User Manual on AuthShield – Two Factor Authentication – Mobile Token

By

AuthShield Labs

Table of Contents

1. AuthShield 2FA – Mobile Token – Overview 3

2. Available OS 4

3. Installation and Activation 5

4. Generate One Time Password 10

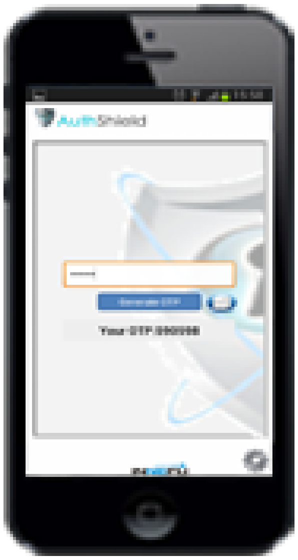
5. Settings 11

6. Trouble-Shooting 12

7. Support 14

1. AuthShield 2FA – Mobile Token – Overview

AuthShield’s mobile token is an application installed on smart phones which generates an OTP for the user on the phone itself. The password is based on a pre defined unbreakable randomized algorithm.



AuthShield authenticates and verifies the user based on –

- Something only the user knows (user id and password)
- Something only the user has (Mobile token)

The technology uses a dual mode of identification where along with the user id and password, verification is done through a secure randomly generated one time password (OTP)

The OTP is generated by a mobile application installed on the smart-phone of the authorized users. Users have to enter a PIN to generate OTP.

Thereby, the device enables the server to authenticate the digital identity of the sender using a mobile phone apart from his user name and password.

2. Available OS

AuthShield Two Factor Authentication works on multiple OS including Android, iOS, Blackberry, Windows Mobile Phones etc.

Android OS: 2.3 and above

iOS: 7.0 and above

Blackberry: 5.0 and above

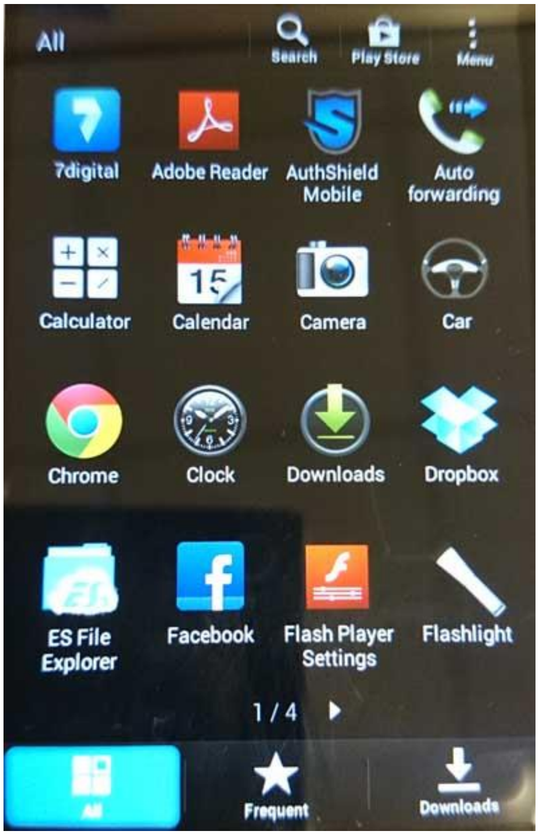
Windows Mobile OS: 7.0 and above

New Handsets and OS are regularly added to the list. You are requested to contact your Support Team for the latest comprehensive list of Handsets and OS.

