Google Authenticator
Administration & User Guide
(Version 5.7)
Trademarks

Deepnet Unified Authentication, MobileID, QuickID, PocketID, SafeID, GridID, FlashID, SmartID, TypeSense, VoiceSense, MobilePass, DevicePass, RemotePass and Site Stamp are trademarks of Deepnet Security Limited. All other brand names and product names are trademarks or registered trademarks of their respective owners.

Copyrights

Under the international copyright law, neither the Deepnet Security software or documentation may be copied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Deepnet Security.

Licence Conditions

Please read your licence agreement with Deepnet carefully and make sure you understand the exact terms of usage. In particular, for which projects, on which platforms and at which sites, you are allowed to use the product. You are not allowed to make any modifications to the product. If you feel the need for any modifications, please contact Deepnet Security.

Disclaimer

This document is provided “as is” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. Deepnet Security may make improvements of and/or changes to the product described in this document at any time.

Contact

If you wish to obtain further information on this product or any other Deepnet Security products, you are always welcome to contact us.

Deepnet Security Limited
Building 3
North London Business Park
London N11 1GN
United Kingdom

Tel: +44(0)20 3668 1580
Fax: +44(0)20 8446 3182
Web: www.deepnetsecurity.com
Email: support@deepnetsecurity.com
Table of Contents

Introduction ......................................................................................................................... 4
Administration ..................................................................................................................... 4
Install Token ....................................................................................................................... 6
  Manual Entry .................................................................................................................... 6
  QR Scan ........................................................................................................................... 7
Introduction

Similar to the Deepnet MobileID, Google Authenticator is an OATH compliant One-Time Password generator. Google Authenticator is officially available on iPhone, Android and Blackberry.

Deepnet DualShield authentication server natively supports Google Authenticator, in very much the same way that it supports Deepnet MobileID. This document describes how users can use Google Authenticator with DualShield.

Administration

In order for a user to use Google Authenticator in DualShield, the user must first have a Google Authenticator token in their user account in the DualShield server. The token can be manually created by the system administrator for the user using the DualShield Management Console, or automatically created by the DualShield server if the Google Authenticator’s policy is set up to automatically provisioning tokens to users.

The instruction below describes how a system administrator can manually create a Google Authenticator for a user in DualShield server.

In the DualShield Console, navigate to the user’s account. Click the context menu icon of the user account, select “Tokens”. A list of user’s tokens will be displayed in a popup window. Now, click the “Create” button on the toolbar.

In the “Product” list, select “Google Authenticator/Time-Based”. Leave other fields as they are, press “Save” button to save it.
The user now has a Google Authenticator in his/her account.

The user will then need to install the token into his/her Google Authenticator app running on their smart phones.

The system administrator needs to provide the token’s credential data to the user in order for the user to install the token. To display the token’s credential data, click the token’s context menu icon then select “View”.

Google Authenticators provides two ways to install a token, manual entry and QR barcode scan.

If the user is going to install the token by manual entry, the “Credential Seed” must be provided to the user. If the user is going to install the token by QR barcode scan, then the “Serial Number” will be provided to the user.

Note: Google Authenticator is a One-Time Password token. To allow users to use Google Authenticator to logon to an application, the system administrator must add the “One-Time Password” authenticator into the application’s logon procedure.
Install Token

Assuming that the user has downloaded the Google Authenticator app on his/her smartphone, the user can install a token by either manual entry or QR code scan.

Manual Entry

Launch Google Authenticator app, press the “Add an account” button, then press the “Add account manually” button.

In the “Enter your key” field, enter the token’s credential seed provided by the system administrator.

Click “Add” to save the token.
Barcode Scan

To install a token by QR barcode scan, launch a web browser on your PC or laptop and navigate to your DualShield Provisioning Server (DPS) by enter a URL in the format below:

http://your dualshield server address:8072/dps/g/?sn=nnnnnn

or

https://your dualshield server address:8072/dps/g/?sn=nnnnnn

where nnnnnn is your token’s serial number provided by your system administrator.

Below is example:

https://dualshield.deepnetlabs.com:8072/dps/g/?sn=10000003

In the “Domain” field, select the domain where your user account is managed.
Enter your User Name and Password to verify yourself.

Press “Continue” button

Now, launch Google Authenticator app, press the “Add an account” button, then press the “Scan barcode” button.