MobileTrust®

General Information

This General Information section explains the MobileTrust® technology, how it is used, and the purpose for which it is intended.

System Overview

MobileTrust® is an application for mobile devices, such as compatible Android devices, which improves operational security in a multitude of ways. MobileTrust® can launch a securely encrypted mobile browser, a password vault for securely storing any number of login credentials for websites, a one time password (OTP) engine, and a customizable secure password generator. The MobileTrust® app utilizes a system-wide encrypted keyboard which fortifies operational system security both inside and outside of the MobileTrust® app.

System Requirements

The MobileTrust® app is compatible with Android devices running Android 4.0 (and higher versions). Internet connection is required for certain MobileTrust® features to function properly, such as its secure encrypted mobile browser.

User Access Levels

Only registered users can use this application to add, change, and/or delete data to and from its database.

Getting Started

This Getting Started section explains how to install the MobileTrust® app on a compatible Android device.

Installation

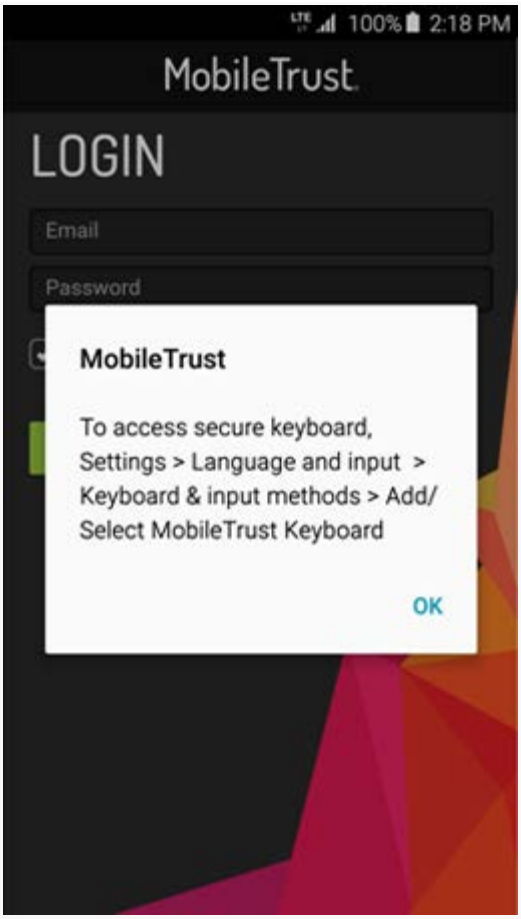
Users can find the MobileTrust® app by searching "MobileTrust" in the Play Store for Android devices. For information regarding how to install an app on a compatible Android device, refer to the specific device's user guide.

Note- In order to access the MobileTrust® app and its features, you must have active login credentials with an up to date software license.

First Launch & Login

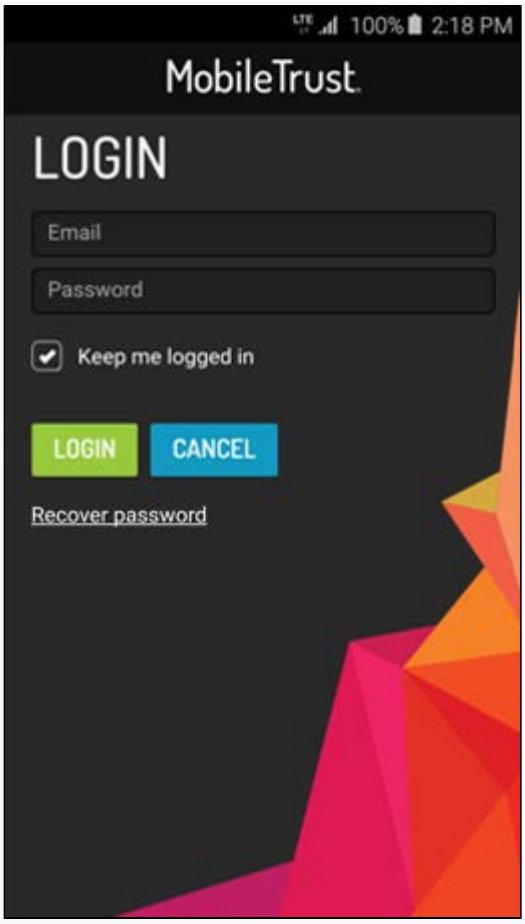
After installing the MobileTrust® app, you will be greeted with the following splash screen when opening the app:

You will then be prompted with the following window which explains how to enable the MobileTrust® secure encrypted keyboard on your Android device:



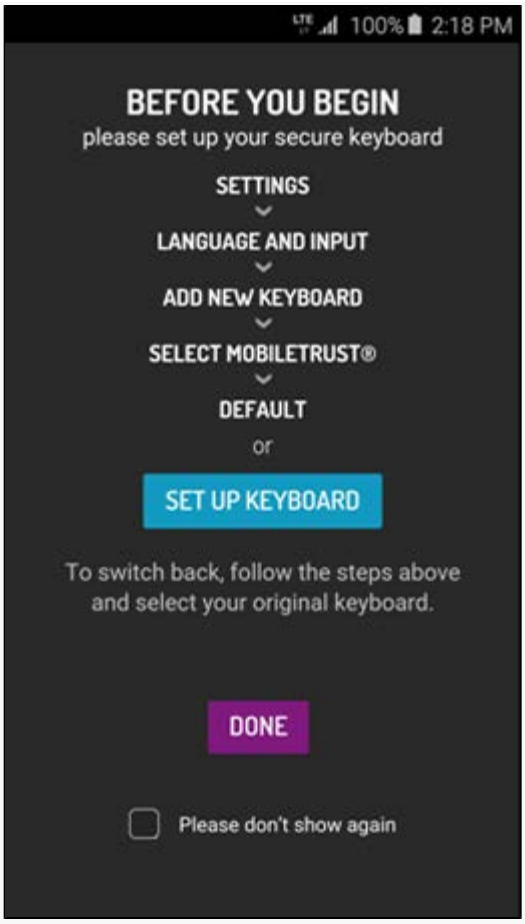
Login Screen

In the "Email" text field, enter the email address you registered when subscribing to the MobileTrust® Mobile Protection Service. In the "Password" text field, enter the password you created when signing up for the MobileTrust® Mobile Protection Service. You may now tick the box that indicates "Keep me logged in" if you would like to save your login credentials and have the app automatically log you in next time. If you do not remember your password, you may click the "Recover Password" link on this page to be guided through resetting your password. You may now press "Login":

