HOW TO USE YOUR YUBIKEY WITH RCDEVS

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.

How to use your Yubikey with RCDevs

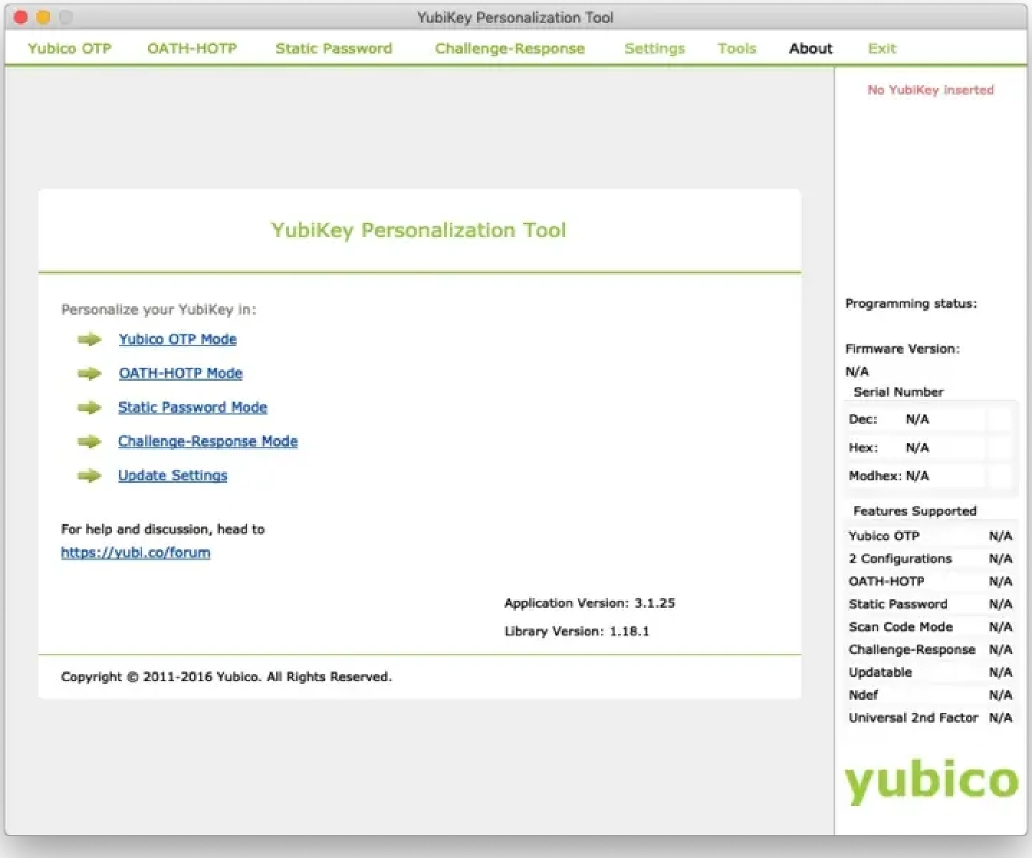
Yubico Yubikeys

1. Overview

In this How-To, we will demonstrate how to reprogram your Yubikey with the Yubikey Personalization Tool, to generate an inventory file through Yubico tool to import the Yubikey in WebADM inventory and how to assign and use your Yubikey with OpenOTP. For this recipe, you will need to have WebADM and OpenOTP installed and configured. Please, refer to WebADM Installation Guide and WebADM Manual.

2. Yubico Personalization Tool

Once Yubico Personalization Tool is installed, open it.



No YubiKey inserted

YubiKey Personalization Tool

Personalize your YubiKey in:

- Yubico OTP Mode
- OATH-HOTP Mode
- Static Password Mode
- Challenge-Response Mode
- Update Settings

For help and discussion, head to https://yubi.co/forum

Application Version: 3.1.25

Library Version: 1.18.1

Copyright © 2011-2016 Yubico. All Rights Reserved.

Programming status:

Firmware Version:
N/A

Serial Number

Dec:	N/A
Hex:	N/A
Modhex:	N/A

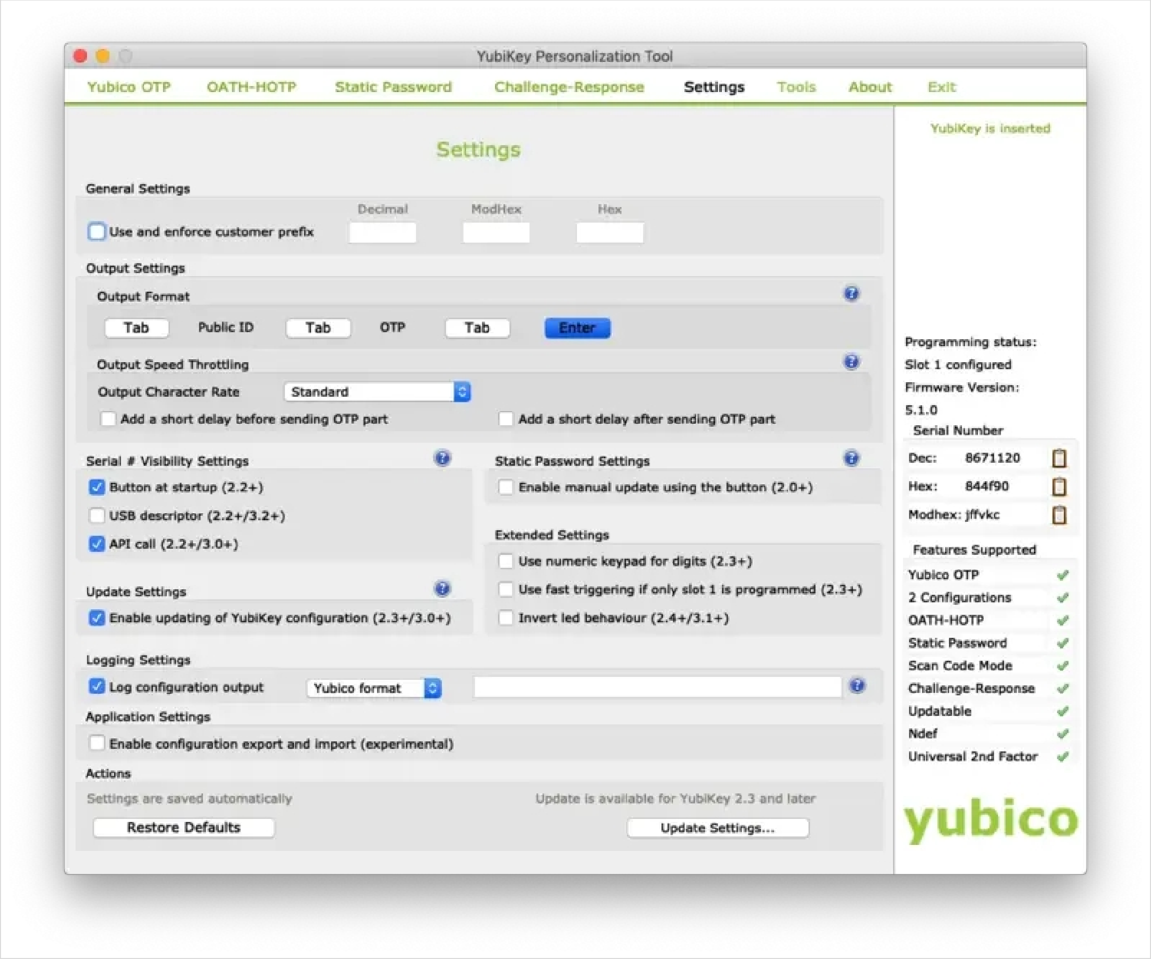
Features Supported

Yubico OTP	N/A
2 Configurations	N/A
OATH-HOTP	N/A
Static Password	N/A
Scan Code Mode	N/A
Challenge-Response	N/A
Updatable	N/A
Ndef	N/A
Universal 2nd Factor	N/A

⚠ Important Note

To be sure that you have the right settings from the beginning, you should click on `Restore Defaults` under `Setting` in the Yubico Personalization Tool before you continue.

When you are under the application, go on the `Setting` page and configure the `Log configuration output` setting to `Yubico format`.



Settings

General Settings

□ Use and enforce customer prefix — Decimal / ModHex / Hex

Output Settings

Output Format: Tab, Public ID, Tab, OTP, Tab, Enter

Output Speed Throttling

Output Character Rate: Standard

□ Add a short delay before sending OTP part

□ Add a short delay after sending OTP part

Serial # Visibility Settings

☑ Button at startup (2.2+)

□ USB descriptor (2.2+/3.2+)

☑ API call (2.2+/3.0+)

Static Password Settings

□ Enable manual update using the button (2.0+)

Extended Settings

□ Use numeric keypad for digits (2.3+)

□ Use fast triggering if only slot 1 is programmed (2.3+)

□ Invert led behaviour (2.4+/3.1+)

Update Settings

☑ Enable updating of YubiKey configuration (2.3+/3.0+)

Logging Settings

☑ Log configuration output — Yubico format

Application Settings

□ Enable configuration export and import (experimental)

