



UTILITIES AND COMMAND LINE TOOLS FOR 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.

Utilities and Command Line Tools for OpenOTP

[script](#)

1. Introduction

In this HowTo, we will demonstrate some useful scripts available for OpenOTP and how to use them.

2. OpenOTP Utilities and Scripts

Some scripts are available in:

```
[root@webadm]# cd /opt/webadm/websrvs/openotp/bin
[root@webadm bin]# ll
total 112
-rwxr-xr-x 1 root root 18882 Oct 12 16:58 authtest
-rwxr-xr-x 1 root root 5858 Oct 12 16:58 pkitest
-rwxr-xr-x 1 root root 13090 Oct 12 16:58 pskc2inv
-rwxr-xr-x 1 root root 37362 Oct 12 16:58 report
-rwxr-xr-x 1 root root 9026 Oct 12 16:58 safenet2inv
-rwxr-xr-x 1 root root 3698 Oct 12 16:58 status
-rwxr-xr-x 1 root root 11954 Oct 12 16:58 yubi2inv
```

3. authtest

This script allows you to perform a test login through the console:

```
[root@webadm1 bin]# ./authtest
Enter username: administrateur
Enter domain: rcdevs.com
Enter LDAP password: password
Enter OTP password: 945796
Authentication success!
[root@webadm1 bin]#
```

4. pkitest

5. pskc2inv

This script can be used to convert a PSKC token seed file into an inventory file supported by WebADM.

This is a PSKC file for an RC200 hardware token (sensitive information are obfuscated):

```
[root@webadm bin]# cat inv.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
OATH PSKC Import File for RCDevs WebADM
Generated on October 11, 2018, 11:29 am
-->

<KeyContainer Version="1.0" xmlns="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xenc="http://www.w3.org/2001/04/xmenc#">
<KeyPackage>
  <DeviceInfo>
    <SerialNo>230852XXXXXX</SerialNo>
    <Model>RCDevs RC200-T6</Model>
  </DeviceInfo>
  <Key Algorithm="urn:ietf:params:xml:ns:keyprov:pskc:totp" Id="230852XXXXXX">
    <AlgorithmParameters>
      <ResponseFormat Length="6" Encoding="DECIMAL"/>
    </AlgorithmParameters>
    <Data>
      <Secret>
        <PlainValue>tdxn5XXXXXXXXXXXXXXXXXjUxaZXc=</PlainValue>
      </Secret>
      <Time>
        <PlainValue>0</PlainValue>
      </Time>
      <TimeInterval>
        <PlainValue>30</PlainValue>
      </TimeInterval>
    </Data>
  </Key>
</KeyPackage>
</KeyContainer>
```

```
[root@webadm bin]# ./pskc2inv
WebADM Inventory converter for OATH PSKC files
Usage: pskc2inv <pskc-file> <inventory-file> [<decryption-key>]
```

```
[root@webadm bin]# ./pskc2inv inv.xml webadminventory.csv
Successfully converted 1 PSKC tokens.
[root@webadm bin]#
```

```
[root@webadm bin]# cat webadminventory.csv

# OpenOTP Inventory export for OATH PSKC
# Generated by OpenOTP on October 11, 2018 11:32 am

"Type", "Reference", "Description", "Data"
"OTP Token", "230852XXXXXXX", "RCDevs RC200-T6",
"TokenType=VE9UUA==,TokenKey=tdxn5XXXXXXXXXXXXXXXXXjUxaZXc=,OTPLength=Ng==,TOTPTimeStep=
```

This inventory file can be imported through WebADM GUI and used for OpenOTP authentications. So with this script, you are able to convert every standard OATH Tokens seeds file from any provider to the WebADM format and use it with OpenOTP.

6. report

This script can be used to generate a reporting of activated users. Options are describe below:

```
[root@rcvm8 bin]# ./report
Usage: report [-y] [-r] [-t] [-d] [-s <user settings>] [-f <search filter>] DOMAIN1 [DOMAIN2] ... [DOMAINX]
Domain 1..X is a list of WebADM Domains where OpenOTP user activity will be reported.
Options:
-y : Do not prompt for validation (to be used with cron jobs).
-r : Reset statistic data.
-t : Include OTP Token information (type, serial and model).
-d : Include U2F Device information (version).
-b : Include user blocking information.
-e : Include AD password expiry information.
-s <user settings> : Display user settings (ex: "LoginMode,OTPType")
-f <search filter> : Use a custom LDAP search filter.
If no search filter is defined, all user objects with the webadmAccount
extension will be included in the report.
```

We need the domain which contains users, we can find it in `Admin > User Domains`:

LDAP Server 1 (RCDevs Directory) ↻

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

WebADM Server Administration

WebADM v2.0.6 (64bit) running on server webadm1 (192.168.3.180) in cluster mode (2 servers). Currently handling 1 connection(s).

Server Version Details: Apache/2.4.46 PHP/7.2.34 OpenSSL/1.1.1h
Internal Server Time: 2020-10-21 14:46:35 Europe/Berlin (NTP check Ok)
Hardware Modules: No HSM Connected
WebADM Features: WebApps (Enabled), WebSrvs (Enabled), Manager (Enabled)
RCDevs Cloud Services: BASE, LICENSE, PUSH, SMS, PROOF (Connected)

Active LDAP Server: LDAP Server 1 (192.168.3.180) Active SQL Server: SQL Server 1 (192.168.3.180)
Active Session Server: Session Server 2 (192.168.3.181) Active PKI Server: PKI Server (192.168.3.180)
Active Mail Server: SMTP Server (78.141.172.203)

User Domains (3)

Associate domain names with LDAP user search bases.

Client Policies (4)

Define custom policy settings for consumer applications.

Access Devices (1)

Hardware devices for badging and physical access control.