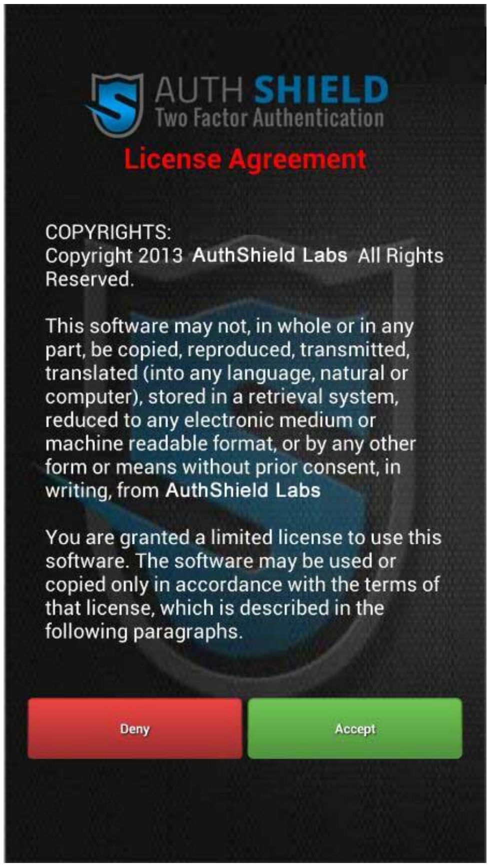
3. Installation and Activation

Installing the Mobile Token:

a. Download the Token – AuthShield Mobile in your smart phone. Token installation will ask for necessary permissions



b. User has to accept - End User License Agreement to proceed



License Agreement

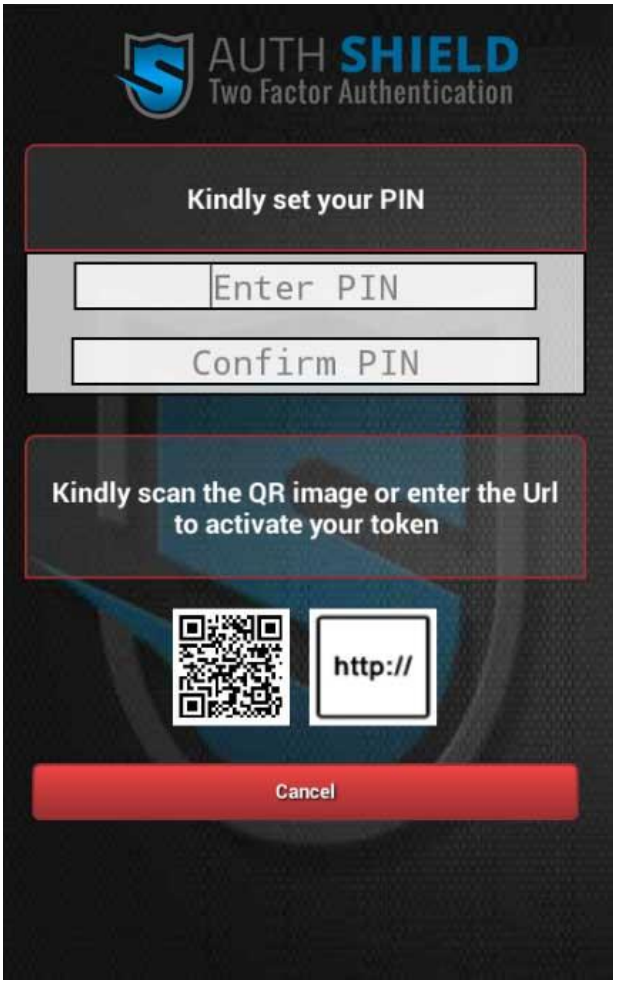
COPYRIGHTS:
Copyright 2013 AuthShield Labs All Rights Reserved.

This software may not, in whole or in any part, be copied, reproduced, transmitted, translated (into any language, natural or computer), stored in a retrieval system, reduced to any electronic medium or machine readable format, or by any other form or means without prior consent, in writing, from AuthShield Labs

You are granted a limited license to use this software. The software may be used or copied only in accordance with the terms of that license, which is described in the following paragraphs.

Activating the Mobile Token:

AuthShield Mobile Token can be activated by using a URL or a QR Code. The token can be activated in Online as well as Offline mode.