Actions

Settings are saved automatically

Update is available for YubiKey 2.3 and later

YubiKey is inserted

Programming status:
Slot 1 configured
Firmware Version:
5.1.0

Serial Number

Dec:	8671120
Hex:	844f90
Modhex:	jffvkc

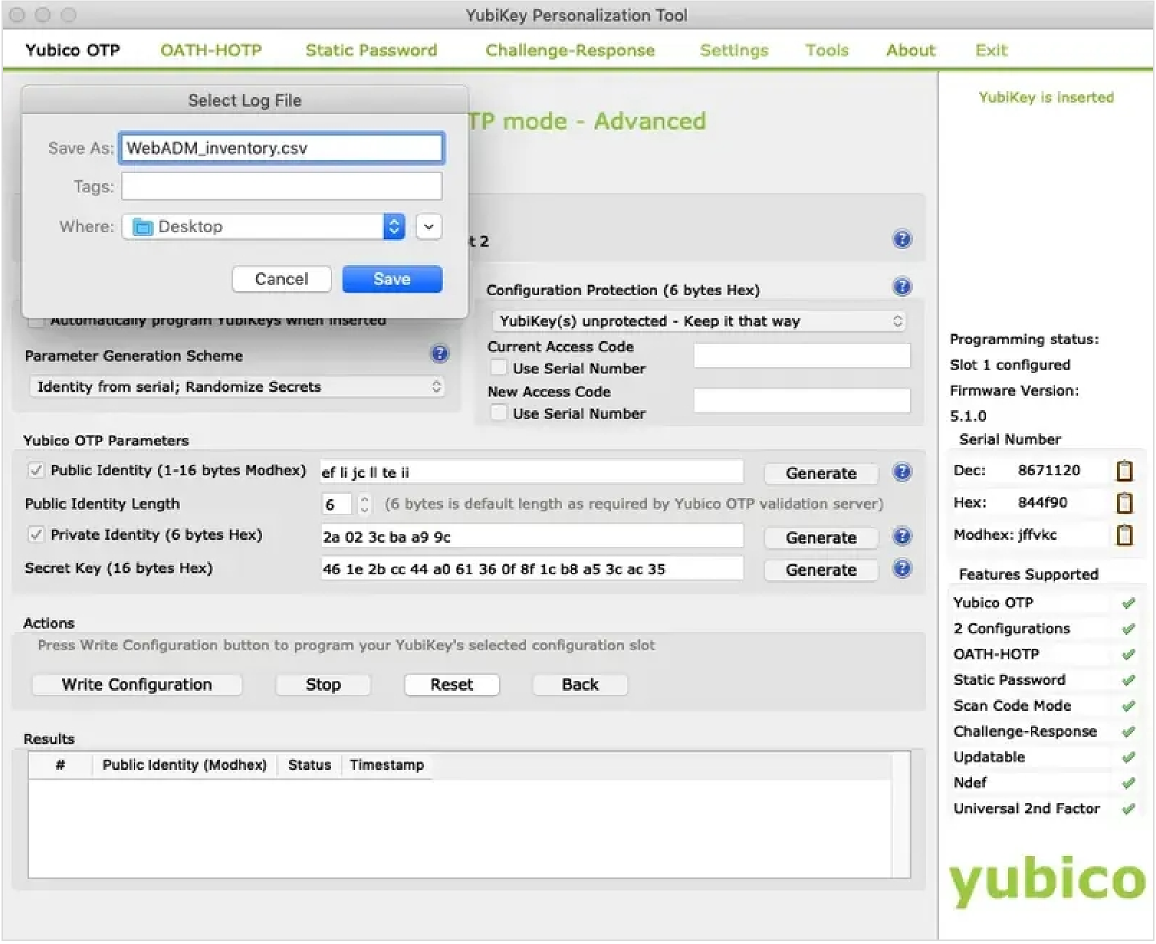
Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✓
Universal 2nd Factor	✓

When you have configured this setting, plug in your Yubikey. Then switch to the `Yubico OTP` tab and click on `Advanced`. Select Configuration Slot 1.

Click on the 3 `Generate` buttons to generate a new Public/Private Identity and a new Secret Key.

After that, click on `Write Configuration` button, and you will be prompted to save the inventory file:



Select Log File

Save As: WebADM_inventory.csv

Tags:

Where: Desktop

TP mode - Advanced

t 2

Configuration Protection (6 bytes Hex): YubiKey(s) unprotected - Keep it that way

Current Access Code
□ Use Serial Number

New Access Code
□ Use Serial Number

Automatically program YubiKeys when inserted

Parameter Generation Scheme: Identity from serial; Randomize Secrets

Yubico OTP Parameters

☑ Public Identity (1-16 bytes Modhex): ef li jc ll te ii

Public Identity Length: 6 (6 bytes is default length as required by Yubico OTP validation server)

☑ Private Identity (6 bytes Hex): 2a 02 3c ba a9 9c

Secret Key (16 bytes Hex): 46 1e 2b cc 44 a0 61 36 0f 8f 1c b8 a5 3c ac 35

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

Results

#	Public Identity (Modhex)	Status	Timestamp

YubiKey is inserted

Programming status:
Slot 1 configured
Firmware Version:
5.1.0

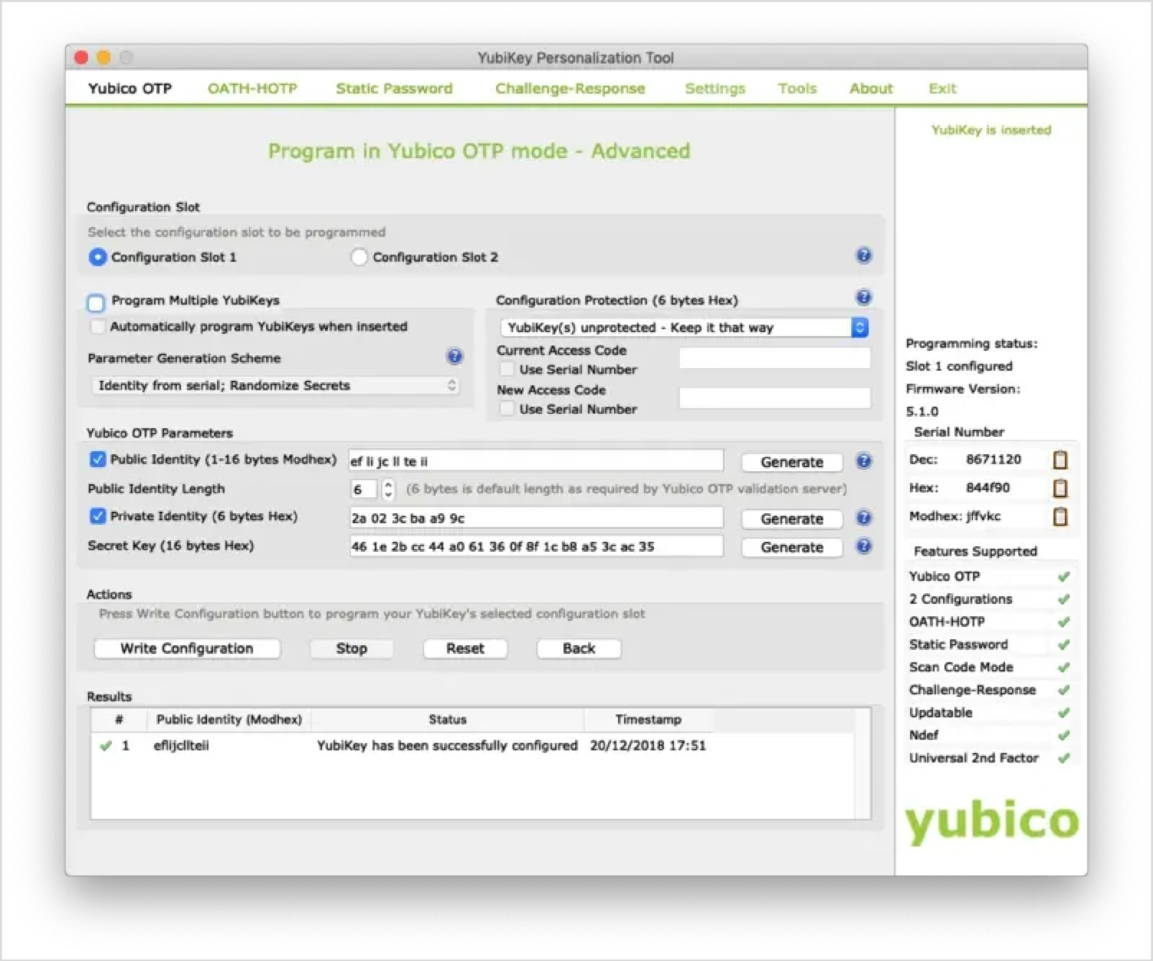
Serial Number

Dec:	8671120
Hex:	844f90
Modhex:	jffvkc

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✓
Universal 2nd Factor	✓

Save this file. We will import it in WebADM inventory in the next step.



Program in Yubico OTP mode - Advanced

Configuration Slot

Select the configuration slot to be programmed

● Configuration Slot 1 ○ Configuration Slot 2

□ Program Multiple YubiKeys

□ Automatically program YubiKeys when inserted

Parameter Generation Scheme: Identity from serial; Randomize Secrets

Configuration Protection (6 bytes Hex): YubiKey(s) unprotected - Keep it that way

Current Access Code
□ Use Serial Number

New Access Code
□ Use Serial Number

Yubico OTP Parameters

☑ Public Identity (1-16 bytes Modhex): ef li jc ll te ii

Public Identity Length: 6 (6 bytes is default length as required by Yubico OTP validation server)

☑ Private Identity (6 bytes Hex): 2a 02 3c ba a9 9c

Secret Key (16 bytes Hex): 46 1e 2b cc 44 a0 61 36 0f 8f 1c b8 a5 3c ac 35

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

Results

#	Public Identity (Modhex)	Status	Timestamp
✓ 1	eflijclteli	YubiKey has been successfully configured	20/12/2018 17:51

YubiKey is inserted

Programming status:
Slot 1 configured
Firmware Version:
5.1.0

Serial Number

Dec:	8671120
Hex:	844f90
Modhex:	jffvkc

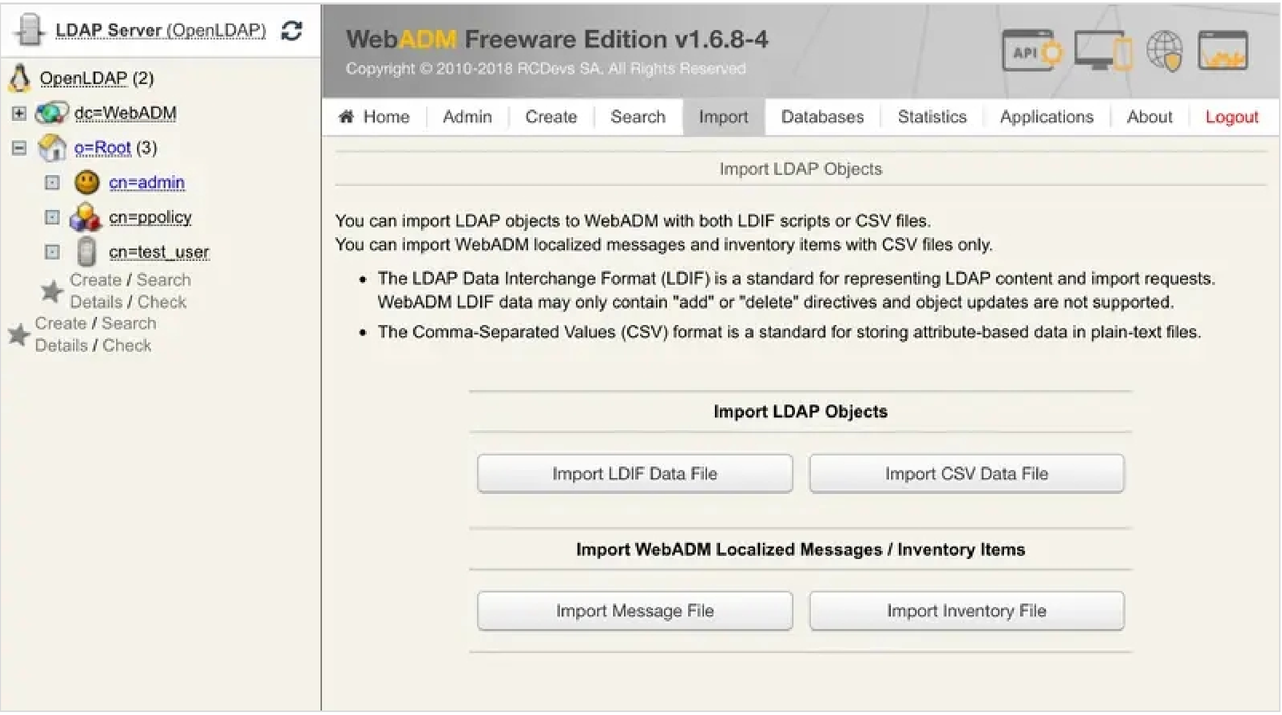
Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✓
Universal 2nd Factor	✓