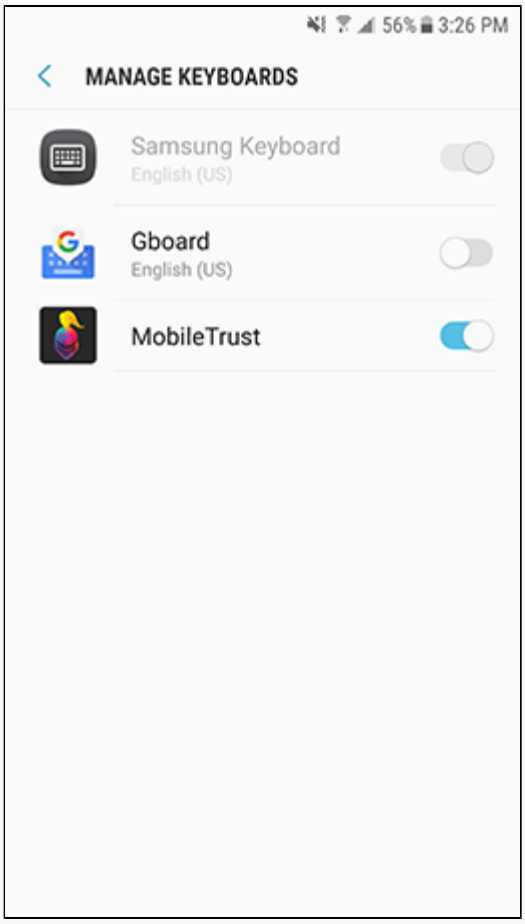


Keyboard Setup

After logging in, you will be greeted by the following screen which instructs you on how to enable the MobileTrust® secure encrypted keyboard on your Android device:



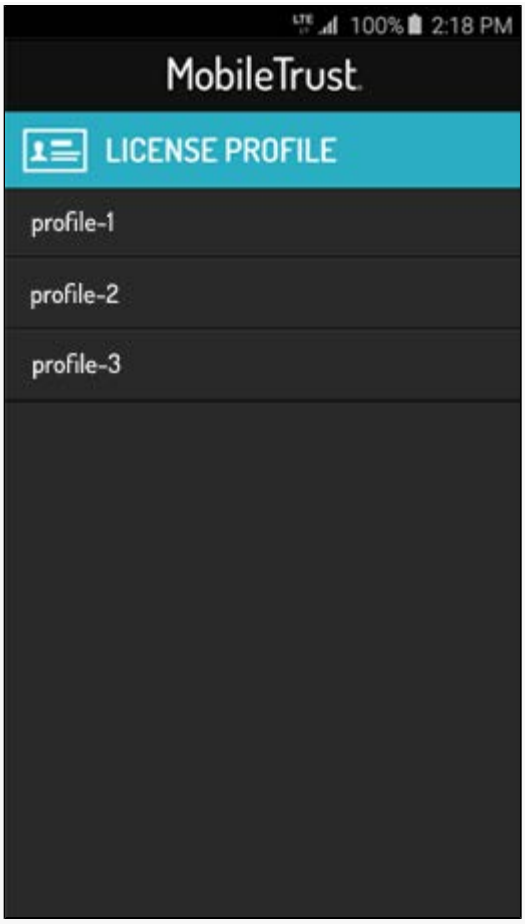
Tap the blue "SET UP KEYBOARD" button which will automatically display the Android system settings menu in which you must enable the MobileTrust® Secure Keyboard as seen below. If your device asks you for permission to allow this change, you must grant permission to continue.



Once you have enabled the MobileTrust Secure Keyboard, you must return to the MobileTrust app then tap the "DONE" button to continue.

License Profile Selection

After tapping "Done" on the "Before you Begin" window which instructs you how to set the MobileTrust® secure encrypted keyboard as the default system-wide keyboard, you will be greeted with the License Profile window. This window allows you to select the appropriate license profile with which you have subscribed to the MobileTrust® Mobile Protection Service. If multiple license profiles exist, you can now select which license profile you would like to activate on your device. If your email address is only associated with a single license profile, the app will automatically select the profile for you. The following sample License Profile window shows an example of multiple License Profiles:



