



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 4

4. Authenticate via One Touch Authentication 8

5. Logs 10

6. Trouble-Shooting 11

7. Support..... 12

1. AuthShield 2FA – Desktop One Touch Authentication – Overview

AuthShield's Desktop 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 desktop 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 desktop / laptop 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.

AuthShield authenticates and verifies the user based on –

- Something only the user knows (user id and password)
- Something only the user has (Desktop / Laptop)

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.

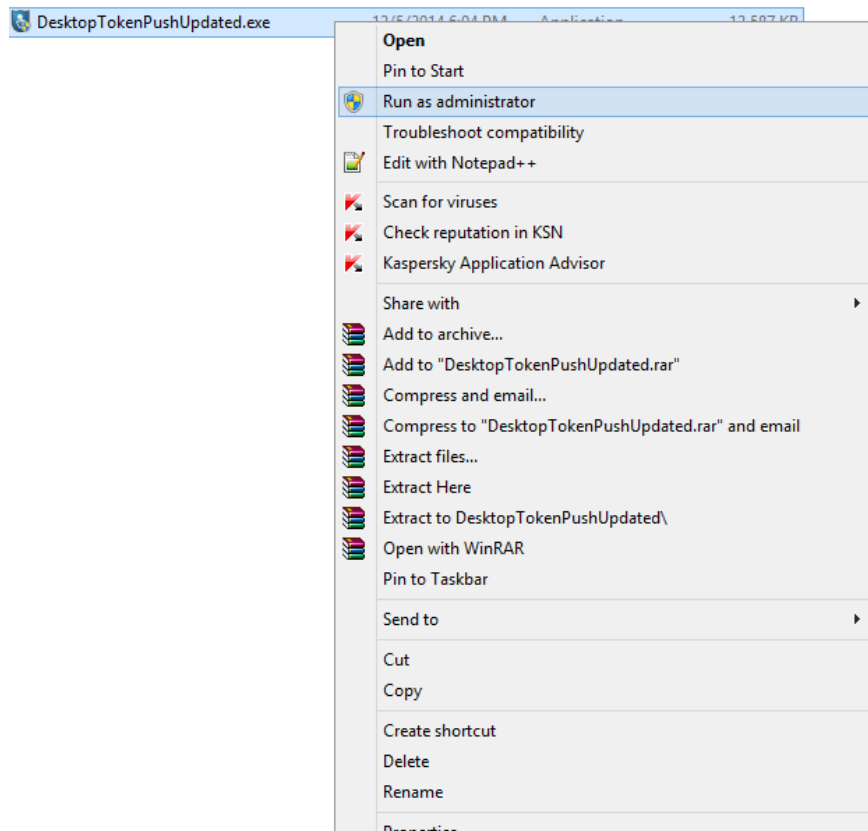
2. Available OS

AuthShield Two Factor Authentication works on all OS.

