Alcea Tracking Solutions Security Precautions Document

Public Document – Version 2.1

Contents

Introduction

This document divides the Alcea product offering into two separate components, both of which must be considered with respect to security and maintenance of the entire system. The core process is the proprietary ATS (Alcea Tracking Solutions, formerly FIT) process which runs for all customers. In addition, the server infrastructure is the platform which is used to install the core process and this can be different for customers who license the system and run it on their own server.

Central ATS Process

The Alcea Tracking Solution begins with a proprietary process known as ATS, which runs as a separate process for each customer on a central server. The ATS process mimics a webserver process, which accepts and validates client requests to a central archive of data. ATS installs as a standalone product, using minimal resources. The following optional addons are also common:

Webserver: to minimize the ports running on a server and make use of the existing web ports, Apache2 or IIS is usually used to forward traffic on the server to the ATS process.
Database: If desired, any JDBC compliant database can be used to store data.
Email Server: Email notification requires an email server for outgoing mail.

Audit Trail / Logs

ATS keeps a full, read-only audit trail of time and date stamped entries. These entries show the user that made the change as well as any changes that were made in that entry. It is not possible for users to change the time or date, as it is maintained by the server (with regular checks to make sure that it is correct). ATS also logs administration changes to the system.

Electronic Signatures

Each user is granted a unique username and sets a password which is encrypted and stored on the server. All passwords are encoded using the SHA1 encryption algorithm and safe password options are available in the Server Configuration Security tab, which include:

- Strict password options (enforce length, enforce upper/lower/number/alphanumeric)
- Case sensitive logins
- Enforcement of password changes
- Password resets
- Session timeouts
- Unsuccessful login attempt Limit

Access Levels

As noted above in the audit trail, any change to a record made by a user will show that user's unique ID. ATS is structured so that you can create groups to only grant access of data to specific individuals. Using Groups, Field Controls, Workflow and or Tracks, you can successfully shield information from any sets of individuals in your system. This can take the form of groups within an organization or for limiting the data available to specific customers or clients.

Generally, our system uses groups to separate access levels for users. A user can be assigned to more than one group. There is no concept of roles in our system, but the group functionality should handle any access configuration needed. Groups and field controls can be used to make fields read/write, read only, hidden or required (i.e. must be filled out before changes can be saved).

Software Certification

Our software has not been certified by any third party at this point. We are happy to share the cost if this is necessary. Many large organizations have been using the software for years with no issues. Although we have no certification, our software is written to store a full history of all changes to the system and we believe it to be ISO compliant.

Server Infrastructure

The ATS process requires minimal resources and runs as a Java application on any sever which will run a Java Virtual Machine. Typically, the base infrastructure should include a quad-core server running Linux or Windows, with 100G of space and 8G RAM as a starting point. Resources can be increased over time if needed depending on number of tickets and size of attachments. Our ATS product can be licensed and installed locally at a company, or hosted with our experienced support team.

Encryption and Integrity

The hosted option offers a safe and secure infrastructure which can be configured and monitored by our team, allowing us to handle updates and maintenance. Our hosted servers are housed at IBM Softlayer (recently renamed to IBM Bluemix). Currently, we offer data centers in Toronto, Dallas and London but they also offer other fully audited facilities worldwide. IBM is a reputable company with a commitment to excellence and offers compliance to all major standards (SOC 1/2/3, ISO27001, CSA, PCI, HIPAA, ..) : https://www.ibm.com/cloud/compliance

Encryption in Transit is a standard configuration. The ATS application provides a secure DigiCert SHA2 Secure Server SSL certificate, which provides full 256 bit encryption between client and server.
Encryption at rest is an option available where we encrypt the storage drives on newer machines. This option requires an alternate backup setup due to encryption, noted in backup section.
ATS offers all major email notification security standards as part of the Java Mail framework.

Access Controls

Machines are dedicated completely to ATS customers
Limited access to hosted servers with client data
Controlled SSH access with no direct root access
Firewalls configured on all machines
Our employees are required to maintain both anti-virus and malware software on their direct machines.
Access logs from firewalls are kept for 30 days
Embargoed countries are blocked as part of Softlayer infrastructure.
All traffic to servers and ATS instances is logged on a server and application basis.
Options for AD/LDAP authentication and SAML/ADFS/OCTA session management

Maintenance and Monitoring

Hosted Servers run on Debian Linux and regular patches are done on a monthly basis or as they become available. Clients are not permitted on the systems, so virus threats not a major concern, since it is only our software running other than the OS.
Alcea runs a Nagios server for continuous reporting of server availability, disk requirements and instance availability. Availability of each server is also monitored as part of the Softlayer network.

