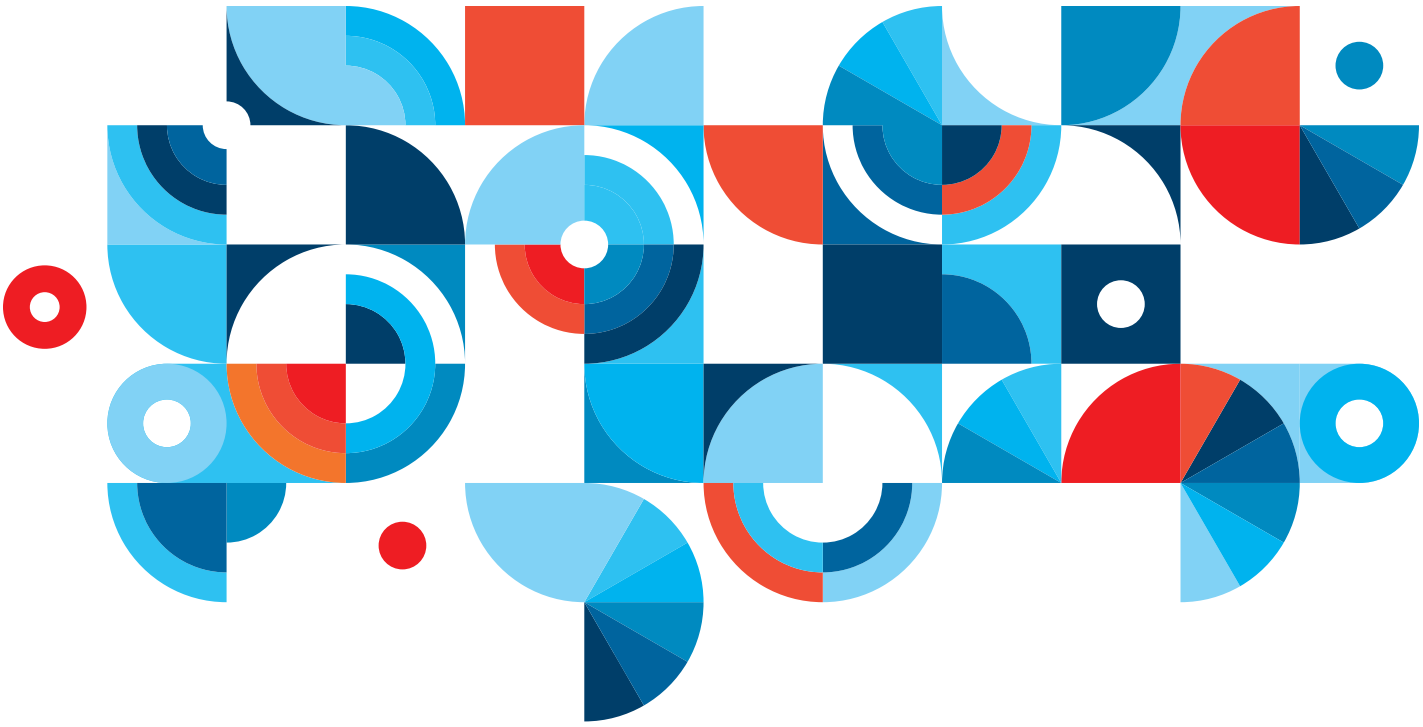
September 2014

IBM Connections Cloud Security



IBM

Contents

Introduction

IBM Connections Cloud (https://www.ibmcloud.com/social) is an integrated suite of collaboration tools that combine your business social network with web conferencing and collaboration capabilities, like file storing and sharing, instant messaging and activity management. IBM Connections Cloud provides essential collaboration services, leveraging IBM's unique position as a world-renowned security leader and trusted partner.

IBM Connections Cloud can be purchased based on a set of service plans that incorporate different capability sets.

This white paper is applicable to IBM Connections Cloud as a whole, regardless of the service bundle. Individual white papers that go into additional details about email specific security features of the SmartCloud Notes and IBM Web Mail Cloud email services are also available.

For up to date information on service plans please visit https://www.ibm.com/cloud-computing/social/us/en/planspricing/

Security is a competitive differentiator for IBM Connections Cloud. Connections Cloud business-ready security is based on a deep understanding of security and privacy best practices developed at IBM over decades of managing data and systems on behalf of IBM and its clients. IBM's security controls provide privacy and controlled authorization to sensitive information while enabling business operations. Connections Cloud protects our customers' information through governance, tools, technology, techniques, and personnel, each of which we discuss in more detail below.

