

SEEDS FILE CONVERSION

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.



Seeds file conversion

[Token](#)

1. Overview

In this how-to, we will demonstrate the possible ways to convert token seed files from different formats into WebADM inventory format, allowing you to use third-party hardware tokens with RCDevs security solutions. We will also demonstrate how to re-use software tokens already registered on end-users devices with RCDevs solutions.

2. Seeds Files Format supported by WebADM

2.1 Un-encrypted Inventory

This is the format of an unencrypted RCDevs inventory file which can be imported in WebADM without any conversion:

```
# CSV import file for RCDevs WebADM
# Generated on April 9, 2019, 4:13 pm
```

```
Type, Reference, Description, Data
```

```
"OTP Token", "5292530833003", "RCDevs RC200-T6",
```

```
"TokenKey=tdxn5faLI0joNLljLrIMjUxaZXc=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,T
```

As you can see, it is CSV file with four entries for each token:

- > Type: Referring to the object type (TOTP, HOTP, OCRA or YUBIKEY)
- > Reference: The serial number of the Token
- > Description: Brief description of the object
- > Data: Configuration data for the token

This information can be seen in [WebADM](#) > [Databases](#) > [Inventoried Devices](#) like this:

WebADM Enterprise Edition v2.0.7
Copyright © 2010-2020 RCDevs Security. All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

Filters (0)

Item Type Equals Add Filter

Valid Lost Broken Expired Enabled Disabled

Display Options

Retrieve max 1000

Page results 30

Refresh

Inventory Actions

- Delete selected items
- Scope selected items
- Re-encrypt inventory
- Check Links / Scopes
- Import from CSV file
- Export as CSV / XML

	Item Type	Reference	Description	Import Date	User DN	Usage Scope	Inventory Data	Enabled	Status
<input type="checkbox"/>	OTP Token	8142984577510	Yubddikey #2573127	2020-11-09 11:22:49	Link [NA]	Add [NA]	5 Data (Software encryption)	<input checked="" type="checkbox"/>	Valid

As you can see from the above inventory example, the Data field contains multiple items that you need to adjust according to the properties of your tokens.

Note

All entries below must be base64 encoded to be imported into WebADM.

The **Data** field contents in RCDevs inventory files are the following:

- › TokenKey: Token secret key value.
- › TokenType: TOTP (time-based), HOTP (event-based), OCRA or YUBIKEY according to your token type.
- › TokenState: This is the time offset value for TOTP and counter value for HOTP tokens. Set to 0 by default. If you are not able to provide the actual value, a Token resynchronization may be required.
- › OTPLength: 6, 8 or 10. This setting depends on your OTP length generated by your tokens.
- › TOTPTimeStep: 30 or 60 seconds. Useful for TOTP Token. Must match the TOTP Time Step setting of your OpenOTP server.

2.2 Encrypted Inventory

In case you have purchased RCDevs hardware tokens and are using Enterprise Edition of OpenOTP you will receive an encrypted inventory file. To protect the token secrets, the encrypted inventory file can only be imported and decrypted by WebADM running with the correct associated license file. Without the proper enterprise license, you will not be able to import it in WebADM.

An RCDevs encrypted seeds file looks like:

Inventory Import File for RCDevs WebADM
Generated on June 20, 2019, 12:55 pm
Encrypted for use with <CUSTOMER> customer license
MD5: 68bc02730eefba1216570d8f38a4e7bd

