Infrastructure and Security

Introduction

ActionStep is a "Cloud" based service meaning that the software and data are centrally hosted and accessed by clients using a web browser and Internet connection. This document is intended to answer questions around the infrastructure, security, and intellectual property rights associated with the software and the data.

ActionStep takes data security very seriously and follows generally-accepted best practices to ensure that clients' data is backed-up and protected against unauthorized access.

Hosting Environments

Except for New Zealand, ActionStep uses the secure Amazon Web Services (AWS) infrastructure to provide a secure and scalable platform to clients around the world. ActionStep clients are generally hosted in the AWS region that meets their data sovereignty and performance requirements. Security specifications can be found on http://aws.amazon.com/security/, and locations at http://aws.amazon.com/about-aws/globalinfrastructure/ .

United Sates and Canada

Clients can choose between the following regions:

- AWS US West 2 (Oregon)
- AWS US East 1 (N. Virginia)

United Kingdom and Europe

AWS EU West 1 (Ireland).

New Zealand

In New Zealand the servers are located in purpose-built high-availability data centres with a Tier II or higher classification. The data centres have 7×24 video surveillance, sophisticated access control policies (for example biometrics and photo ID), fire protection, and power backup.

Australia

AWS AP Southeast 2 (Sydney).

Data Sovereignty

New Zealand clients are hosted at primary and secondary data centres in New Zealand and no hosted information is stored outside of New Zealand. Australian clients can choose have their data hosted in New Zealand or on any of the currently supported AWS regions. Clients in other countries can choose to have their data hosted on one of the currently-supported AWS regions.

Password Policies

ActionStep allows clients to implement password policies by system role. The password policies include the following settings:

- Minimum length
- Inclusion of special characters
- Forced mixed case or numeric content
- Expiry time
- Password rotation minimum
- Time of day and day of week access windows
- Source IP address restrictions

User Permissions

Clients can control who has access to the system by adding and removing logins as required. Each login is associated with a specific system role which governs the access rights to all aspects of the application such as which pages or menu items they can see and whether they can create, view, edit or delete data.

Audit Trails

Audit trails and session logs record user activity and changes made to the data by each user.

Intrusion Detection

The servers run perimeter protection software and log unauthorized attempts to access the systems and add these to blacklists.

Network Layer Security

The networks are split into private (non-routable) and public subnets with a firewall between them. Access to the private subnets can only be achieved over encrypted Virtual Private Network (VPN) links. The public subnets restrict access to HTTP(S) ports only and all other ports are disabled. Password access is disabled for all servers and the only access is via encrypted keys over SSH.

Application Layer Security

All data transmitted between ActionStep and the user is encrypted via HTTPS.

System Administration Procedures

Systems administrators monitor the systems in real-time for any errors or unusual activity and record the events and action taken in an electronic log.

Frequently Asked Questions

Is my data encrypted?

All data transmitted between you and ActionStep are encrypted using SSL.

Can full backups of data be provided as an automatic download?

Yes. You can extract your data to vendor-neutral spreadsheet and HTML formats and documents are provided in their original formats (DOC, XLS, JPEG, etc). You can request a backup whenever you wish by

pressing the "Backup" button in Workflow Admin and providing an encryption password to protect your backup during download. Once the backup is completed you will be emailed a download link.

Alternatively to can arrange to have a dedicated backup to one of your internal servers. ActionStep will send an initial full backup to your server followed by nightly incremental backups. Additional fees apply for this service.

Who owns the intellectual property?

Anything you enter into ActionStep belongs to you. ActionStep owns the core system and any modules or extensions we develop. Data ownership rights are clearly set forth in the Terms of Use – See http://www.actionstep.com/terms.

The intellectual property with respect to workflow configurations and associated document templates are owned by the originator. If a client creates their own custom configurations then these intellectual property rights belong to the client. Configurations can be distributed or sold by the copyright holder if they wish.

Who has access to your data and under what circumstances?

The client has exclusive access to the data via username and password. ActionStep support staff may access client's data for support purposes with the client's permission.

Can ActionStep staff see my password?

No. Passwords are encrypted on the servers. If you forget your password ActionStep can create a new password for you but are not able to see your current password.

If you terminate the service, how is your data returned to you?

You can request a full backup of all your data and documents upon termination of the agreement.

If you terminate the service, what happens to your data on the provider's servers?

ActionStep will remove all data from the servers after termination.

Does the provider have a policy to ensure confidentiality?

Yes. Confidentiality is set forth in the Service Utilization Agreement between the client and ActionStep. ActionStep staff are required to enter into a confidentiality agreement under the terms of their employment.