IBM Connections Cloud 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

IBM Connections Cloud is deployed in hardened data centers, which provides physical protection to systems and data. The data centers are located on the east & west coasts of the USA, and in two widely separated locations in Japan. The data centers use 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 centers utilize 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.

Additional guidelines for controlled access areas include:

- Enterprise systems and network infrastructure components providing production services are physically located in controlled access areas.
- LAN management systems, wireless access points and other small servers are located in a locked area when unattended.
- Entry into controlled access areas is prohibited from building areas that are open to the general public.
- The controlled access area is locked, even when attended.
- Slab-to-slab barriers or intrusion detection are used to help deter unauthorized access to the area.
- Access authorization procedures are defined and implemented for controlled areas.
- Persons with authorized access must have a current business requirement for that access. The area owner is expected to determine what constitutes a business requirement.
- Physical access control mechanisms are used to electronically record access to controlled areas.

The area's authorized access list is verified and signed (hard copy or electronic) by the area owner on a regular basis.

- Persons who have had their access authorization revoked, either by request or implicitly through termination of employment, are removed from the access list.
- A current log of non-routine accesses to controlled areas is kept.
- Emergency exits all have audible and monitored alarms which are periodically verified.

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 IBM Connections Cloud 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. The physical architecture is configured with many controls to help protect against denial of service and spam attacks.

Connections Cloud leverages IBM's Information Protection Services (formerly Arsenal Digital) to help provide robust data and systems backup and recovery capabilities. It utilizes a local device to capture and retain backup data and information. Local Backups are performed on a daily basis and replicated to another IBM Data Center, This process is designed to help ensure high availability and recovery services.

People and Processes

IBM Connections Cloud services have 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 Connections Cloud.

All personnel roles across Connections Cloud and their access authorizations are recorded in a Separation of Duty matrix. These include system developers, operators, customer support personnel, and other stake holders. Connections Cloud is covered by numerous security assurance activities throughout its entire lifecycle. The separation of duties matrix is designed to prevent any one individual from having two or more responsibilities or accesses that would allow them to misuse or divert company assets. This covers all business user transactions with the services as well as all administrative support and IT tasks such as development, testing and administration. All staff roles are documented and cross checks are done to ensure there are no conflicts. For example, it ensures that developers have no access to the production environment.

No IBM staff has or requires routine access to client data as part of their job. Under normal operational conditions there is no reason for IBM staff to be viewing client data, and thus access to client data is not provided to IBM staff. The service is designed to support this proactive approach to client data privacy, which is far more effective than relying on after the fact audits to catch violations.

Logs are kept for both IBM Staff and end user actions. Log access is restricted based on the separation of duties matrix. Logs are reviewed regularly for suspicious activity.

The type of information captured in application logs includes:

- Any unauthorized application access attempts
- Any action the user is prevented from performing
- Any customer or subscriber changes

In addition, the data center logs include events such as:

- Successful and unsuccessful logon access attempts
- Activities performed by users with system or security administrative authorities, i.e., privileged users
- For network address management systems, all successful assignment and release of network IP addresses
- At least the following information: date, time, user identifier and type of access attempt or activity

Client administrators can enable and receive daily journals of logged activity for their organization.

Human resources security ensures that employees, contractors and third party users understand their responsibilities and to reduce the risk of theft, fraud or misuse.

- All assignments have documented job descriptions.
- Employees and contractors periodically certify their understanding of the policies regarding business conduct and security requirements.
- An employee's or contractor's employment termination or change in employment within the organization is managed, as is the return of all IBM equipment and the removal of all access rights

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 and targets the unique application and infrastructure configuration in Connections Cloud. IBM compliance programs are deployed throughout the delivery environment. IBM strives to take corrective action for all vulnerabilities detected. Security advisory patches are installed within the time limits specified by IBM using the formal change control process.

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/.

Security by Design

Key to the security of the Connections Cloud are the processes that ensure that security is designed into the product from the start. Connections Cloud has a dedicated security architecture team that is part of the development group, separate from the operational security team. Security reviews are a core, mandatory, element of the design, test and release process.

During the development process a number of automated and manual measures are utilized, which are designed to help catch security or vulnerability issues.

The manual measures are:

1. Cross Site Scripting training to all developers in the team.
2. A Secure Coding check list is created against which each component is checked.
3. Code reviews are held regularly for new functionality.
4. A Security review is performed for every component or major feature of a component to check for any issues that are related to security or privacy in that component
5. Security and Privacy checks are part of the "Go/No Go" check list that has to be done before any build is deployed to production.
6. Any issue highlighted in the 'vulnerability' category of our issue tracking system is subject to special expedited handling.