-----BEGIN RCDEVS INVENTORY DATA-----

MCW7jYTpRgP9g0Z5N+Y2+7DobUzK2buPg9yVelhAH+LwDwLQwLZVUamK+164mGx
yckzsWINYX97kN2CylwZxw/qm+Y172v9GwGbQKNRmPaLMQVt3K7X/zlYYtDW1lo
oKSDN2iNovPPTH5RjDLuCbC3qXvWkTktQN7GqrMJnOyZyAXzT6klJoleNUBVMrV6
MCRdPp44Zbefnwhq50gH0dF9g2XglZGogmAbBujkRlbl5QzGvj5Y3OoHR74TzprF
njOlutexlFfKchOG0gtLjmX/GBpme4E8k/z+uaZq8Bjf5xDxAoXB2mRqfkzYeZXy
Rg/hSuKmvQrg051hx4cQfPIRootYsXMudXJ4vvKQTC1h5gCJ6g8yeCR3okFhpYnk
1q7EAiaM24qo2MXq6Hg6iDwxdXuSYKOUuX9nHGngu1aFfK449Z77TrnrqDAenvyCI
kLFGZ9zgHqsmHEz4syV66PF1rjt3qiaU41AobSKOKPz2MRMIBZ8RSr6zAUcBlimj
Uexg1HUktNDvkGG5mJnNztBukrg6f79gsZNUDipb0VljpYCXT4Jkleg/pKe44qEI
lMgRqqi+cCDoSWidWXfacdr7Vn/RTL01katNTwP5nZluMdkCzPTfA5kjv0lQyB9y
mlRf2XoKcB8gM210hgQKQ9FIdDNMHBp9733iK4R3Ya2+Q/T82P5mtdHuYhPWRkFH
mkCy8YJ448Fi+71qwN1HrdDiK+/Xg2261DOX/dQ1AwNSuNLB5RdSDwHa0AOiq3ps
SFcK+vhK0n/OyLZpP5zOHEYS94ElkAVNQF+YFwGcRZE0ki4lySPDtgknnETZireb
hXy6OsqfHb3R3IZjxFLU7TUqbkdXlJnx+QckjiYsDwK6JKwUn0BgBkNlJ91Wwlz
BYZimc+W0GS7iLbe1TqgCN/epZQhg3gqmtYUelHPamW9a37sq48cyFG/EB0P2G/r
FSq5Tjz+gjQYFpyAhD0VWjO9/gFqBp8QuBLg5kzoupgT3boGsogy0CDe8u0eVTkP
F3HRHhg8j57CtR0oRHggo9y2alnYKqz7NdCYtc71N6lzhQNfEixU0MvcTllwTV/dy
OjtU+fTE7cbrPmBvg4+8elCMEeCEd2QwZdTqBuSM6OEI/2XenGB2K/R70MUeNtSM
k/qoOSlker0UIYvyWAl4WBqbQG9pvD926I2vp/gHkhR52I9KK2f2pB+qiO9Y2KNh
GUdes6mNTrKBZ58kES3ZH8JCgaEiPujboOI8rRdtzuv0yLXxaGYlgdfsoyCv/ba9
aB75XuNSXswsd26jlldc01txPRjx5idp3W9Pyskmfju03n2SZDlpjM6gybe+AxfS
K43uzVHEk6nOmrqb+1uXwjih3T81t81t7HmqI0yzaIFO7WS6QgzniQNo3mTdLgzY
RXUtiB0pRBaRblVeFM5UzO7z+tjzyhGETPG/hX00ESvBB9zRINSZzRQkHOkDGy5C
wiO6sF5JjvPo9M+3/Ughpili845nGKMIjd2QC5otOZwzQqDvzgb+WLqavqNRdHdd
p2x2rns+GLX6187ncvUDmcKukB/ANCSggz3iedbco1DdnNQNCv2KMQM6LHovcNZ
VVUraZ7QuVAfuGHYBZzCDUKU7vO/zwvMu7hPnuS1GVf0Xm68EApuOAeajYA615Es
s1S2YkMEa1ALimHoV6T4ND26Sw0D+GxaW6q33qBJEvWSecy0x1biUbCEl3kAjSoT
0g7SA82WoOa6NH+jQBWdY0IfID1JZu8ctJGf77iZ523WpHtcqjmNfUM8Xq0DMVjV
8g3gCOBvYgIpHITp7OSa4scloVhmJE723Rxt7I1kCH+dcjioWBuj1/S/Oh97IEXsj
PVQqhux/BmxMwqM5lihG68k/Va0OPuWJUG5+UEHD5yx2md6rijmio228p8X6Zsvh
v2A/PnXaA7z8F9BiRFMcyTHzNQWNjTodi52Htnf0LOK1gCIHfTBEOvGVLs5FnOx
nVupskBe/QE6E8uOXQ65Ue3qlG5iWG6cu+igHCtDPV7m0C7KX0TXCnel6k7qbNPQ
SmoC/4N627k5aR5Em/LEzcDH8vmCyde+UeaAOm5hPBEDSaDAeeolFRFrFVduO0F6
ldnBVTUjwjBolnBJ71QlJZHse6zwLw1/RBpLpR1k9v1Jf1+ZPQAogxu5vXkSBVXb

-----END RCDEVS INVENTORY DATA-----

No conversion or data extraction is possible with this kind of inventory file. If your objective is to use the RCDevs Tokens with another solution than WebADM, you should contact the RCDevs sales team and ask for Token seeds in standard PSKC format.

3. Seeds Files Conversions for Hardware Token import

To use hardware Tokens from another provider, you have to convert the seeds file from your provider to the format supported by WebADM. The format is described in part [2.1 Un-encrypted inventory](#). Once the file is adjusted, then you can [import your new inventory file](#) into WebADM database.

