Security Matters

AMmobile
Your mobile solution for AccountMate

User Security

Each installation of AMmobile must be authorized for use by an administrator within AccountMate. If AMmobile is uninstalled then re-installed at a later time, the new installation must be re-authorized. AMmobile users are separate from AccountMate users, giving you the ability to set up separate user rights as well as AccountMate only users and AMmobile only users. Users can be restricted to have access to only certain companies. Failed login attempts are logged and tracked. Too many failed login attempts, and the user and the device are automatically locked until unlocked by an administrator. AMmobile employs an auto-timeout feature that automatically logs the user out of the app after a pre-specified time of inactivity.

Data Security

The database file is stored in an encrypted format on disk and cannot be read from or written to while the device is locked or booting. User's passwords are not stored on the device. Customer Credit card numbers are not stored on the device, nor are they transmitted to the server. Credit card numbers are only transmitted directly to Authorize.net using Authorize.net's own Application Programming Interface (API) and Software Development Kit (SDK). To see how you can better secure your company's iPads, go to http://bit.ly/securitymatters.

Network Security

AMmobile transmits all data over the https:// protocol, creating a secure socket in which to transmit data. An added layer of security can be added by purchasing a verified SSL certificate from a trusted certificate authority. Even more security can be added by connecting to your company's VPN using the iPad's built in VPN feature.

Contact your AccountMate® Solution Provider today for more information!

www.AMmobile.net • Lisa@AMmobile.net • (760) 247-0644