

## **User Manual on AuthShield – Two Factor Authentication – Mobile One Touch Authentication**



**By**

**AuthShield Labs**





**Table of Contents**

1. AuthShield 2FA – Mobile One Touch Authentication – Overview ..... 3

2. Available OS ..... 4

3. Installation and Activation ..... 5

4. Authenticate via One Touch Authentication ..... 11


5. Logs ..... 12

6. Trouble-Shooting ..... 12


7. Support..... 14


## 1. AuthShield 2FA – Mobile One Touch Authentication – Overview

AuthShield's Mobile One Touch Authentication is the latest Two Factor Authentication mechanism brought out by Innefu Labs. The authentication mechanism bypasses the entire concept of One Time Passwords by converting the user's handset into a secondary form factor using a challenge Response mechanism. Any time the user wishes to log in, a 'push' notification is sent to the registered handset of the user with the login details including IP address, Time stamp, location (based on IP) etc. The user has to 'approve' or 'deny' the request to login. It's a complete 'Hackproof' token and cannot be compromised even by compromising the server or the device.



**Login Request**

 **tarun**  
outlook

  
Logs

<b>IP Address</b>	192.168.1.170
<b>Time</b>	06:56 PM GMT+05:30 Dec 07, 2014
<b>Organisation</b>	reliance
<b>Detail</b>	

Approve

Deny

**AuthShield** authenticates and verifies the user based on –

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

The technology uses a dual mode of identification where along with the user id and password, verification is done through a PKI Architecture using a smart phone as a container for Private Key

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, Windows Mobile Phones etc.

**Android OS:** 2.3 and above

**iOS:** 7.0 and above

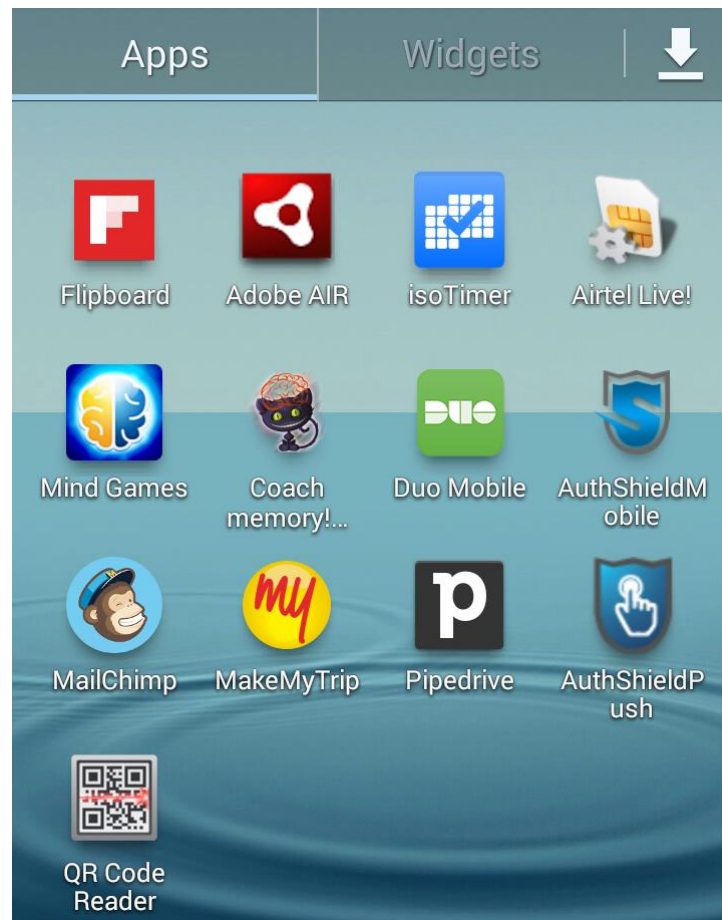
**Windows Mobile OS:** 7.0 and above

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 One Touch Authentication in your smart phone. Token installation will ask for necessary permissions



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



### **Activating Mobile One Touch Authentication:**

AuthShield Mobile One Touch Authentication can be activated by using a Sixteen (16) Digit License key or a QR Code. The token can be activated in Online as well as Offline mode.