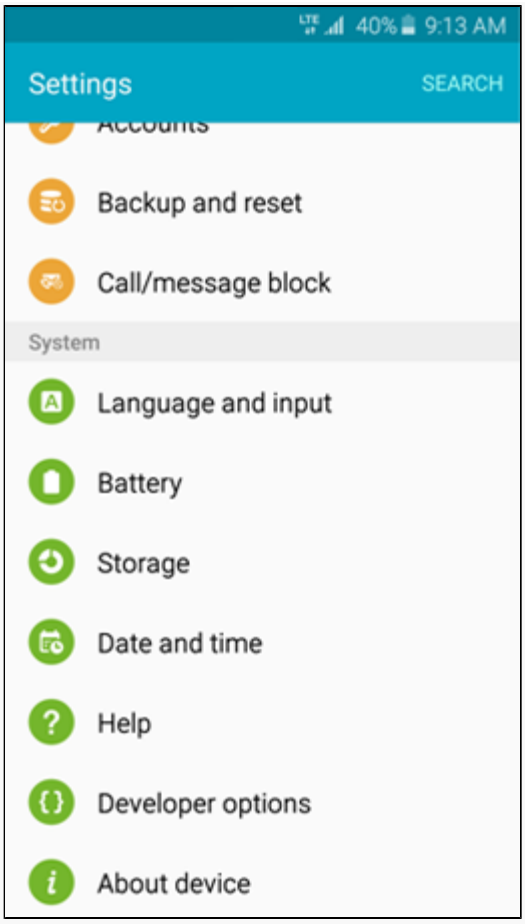
Note- The MobileTrust® app will check for an updated license profile every 48 hours until the selected license expires. If your license has expired, you must renew your license with the appropriate vendor. If the currently used license profile has an expired license, the MobileTrust® app will automatically select a different license profile if one exists with an up-to-date license.

Enabling the MobileTrust Secure Keyboard

In order to properly utilize MobileTrust's® encrypted keyboard, users must enable the MobileTrust® secure keyboard in their Android device system settings. Performing this step will result in the MobileTrust® encrypted keyboard becoming accessible for use both inside and outside of the MobileTrust® app.

For Android Users:

Open system settings and scroll down to "Language and input". Tap "Language and input". Note: On certain Android 7.0 systems, the "Language and input" option may be located within "General management".



In the menu "Language and input" menu, tap "Default Keyboard" and then tap "Set Up Input Methods" if the "English (United States) MobileTrust" setting is not available. Note: On certain Android 7.0 devices, this option may be configured by tapping "Virtual Keyboard" then tapping "Manage keyboards".

:: Strike Force ::

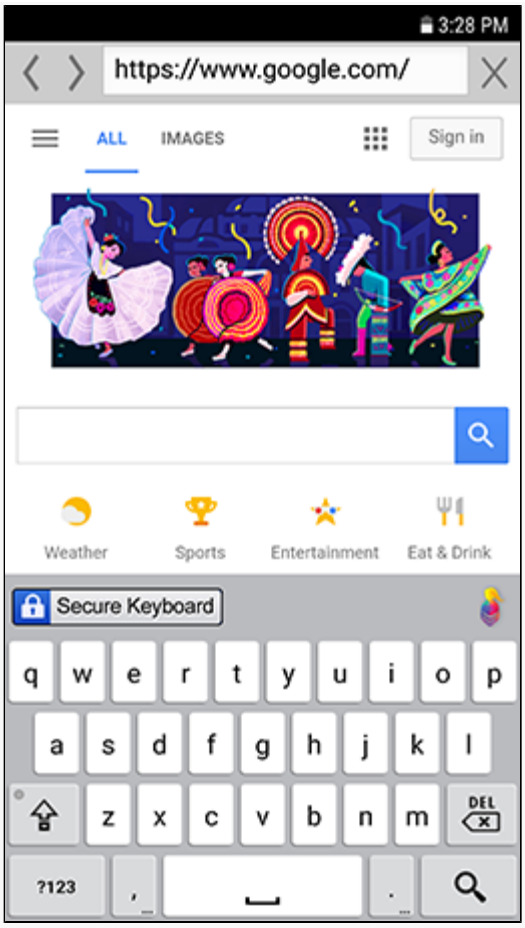
In the "Set Up Input Methods" menu or the "Manage keyboards" menu, use the toggle switch to enable the "MobileTrust" keyboard, then you may set the "MobileTrust" keyboard as the default system keyboard in the previous menu.

Using MobileTrust®

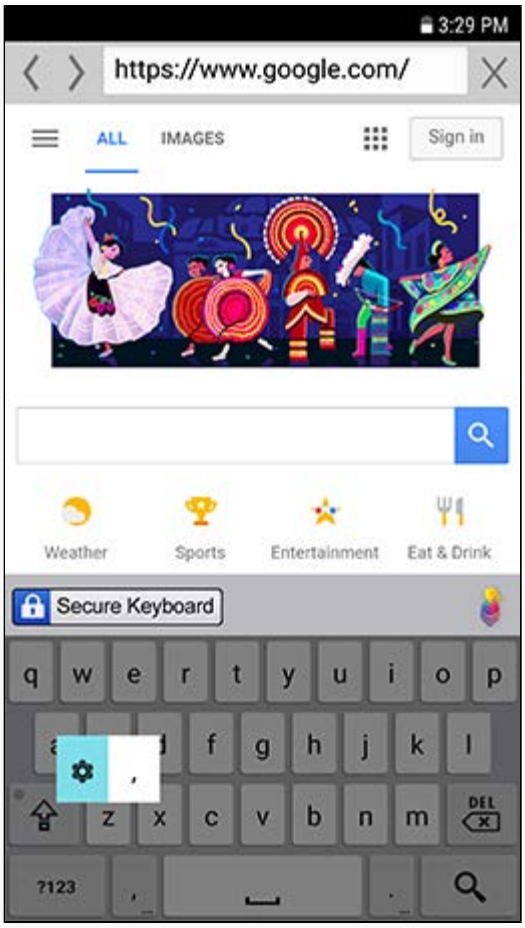
The following image is the main menu of the MobileTrust app. This menu gives you easy access to all of MobileTrust's functions. You may tap the "i" info icon to access more information about each of MobileTrust's® functions.

