Act! Products Security and Privacy Overview

July 19, 2023

Contents

Purpose

This document describes the technical and organizational security measures taken by Act! in relation to:

- Act! products
- **Personal data added by end users**, which Act! processes on behalf of its end users as a data processor
    - This is the data added to and stored in a respective end user's Act! database.
- End users' personal data, **which Act! collects from the end user** (its customer) and controls as a data controller
    - This data allows Act! to conduct business with those end users/customers.

This document is to assist **end users** in complying with their internal security requirements and external obligations under regulatory bodies when they contract with Act!.

Act! Product Types

Act! offers two deployment models for its Customer Relationship Management (CRM) products. The physical and technical security measures taken differ for each deployment model.
The deployment models are:

- Act! Premium
    - This model is also referred to as Desktop or Self-Hosted. The Act! Premium product is installed in the end user's environment by the end-user or an Act! Certified Consultant (ACC).
- Act! Premium Cloud
    - This model provides the end user access to their Act! software that is securely hosted on Amazon Web Services (AWS) by Act!.

Act! Premium (Self-hosted or Desktop)

This section highlights key points and considerations when deploying Act! Premium on the end user's internal or local environment/network. Act! Premium can be installed as a Windows desktop/server application or the Web Client can be installed on a web server within the end user's environment or a combination of the two.

Act! Premium Security

The end user's IT team or an ACC is responsible for the installation and configuration of the Act! application and database. Network security, anti-virus protection, and physical security of the database are the responsibility of the end user.

There are in-product security features that can be configured by the end user's IT team, Act! administrator or an ACC. Examples of these in-product security features are:

- Username and passwords
- Definable password policy
- Field-level security (controlling what individual users can see)
- Record-level access (controlling access to specific entities)
- Five security roles (controlling actions a user can perform)

Product updates are available free of charge for those on a current subscription and installed by the end-user or an ACC.

Act! Premium Cloud

This section covers Act! Premium Cloud, our CRM product hosted by Act!.

This model features the Act! product securely hosted on an AWS data center. It is provisioned or configured by the Act! team. All product, database, and operating system updates are performed by Act! at no additional cost to the end users. Database copies or downloads are available to the end user upon request.

General Security of Act! Premium Cloud

All Act! Premium Cloud instances are configured to allow the end user's administrator to take advantage of most of the in-product security features, and those that are not accessible are pre-configured to industry best practices. When the end user's "copy" of Act! is added to the Cloud (Provisioned), all configuration and deployment are fully automated. Use of these automated workflows guarantees all instances are identical allowing for the security and maintenance-related processes described below to function. This entire process has been validated by the SOC 2 audit process.

Data Center Security

Act! selected Amazon Web Services (AWS) as its hosting partner/provider. Act! has a strenuous vendor selection process that has been evaluated as SOC 2 compliant. Information on AWS Data Center Security is available at: https://aws.amazon.com/compliance/data-center/controls/
End user data center location defaults to their region based on their billing zip code or postal code. Act! does not store any of its end users' databases or data at its office locations.

End-User Access to Act! Premium Cloud

When you access Act! Premium Cloud, you do so via a browser on your local device. This means you should ensure this device is secure.

Your device will communicate with Act! Premium Cloud using industry-standard encryption. Currently (July 2023), we support TLS 1.2.

Multi-factor authentication (MFA) can be enabled on Act! Premium Cloud, offering additional security for those desiring it.

Act! Premium Cloud Hosted on Amazon Security

Each end user's Act! database is stored and backed up as an independent database. This means it is not possible for one end user's data to be mixed up with any other end users, or for one end user to access another end user's data.

Each server has an anti-virus solution including End Point protection installed. This solution is updated daily via an automated scheduler. All servers are monitored not only for performance but also for any abnormal activity. In the event this monitoring raises an issue, the Act! DevOps team is alerted. There is an Engineer "on duty" after normal business hours, thereby providing 24/7 response to alerts. Act! monitoring is enhanced by its partnership with Rapid7 (https://www.rapid7.com/). This partnership adds an additional layer of security with 24/7 threat monitoring using state-of-the-art tools and security experts.

End-User Data Privacy and Security

As an Act! Cloud customer, you own the data you store in your Act! Database. Act! does not process it, share it, or access it. Act! provides its end users a hosted Act! database on a controlled and secure hosting platform for their use.

Act! Premium Cloud instances are managed and maintained using the AWS Management Console. Access to this console is limited to carefully screened teams of four or fewer employees. They are monitored daily by a Director-level role or higher. Access to the console is also restricted to logins from the Act! secure internal network or the secure VPN. MFA is enabled on the console as an additional layer of security.

In the event the Act! Support Team is contacted by an end user and database maintenance is required, nearly all tasks are performed using a suite of tools. The use of these tools means the Support Tech never has access to or sees your data.

In the unlikely event of a database issue, the actual database will be accessed. This action will follow a SOC 2-compliant process. First, the end user's support case/ticket is immediately escalated to a select team of screened and monitored employees. Act! employees will not access the end user's database without specific consent from the end user. The consent is then documented.

In summary, no Act! employee can or will access any end-user data outside the support situation mentioned above.

The Act! Global Privacy Policy (https://www.act.com/legal/privacy-policy/) outlines how Act! processes and controls data collected from its end users in order to do business with those end users.

This document, coupled with the SOC 2 Audit Report (NDA required), and the SOC 3 Audit Report (available on request) outlines privacy processes to protect and secure our end users' data hosted on our Cloud product.

Encryption and Availability

End users' data stored in the Act! Premium Cloud Database, as mentioned before, is encrypted in transit to AWS using TLS 1.2. Once in the Act! database, it is encrypted at rest, SHA 256.

End users' databases are backed up using database backups and a server Snapshot at least four times each day. These backups are encrypted and are **not** stored on the same server as the database.

Act! has a SOC 2-compliant Emergency Response Process and Team to provide a framework for resolving any critical or emergency events that could impact its business including Cloud/AWS outages or interruptions. This process, coupled with our SOC 2-compliant Business Continuity Process, provides assurance to our end users that their Act! database is accessible, and they have access to support and other services regardless of events outside of our control.

Conclusion

The Act! Team has dedicated extensive efforts to enhance the security of our Act! Cloud and refine our product. With our reliable backup and maintenance processes, we eliminate the burden of internal IT costs and maintenance for you. This empowers you and your employees to focus on driving success within your organization.

For additional information contact Act! at:
www.act.com
866-873-2006