3. Import Yubikey inventory file in WebADM

We have now reprogrammed our Yubikey and generate an inventory for it. We will now import the inventory file under WebADM to be able to use this Yubikey with OpenOTP, Spankey…

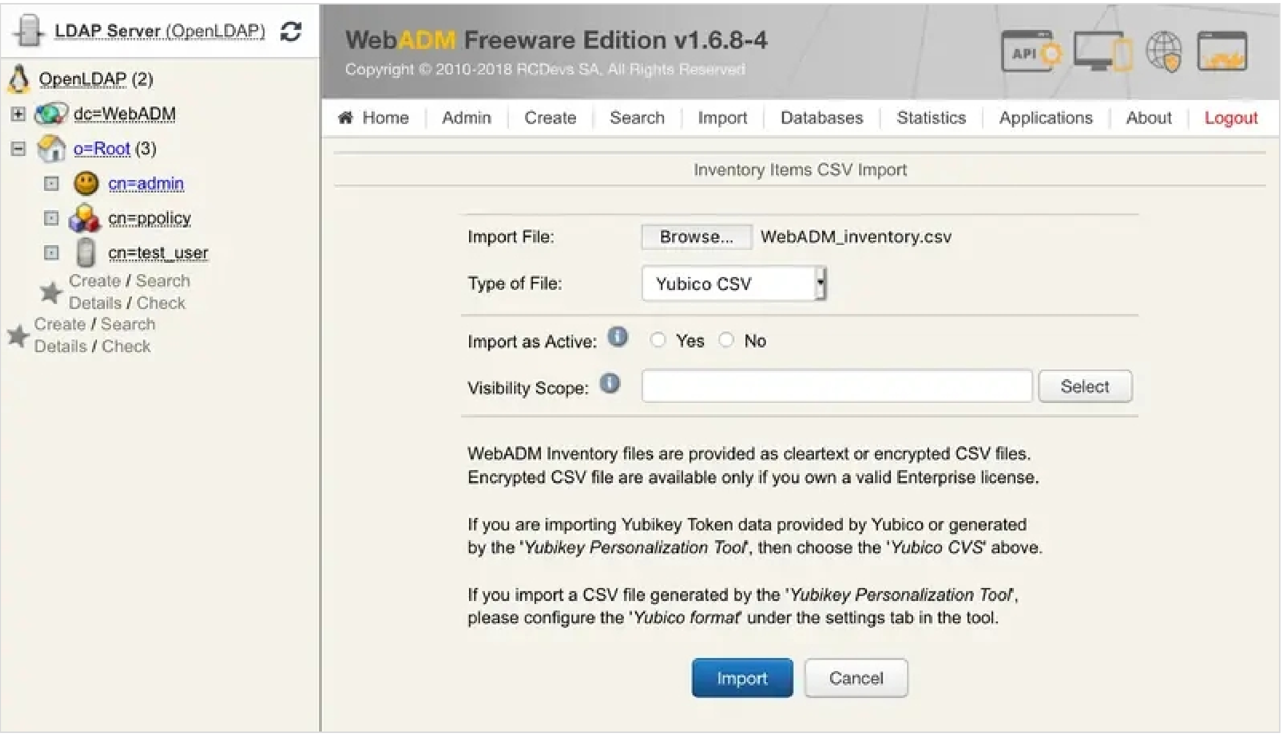
Now, go on the WebADM Admin GUI and click on the `Import` tab.



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.

On that page, click on `Import Inventory File` button.



Import File: Browse... WebADM_inventory.csv

Type of File: Yubico CSV

Import as Active: ○ Yes ○ No

Visibility Scope: Select

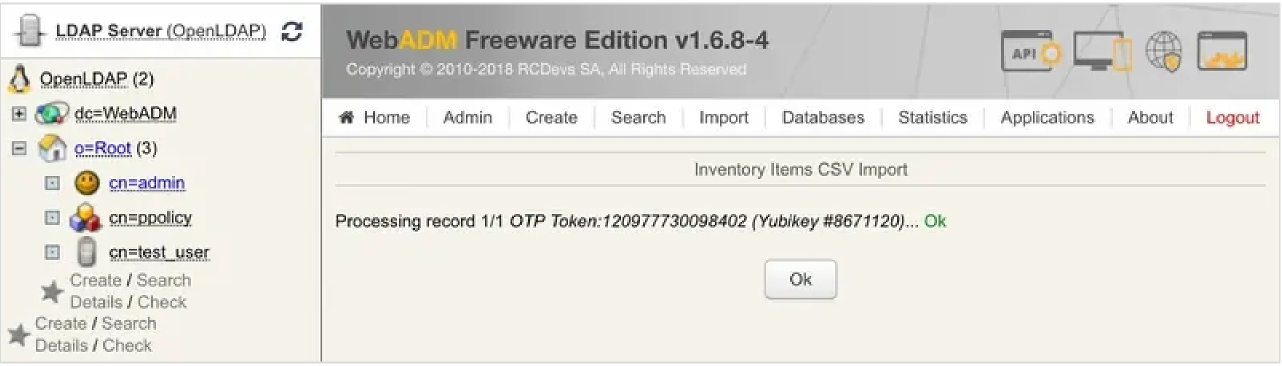
WebADM Inventory files are provided as cleartext or encrypted CSV files.
Encrypted CSV file are available only if you own a valid Enterprise license.

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.

In `Type of File` select: `Yubico CSV` and browse your Inventory file previously created through the Yubikey Personalization Tool.

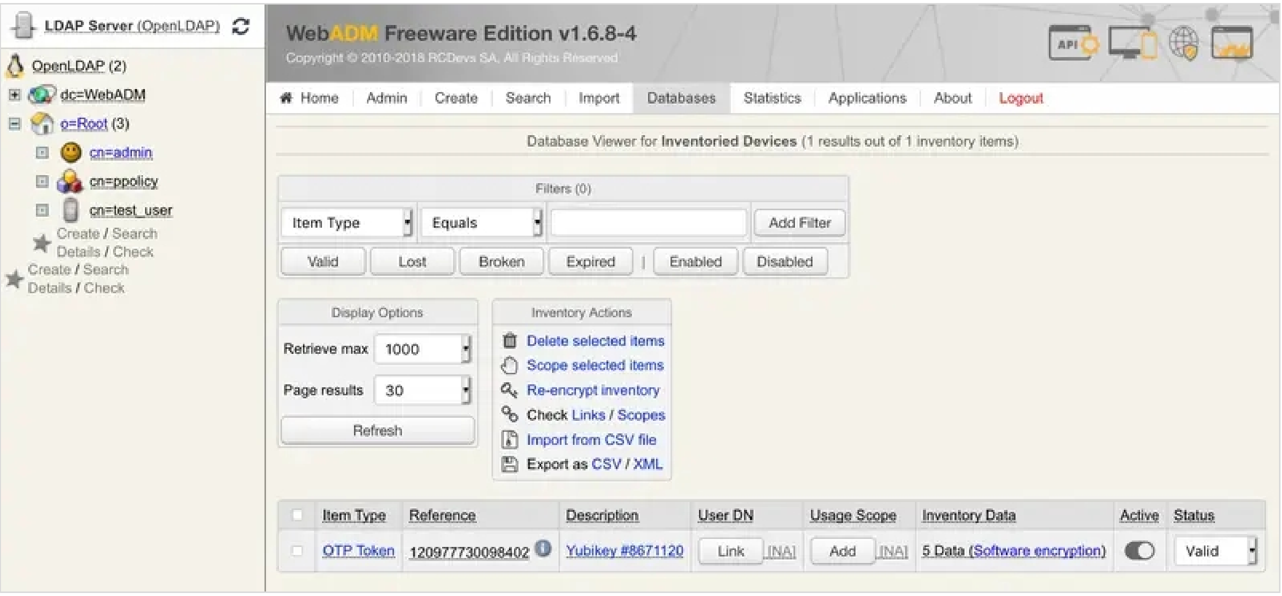
Click the `Import` button and the Yubikey should be successfully imported.



Inventory Items CSV Import

Processing record 1/1 *OTP Token:120977730098402 (Yubikey #8671120)*... Ok

You can check the Inventory table to see the new entry. Click on `Databases` tab and `Inventoried Devices`. You can see my new entry below.