Secure Keyboard

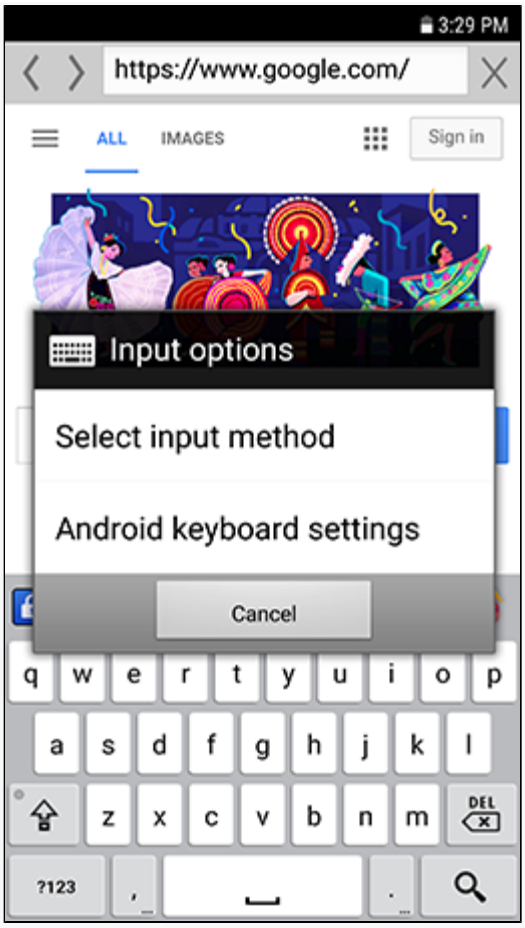
The MobileTrust® Secure Keyboard is designed to actively encrypt every keystroke you type with it. The following image shows the MobileTrust® Secure Keyboard "Light" theme.



To access different keyboard themes, as well as to access various other keyboard settings, long-press the comma/microphone key located to the left of the spacebar and slide the selector to the settings icon shown below:

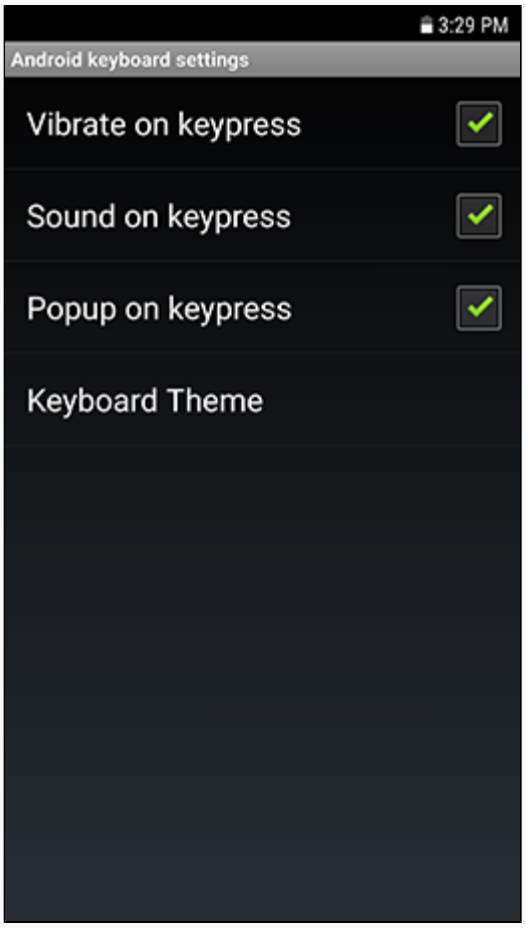


Doing so will bring you to the "Input options" dialog box at which point you can select "Android keyboard settings" shown below:



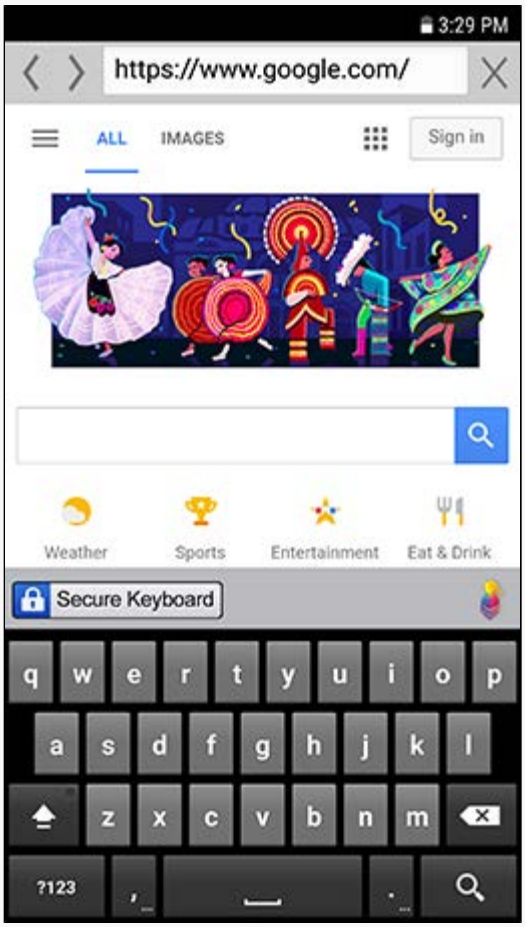
In the "Android keyboard settings" window, you can toggle options such as "vibrate on keypress", "sound on keypress", "popup on keypress", as well as select a "Dark" theme from the "Keyboard Theme" selection window.

