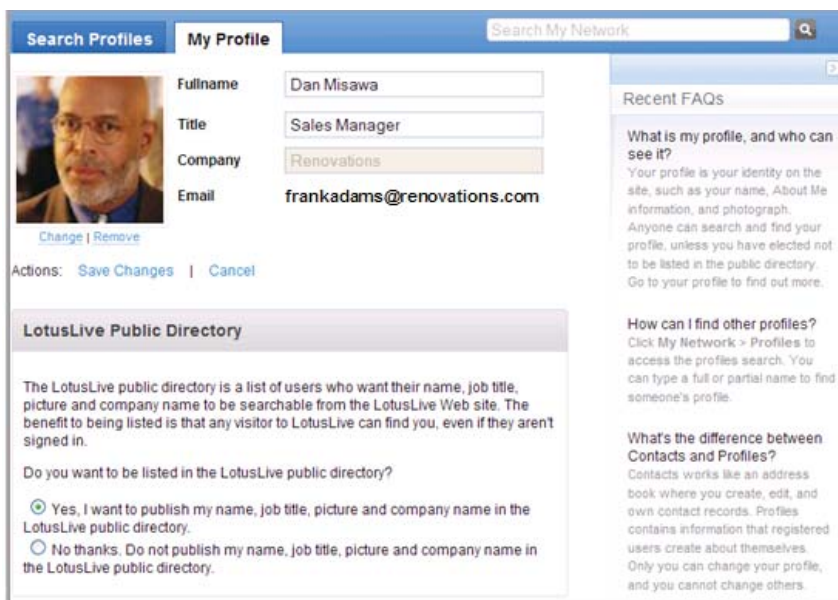
Full Name

Email

Role

Visibility

Figure 1: Administrative protection of user externally facing information



Search Profiles | My Profile | Search My Network

Fullname: Dan Misawa
Title: Sales Manager
Company: Renovations
Email: frankadams@renovations.com

Change | Remove

Actions: Save Changes | Cancel

LotusLive Public Directory

The LotusLive public directory is a list of users who want their name, job title, picture and company name to be searchable from the LotusLive Web site. The benefit to being listed is that any visitor to LotusLive can find you, even if they aren't signed in.

Do you want to be listed in the LotusLive public directory?

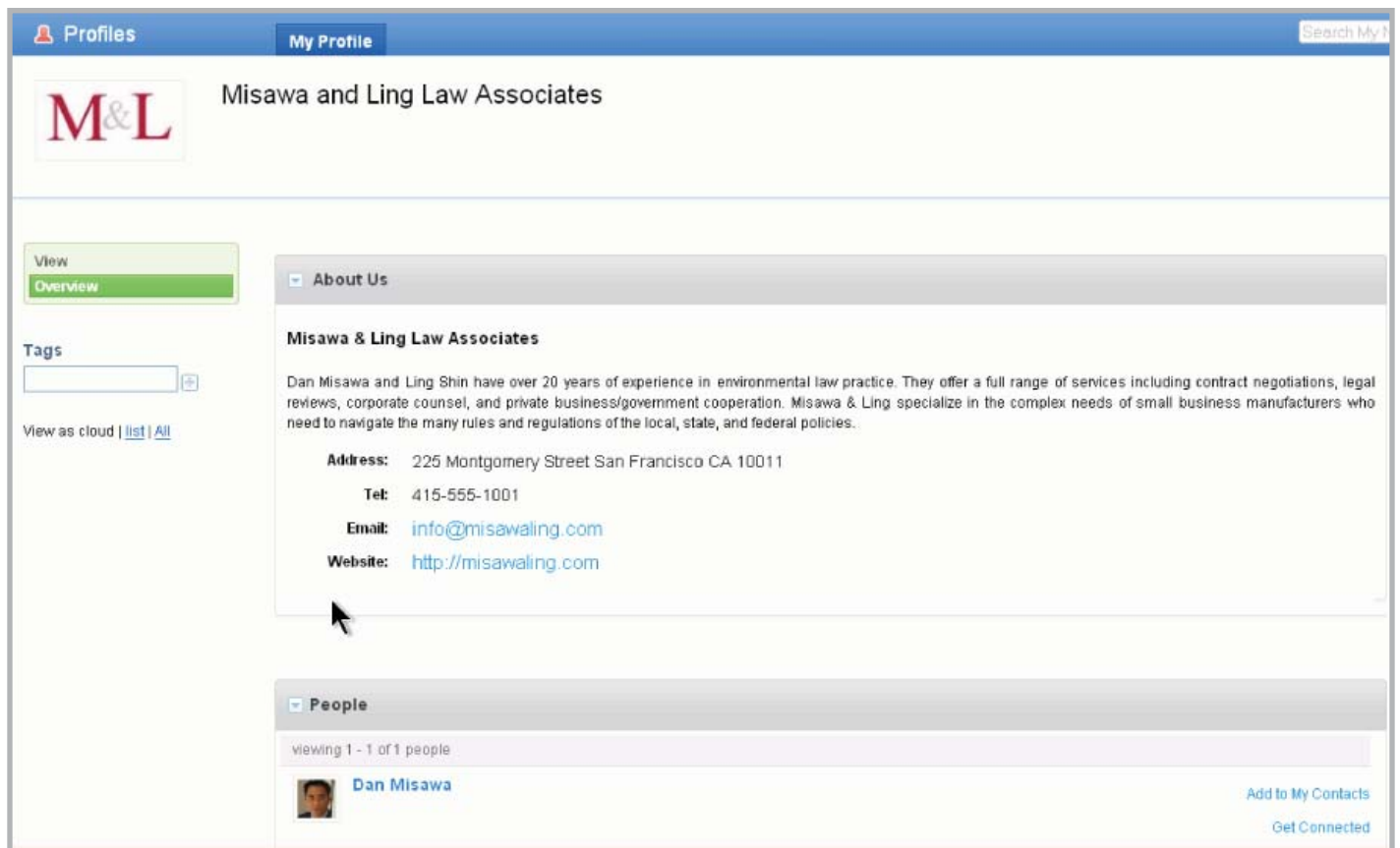
Yes, I want to publish my name, job title, picture and company name in the LotusLive public directory.