LDAP Mount Points (2)

Connect secondary LDAP servers to the tree view.

LDAP Option Sets (1)

Define LDAP tree constraints for your 'other' administrators.

Administrator Roles (1)

Create admin role templates for your 'other' administrators.

RCDevs Directory (4)

- dc=WebADM
- o=Root (7)
 - cn=admin
 - cn=ppolicy
 - cn=test_group
 - cn=test_user1
 - cn=test_user2
 - ou=groups
 - ou=users
- Create / Search Details / Check
- ou=bercdevs.com
- ou=yorcdevs.com
- Create / Search Details / Check

In our case, we use *Default*, with the user search base corresponding to *o=root*:

LDAP Server 1 (RCDevs Directory) ↻

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

Registered LDAP Domains

- Default** (cn=Default,dc=Domains,dc=WebADM) ⓘ

Status: **Enabled** [CONFIGURE] [RENAME] [REMOVE]

Aliases: WORKGROUP

User Search Base: o=root
- bercdevs.com** (cn=bercdevs.com,dc=Domains,dc=WebADM) ⓘ

Status: **Enabled** [CONFIGURE] [RENAME] [REMOVE]

Aliases: BERCDEVCS

User Search Base: ou=bercdevs.com
- yorcdevs.com** (cn=yorcdevs.com,dc=Domains,dc=WebADM) ⓘ

Status: **Enabled** [CONFIGURE] [RENAME] [REMOVE]

Aliases: YORCDEVCS.COM

User Search Base: ou=yorcdevs.com

Group Search Base: ou=yorcdevs.com

RCDevs Directory (4)

- dc=WebADM
- o=Root (7)
 - cn=admin
 - cn=ppolicy
 - cn=test_group
 - cn=test_user1
 - cn=test_user2
 - ou=groups
 - ou=users
- Create / Search Details / Check
- ou=bercdevs.com
- ou=yorcdevs.com
- Create / Search Details / Check

```

[root@rcvm8 bin]# ./report -t Default
Are you sure you want to run report (y/n)? y
# OpenOTP user activity report.
# Generated on March 9, 2020 11:20 am

Domain, UserDN, LastLogin, LoginCount, RejectCount, TokenType, TokenSerial, TokenModel, TokenExpire,
Token2Type, Token2Serial, Token2Model, Token2Expire, Token3Type, Token3Serial, Token3Model,
Token3Expire
"Default", "cn=admin,o=Root", "2020-03-04 10:19:07", "1", "1", "TOTP", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=test_emerg,o=Root", "Never", "0", "0", "TOTP", "None", "None", "Never", "None", "None",
"None", "Never", "None", "None", "None", "Never"
"Default", "cn=centos6_ccc2b503,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=centos7_8bd783f6,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=centos8_830bc1cb,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=fedora29_ef05d856,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=fedora30_04f5ff9d,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=fedora31_e2df0dea,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=ubuntu16_4168b59b,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=ubuntu18_19b7048c,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=ubuntu19_929b83ad,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=debian8_8ae5004d,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=debian9_01aebdd,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=debian10_27e1a6b5,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"
"Default", "cn=pureos9_3b2baae3,o=Root", "Never", "0", "0", "None", "None", "None", "Never", "None",
"None", "None", "Never", "None", "None", "None", "Never"

# Generated OpenOTP report for 15 LDAP users in 0 seconds.

```

7. safenet2inv

This script allows you to convert SafeNet Token seeds into a WebADM format to use SafeNet Token with OpenOTP.

```
[root@webadm bin]# ./safenet2inv
WebADM Inventory converter for SafeNet files
Usage: safenet2inv <safenet-file> <inventory-file> <token-type>
Token type can be TOTP or HOTP
```

8. status

This script can be executed to know the OpenOTP server status and connector status.

```
[root@webadm bin]# ./status
Server Status: 1
Server: MFA Authentication Server 1.4.1-2 (WebADM 1.6.8)
System: Linux 3.10.0-862.11.6.el7.x86_64 x86_64 (64 bit)
Listener: 127.0.0.1:8080 (HTTP/1.1 SSL)
Uptime: 35 (0 days)
Memory: 550.84K
Total Requests: 0
Active Requests: 0
Connectors: OK (4 alive & 0 down)
```

9. yubi2inv

This script can be executed to convert a Yubico CSV file to a CSV inventory which can be imported in WebADM.

```
[root@webadm bin]# ./yubi2inv
WebADM Inventory converter for Yubico CSV files
Usage: ./yubi2inv <yubikey-file>
```

A Yubico CSV file has the following type of content:

```
[root@webadm bin]# cat /yubico.csv
8910111,hiuvdsnfcdee,2a8d7a21f7f9,d27f41c418b9b641ab70592835a92a55,000000000000,2020-08-13T16:07:45,
1234567,rihiuhffcdee,dd2g8a227f9,04d275c418b9b641ab70592835a92a55,000000000000,2020-08-13T16:07:45,
```

Executing the yubi2inv will output the following CSV inventory file:

```
[root@webadm bin]# ./yubi2inv /yubico.csv
# OpenOTP Inventory export for Yubikey
# Generated by OpenOTP on October 21, 2020 3:00 pm

>Type", "Reference", "Description", "Data"
"OTP Token", "0", "Yubikey #8910111",
"TokenType=WVVCStFWQ==,TokenID=,TokenKey=0n9BxBi5tkGrcFkoNakqVSqNeiH3+Q==,TokenState=M

"OTP Token", "219249058775603", "Yubikey #1234567",
"TokenType=WVVCStFWQ==,TokenID=x2fmRAIz,TokenKey=BNJ1xBi5tkGrcFkoNakqVQ==,TokenState=MA
```

This manual was prepared with great care. However, RCDevs Security S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alteration 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