
## Issue and Defect Tracking
**For professional development teams**

# Admini*Track* Security Statement

**www.AdminiTrack.com**

Last updated on September 8, 2016

# Admini*Track*

## Issue and Defect Tracking for Professional Software Development Teams

***By AdminiTrack, Inc., Atlanta, GA USA***

*AdminiTrack is a web-based,hosted application for software development teams that permits developers, quality assurance testers, project managers, business sponsors and other staff to share vital project information quickly and easily from anywhere in the world. Local applications installed on your network are too limiting when your team members, users and customers may be in multiple locations and need information now, not later.*

*The application is hosted by AdminiTrack.com in a state-of-the-art data center so all of the implementation, database design, internet access, maintenance and security have been taken care of for you. All you have to do is setup your users and projects and start sharing vital information about your project. AdminiTrack was designed to be fast and easy to use, yet provide all the features you would expect in a premier application.*

*Find out what others already have known…from small consulting companies to Fortune 500 companies around the world. AdminiTrack is the cost effective solution that no software development project should be without.*

# AdminiTrack Security Statement

# Table of Contents

## 1.1 Purpose

This document is intended to provide basic security information for current and prospective customers/subscribers of the AdminiTrack Issue and Defect Tracking application. Some details cannot be provided for security reasons. Contact AdminiTrack at support@adminitrack.com if you have specific questions or concerns not addressed in this document.

## 1.2 Company Background

AdminiTrack is privately held company which was co-founded in 2000 by technology industry experts (Don Draper and Krishen Kota) who have a combined 35+ years of experience in information technology and enterprise computing within the corporate and government agency environments.

Development on AdminiTrack started in 1999. The company was incorporated in 2000 (Atlanta, Georgia, USA - Georgia Secretary of State control#: 0052529), and the AdminiTrack Issue Tracking system went live in mid-2001. AdminiTrack is a privately held and profitable corporation that has consistently grown its customer base since the system went live. The company's success has been based on providing a powerful, yet easy-to-learn web-based application backed by responsive customer support. AdminiTrack currently serves customers in over 22 different countries.

AdminiTrack takes security very seriously and employs industry standard processes and practices to ensure customers' data are safe. AdminiTrack hosts the issue and defect tracking system for Global 1000 companies around the world.

Unlike its competitors, AdminiTrack does not advertise or disclose its customers' identities in order to provide an additional layer of protection. We feel that while advertising our more prominent customers would bring us more business, it could also make us a target for adversarial persons or groups seeking to gain access to our customer's knowledge base. Select customer references can be provided upon request and are available only through the express written consent of those customers.

While no system is completely safe from attack, AdminiTrack employs all industry standard techniques to safeguard our systems and your data. We take security very seriously.

## 1.3 Data Center Security

AdminiTrack operates in a state-of-the-art data center (www.qualitytech.com, formerly www.edeltacom.com) located in Atlanta, GA. This is a 376,000 sq. ft. unmarked facility employing around-the-clock security and technology personnel. Security features for this data center include but are not limited to:

- The building is unmarked with no signage.
- Hidden physical barriers provide physical protection to the building.
- Physical check-in by security personnel 24 hours per day required to reach data center floor.
- Electronic badge access is required to access the data center floor.
- Three biometrically protected check points utilizing both finger-print and retinal scan technology must be passed to reach data center floor.
- Employs multiple, redundant Internet access feeds from multiple providers.
- Employs dual power feeds from Georgia Power with the ability to keep power to our systems up for weeks in the unlikely event of a massive power loss. This is done using underground flywheel power generation and advanced power-systems technology.

Many other well-known companies have hosted systems at this same facility including Google.

## 1.4 Corporate Security

Due to AdminiTrack's tightly focused, high-quality offering, all staff members are rigorously screened and background verified. In addition, each staff member signs a non-disclosure agreement (NDA) in regards to corporate and customer data. All AdminiTrack technical staff members are considered among the best and most talented in their respective areas of expertise.

AdminiTrack also follows and implements the security standards of the Payment Card Industry (PCI) Data Security Standards. While these standards are targeted toward online payment systems, the security recommendations are excellent covering a broad spectrum of best practices. These standards are supported by many respected industry leaders including Symantec, Verisign, GeoTrust Inc. and Authorize.net.

AdminiTrack is *GeoTrust Secured*™ site and an *Authorize.net Verified*™ merchant.

## 1.5 Systems Security

AdminiTrack employs industry standard security software and hardware at various levels throughout our network.

### 1.5.1 Network, Anti-Intrusion and Virus Scanning

For network security, we run behind advanced, redundant firewalls along with hardware and software based anti-intrusion detection systems to monitor and pro-actively protect our systems that must communicate directly with the Internet. All of our systems stay updated on current security patches and security audits are

routinely run to ensure no gaps have opened up.