No thanks. Do not publish my name, job title, picture and company name in the LotusLive public directory.

Figure 2: User opt out of personal externally facing information.

Policy Enforcement Points Provide Application Security (cont.)

The figure below shows an example of an externally facing company page, and how the users who are included in the company page are represented. Only the user's name, picture, and title are shown in the company page if they are included there.



The screenshot displays a web interface for a company profile. At the top, there is a navigation bar with 'Profiles' and 'My Profile' tabs, and a search box labeled 'Search My 1'. The main header features the company logo 'M&L' and the name 'Misawa and Ling Law Associates'. On the left side, there is a 'View' dropdown menu with 'Overview' selected, a 'Tags' input field, and a 'View as cloud' option with links for 'list' and 'All'. The main content area is divided into two sections: 'About Us' and 'People'. The 'About Us' section contains the company name 'Misawa & Ling Law Associates', a paragraph of text describing their 20+ years of experience in environmental law practice, and contact information: Address: 225 Montgomery Street San Francisco CA 10011, Tel: 415-555-1001, Email: info@misawaling.com, and Website: <http://misawaling.com>. The 'People' section shows 'viewing 1 - 1 of 1 people' and a profile for 'Dan Misawa' with a small profile picture and buttons for 'Add to My Contacts' and 'Get Connected'.

Figure 3: Company page with externally facing user information

Policy Enforcement Points Provide Application Security (cont.)

Email names are treated with particular sensitivity by all LotusLive components, because of their use in contacting and identifying users, and their attractiveness to attackers such as spammers and phishers. A user's email name is only shown to others in the organization through the organization's directory, and to external others only after the user explicitly agrees to "connect" with them. A registered user's email address is their confirmed and verified personal identifier. To complete their LotusLive registration, users prove they control their registered email address by following a URL with a randomly generated nonce sent to that address.

Application level access controls are available on the collaboration data in every Engage component. These controls provide the organization as a fundamental unit of sharing, while also allowing users to share at the individual, group, and/or public level. Public access is restricted to LotusLive registered users, each of which has proven they control access to their registered email address. In the figure below, an additional author is being added to the shared file.

Y Share files

File(s) : GettingStarted.pdf

Share with:

- People/Groups (give specific file permissions to others)
- My Company (visible to everyone in my company)
- Public (visible to anyone)

Permissions: Type in the name of a person or group to give them permissions.

Readers

Authors

Message: (optional)
Frank - please verify that slide 12 is valid - thanks

Share **Cancel**

Figure 4: Adding a user who can update a shared file.

Human Centered Security

The third pillar of LotusLive Engage’s security strategy recognizes that end users make the day to day decisions on what to share and what to protect, based on their best understanding of their responsibilities to their company. Security that is confusing or not understandable by the average user offers little benefit. Security that places unrealistic requirements on user actions will not offer appropriate protection. Engage provides useful and usable security within the context of business collaboration with colleagues, partners, and customers. For example, there is a single view of a file that provides all sharing and upload information, giving the user full information on the security of that file in the context of file use. It shows who a file has been shared with, who has downloaded which version, and what comments have been made on a file. The view also allows actions on the file including changing the sharing and control state, and changing the file itself.