- a. User has to click 'Register' to proceed



Register

**Please enter the assigned 16 digit License Key**

**Please enter the Authentication Server IP address /  
Host Name and Port(if any)**

- b. After Registering user will be shown the following screen



The image shows a mobile application interface for AUTH SHIELD Two Factor Authentication. At the top is a status bar with icons for alarm, Wi-Fi, cellular signal, and battery, along with the time 14:46. Below the status bar is the AUTH SHIELD logo. The main heading is "Get license key through QR Code". A QR code is displayed in the center. Below the QR code is the word "OR". A red instruction "Please enter the assigned 16 digit License Key" is followed by a form with four empty input boxes. Another red instruction "Please enter the Authentication Server IP address / Host Name and Port(if any)" is followed by a form with two input boxes labeled "Authentication Server" and "Port". At the bottom are two buttons: a green "Submit" button and a red "Cancel" button.

14:46

**AUTH SHIELD**  
Two Factor Authentication **PUSH**

**Get license key through QR Code**



OR

**Please enter the assigned 16 digit License Key**

--	--	--	--

**Please enter the Authentication Server IP address / Host Name and Port(if any)**

Authentication Server	Port
-----------------------	------

**Submit** **Cancel**

- c. User has option of either scanning a QR Code to activate the token (in which case he will not have to enter any other details). On pressing QR button, the camera would automatically start. User has to scan the QR code to activate the token
-



- d. The other option for the user is to enter a sixteen digit license key. The user will also have to enter the URL of Authentication server. The license key will be validated by the authentication server and the token activated.

### **Online Activation Mode -**

When a user is assigned a Mobile One Touch Authentication, 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
- License Key with details on Authentication server and Port number

### **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

Pre-Requisites:


- a. Internet Connection on the Phone
  - b. Mobile One Touch Authentication installed on Handset
  - c. QR Code / License Key to activate Token
-


#### 4. Authenticate via One Touch Authentication

To authenticate via One Touch Authentication a user has to approve or deny the request sent to his phone. The request has the IP address from which the request has been made enabling the user to approve or deny the request. It also has details on time stamp when the request has been made.



Login Request

**tarun**  
outlook

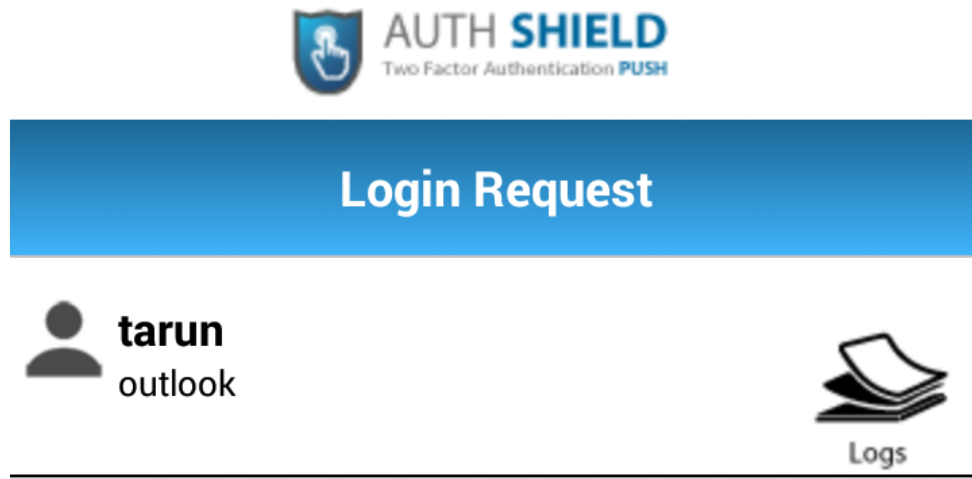
  
Logs

IP Address	192.168.1.170
Time	06:56 PM GMT+05:30 Dec 07, 2014
Organisation	reliance
Detail	

Approve

Deny

## 5. Logs



Logs show all requests received by the user. It also shows the requests accepted or denied by the user.

## 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 the license key and server details

### **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 does not receive notifications on the phone**

AuthShield One Touch Authentication uses standard services to send Notifications. In case the user does not receive notifications on his handset, please check the connectivity details on the phone. In certain cases, user may have to disable and then enable mobile data / WiFi

In extremely rare cases when the user still does not receive notifications, please restart the application by using the following steps –

- Go to Settings - > Application Manager - > AuthShield Push
- Force Stop the application
- Go back to Home Screen and click on the Application again



#### **e. Uninstalling the Application**

The user can uninstall the application by moving into his Application Manager and uninstalling AuthShield Push

### **7. Support**

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