Confidentiality and Privacy

SoftLayer maintains hardware in state of the art facilities and take confidentiality extremely seriously: http://www.softlayer.com/privacy-agreement

Hosted servers are maintained by employees at Alcea Technologies. All our employees are screened and have Secret Security Clearance with the Canadian Government. Alcea is conscious of the need for privacy with your data and would never share the information with any external party. All employees are bound to confidentiality agreements. Additional information is available in our company privacy document, which all employees must follow.

Related Private Document: Alcea Tracking Solutions Privacy Document

Availability

SoftLayer offers an industry best 100% Network Uptime Guarantee.

Our application support personnel are available by email support and offer immediate response to any urgent helpdesk tickets (24 hour online paging service for urgent requests).
Please discuss if any specific arrangements are necessary. We are happy to work with our customers to guarantee they are happy with the service.

Backups

Most hosted systems are backed up to a second location on an hourly basis, using Idera r1soft software with the following policies:

One for each of the last 24 hours (hourly)
One for each of last 4 nights (midnight)
One for each of last 4 weeks (weekend)

Encrypted Drives: Although R1soft can encrypt regular backups, it does not support backups of encrypted drives. Therefore, if encrypted drives are requested, an alternate rsync backup will be performed daily and weekly (between encrypted drives on separate machines), rather than the r1soft solution.

Related Private Document: Alcea Backups and Disaster Recovery

Development and Testing

Our developers are very familiar with the systems and strive to test their code changes as best they can before be submitting their changes to the code stream. In addition, our development environment includes continuous and immediate unit testing for all code changes before builds are created.
Before a build is added to our website, it undergoes extensive testing on our internal systems (which we use internally) and we also use our TestSpec module where we have built a substantial list of test cases to be run manually.

Vulnerability Management

All employees are required to run Anti-Malware software (Malwarebytes) in addition to anti-virus software (Windows Defender / Mcafee Total Protection)

Scans of hosted machines is done daily. More details in Sandboxing section.

OWASP is defined as an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. It's mandate is to "provide unbiased, practical, cost-effective information about application security".

As of January 2018, Alcea Technologies has educated our development staff on the benefits of learning OWASP Principles and Proactive Controls. In addition, we have started to conduct quarterly tests of our software, using OWASP tools, starting with OWASP ZAP:

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Common Vulnerabilities Tested by ZAP include the following:

- Cross Site Scripting Attacks
- Injection Attacks

Alcea is open to work with any third-party testers as required.

Vulnerability Sandboxing Configuration

Although regular scans of files on a system is imperative, it is not a complete solution because ATS allows users to upload files with tickets.

The sandboxing feature can be configured to protect users from files that have not yet been scanned. When this feature is configured, any new attachment is flagged in a sandbox state, until it is scanned by a separate scanning process.

Configuration of the sandbox feature with the following two config variables in the base track:

- FILESCANNING:

  Setting to value of “1” will turn the feature on.

- sFileScanningCommand
  This string is used to define the external command line scan which can be called from ATS as an On Demand scan. ATS will substitute the name of the attachment file for the text INFILE and scan the output of this command for the text in the third custom string sFileScanningConfirmText detailed below. The command line should include a move attribute which moves infected files to an existing FITQUARANTINE directory.

  Mcafee Example Setting: c:/scan/scan.exe INFILE /MOVE "FITQUARANTINE"

  Clamscan Example Setting: clamscan INFILE --move=FITQUARANTINE

- sFileScanningConfirmText:

  ATS will search the on demand command output for this string to verify that the scan was clean. ClamScan Example Setting: “Infected files: 0”

  Mcafee Example Setting : “Clean:..... 1”

Additional Documentation

Alcea has taken steps to guard against intruders and malicious activity. The following private documents have been compiled for internal staff as contingencies in the event of an unforeseen event. Some of the information in these documents is private, so we do not offer it to the general public but like you to know that we are ready to act if needed.

Alcea Data Breach Action Plan: Outlines the steps to be followed by Alcea in the event of a customer data breach.

Alcea Backups and Disaster Recovery: Outlines the steps required to bring a customer system online from a backup location.