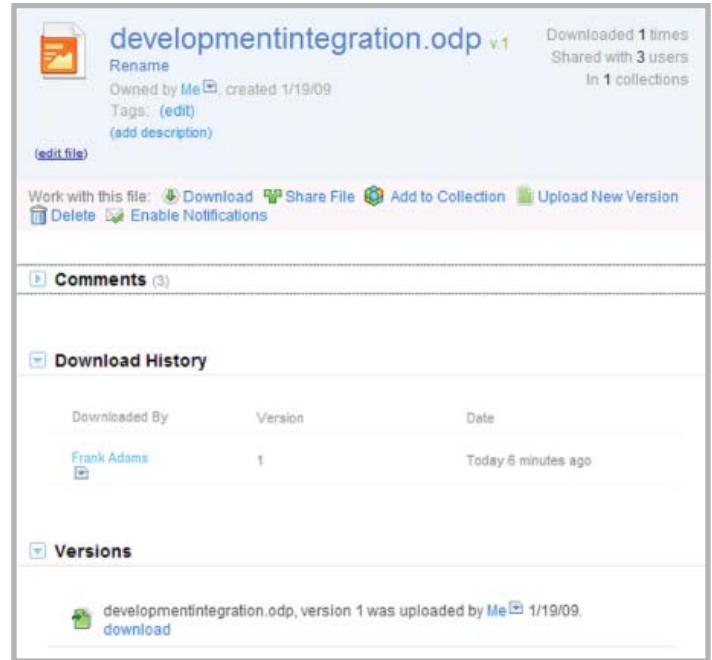


Figure 5: Security, sharing, and history context of a file

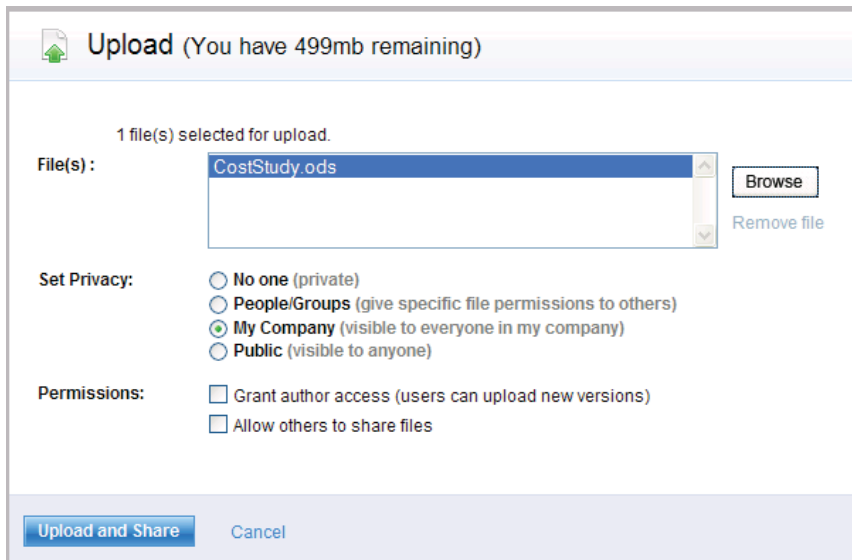


Figure 6: Sharing a file with your company

Transparent feedback and safe defaults within LotusLive ensure user security awareness without intrusiveness. For example, a newly uploaded file is private by default, reducing the potential for mistakenly sharing work in its early stages. In the figure below, the radio button “No One” is always the default during a new file upload. The user sees this default when creating new content, and may change it at any time. In the figure below, the user is choosing to share the newly uploaded file with their organization instead of keeping it private.

Future Considerations

A number of security related features are under active consideration for near term updates to LotusLive Engage.

Some organizations may wish to directly authenticate their members to LotusLive, controlling all aspects of the authentication credentials of their users. Tivoli Federated Identity Manager (TFIM) provides support for service providers such as LotusLive to accept identity assertions from such organizations, using standards based protocols such as SAML and OpenID. Identity integration with partners will also require similar identity synchronization features. Partner integration will also require authorization controls to enable specific applications access to user data at the organizational granularity. OAuth may provide those controls.

Extended compliance and oversight features are also a topic for future considerations. Support for customer-controlled encryption of files and other content is a topic of discussion with the LotusLive partner ecosystem. Extended reporting features may include dashboard views that show the flow of information across organizational boundaries, and integration of the extensive compliance reporting facilities available from Tivoli Compliance InSight Manager (TCIM).

The information on new features or any forward-looking statements in this document is intended to outline our general product direction and should not be relied on in making a purchasing decision. The information on new features to this service is for informational purposes only and may not be incorporated into any contract. The information is also not a commitment, promise, or legal obligation to deliver any material, code or functionality. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

...Extended compliance and oversight features are also a topic for future considerations. Support for customer-controlled encryption of files and other content is a topic of discussion with the LotusLive partner ecosystem.

Conclusion

LotusLive Engage allows users to exchange information and meet online to collaborate without security concerns. Its security approach is based on a security-rich infrastructure, policy enforcement points providing application security, and human centered security. LotusLive Engage draws on security competency centers across IBM, including Software Group, Services, and Research. Our innovation and leadership on cloud collaboration security will continue as we expand on and improve our services.



© Copyright IBM Corporation 2009

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates. The information is provided "as is" without warranty of any kind, express or implied and is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this information. Nothing contained herein is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable agreement governing the use of IBM products or services.

IBM, the IBM logo, Lotus, and LotusLive are trademarks of International Business Machines Corporation in the United States, other countries, or both. Other company, product and service names may be trademarks or service marks of others.