iSpring Web Services: Overview of Security Processes

Last updated: November, 2016

Author: Slava Uskov,
VP of Product Development
iSpring Solutions

Notice

This document is provided for informational purposes only. It represents iSpring's current practices of protecting customers' data as of the date of issue of this document, which are subject to change without notice. This document does not create any warranties, representations, contractual commitments, conditions or assurances from iSpring, its affiliates, suppliers or licensors.

Table of Contents

Introduction

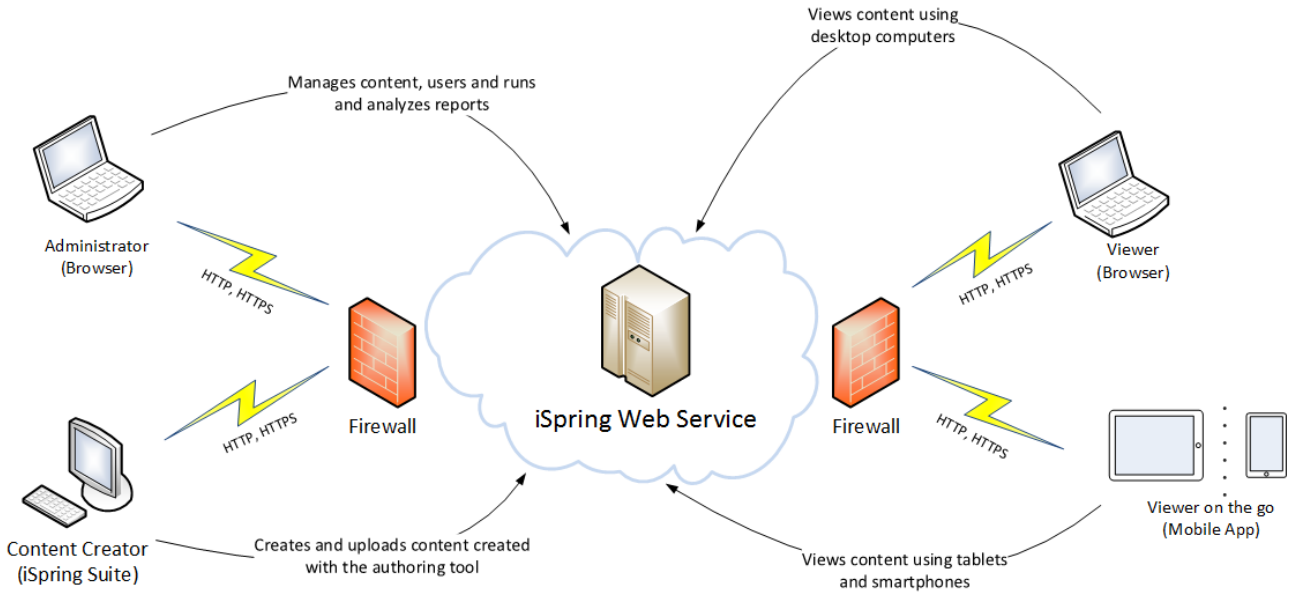
Helping to protect confidentiality, integrity, and availability of our customers' data is of the greatest importance to iSpring, as is maintaining customer trust and confidence. The purpose of this document is to answer the question "How does iSpring help me to protect my data?" Specifically, iSpring physical and operational security processes are described for network and server infrastructure under iSpring control as well as service-specific security implementations.

iSpring Web Services Overview

iSpring provides the following Web Services:

1. iSpring Learn is a hosted Learning Management System (LMS) for teaching and assessing employees or students online.
2. iSpring Cloud is a presentation sharing service that allows to share iSpring content on any device.

Both web services are tightly integrated with iSpring Suite, an eLearning authoring tool, and iSpring's mobile applications.



Secure Design Principles

iSpring Web Services were designed to provide secure hosting of users' personal data and delivery of users' content, databases and analytics over an untrusted network. During the development of the software, security considerations were prevailing over usability concerns.

Secure Facilities

iSpring uses reliable hosting providers with high security standards to run components and services of iSpring Learn LMS and iSpring Cloud. iSpring doesn't rely on a single hosting provider, so it is possible to switch operation from a primary hosting provider to a secondary one in case of any unexpected issues.

We use the following hosting providers for iSpring Web Services:

- Softlayer (SSAE 16 certified)
- Amazon Web Services (ISO 27001 certified)

Our hosting providers restrict physical access to their servers according to SSAE 16 and ISO 27001 standards.

Secure Network

iSpring uses software (operating system level) firewalls which are configured to prevent denial of service (DoS attacks) and log denied connections. All firewalls are configured in a deny mode by default with a few opened ports to allow inbound traffic.

Secure Platform

iSpring Learn and iSpring Cloud servers run on Debian Linux with the latest security patches installed. Penetration tests were performed for all servers and system logs are constantly audited to identify suspicious activity.