:: Strike Force ::



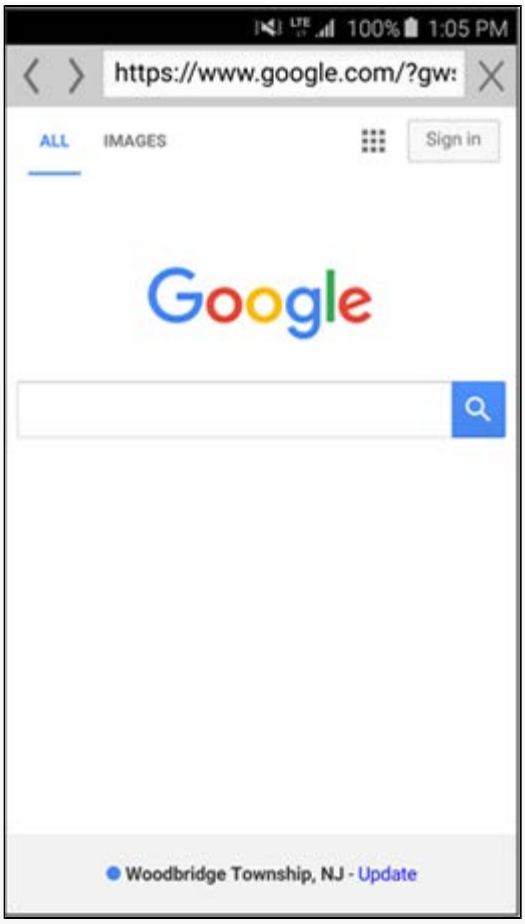
®

The below image shows the MobileTrust Secure Keyboard "Dark" theme being used:



Secure Browser

The secure browser allows the user to browse the internet in a safe and secure encrypted browser. The following image is an example of an Android device running MobileTrust's® secure browser:



Tapping the "‹" icon will navigate to the previously loaded page.
Tapping the "›" icon will navigate to the next page.
Tapping the "X" icon will close the secure browser.

Password Vault

The Password Vault allows users to store usernames and passwords for website logins. Users are able to enter:

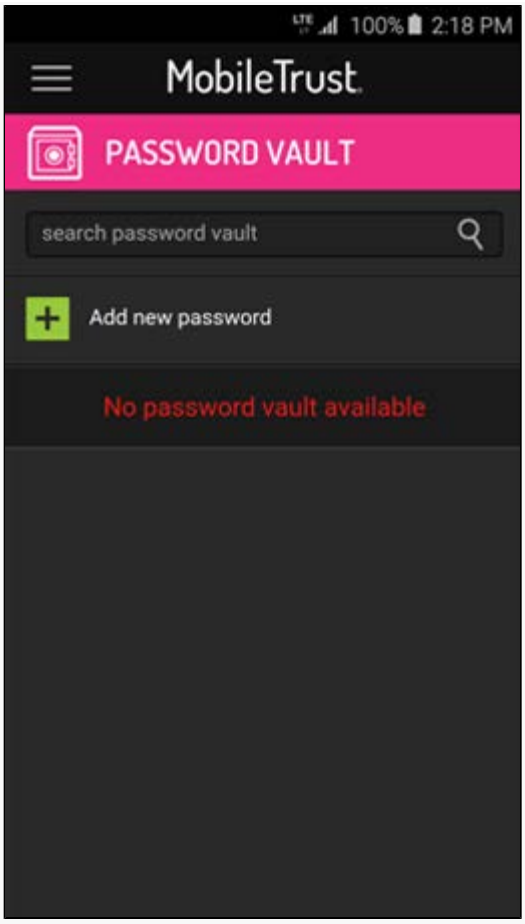
Description: A description of the website/service that the Password Vault is storing credentials for.

Username: Login username for a website.

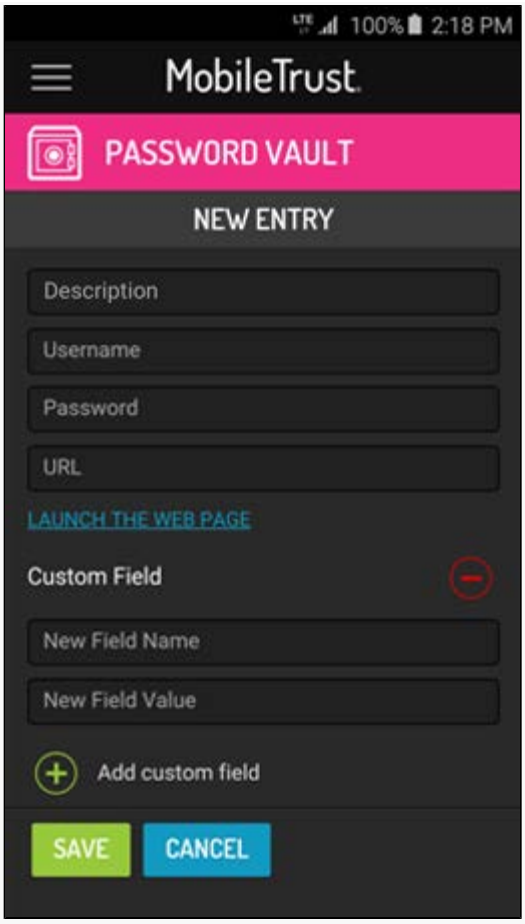
Password: Password associated with the login name.

URL: A link to the website which allows the MobileTrust® app to automatically launch it for you using the bundled Secure Browser.

The following image is a sample empty Password Vault. To add a new entry, you may tap the "Add new password" text or the "+" icon.

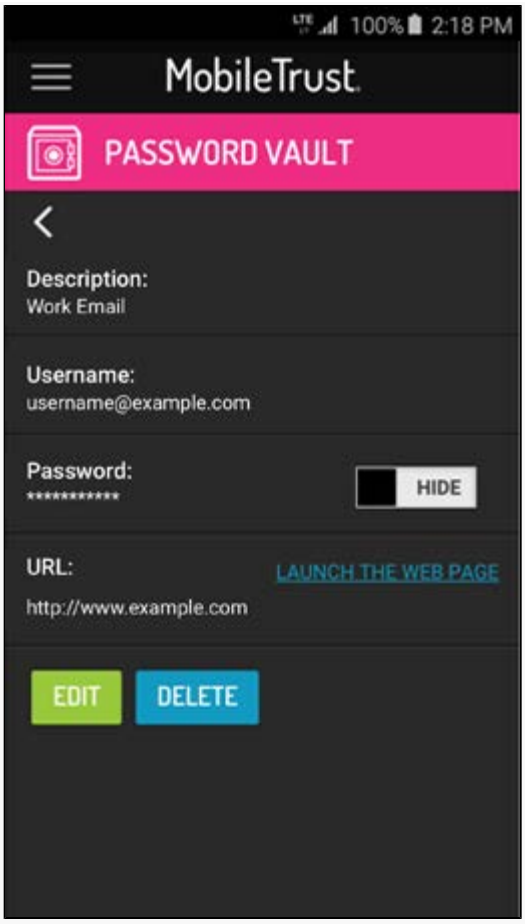


Once the Password Vault New Entry window is open, you may enter a description, username, password, and website URL into the appropriate text fields and tap the green "Save" button:



Once login credentials have been saved in MobileTrust's® Password Vault, you may view the saved login credentials by tapping the description, which was entered during creation of the password, in the main Password Vault menu. Doing so will display the following window with login credentials, the ability to hide/show the saved password, and a "Launch the Web Page" link which launches the specific website using the bundled Secure Browser.

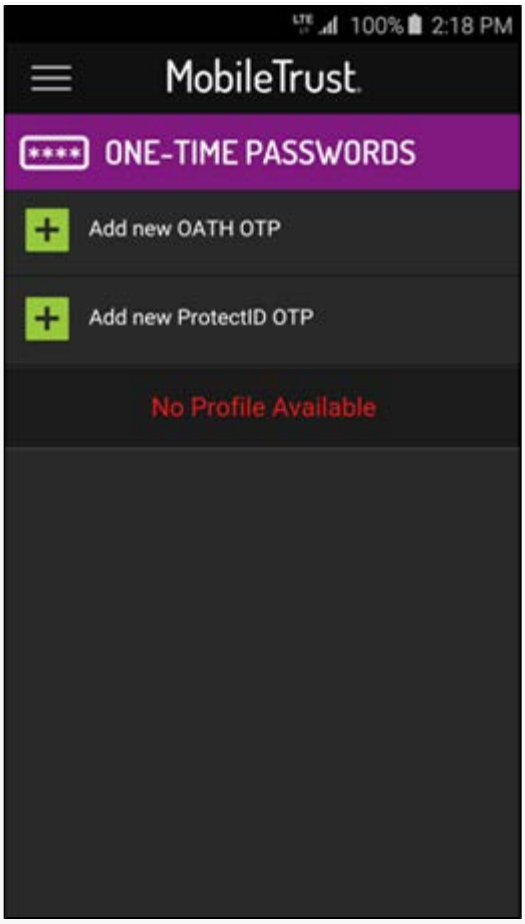
:: Strike Force ::



One-Time Passwords

MobileTrust's® One-Time Password Generator is based on "Open ID". Open ID is a widely used open protocol standard that enabled users to authenticate themselves in a decentralized manner and does not rely on a central authority to authenticate a user's identity. Open ID enables users to consolidate their digital identities. Users may create accounts with their preferred Open ID identity providers, and then use those accounts as the basis for signing on to any website which accepts Open ID authentication.

The following image is MobileTrust's® homepage for One-Time Passwords. The user is able to choose between "Add new OATH OTP" and "Add new ProtectID OTP".



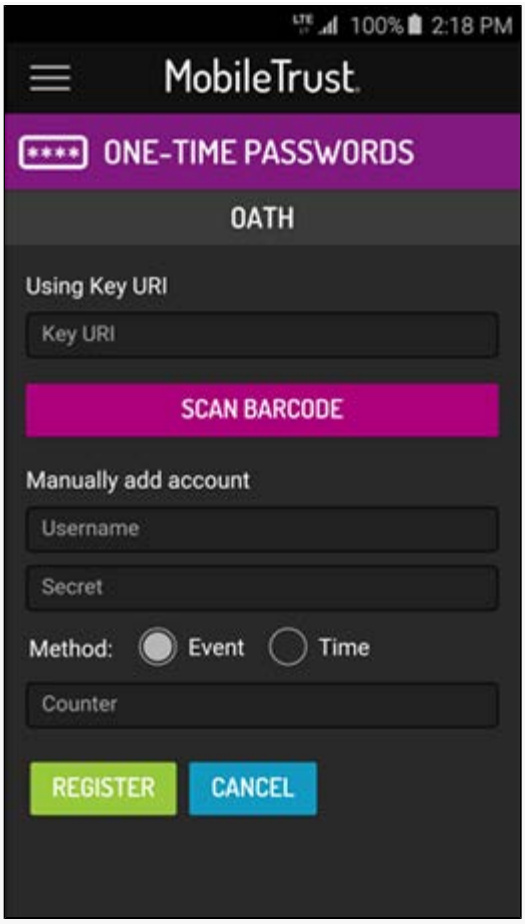
Add New Oath OTP

In this Add New Oath OTP section, users can register themselves using any one of the following three options:

Using Key URL: User must input the key URL in the corresponding field and then click on the Register button.

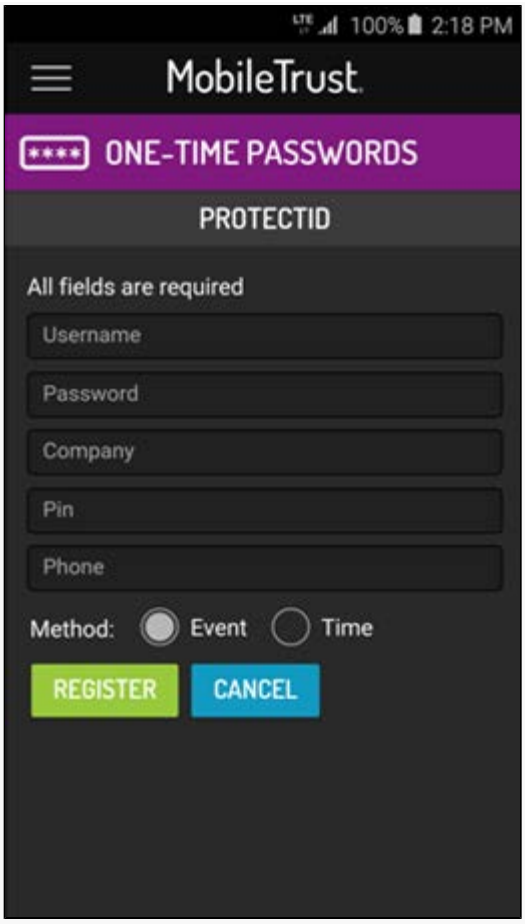
Scan Barcode: User must use their Android device camera to scan their barcode then click on the register button.