Database Viewer for **Inventoried Devices** (1 results out of 1 inventory items)

Retrieve max: 1000

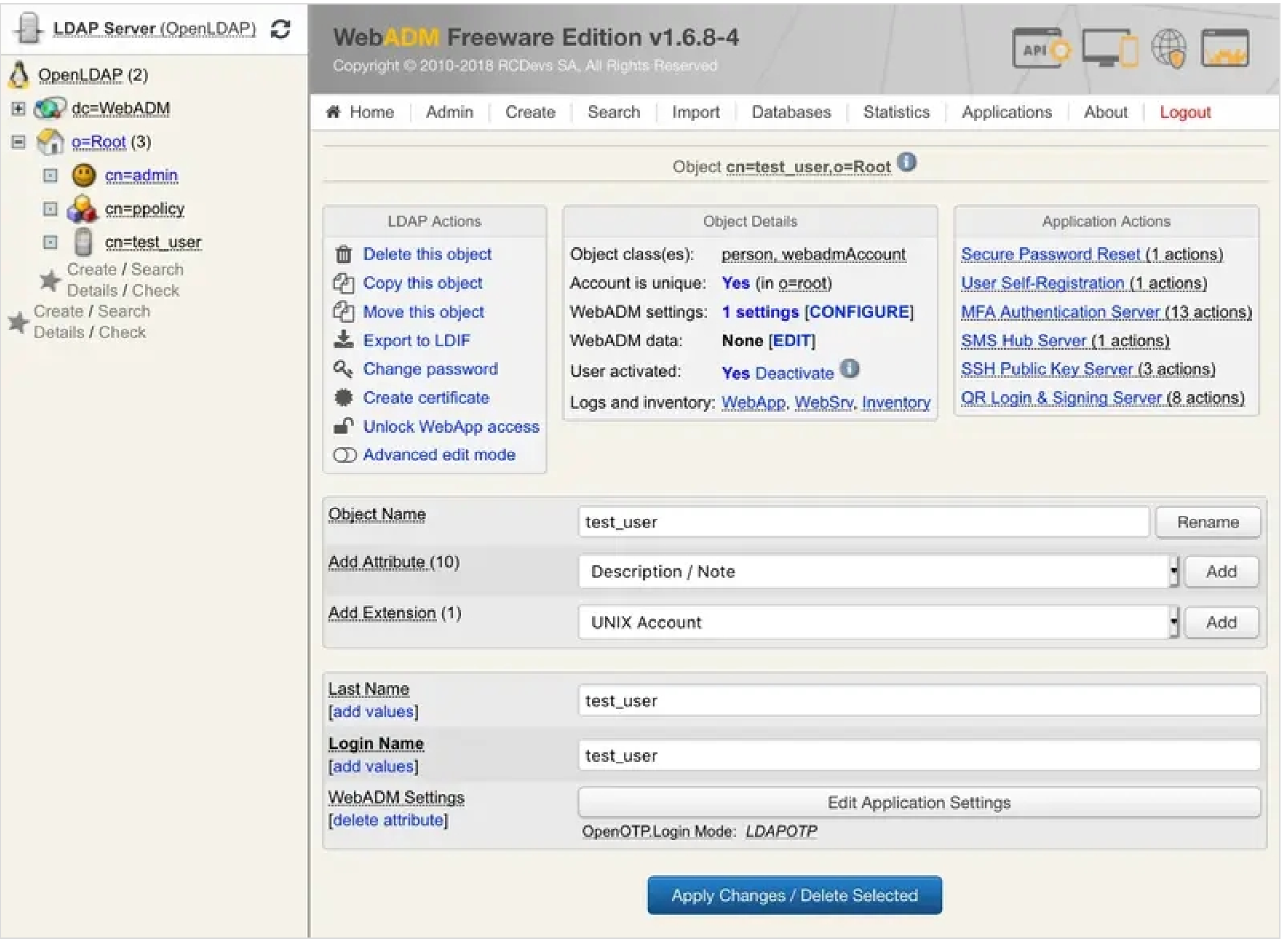
Page results: 30

□	Item Type	Reference	Description	User DN	Usage Scope	Inventory Data	Active	Status
□	OTP Token	120977730098402	Yubikey #8671120	Link [NA]	Add [NA]	5 Data (Software encryption)	●	Valid

I'm now able to assign this Yubikey to a user account, that step will be the part of the next section.

4. Assign a Yubikey to a user account

The Yubikey can be assigned to a user through the WebADM Admin GUI or through the User Self-Service Desk (SelfDesk) and User Self-Registration (SelfReg) applications. Here we will assign the Yubikey to the user through the Admin GUI. Click on an Activated User account in the left tree.



Object cn=test_user,o=Root

LDAP Actions
- Delete this object
- Copy this object
- Move this object
- Export to LDIF
- Change password
- Create certificate
- Unlock WebApp access
- Advanced edit mode

Object Details

Object class(es):	person, webadmAccount
Account is unique:	Yes (in o=root)
WebADM settings:	1 settings [CONFIGURE]
WebADM data:	None [EDIT]
User activated:	Yes Deactivate
Logs and inventory:	WebApp, WebSrv, Inventory

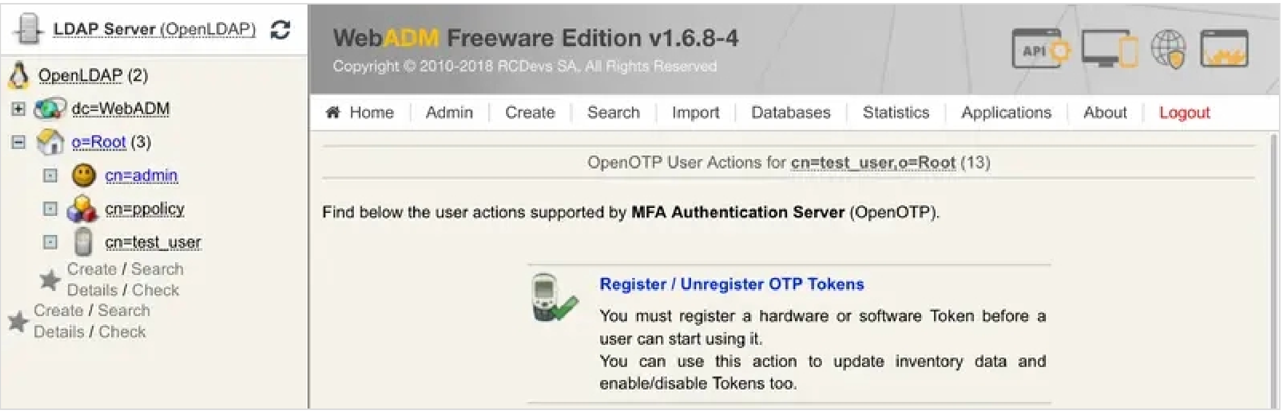
Application Actions
- Secure Password Reset (1 actions)
- User Self-Registration (1 actions)
- MFA Authentication Server (13 actions)
- SMS Hub Server (1 actions)
- SSH Public Key Server (3 actions)
- QR Login & Signing Server (8 actions)

Object Name	test_user	Rename
Add Attribute (10)	Description / Note	Add
Add Extension (1)	UNIX Account	Add

Last Name [add values]	test_user
Login Name [add values]	test_user
WebADM Settings [delete attribute]	Edit Application Settings OpenOTP.Login Mode: *LDAPOTP*

Apply Changes / Delete Selected

Click on `MFA authentication Server` under `Application Actions` Box and then `Register/Unregister OTP Tokens`.



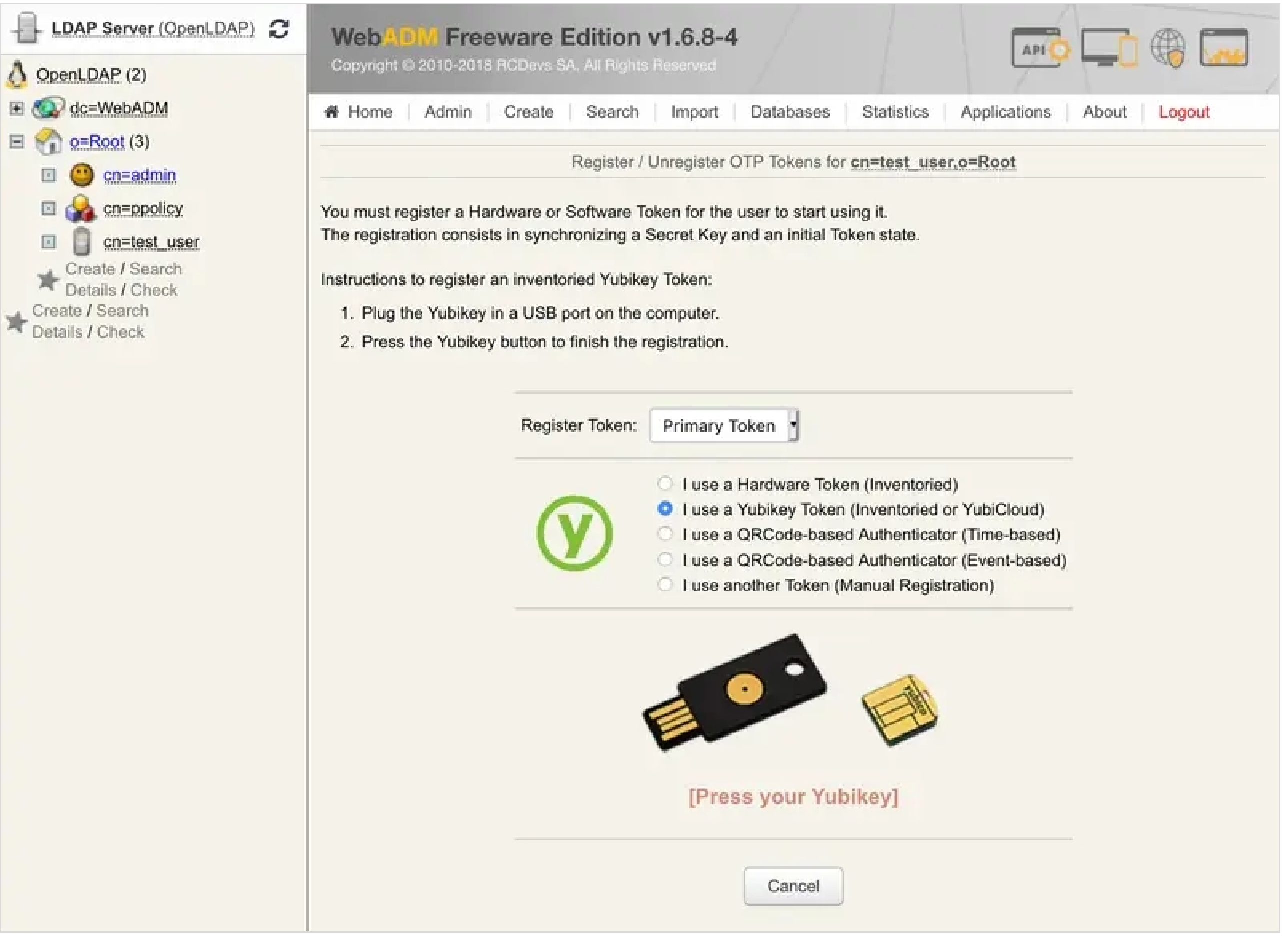
OpenOTP User Actions for cn=test_user,o=Root (13)

Find below the user actions supported by **MFA Authentication Server** (OpenOTP).

Register / Unregister OTP Tokens

You must register a hardware or software Token before a user can start using it.
You can use this action to update inventory data and enable/disable Tokens too.

Register your Token and choose `Primary Token` and check the box `I use a Yubikey Token`.