Both anti-intrusion and virus scanning are deployed at our network edge (security appliances), in our SMTP email servers and again at each server. This approach provides us with multiple layers of protection and added intrusion detection capability.

AdminiTrack utilizes Virtual Private Networking (VPN) for all access to our systems by corporate personnel. This is an industry standard technique utilizing high-levels of encryption and data security to protect against data packet sniffing and other public wire techniques to obtain data. All access using our VPN requires internal software, is passcode protected and fully logged by user identity.

Secure data access to the AdminiTrack application is always enforced by default. Traffic between your clients and our servers is always encrypted using 128-bit secure sockets (SSL), an industry standard form of in-transit encryption security. Non-secure traffic is never allowed.

All customer data is stored in an enterprise SQL server database including attachments which are uploaded as documents either to a project or to an issue. No data is accessible from the file system which provides another level of protection.

Access to the AdminiTrack application is logged at multiple levels including web servers, database servers, anti-intrusion systems, email systems, and public facing firewalls including VPN access. Application user logins are logged including source login credentials, source IP, User Agent and more. Logs are periodically reviewed for any signs of inappropriate use and any suspicious users may be blocked at the firewalls and servers by IP address or by user account or both.

The AdminiTrack Issue Tracking application employs anti-hammering against the login form preventing brute-force guessing of passcodes. Once a specific number of failed attempts are detected, the user is automatically locked out for specified amount of time and technical staff notified.

In 2013, AdminiTrack increased our requirements for passcodes for additional security. Users with passcodes that did not meet the new requirements were forced to create a new passcode that did meet the new standard before being allowed access. New and changed passcodes must meet the new minimal standard.

Our code uses parameterization for passing variables to our database and all scripts are searched and examined for any scripting that might be susceptible to SQL injection and are corrected before being applied to production systems. Our development team is constantly made aware of state-of-the-art techniques used to keep software safe from outside intrusion.

The application forces the user of secure cookies (HTTPS) as well as other techniques to prevent cross-site scripting. This along with other software settings aid in preventing malign-based scripting attacks.

Sensitive customer data such as billing names, credit card numbers, passcodes, etc. is stored in encrypted format using 256-bit AES encryption.

AdminiTrack reserves the right to block any known entities that we feel may be inappropriately using the system. Our systems are monitored around the clock from both onsite and offsite locations with manned and automated notifications to engineers should a problem occur. Physical access to our systems is limited to a small number of engineers who monitor and maintain them.

## 1.5.2 Delineation of Customer Data across Accounts

Customer account data is delineated from each other by an account number that is assigned to each customer account. This number is stored inside a cookie to populate the login form and assist users when logging into the system but is never passed to the application except while logging into the application where all credentials including passcode are required. Once a user has successfully logged into the application with proper credentials (three items are required), the account number is maintained only in session state on the server. This technique makes it impossible for someone to pass a known account number in an attempt to gain access to another account. This is an industry standard technique employed by nearly all online systems including banking, commerce and more.

## 1.5.3 Customer Data Backups

Data is maintained on redundant servers utilizing RAID drives and backed up to hot backup servers in real-time. AdminiTrack maintains multiple backup copies of production data locally in the same, secure facility. Full backups are copied to external provider storage weekly. In addition, we ship logs of data up to 4 times per hour to and off-site location for disaster recovery purposes. All communication to off-site providers is performed using industry standard encrypted communications.

After an account is closed, Customer data is held for up to 3 months unless the customer requires that the data be destroyed immediately. Customers may export their own issue and comment/history data on demand in CSV or XLSX (spreadsheet) format. In addition, we can export this data in an automated fashion for customers that require this.

**Drive Redundancy with RAID**

The RAID concept (Redundant Array of Inexpensive Disks) permits data to be written to multiple, physical hard-disks platters at the same time. This redundancy provides protection in the event that a hard-disk failure occurs. The moment a hard-disk fails inside the array, another hard-disk drive known as a hot-spare immediately gets a copy of the data from the remaining good drive. Once the hot-spare has been created, the redundancy is restored and the engineers are alerted that the hot-spare drive needs to be replaced.

We employ RAID-6 based SAN devices (Storage Area Network) for our servers so that they may share data. This is required for our Virtualized software.

### Server Redundancy with Hot-Backup Servers

AdminiTrack maintains a hot-backup server for each production server. The hot-backup server is a mirror image of the production server in most respects. Customer data is periodically shipped (copied) from the production server to the hot-backup server so that the hot-backup server is never more than a few minutes behind. In the advent of a catastrophic failure of a production server, the hot-backup server can be brought online and used to replace the failed server. This is another way that AdminiTrack provides redundancy of customer data and provides for minimal down-time in the advent of serious server failure.