Manually Add Account: Users can also add accounts manually by inputting a username, a secret code, choosing a method, and setting a counter in the corresponding fields and then clicking on the Register button.



Add New ProtectID OTP

In this Add New ProtectID OTP section, users can register themselves by filling in the Username, Password, Company, PIN, Phone, and Method fields with the appropriate information/choice. The user may then begin the registration process by tapping the "Register" button.



After inputting the necessary information and tapping the "Register" button, the app will call the Web method with the inputted username, password, company, PIN, phone number, ticket, locale, and device ID. Upon successful execution on the web method, the app will return a URL corresponding to a specific customer. Using this URL, a separate web method is called. This web method validates the unique User ID and Device ID, registers the data in the server, and returns back a Device PIN.

Password Generator

The MobileTrust® Password Generator is a feature which allows the user to generate a customizable strong password. Using the options in the following image, the user can create a customized strong password with the following optional parameters:

Password Length: Allows you to specify the length of your generated password (Up to 99 characters).

Lower Case: Toggles whether or not lower case letters will be included in the generated strong password.

Upper Case: Toggles whether or not upper case letters will be included in the generated strong password.

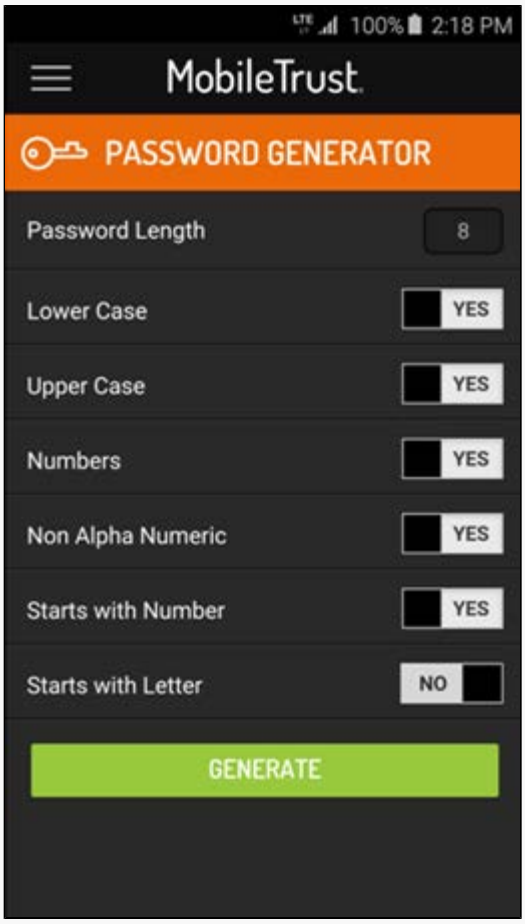
Numbers: Toggles whether or not numbers will be included in the generated strong password.

Non Alpha Numeric: Toggles whether or not characters other than letters and numbers will be included in the generated strong password.

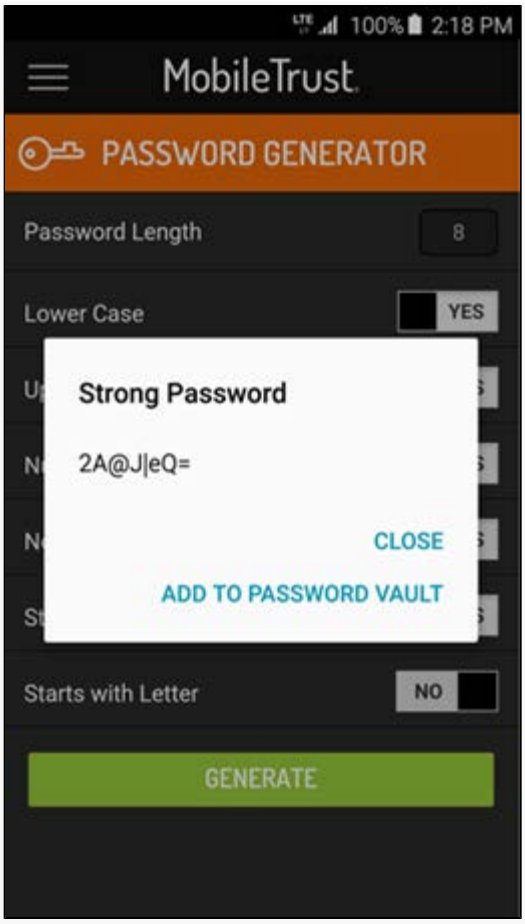
Starts With Number: Toggles whether or not the generated

strong password will start with a number or a letter.

Starts With Letter: Toggles whether or not the generated strong password will start with a letter or number.