The automated measures are:

1. Unit tests scan the code during build and check the code is compliant with a secure coding check list. Any compliance issues are flagged and cause the build to fail. Some example checks are non-escaping of html and XSS vulnerabilities.
2. Rational AppScan is used by the test team and is part of the Go/No Go check list for each release.

Connections Cloud utilizes specialist ethical hacking teams from within IBM to carry out full Application Vulnerability Tests. Members of the Connections Cloud team engage in ethical hacking tests as part of the quality assurance process, and an outside third party is also used to provide a periodic independent test of the entire service.

IBM also encourages clients to alert us to any perceived vulnerabilities and provides a reporting link in the Connections Cloud Forum backed up by a formal process to acknowledge and investigate any reported threats and concerns.

Third Party Audit & Certification

IBM ensures that the data center and operational processes are consistent with SSAE 16 (formerly SAS70) controls and are subject to an annual compliance audit conducted by an independent auditor. IBM enforces that all third party services providers are similarly SSAE 16/SAS70 Type II certified. IBM does not permit customer (or customer appointed third party) audits of the facilities.

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. Connections Cloud authentication policy is provided by the widely utilized IBM Tivoli Access Manager software, which provides single sign-on for registered users to all Connections Cloud 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

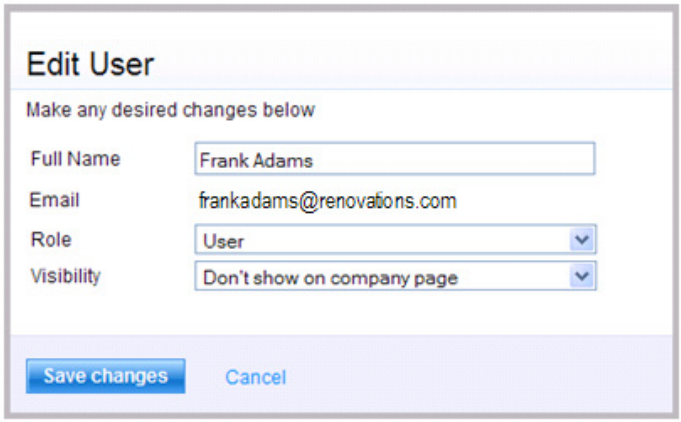


Figure 1: Administrative protection of user externally facing information

organization as an information boundary. Different controls and policies apply within and across organizational boundaries. A directory of subscribers within a specific Connections Cloud 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, Connections Cloud 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 Connections Cloud search feature.

Figure 3 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.

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

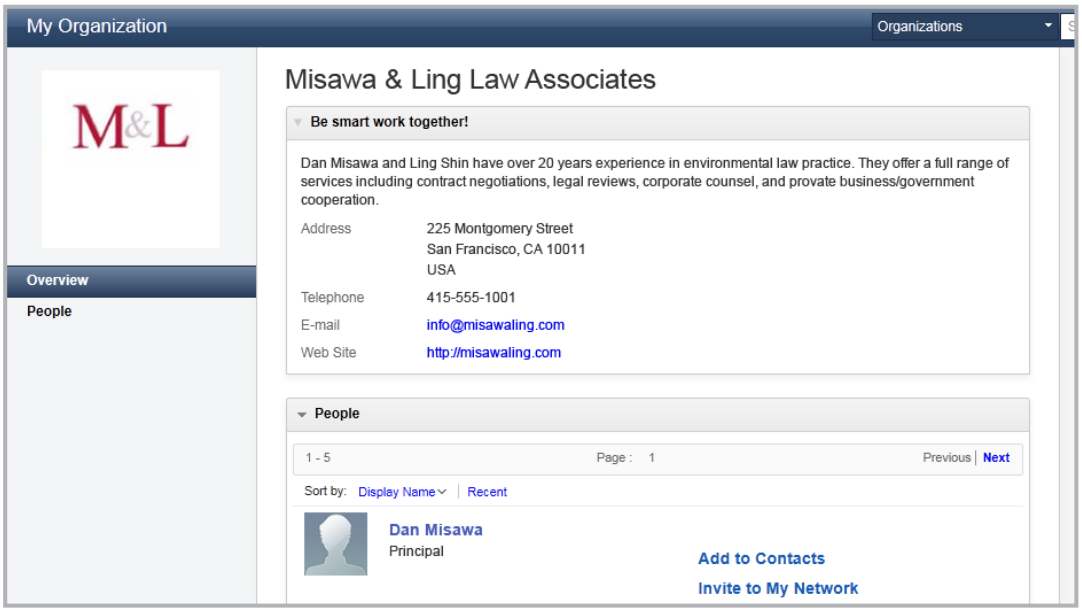


Figure 3: Company page with externally facing user information

Email names are treated with particular sensitivity by all Connections Cloud 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 their own organization through the organization's directory, and to other company's users of Connections Cloud 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 Connections Cloud registration, users prove they control their registered email address by following a URL with a randomly generated nonce sent to that address.