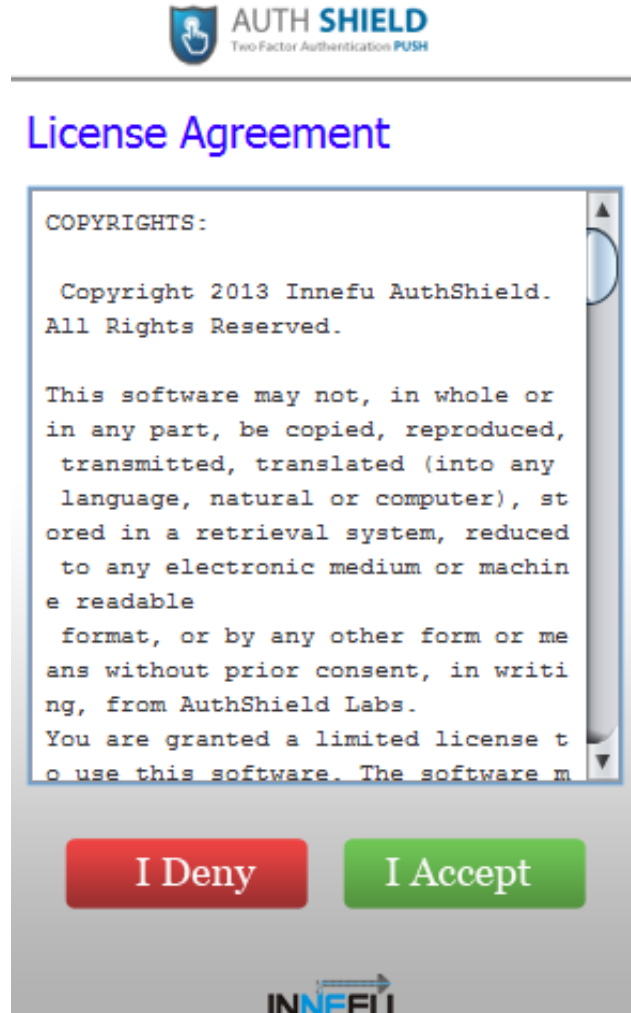
3. Installation and Activation


Installing the Desktop One Touch Authentication:

- a. Install DesktopTokenPushUpdate with Administrator privileges



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






License Agreement

COPYRIGHTS:

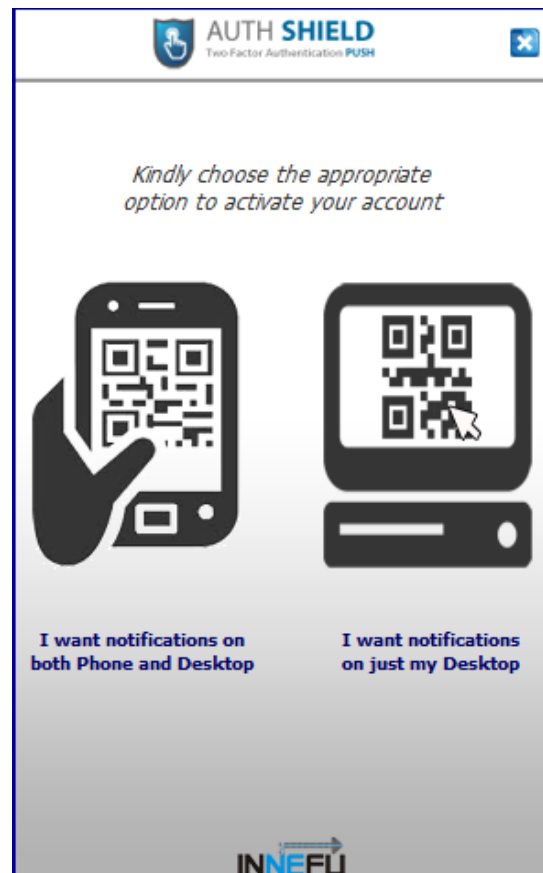
Copyright 2013 Innefu AuthShield.
All Rights Reserved.

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 m



Activating Desktop One Touch Authentication:

AuthShield Desktop One Touch Authentication can be activated by importing a QR Code. User has to decide whether he would like to receive notifications on both phone as well as desktop or only desktop alone.