Kindly set your PIN

Enter PIN

Confirm PIN

Kindly scan the QR image or enter the Url to activate your token

a. User has to enter a PIN to proceed. The PIN has to be a five digit alpha numeric string with at least one special character. This PIN will be required by the user anytime he wishes to generate the OTP. For the protection of the application as well as for protecting user's credentials, we recommend that the user keeps this PIN confidential. User has to then either use the QR code button or the URL button to activate the token

b. On pressing QR button, the camera would automatically start. User has to scan the QR code to activate the token

c. On pressing the URL button, the user will be prompted to enter the URL provided to him to activate the token

Online Activation Mode -

When a user is assigned a Mobile Token, he immediately receives a mail with the following information –

- Information on how to download the Token
- User credential to log into the portal to activate the Token

Offline Activation Mode –

When a user is assigned a Mobile Token, he immediately receives a mail with the following information –

- Information on how to download the Token
- User Manual
- QR Code for activation attached with the mail

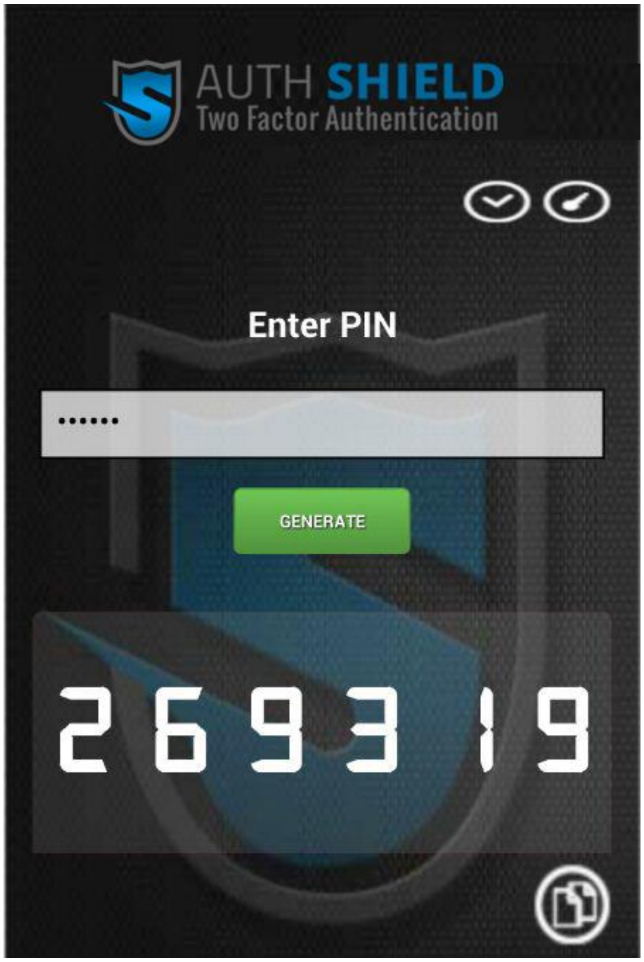
P.S – We request all users using Offline Activation mode to immediately delete the mail and destroy the QR code as soon as the token has been activated

Pre-Requisites:

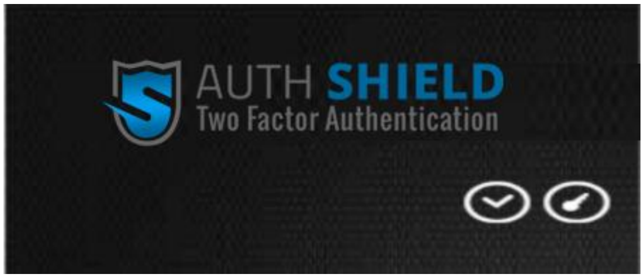
a. One Time - Internet Connection on the Phone
b. Mobile Token Application installed on Handset
c. QR Code / URL to activate Token
d. For Blackberry – The phone must have SD card installed

4. Generate One Time Password

To generate One Time Password user has to enter the PIN which he had entered at the time of installation. In case the user enters the correct PIN, OTP will be generated and shown to the user. In case



5. Settings



There are two buttons available on the Application for settings –

- Clock –
    - The setting is specifically to Re-sync clock in case the user changes his system time. The user needs to have data connection to re-sync his clock

- Change Pin –
    - The setting is used by the user to reset his PIN. User has to enter his Old Pin and then enter the new PIN. The old PIN will no longer be usable

6. Trouble-Shooting

a. Application not installed

Application may not get installed in the phone if the user does not provide necessary permissions. Though AuthShield supports a wide variety of devices in certain cases, the application version may not be compatible with the OS on the phone.