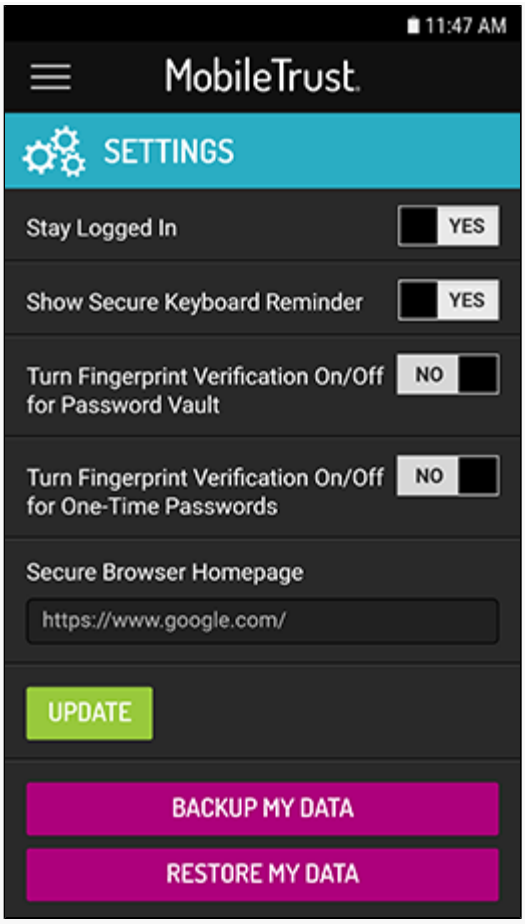


The following image is an example of an 8-character generated password. By tapping "Add to Password Vault ", you will automatically add this generated password to your password vault which you can then access at any time for any website login credentials of your choosing:



Settings

The MobileTrust® settings allow you to enable certain features and modify certain values of the MobileTrust® app. The following image is an example of the MobileTrust® settings window:



The user is able to change/view the following settings:

Stay Logged In: Toggles whether or not you will have to sign in to the MobileTrust® app with your email and password upon each launch.

Show Secure Keyboard Reminder: Allows the user to set whether or not they will receive a reminder to enable the MobileTrust® Secure Keyboard every time they launch the MobileTrust® app.

Turn Fingerprint Verification On/Off for Password Vault: Allows the user to set whether or not their fingerprint will be required to access the Password Vault feature on compatible Android devices with currently registered fingerprint(s).

Turn Fingerprint Verification On/Off for One-Time Passwords: Allows the user to set whether or not their fingerprint will be required to access the One-Time Passwords feature on compatible Android devices with currently registered fingerprint(s).

Secure Browser Homepage: Allows the user to set a custom homepage for the MobileTrust® Secure Browser.

Backup My Data: Allows the user to back up his/her data within an encrypted zip container located at (/sdcard/mobiletrust/archive.zip) for Android devices.

Restore My Data: Allows the user to restore his/her data.

Version: Displays the currently installed version of MobileTrust®. Cannot be modified.

Machine ID: Displays an ID unique to your device. Cannot be

modified.

Backup My Data

The MobileTrust® Backup My Data option allows you to backup your Password Vault, amongst other app information and preferences, in an encrypted zip which is then saved locally on your mobile device's internal storage. In some cases, you may find it helpful to store a copy of this encrypted zip on your PC/Mac. In order to do so, follow these steps:

- Connect your mobile device to your PC/Mac.
- Open your mobile device's SD card.
- Navigate into the MobileTrust folder.
- Copy "archive.zip " to your PC/Mac.

MobileTrust® Usage Info Bubbles

Secure Browser

MobileTrust's® Secure Browser is designed to have a multitude of security features beyond those of your average desktop browser. The MobileTrust® Secure Browser implements security features such as:

- Runs in a sandbox environment.
- Clears cookie & session caches upon launch.
- Does not allow potentially malicious and/or vulnerable browser extensions which mitigates the likelihood of man-in-the-browser attacks.
- Does not allow potentially malicious and/or vulnerable simultaneous tabs which mitigates the likelihood of cross-site request forgery (CSRF) and tabnapping attacks.

Password Generator

MobileTrust's® Password Generator allows the user to automatically create customizable strong passwords of varying lengths. MobileTrust's® Password Generator allows you to customize the following settings:

- **Password Length:** Determines how many characters, in terms of length, the generated password will be.
- **Lower Case:** Toggles whether or not the generated password will include lower case letters.
- **Upper Case:** Toggles whether or not the generated password will include upper case letters.
- **Numbers:** Toggles whether or not the generated password will include numbers.
- **Non Alpha Numeric:** Toggles whether or not the generated password will include characters other than numbers and letters.

Starts with Number: Toggles whether or not the generated password will begin with a number as opposed to a letter. **Enabling "Starts with Letter" setting with automatically disable this setting.**

Starts with Letter Toggles whether or not the generated password will begin with a letter as opposed to a number. **Enabling "Starts with Number" setting will automatically disable this setting.**

Having a difficult-to-guess password is crucial in protecting your online account login credentials. Using MobileTrust's® password generator will allow you to easily store the generated password directly into MobileTrust's® Password Vault.

Password Vault

MobileTrust's® Password Vault allows you to store, and search through, both generated and manually entered passwords. The Password Vault also enables our secure browser to automatically launch the websites for which you have your credentials stored. The Password Vault allows you to enter 4 key pieces of information to save your login credentials:

Description: In this text field, enter a description of the website/service for which you would like to save the login credentials.

Username: In this text field, enter the username associated with the account for which you would like to save your login credentials.

Password: In this text field, enter the password associated with the account for which you would like to save your login credentials.

URL: In this text field, enter the URL of the website for which you would like to save your login credentials. An example of a URL would be "www.google.com" without the quotation marks.

Add custom field: In this optional text field, you may elect to enter additional notes which expand upon your to-be saved login credentials.

Once you have multiple passwords saved, you may search through your saved passwords with the search bar at the top of the Password Vault menu.

One-Time Password Generator

MobileTrust's® One-Time Password (OTP) Generator allows you to generate both ProtectID and OATH based one-time passwords for two-factor authentication purposes.