Register / Unregister OTP Tokens for cn=test_user,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 register an inventoried Yubikey Token:

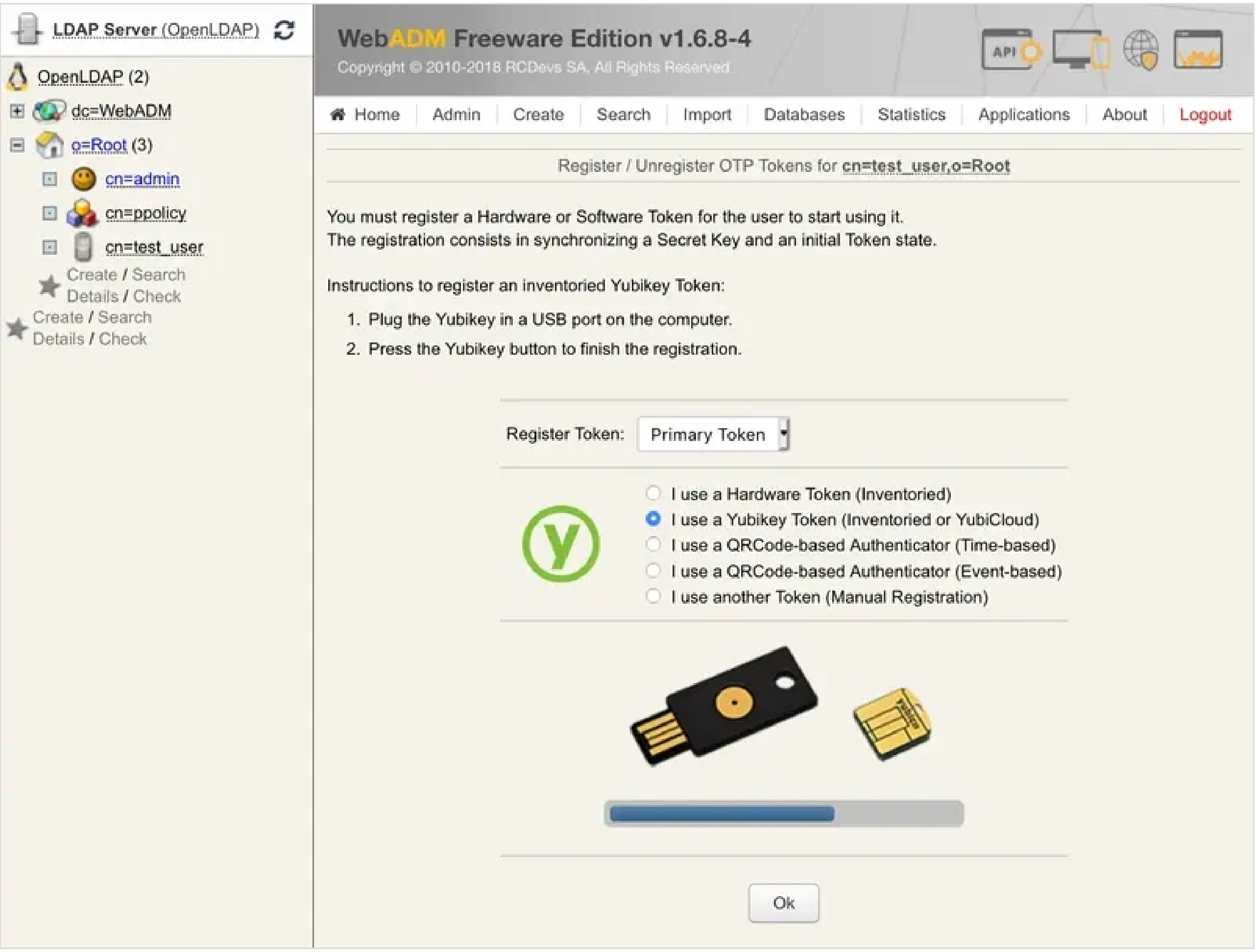
1. Plug the Yubikey in a USB port on the computer.
2. Press the Yubikey button to finish the registration.

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)

[Press your Yubikey]

At this step, you just have to short touch your Yubikey for selection Slot 1 and to enroll it on the user account.



Register / Unregister OTP Tokens for cn=test_user,o=Root

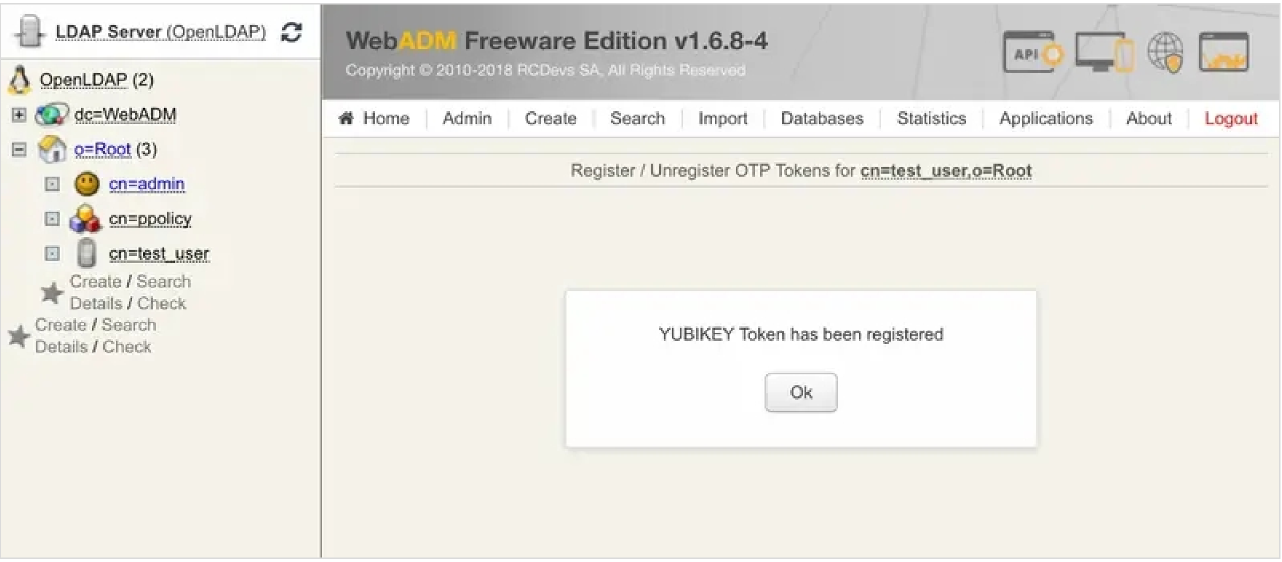
You must register a Hardware or Software Token for the user to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register an inventoried Yubikey Token:

1. Plug the Yubikey in a USB port on the computer.
2. Press the Yubikey button to finish the registration.

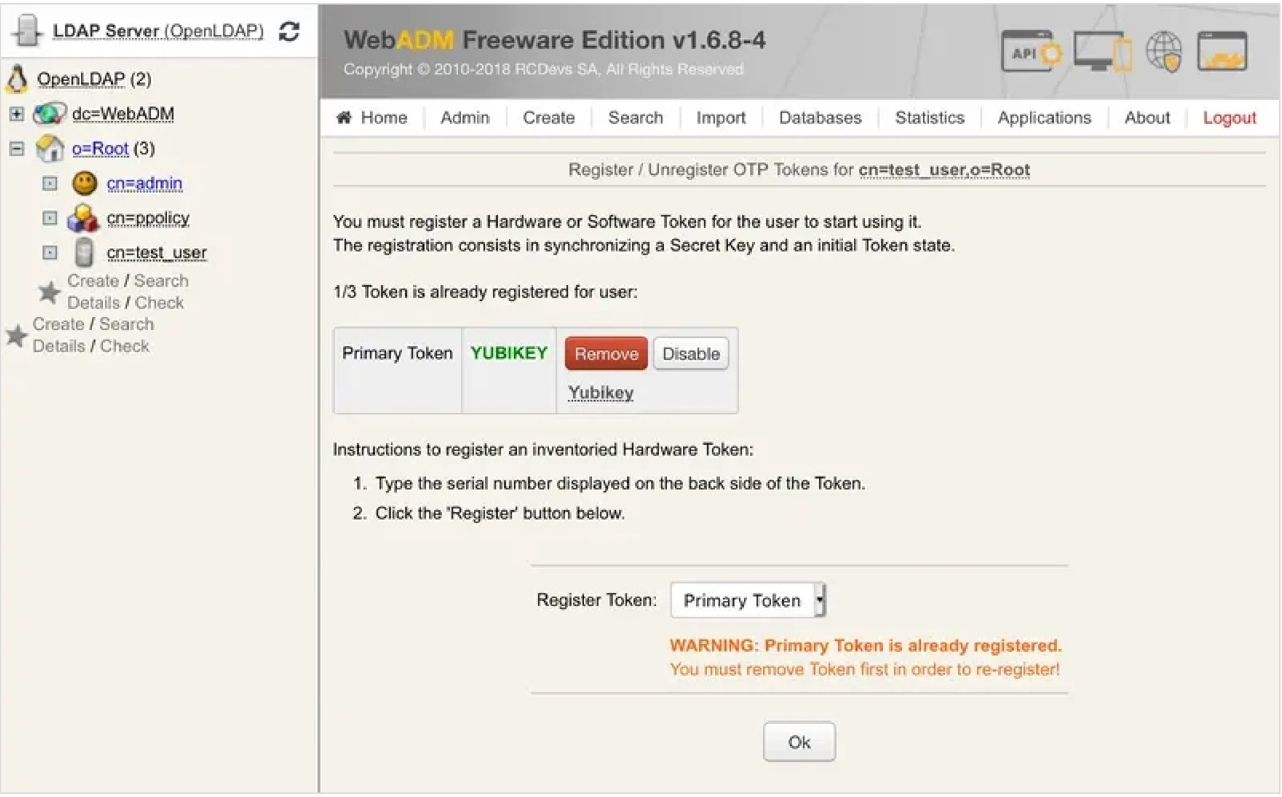
Register Token: Primary Token

○ 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)



Register / Unregister OTP Tokens for cn=test_user,o=Root

YUBIKEY Token has been registered



Register / Unregister OTP Tokens for cn=test_user,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	YUBIKEY	Remove Disable Yubikey