Please uninstall the application. Check for available OS, and install the application again

b. User is not able to scan the QR Code

AuthShield QR code is one of the lightest QR code available and even a camera with a low resolution should be able to scan it, in case the user has a faulty or an inactive camera, he will not be able to scan the QR code.

In these cases, we request the user to ask his administrator to provide him with an option to activate the token by entering an URL and not scanning the QR code.

c. Tabs out of Place

Like most Mobile applications, AuthShield works with all supported handsets with a common GUI. However, in case your user look is out of shape, please contact the system admin. It may be possible, that the handset resolution may not be an acceptable resolution.

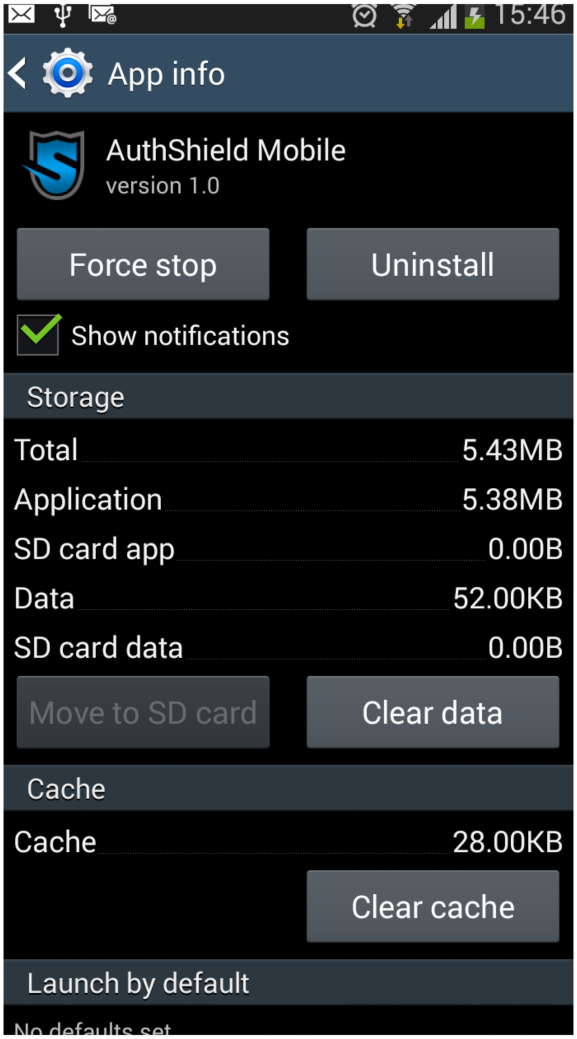
d. User is not able to login with the generated OTP

It is possible that due to changes in users settings on the handset, the generated OTP may not match with the server. In such cases, user is requested to use the Re-Sync clock button on the application GUI to re-sync his clock. The user needs to have internet connection for the same

e. Forgot PIN

Please note that to ensure complete security for the user as well as security of the application, the application PIN is not stored anywhere in the handset or on the server. As a result, in case a user forgets his Pin, he is requested to reset the application and activate his token again. User can reset his application by going to his Application settings and log into AuthShield Mobile -

- Clear data
- Force Stop the Application



AuthShield Mobile
version 1.0

☑ Show notifications

Storage

Total	5.43MB
Application	5.38MB
SD card app	0.00B
Data	52.00KB
SD card data	0.00B

Cache

Cache	28.00KB

Launch by default

No defaults set

f. Uninstalling the Application

The user can uninstall the application by moving into his Application Manager and logging into AuthShield Mobile.

7. Support

We request the user to contact his system administrator / IT team for further support.