



DIGIPASS GO 6 TOKENS WITH OPENOTP

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs Security.

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

Digipass GO 6 Tokens with OpenOTP

[Token](#)

1. How To use Digipass GO6 Tokens with OpenOTP

OpenOTP supports [Digipass GO6 Hardware Tokens] (<https://www.onespan.com/resources/digipass-go-6/datasheet#tech-specifications>).

Supported algorithms

Digipass GO6 token can work with OATH-HOTP (event-based) and OATH-TOTP (time-based), but the default algorithm is Digipass event and time-based (DES, 3DES and AES). When ordering to OneSpan, do not forget to ask them to produce the token with OATH-HOTP or OATH-TOTP algorithms.

2. Manual registration

If you know the type of your token and the secret seed, you can register an individual token directly to a user with “Manual Registration” in WebADM or Self-Desk. For Manual Token Registration through WebADM GUI, go to **WebADM GUI** > **<USER_ACCOUNT>** > **MFA Authentication Server** > **Register/Unregister OTP Tokens** > **I use another Token (Manual Registration)** and provide information regarding your token.

WebADM Enterprise Edition v2.0.6
 Copyright © 2010-2020 RCDevs Security, All Rights Reserved

API | [Icons]

Home | Admin | Cluster | Create | Search | Import | Databases | Statistics | Applications | About | Logout

Register / Unregister OTP Tokens for **cn=test_user1,o=Root**

You must register a Hardware or Software Token for the user to start using it.
 The registration consists in synchronizing a Secret Key and an initial Token state.


1/3 Token is already registered for user:

Primary Token **HOTP** Remove Disable

Instructions to manually register a new Hardware or Software Token:

1. With Software Tokens, install the Token application and setup a new registration.
2. If the Software Token generates the Secret Key itself then enter the key in the required format below.
 The Secret Key size is 20, 32 or 64 bytes (40, 64 or 128 hexadecimal characters).
3. If the Software Token asks for a pre-generated Secret Key, choose 'Key generated by server' in the Key Mode below.
4. Click the 'Register' button below.

Register Token: Second Token


 I use a Hardware Token (Inventoried)
 I use a Yubikey Token (Inventoried or YubiCloud)
 I use a QRCode-based Authenticator (Time-based)
 I use a QRCode-based Authenticator (Event-based)
 I use another Token (Manual Registration)

Token Type: OATH TOTP (Time-Based)

Key Mode: Key generated by Token (Default)

Key Algorithm: SHA1 (Default)

Key Format: Hex (Default)

Secret Key:

Optional Information

Expiration Date: Edit

Register Cancel





3. Registration through inventory

To register a Digipass GO6 Token with a serial number, you must import them into the WebADM inventory. For this you need a compatible inventory file. The Digipass GO6 is normally provided with a PSKC import file by OneSpan, which can be converted to WebADM compatible format. The file includes the Token secret key in an encrypted format. The decryption PSKC key is provided by OneSpan in a separated document.

First, convert the PSKC file with the conversion tool in `/opt/webadm/websrvs/openotp/bin/pskc2inv`. This tool will convert the encrypted PSKC file to a CSV file containing the Token serial numbers and OATH keys. You can find more details on that command [here] (http://localhost:1313/howtos/utilities_cmd_tool_openotp/utillsopenotp/#4-pskc2inv).

Then, import the generated inventory file in WebADM under **WebADM GUI** > **Import** menu:

WebADM Enterprise Edition v2.0.6
Copyright © 2010-2020 RCDevs Security. All Rights Reserved

API    

Home Admin Cluster Create Search **Import** Databases Statistics Applications About Logout

Import LDAP Objects

You can import LDAP objects to WebADM with both LDIF scripts or CSV files.
You can import WebADM localized messages and inventory items with CSV files only.

- The LDAP Data Interchange Format (LDIF) is a standard for representing LDAP content and import requests. WebADM LDIF data may only contain "add" or "delete" directives and object updates are not supported.
- The Comma-Separated Values (CSV) format is a standard for storing attribute-based data in plain-text files.

Import LDAP Objects

Import LDIF Data File Import CSV Data File

Import WebADM Localized Messages / Inventory Items

Import Message File Import Inventory File

Import failure

If the PSKC import fails, please ask OneSpan for an import file compliant with PSKC RFC-6030.

3. Configuration of OpenOTP

3.1 Per-user configuration

If only some accounts are using a Digipass GO 6 token, you can configure the user account with TOKEN TokenType. With Digipass GO 6 tokens, set the TOTP Time Step to 30 seconds (this is the Digipass GO 6 default). The Time Step is very important and Token will not work if not correctly set.

3.2 General configuration

If you use only Digipass GO 6 tokens, you can configure the TOTP Time Step at the OpenOTP application level in the Applications/OpenOTP WebADM menu.

HOTP token re-synchronisation

In case of event based tokens, it might be required to re-synchronise the token through

WebADM GUI > <USER_ACCOUNT> > MFA Authentication Server > Resynchronize Tokens.

responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs Security S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs Security S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs Security S.A. The latter especially applies for data processing systems. RCDevs Security S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs Security. © 2024 RCDevs Security S.A., All Rights Reserved