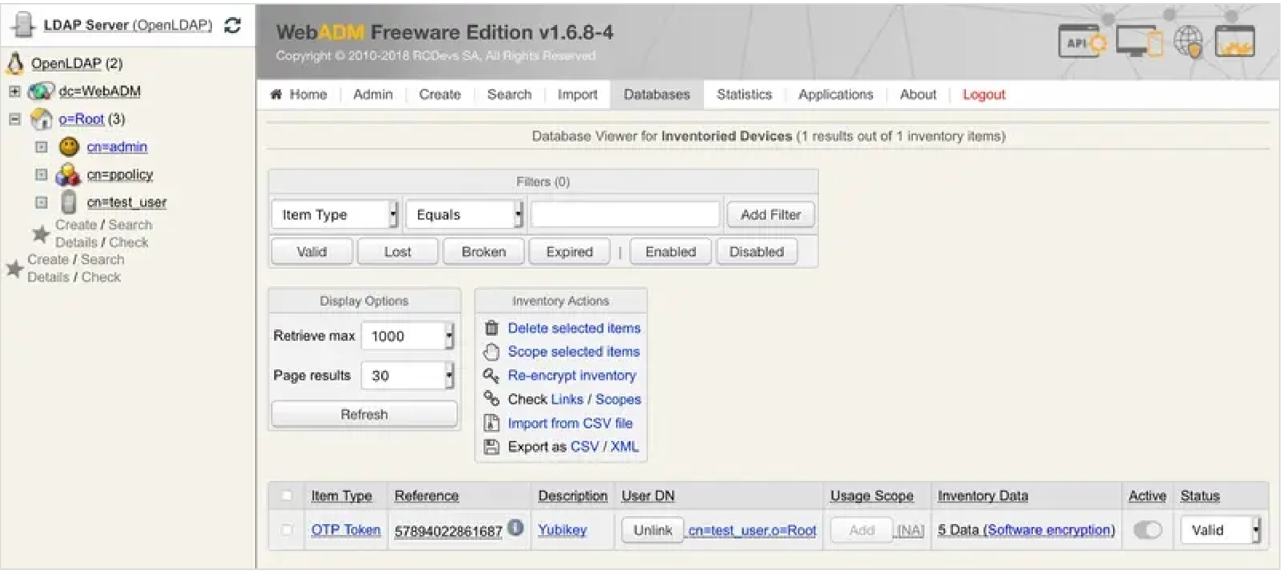
Instructions to register an inventoried Hardware Token:

1. Type the serial number displayed on the back side of the Token.
2. Click the 'Register' button below.

Register Token: Primary Token

WARNING: Primary Token is already registered.
You must remove Token first in order to re-register!

The Yubikey is correctly assigned to the User account. Now if you come back to `Databases` tab `Inventoried Devices`, you can see a link between Yubikey database entry and the LDAP user.



Database Viewer for **Inventoried Devices** (1 results out of 1 inventory items)

Filters (0)

Item Type · Equals · Add Filter

Display Options

Retrieve max: 1000

Page results: 30

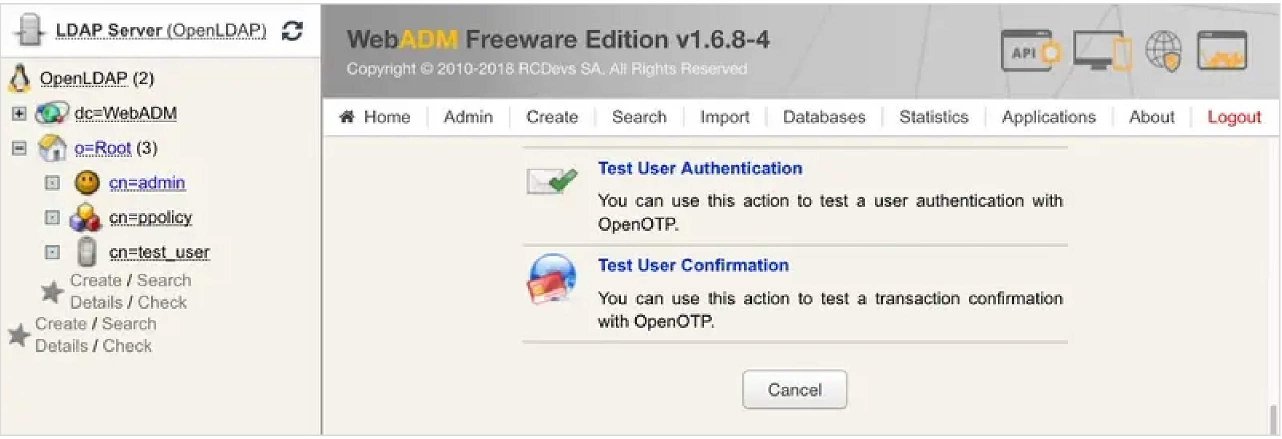
□	Item Type	Reference	Description	User DN	Usage Scope	Inventory Data	Active	Status
□	OTP Token	57894022861687	Yubikey	Unlink cn=test_user,o=Root	Add [NA]	5 Data (Software encryption)		Valid

⚠ Important Note

A Yubikey can be assigned to many users but for this, you have to remove the User DN link in databases on the Yubikey entry. Remove the link between the Yubikey and the user didn't remove the Yubikey on the User account. The first user who has enrolled the Yubikey will always be able to use the Yubikey to log in.

5. Test OTP Authentication

Let's try a Test User Authentication. Return to the `MFA Authentication Server` in the Application Actions box for the user and click the `Test User Authentication` action.



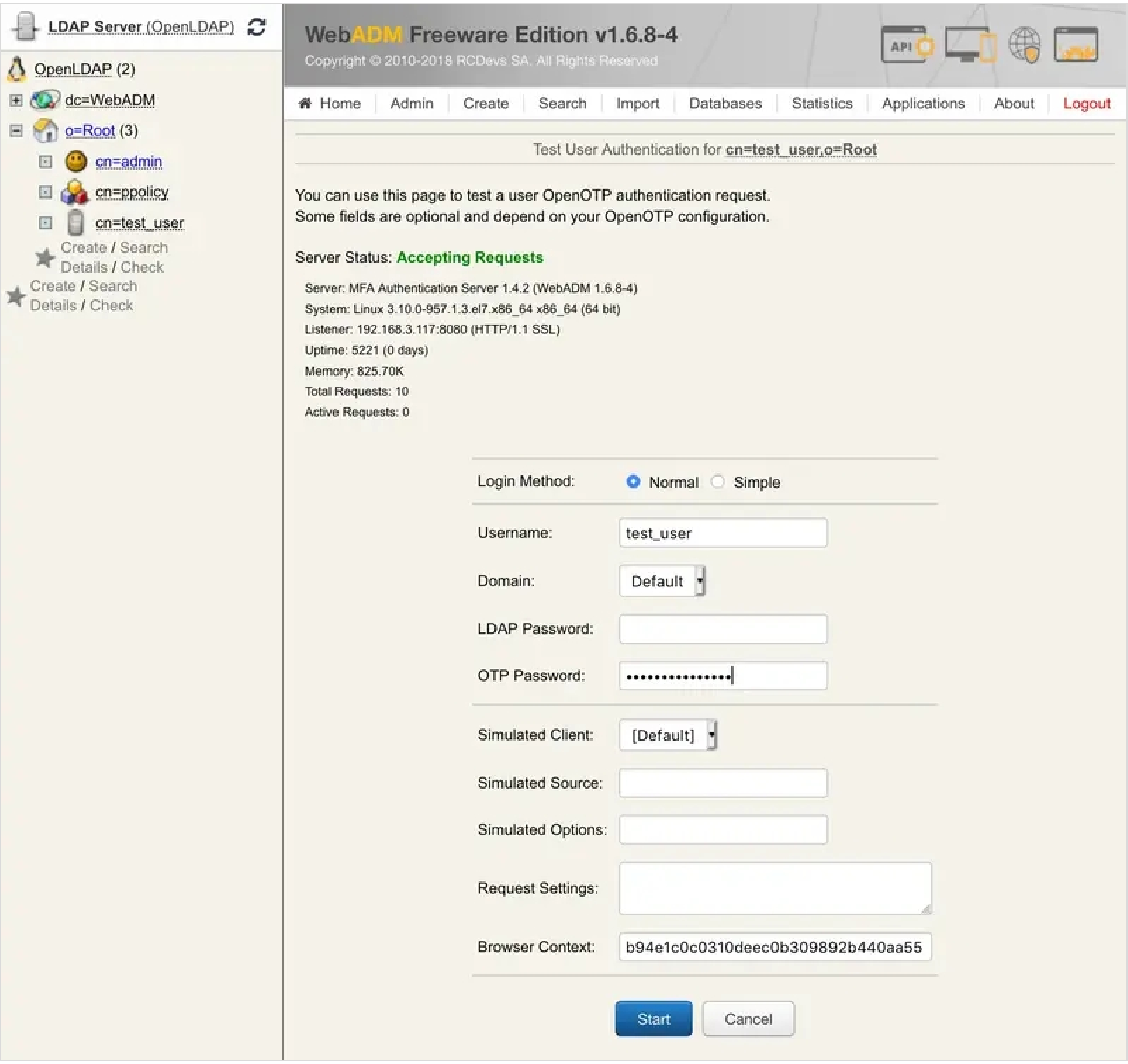
Test User Authentication

You can use this action to test a user authentication with OpenOTP.

Test User Confirmation

You can use this action to test a transaction confirmation with OpenOTP.

Put the cursor in the OTP Password field and short touch your Yubikey for activating Slot 1.



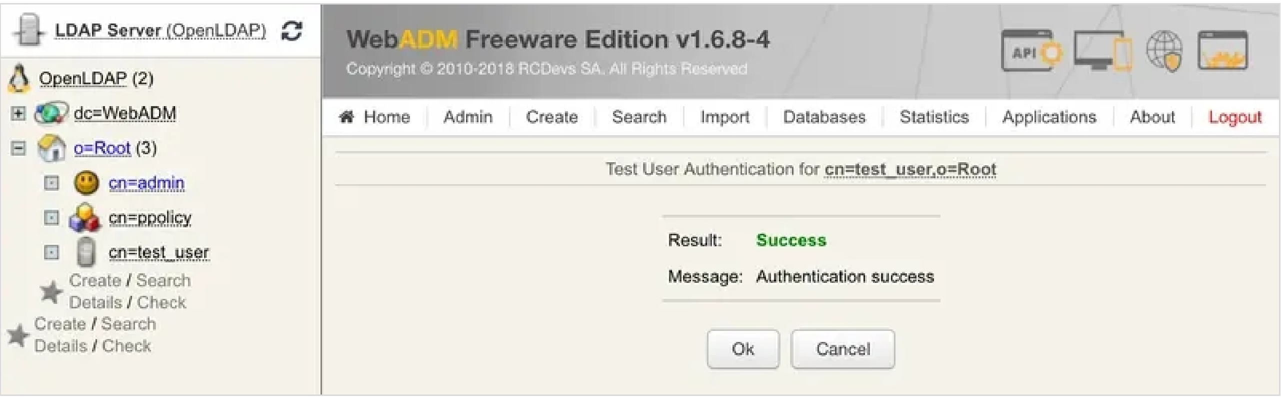
Test User Authentication for cn=test_user,o=Root

You can use this page to test a user OpenOTP authentication request.
Some fields are optional and depend on your OpenOTP configuration.