3.1 Deepnetsecurity Tokens (SafeID/Mini) conversion into WebADM Inventory

This is an example of Deepnet Security inventory file:

```
<data>

<header>

<manufacturerCode>DN</manufacturerCode>

<productCode>ST</productCode>

<encode>HEX</encode>

<encrypt>AES256</encrypt>

</header>

<tokens>

<token>
<serial>12345678</serial>
<seed>1A2B2395A3B45D11AFBADC510FE860035C4ED6925B12064B3B02D6FB99C5519A</seed>
</token>

</tokens>

</data>
```

In this case, the secret is `1A2B2395A3B45D11AFBADC510FE860035C4ED6925B12064B3B02D6FB99C5519A` in Hexadecimal format (this means that you have to convert first the value from Hexadecimal to Base64 to be managed by WebADM).

› **HEXADECIMAL** = 1A2B2395A3B45D11AFBADC510FE860035C4ED6925B12064B3B02D6FB99C5519A

Converted to:

› **Base64** = Gisjla00XRGvutxRD+hgA1xO1pJbEgZLOWLW+5nFUZo=

The **Serial** value must be used as **Reference** value after conversion for WebADM. This value is used for Hardware Token assignation and **should not be converted**.

After conversion, the seed file looks like this:

Type, Reference, Description, Data

"OTP Token", "12345678", "SafeID/Mini",

"TokenKey=Gisjla00XRGvutxRD+hgA1xO1pJbEgZLOWLW+5nFUZo=,TokenType=VE9UUA==,TokenState=M.

I can now import that file into my WebADM inventory database.

WebADM Enterprise Edition v2.0.7

Copyright © 2010-2020 RCDevs Security, All Rights Reserved

API

Home

Admin

Cluster

Create

Search

Import

Databases

Statistics

Applications

About

Logout

Inventory Items CSV Import

Import File:

Browse...

tokens.csv

Type of File:

RCDevs Inventory

Import as Active:

Yes No

Visibility Scope:

Select

WebADM Inventory files are provided as cleartext or encrypted CSV files.
Encrypted CSV file are available only if you own a valid Enterprise license.

If you are importing Yubikey Token data provided by Yubico or generated
by the 'Yubikey Personalization Tool', then choose the 'Yubico CVS' above.

If you import a CSV file generated by the 'Yubikey Personalization Tool',
please configure the 'Yubico format' under the settings tab in the tool.

Import

Cancel

WebADM Enterprise Edition v2.0.7

Copyright © 2010-2020 RCDevs Security, All Rights Reserved

API

Home

Admin

Cluster

Create

Search

Import

Databases

Statistics

Applications

About

Logout

Inventory Items CSV Import

Processing record 1/5 OTP Token:8142984577587 (dddYubikey #2573124)... Ok

Processing record 2/5 OTP Token:8142984577588 (Yubikedy #2573125)... Ok

Processing record 3/5 OTP Token:8142984577589 (Yubikeyd #2573126)... Ok

Processing record 4/5 OTP Token:8142984577510 (Yubddikey #2573127)... Ok

Processing record 5/5 OTP Token:8142984577511 (Yubikdey #2573128)... Ok

Ok

WebADM Enterprise Edition v2.0.7
Copyright © 2010-2020 RCDevs Security. All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

Filters (0)

Item Type Equals Add Filter

Valid Lost Broken Expired Enabled Disabled

Display Options

Retrieve max 1000

Page results 30

Refresh

Inventory Actions

- Delete selected items
- Scope selected items
- Re-encrypt inventory
- Check Links / Scopes
- Import from CSV file
- Export as CSV / XML

Item Type	Reference	Description	Import Date	User DN	Usage Scope	Inventory Data	Enabled	Status
OTP Token	8142984577510	Yubddikey #2573127	2020-11-09 11:22:49	Link [NA]	Add [NA]	5 Data (Software encryption)	Enabled	Valid

I can assign this token to a user using the Token Reference. Have a look on the following documentation for [Hardware Token Assignment](#).

The Token may require resynchronization to be used correctly. Have a look on part [Resync Hardware or Software Tokens](#) to perform the token resynchronization.

3.2 PSKC Files conversion into WebADM Inventory

If you already have a standard PSKC file from your Token provider, then you can use the following script on your WebADM instance to convert your PSKC file into a WebADM inventory file:

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

Here is an example of PSKC seeds file who can be provided by RCDevs (PSKC format is only provided by RCDevs if asked by the customer):

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

```

<?xml version="1.0" encoding="UTF-8"?>
<!--
OATH PSKC import file for RCDevs WebADM
Generated on April 9, 2019, 4:13 pm
-->

<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>5292530833003</SerialNo>
    <Model>RCDevs RC200-T6</Model>
  </DeviceInfo>
  <Key Algorithm="urn:ietf:params:xml:ns:keyprov:pskc:totp" Id="5292530833003">
    <AlgorithmParameters>
      <ResponseFormat Length="6" Encoding="DECIMAL"/>
    </AlgorithmParameters>
    <Data>
      <Secret>
        <PlainValue>tdxn5faLI0joNLljLrIMjUxaZXc=</PlainValue>
      </Secret>
      <Time>
        <PlainValue>0</PlainValue>
      </Time>
      <TimeInterval>
        <PlainValue>30</PlainValue>
      </TimeInterval>
    </Data>
  </Key>
</KeyPackage>
</KeyContainer>