### Off-site Data Storage

All customer data is periodically backed up and moved off-site by AdminiTrack personnel at regular intervals. Several days worth of backups for issue data is maintained onsite and this data is periodically removed offsite to prevent a total loss of data should the data center be compromised. As mentioned previously, this data is also shipped off-site to an alternate service provide (AWS) for disaster recovery purposes. Data transmitted in this fashion is also protected through industry SSL encryption.

### Security Audits and Review

AdminiTrack performs annual security audits and bi-annual reviews. Prior to 2013 our security audits were handled internally on an annual basis with an exception being when any new technology or hardware was introduced. In 2013, an exhaustive security-audit was performed by an external entity as part of our upgraded deployment platform. Any issues brought to light were addressed and the audit was closed as successful. We continue to self-audit annually and perform security/educational reviews bi-annually.

### Virtualization

AdminiTrack employs virtualized servers (VM) using VMWare. This allows us to several servers on a single, physical machine. The technology also allows us to perform snapshots (point-in-time recovery) and backups of virtualized machines that may be recovered much more quickly than standard backups. Also, this allows virtual servers to be moved across physical servers without any interruption to customer service. Using this technology, AdminiTrack is working towards never having to schedule maintenance windows and increasing up-time.

## 1.6 Uptime and Availability

AdminiTrack does not require contracts as accounts may be canceled at any time. AdminiTrack can offer a Service Level Agreement (SLA) for customers that require one and purchase 6 months or 1 year of service in advance. Contact support@adminitrack for further information regarding this subject.

AdminiTrack guarantees a level of uptime and availability to the subscribers. Uptime is defined as the ability of an active user in the Subscriber’s account to login into the

AdminiTrack application and access account data. AdminiTrack, Inc. guarantees an uptime of 99% over the period of any calendar month excluding scheduled downtime for maintenance or upgrades. AdminiTrack has not been off-line for more than three hours (excluding scheduled maintenance) since going online in 2001.

While no system can guarantee complete protection, AdminiTrack takes security seriously and employs every possible solution to ensure data protection, redundancy and availability.

## 1.7 Customer Responsibility

The following are recommended security procedures for our customers to follow. Since the majority of data security breaches occur from within an organization, the customer shares the responsibility in keeping their data safe.

- Use the term *passcode* rather than *password* to remind users that words should never be used in passwords.
- Create a passcode policy if one is not already in place. (see below)
- Use the "Generate Passcode" button when creating new users for your AdminiTrack account. This generates a random passcode of both letters and numbers and the user may change this later if needed.
- Contact AdminiTrack immediately if you feel your account has been compromised in any way.

### 1.7.1 Sample Passcode Policy

The following items are examples policy rules that could serve in a corporate policy statement concerning the creation and use of passcodes. Note that AdminiTrack enforces a minimum standard requiring mixed-case and one or more numeric values in passcodes.

- Use of both upper-case and lower-case letters (case sensitivity).
- Use acronyms or the first letter of words in a phrase as part of your passcode.
- Inclusion of one or more numerical digits or non-alphanumeric characters.
- Inclusion of special characters in a passcode.
- Prohibit the inclusion of words found in a dictionary or crackers list.
- Prohibit passcodes that are valid calendar dates or license plate numbers.
- Never share a computer account with another user.
- Never use the same passcode for more than one account.
- Never tell a passcode to anyone, including people who claim to be from customer service or security.
- Never write down a passcode; if you cannot remember, do not use it.
- Be careful to log off before leaving a computer unattended.
- Change passcodes whenever there is suspicion they may have been compromised.

## 1.7.2 Controlling Application Sessions

AdminiTrack is the type of application where several minutes to hours may pass between accesses during a normal work day. Because session states on most servers will expire after a few minutes without activity, most web-based applications force the user to login again and again throughout the day which can become quite annoying and time-consuming.

The AdminiTrack application has a special feature that allows users to maintain their session state as long as they are logged into the application and the browser has not been closed. This allows users to work in the application without being forced to repeatedly log into the application if a period of time has lapsed. Regardless of whether this feature is enabled or not, logging out of the application or closing the browser will force a user to re-login again to access the application. Because of this, AdminiTrack encourages users *to always logout of the application* anytime they leave their desk. For added security, the browser should be closed as well. Session will expire after 24 hours so most users are forced to sign-in daily at a minimum. This is standard and used by industry leaders such as Amazon Web Services (AWS).

Note: This feature may be disabled by un-checking the "Disable Auto Logoff" checkbox on the application login form. This option should be used anytime a user is connecting to a publically accessible computer such as a library or computer access facility.