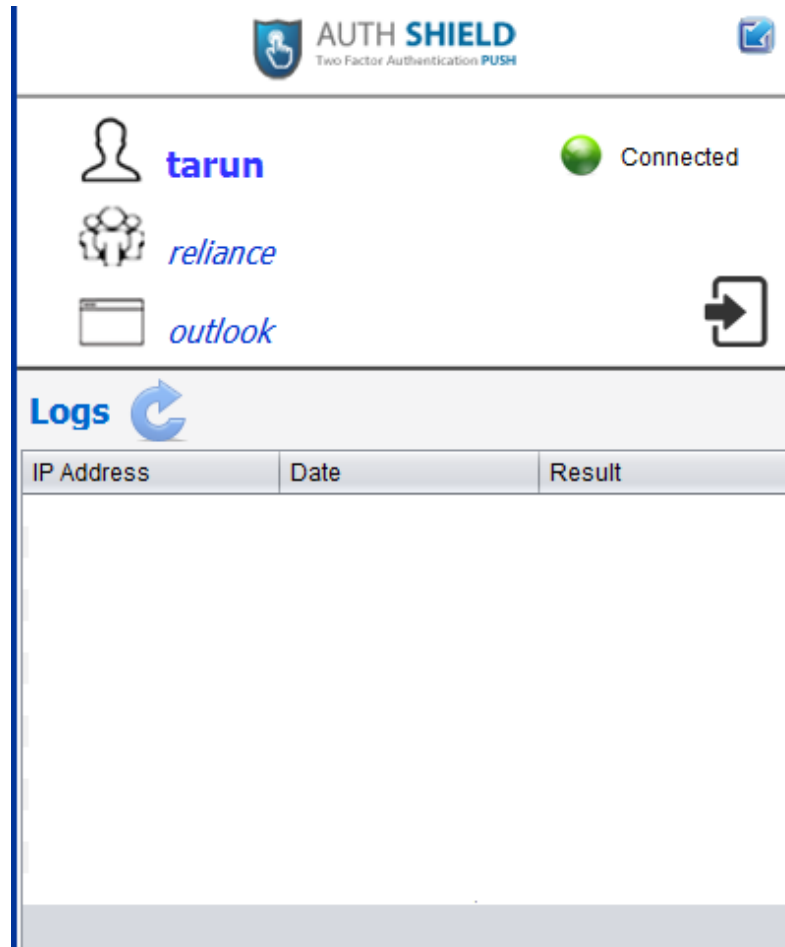
a. User wants notifications on both desktop and Phone –

- User will have to first scan QR code on Mobile One Touch Authentication
- The same QR code then has to be imported into Desktop One Touch Authentication
- The user will receive notifications on both phone and desktop to authenticate his identity

b. User wants notifications on only desktop

- User will import the QR code directly on his desktop. The activation in this case will be done by user's desktop / laptop
 - The user will receive notifications on only his desktop / laptop to authenticate his identity
-


After Registering user will be shown the following screen





4. Authenticate via Desktop One Touch Authentication


To authenticate via Desktop One Touch Authentication a user has to approve or deny the request sent to his desktop / laptop. 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.

 AUTH SHIELD
Two Factor Authentication PUSH



 tarun

 reliance

 outlook

IP Address192.168.1.188

LocationLos Angeles
California
US

Time09:35 PM
Dec 07, 2014

DetailOutlook Login Request

Your local IP address(s):

127.0.0.1
192.168.1.252

Your public IP address(s):


182.69.61.159


IP Address mismatch!!


Approve


Deny


5. Logs


**tarun**

*reliance*

*outlook*

 Connected



Logs 

IP Address	Date	Result
192.168.1.188	09:03 PM Dec 07,	Approved
192.168.1.188	09:03 PM Dec 07,	Missed
182.69.61.159	09:09 PM Dec 07,	Missed
182.69.61.159	09:11 PM Dec 07,	Approved
182.69.61.159	09:11 PM Dec 07,	Missed
182.69.61.159	09:16 PM Dec 07,	Approved
182.69.61.159	09:16 PM Dec 07,	Missed
182.69.61.159	09:16 PM Dec 07,	Missed
182.69.61.159	09:16 PM Dec 07,	Missed
182.69.61.159	09:16 PM Dec 07,	Missed
182.69.61.159	09:16 PM Dec 07,	Missed
192.168.1.188	09:17 PM Dec 07,	Approved
192.168.1.188	09:17 PM Dec 07,	Missed

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 OSs in certain cases, the application version may not be compatible with the OS on the Desktop / Laptop.

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

b. Tabs out of Place

Like most Mobile applications, AuthShield works with all supported Desktops 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 desktop resolution may not be an acceptable resolution.

c. User does not receive notifications on the Desktop

AuthShield One Touch Authentication uses standard protocols to send Notifications. In case the user does not receive notifications on his Desktop, please check the connectivity details on Desktop.

The application will continue to try and connect to the server in case connection is lost.

d. Uninstalling the Application

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

7. Support

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