Secure Shell (SSH) supports authenticated and encrypted remote log-in access by iSpring staff. Any attempts to get unauthorized access to the servers (e.g. dictionary attacks) are monitored and automatically blocked by the intrusion prevention system.

Monitoring

iSpring utilizes an automated monitoring system to provide high level of service performance and availability. The internal monitoring system performs periodical checks of iSpring Learn and iSpring Cloud components and services to monitor their key operational metrics. Alarms are configured to notify iSpring staff via email, instant messaging (Jabber) and SMS when early warning thresholds of key operational metrics are crossed. An on-call schedule is used to guarantee that personnel are always available to respond to operational issues. Documentation is maintained to aid and inform personnel about handling incidents or issues.

Storage and Backup

iSpring uses continuous data protection instead of regular backups at iSpring Learn LMS and iSpring Cloud to avoid loss of data and interruption of service in case of hardware issues. All iSpring Learn and iSpring Cloud data is redundantly stored in multiple physical locations. It works both for files uploaded by customers and their data stored in databases. However, customers' databases are backed up on a daily basis as well.

Employee Access

iSpring requires that staff with potential access to customer data undergo an extensive background check (as permitted by law) depending on their position and level of data access.

iSpring provides access to iSpring Learn servers or its administration console only to iSpring employees who have legitimate business needs for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if he or she continues to be an iSpring employee of iSpring. All access to iSpring Learn servers by iSpring employees is logged and audited routinely.

Business Continuity Management

iSpring Web Services were designed to tolerate system or hardware failures with minimal customer impact. All iSpring Web Services are deployed in 1+1 configuration, so that in case of failure in the primary data center, there would be an option to re-route traffic to a secondary data center. We use dynamic DNS service with an active failover feature to automatically re-route traffic from a temporary unavailable server to a backup server.

Data Encryption

iSpring Web Services use secure (encrypted) connection where it is possible and doesn't affect the overall performance for end users.

The following types of connections from users to iSpring Web-Services are protected by using a 256-bit SSL/TLS encryption:

- All sensitive data such as passwords, contact and billing information is always transferred over SSL.
- Non-sensitive information is transferred over plain HTTP without encryption by default. If content security is under concern, it is possible to turn on the option **Force HTTPS** that makes all connections SSL encrypted.

Only encrypted connections are used to transfer data between iSpring servers:

- All email messages from iSpring Web Services are sent over TLS.
- Database replication between database servers is performed over SSL.
- All file transfers between storage servers are performed over SSL and SFTP.

Password Policy

iSpring Web Services require that every password to be at least six characters long, contain at least one upper-case letter and at least one number. This requirement helps to prevent accounts from being configured with short, common passwords that are easily compromised with a dictionary attack.

Inactivity Time-outs

A user may walk away from a public PC without logging out and leave a home PC unattended. iSpring Web Services address this type of threat by applying inactivity time-outs. Users are automatically logged out of iSpring Web Services if their connection is inactive for several minutes.

Firewall Compatibility

iSpring Web Services are firewall-friendly. The iSpring Suite authoring tool communicates with iSpring Learn LMS over regular HTTP (port 80) and secure HTTPS (port 443) connection. iSpring Suite generates only outgoing HTTP and HTTPS traffic to ports 80 and 443. Since most firewalls are already configured to permit outgoing Web traffic, users don't need to configure their firewall manually.

Storage Device Decommissioning

iSpring policy implies a decommissioning process for removable media and storage devices. This process is designed to prevent customer data from being exposed to unauthorized individuals. When a storage device reaches the end of its operational life, a specially-trained iSpring employee initiates a decommissioning process for it. iSpring uses the techniques described in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device cannot be decommissioned, it will be degaussed or physically destroyed in accordance with industry-standard practices.

Protecting Customer Privacy

iSpring understands that all enterprises that outsource service delivery are concerned about privacy. iSpring has a strong privacy policy that prohibits unauthorized disclosure of personal or corporate information to any third party.

Disclosure of User's Information

To deliver Web Services, iSpring must collect certain user's personal information including first/last name, email address and account-level passwords. iSpring will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed services by all means. With its clients' consent, iSpring sends service update messages to iSpring Web-Services users to email addresses they provided during registration. More information about iSpring Privacy Policy is available at http://www.ispringsolutions.com/company/policy/privacy.html.

Conclusion

iSpring Web Services are reliable solutions for eLearning authoring, secure delivery, tracking and sharing content. iSpring security processes protect all confidential information from unauthorized disclosure to any third party. Continuous data protection, extensive monitoring and load balancing ensure uninterruptable operating. Usage of state-of-the-art encryption keeps confidential information safe. The fact that iSpring Web Services are firewall-friendly allows integrating this solution seamlessly with any company's existing network and security infrastructure.