Server Status: **Accepting Requests**

```
Server: MFA Authentication Server 1.4.2 (WebADM 1.6.8-4)
System: Linux 3.10.0-957.1.3.el7.x86_64 x86_64 (64 bit)
Listener: 192.168.3.117:8080 (HTTP/1.1 SSL)
Uptime: 5221 (0 days)
Memory: 825.70K
Total Requests: 10
Active Requests: 0
```

Login Method:	● Normal ○ Simple
Username:	test_user
Domain:	Default
LDAP Password:	
OTP Password:	•••••••••••••••
Simulated Client:	[Default]
Simulated Source:	
Simulated Options:	
Request Settings:	
Browser Context:	b94e1c0c0310deec0b309892b440aa55



Test User Authentication for cn=test_user,o=Root

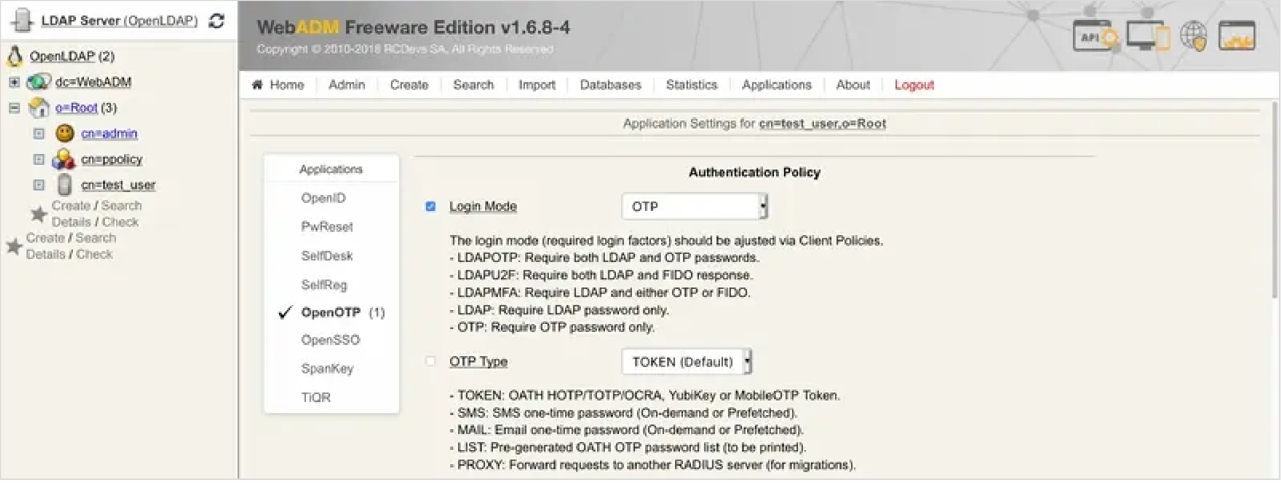
Result: Success

Message: Authentication success

You can now perform a login through OpenOTP with your Yubikey.

Important Note

We didn't type in any LDAP Password because the Login Mode is OTP only. Therefore, select your user and click on `WebADM settings: CONFIGURE`. Then select `OpenOTP` and choose `Login Mode: OTP`.



Application Settings for cn=test_user,o=Root

Authentication Policy

☑ Login Mode: OTP

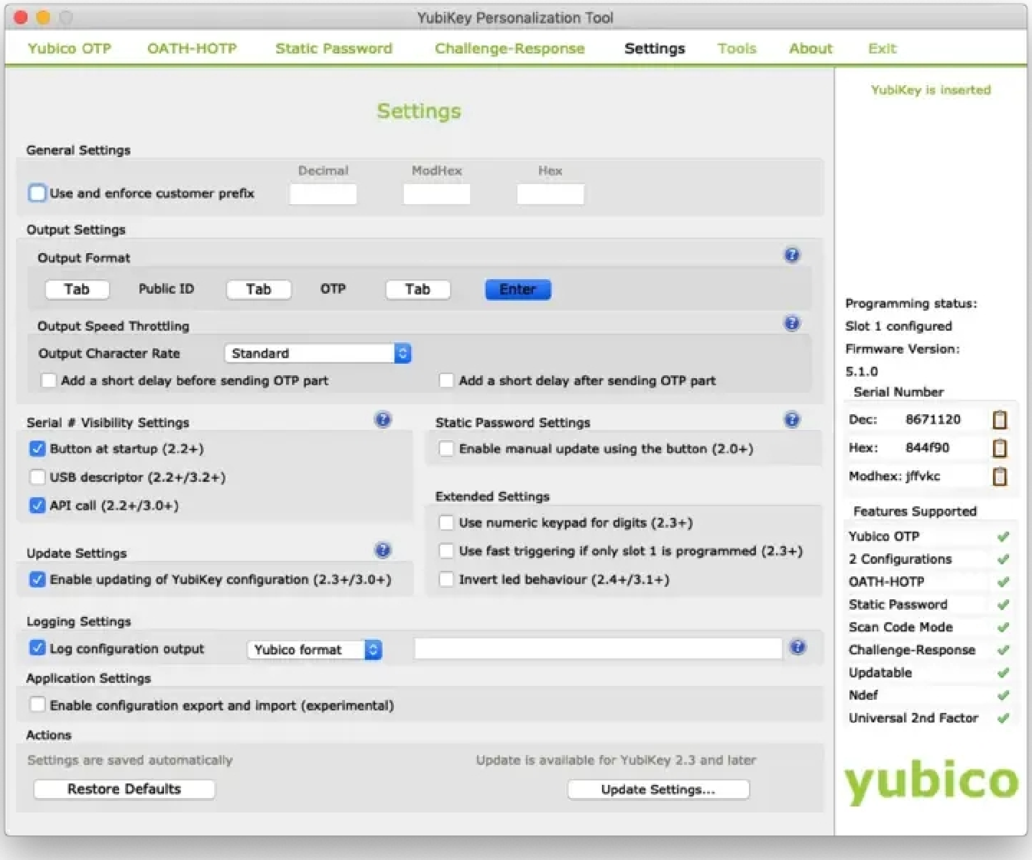
The login mode (required login factors) should be ajusted via Client Policies.
- LDAPOTP: Require both LDAP and OTP passwords.
- LDAPU2F: Require both LDAP and FIDO response.
- LDAPMFA: Require LDAP and either OTP or FIDO.
- LDAP: Require LDAP password only.
- OTP: Require OTP password only.

□ OTP Type: TOKEN (Default)

- TOKEN: OATH HOTP/TOTP/OCRA, YubiKey or MobileOTP Token.
- SMS: SMS one-time password (On-demand or Prefetched).
- MAIL: Email one-time password (On-demand or Prefetched).
- LIST: Pre-generated OATH OTP password list (to be printed).
- PROXY: Forward requests to another RADIUS server (for migrations).

6. Reprogram a Yubikey to generate 6 or 8 digits OTP code

Instead of generating a key of 44 characters when you press the Yubikey, you can configure it to generate a 6 or 8 digits OTP code. But first, you have to edit some settings in the Yubikey Personalization tool. Go on the `Settings` tab and select `Log configuration output: Yubico format` like below:



Settings

General Settings

	Decimal	ModHex	Hex
□ Use and enforce customer prefix			

Output Settings

Output Format

Tab · Public ID · Tab · OTP · Tab · Enter

Output Speed Throttling

Output Character Rate: Standard

□ Add a short delay before sending OTP part

□ Add a short delay after sending OTP part

Serial # Visibility Settings

☑ Button at startup (2.2+)

□ USB descriptor (2.2+/3.2+)

☑ API call (2.2+/3.0+)

Update Settings

☑ Enable updating of YubiKey configuration (2.3+/3.0+)

Static Password Settings

□ Enable manual update using the button (2.0+)

Extended Settings

□ Use numeric keypad for digits (2.3+)

□ Use fast triggering if only slot 1 is programmed (2.3+)

□ Invert led behaviour (2.4+/3.1+)

Logging Settings

☑ Log configuration output: Yubico format

Application Settings

□ Enable configuration export and import (experimental)

Actions

Settings are saved automatically

Update is available for YubiKey 2.3 and later

YubiKey is inserted

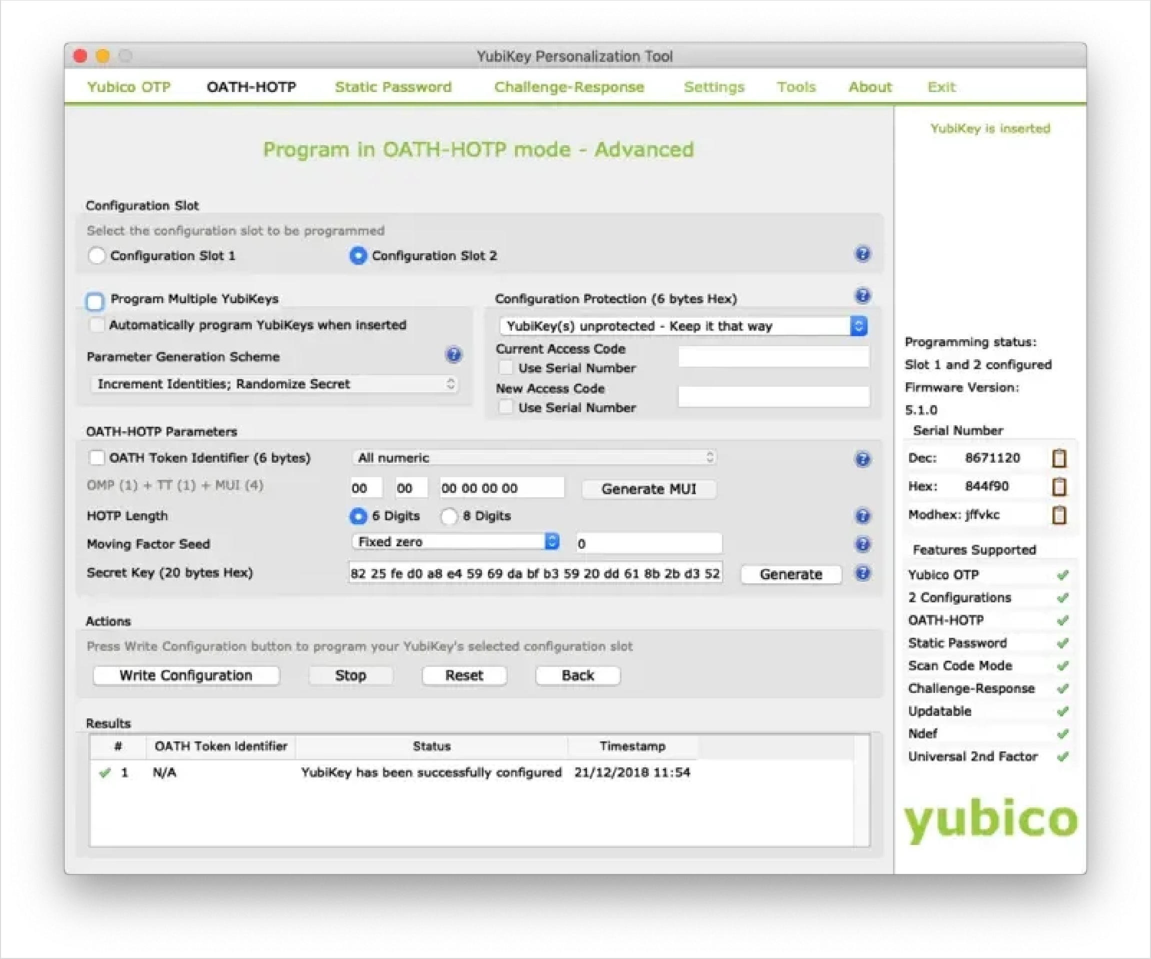
Programming status:
Slot 1 configured
Firmware Version:
5.1.0