```

To convert it into a WebADM inventory file, I use the pskc2inv script like below:

```

[root@webadm bin]# ./pskc2inv pskc.csv webadm_inv.csv
Successfully converted 1 PSKC tokens.
[root@webadm bin]#

```

The new WebADM inventory file has been created and can be imported through WebADM admin GUI.


```
[root@webadm bin]# cat webadm_inv.csv
# OpenOTP Inventory export for OATH PSKC
# Generated by OpenOTP on January 3, 2020 10:03 am

"Type", "Reference", "Description", "Data"
"OTP Token", "5292530833003", "RCDevs RC200-T6",
"TokenType=VE9UUA==,TokenKey=tdxn5faLI0joNLljLrIMjUxaZXc=,OTPLength=Ng==,TOTPTimeStep=MzA=
```

3.3 Safenet/Gemalto Seeds File conversion into WebADM Inventory

RCDevs also provides a script to convert Safenet seeds file into a WebADM inventory file:

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

4. Software Tokens Migration from another Solution to WebADM

If you already have software Tokens registered on end-user devices, the token can be re-used with WebADM and OpenOTP if you still have the secret keys of the registered tokens. This can be done by Manual Token Registration on a user account through WebADM Admin GUI, API or Self-Services.

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 v2.0.7

Copyright © 2010-2020 RCDevs Security, All Rights Reserved

API

Home

Admin

Cluster

Create

Search

Import

Databases

Statistics

Applications

About

Logout


Register / Unregister OTP Tokens for `cn=tester,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.

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: Primary 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

This is the API method and description which can be used to do the same thing:

Register a TOTP Token		
Method: <code>OpenOTP.TOTP_Register</code> Returns: <code>Boolean</code>		
Required Parameters <ul style="list-style-type: none"> • <code>dn</code> (String) • <code>key</code> (Base64) 	Optional Parameters <ul style="list-style-type: none"> • <code>state</code> (String) • <code>session</code> (String) • <code>id</code> (Integer) 	<p>The key is the Token binary random seed and must be base64-encoded. Key length can be:</p> <ul style="list-style-type: none"> - 20 Bytes for a SHA1 OATH Token - 32 Bytes for a SHA256 OATH Token - 64 Bytes for a SHA512 OATH Token <p>The id indicates which Token is registered if multiple Tokens are allowed. By default (when id is not set) the primary Token is selected.</p> <p>Returns true on success and false on error.</p>

For example, I can re-use my Token registered on my Google Authenticator if I know the following information regarding my Token:

- > Token Type: TOTP, HOTP or OCRA.

- › Key Algorithm: SHA1, SHA256, SHA512. (SHA1 by default)
- › Key Format: Hexadecimal, Base32, Base64
- › Secret Key: The secret key of your current Token.

The secret key size depends on the chosen key algorithm. By default, the size of the accepted keys have the following length:

- › SHA1 - 20 bytes
- › SHA256 - 32 bytes
- › SHA512 - 64 bytes

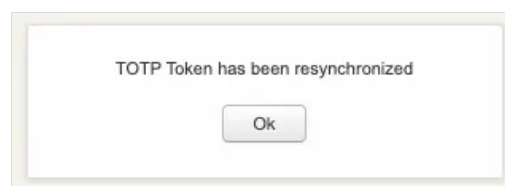
To allow non-standard key sizes, the SHA1 algorithm is assumed for all other key sizes in the WebADM.

5. Resynchronize Hardware or Software Tokens

To resynchronize a Token, the Token must be assigned to a user account. Once the Token is assigned to a user, click on that user account through WebADM GUI > **Application Actions** > **MFA Authentication Server** > **Resynchronize Tokens**. Enter the current OTP provided by the Token and click the **Resync** button.

The screenshot shows the WebADM Enterprise Edition v2.0.7 web interface. The top navigation bar includes links for Home, Admin, Cluster, Create, Search, Import, Databases, Statistics, Applications, About, and Logout. The main content area is titled 'Resynchronize Tokens for cn=ttester,o=Root'. It contains instructions: 'TOTP Token just need to have time correctly set to be synchronized. Adjust the Token time with the time displayed below.' Below this, there is a 'Current Time' field showing '11/09/2020 2:24:46 PM' and a 'Current OTP' field with the value '955878' entered. At the bottom, there are two buttons: 'Resync' and 'Cancel'.

You should have a message like below if the synchronization process worked:



Event-based tokens can be resynchronized either by providing the counter value or by generating two sequential OTP's and providing them in the resynchronization page.

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 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