Human Centered Security

The third pillar of the Connections Cloud 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. Connections Cloud 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.

Transparent feedback and safe defaults within Connections Cloud 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 *Figure 5*, the user is choosing to share the newly uploaded file with their organization instead of keeping it private.

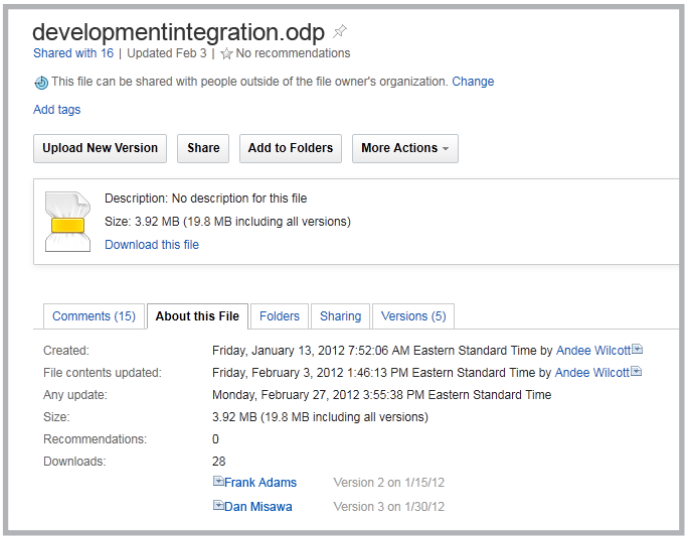


Figure 4: Security, sharing, and history context of a file

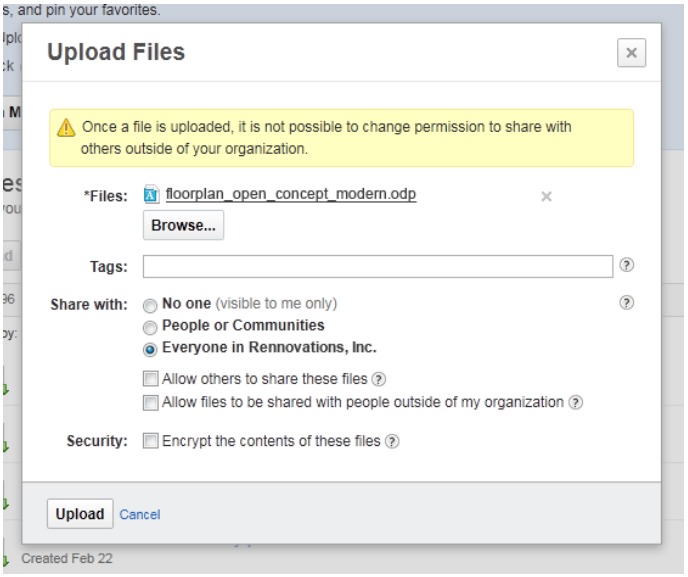


Figure 5: Sharing a file with your company

Application level access controls are available on the collaboration data in every Connections Cloud 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 Connections Cloud registered users, each of which has proven they control access to their registered email address. In *Figure 6*, an additional author is being added to the shared file.

Conclusion

IBM Connections Cloud 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. Connections Cloud 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.

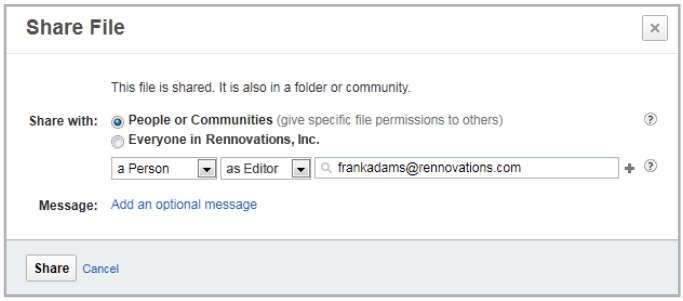


Figure 6: Adding a user who can update a shared file.

IBM Corporation
IBM Software Group
Somers, NY

Produced in the United States of America
September 2014

Please Recycle

LOW14028-USEN-01