Serial Number

Dec:	8671120
Hex:	844f90
Modhex:	jffvkc

Features Supported	
Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✓
Universal 2nd Factor	✓

Now, we will reprogram the Yubikey. Switch to the `OATH-HOTP` tab and select `Advanced` configuration. Please, select Configuration Slot 2. Disable the option `OATH Token Identifier (6 bytes)` like below:



Program in OATH-HOTP mode - Advanced

Configuration Slot
Select the configuration slot to be programmed
○ Configuration Slot 1 ● Configuration Slot 2

□ Program Multiple YubiKeys
□ Automatically program YubiKeys when inserted
Parameter Generation Scheme: Increment Identities; Randomize Secret

Configuration Protection (6 bytes Hex): YubiKey(s) unprotected - Keep it that way
Current Access Code
□ Use Serial Number
New Access Code
□ Use Serial Number

OATH-HOTP Parameters
□ OATH Token Identifier (6 bytes): All numeric
OMP (1) + TT (1) + MUI (4): 00 00 00 00 00 00
HOTP Length: ● 6 Digits ○ 8 Digits
Moving Factor Seed: Fixed zero 0
Secret Key (20 bytes Hex): 82 25 fe d0 a8 e4 59 69 da bf b3 59 20 dd 61 8b 2b d3 52

Actions
Press Write Configuration button to program your YubiKey's selected configuration slot

Results

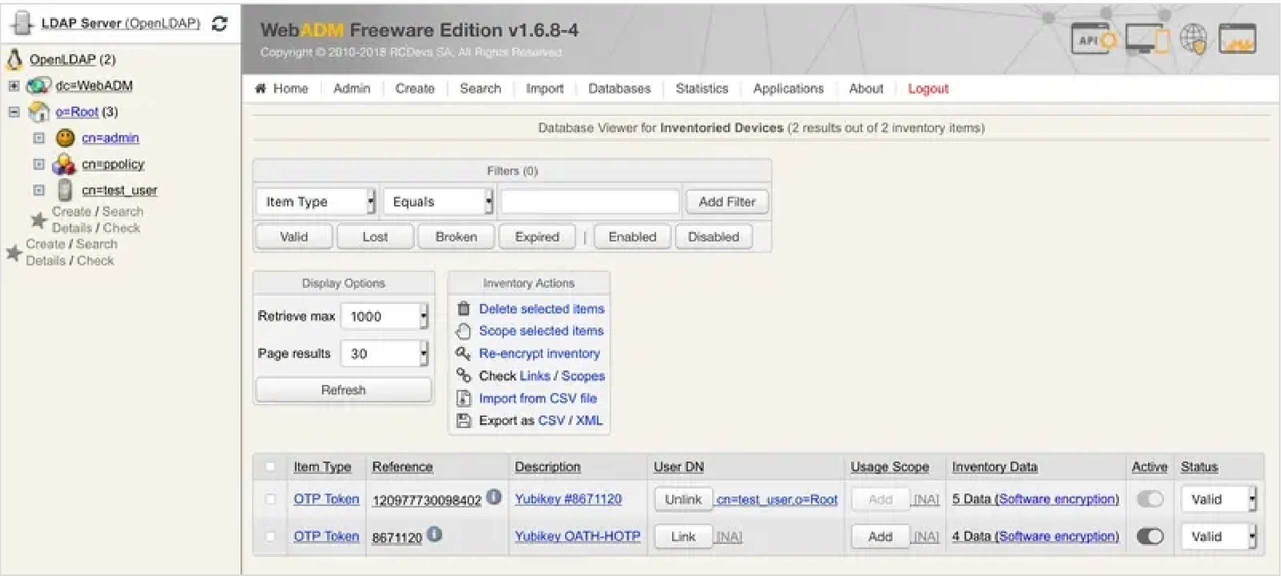
#	OATH Token Identifier	Status	Timestamp
✓ 1	N/A	YubiKey has been successfully configured	21/12/2018 11:54

YubiKey is inserted
Programming status:
Slot 1 and 2 configured
Firmware Version:
5.1.0
Serial Number
Dec: 8671120
Hex: 844f90
Modhex: jffvkc

Features Supported	
Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✓
Universal 2nd Factor	✓

Plug in your Yubikey, click on the `Generate` buttons. Click now on the `Write Configuration` button, and you should be prompted to save the inventory file. Import this file in WebADM inventory like explained in section 3. Your Yubikey is now reprogrammed. At this step, your Yubikey must generate 6 or 8 digits OTP code when you touch it long. If it's not the case, it's useless to perform the next steps.

We will now assign this HOTP Yubikey to a User account through the WebADM Admin GUI. To assign this Yubikey, you will need its `Reference` registered in `Databases` tab `Inventoried Devices`.



Database Viewer for Inventoried Devices (2 results out of 2 inventory items)

Filters (0): Item Type, Equals

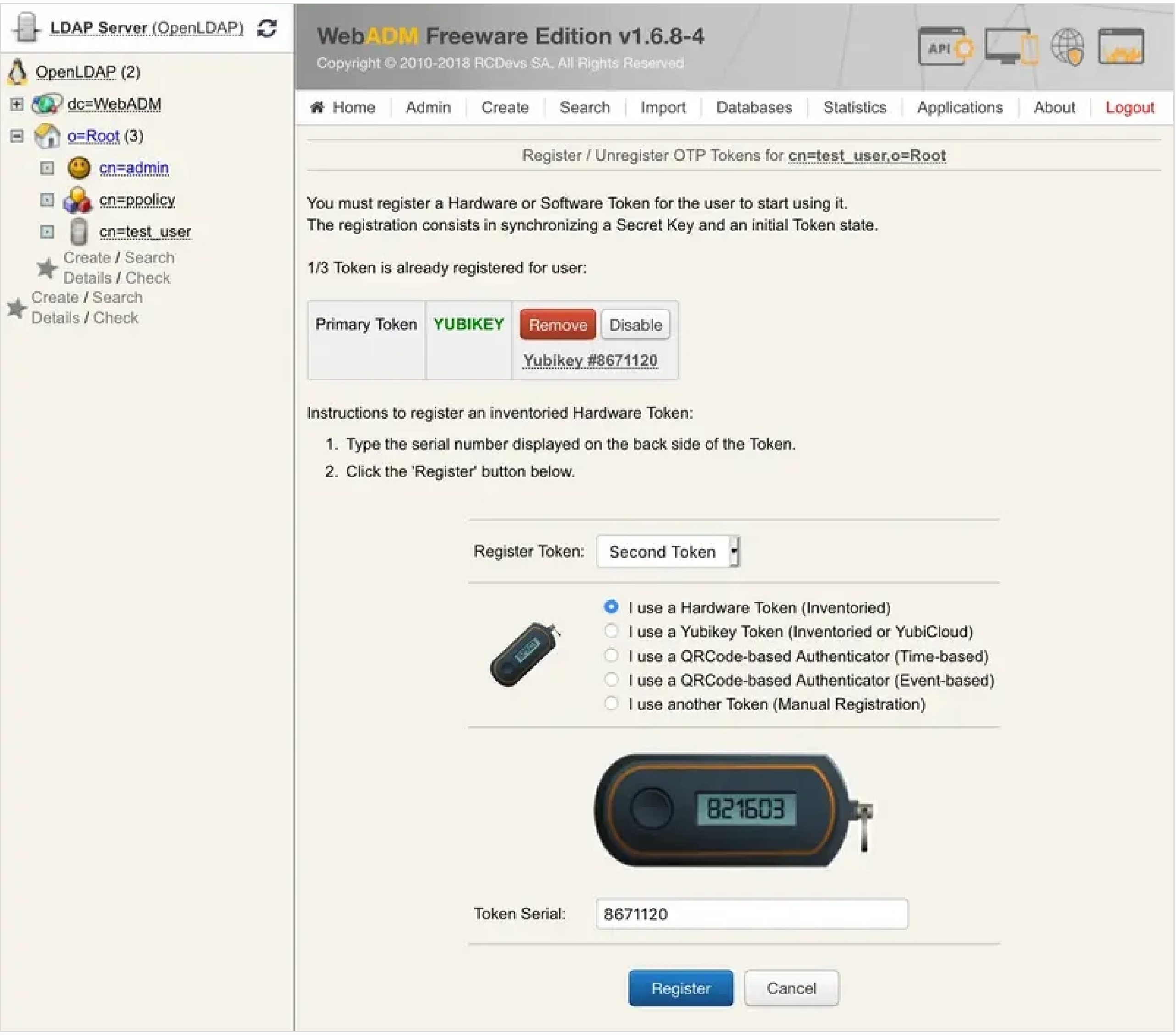
Display Options
Retrieve max: 1000
Page results: 30

Inventory Actions

	Item Type	Reference	Description	User DN	Usage Scope	Inventory Data	Active	Status
□	OTP Token	120977730098402	Yubikey #8671120	Unlink cn=test_user,o=Root	Add [NA]	5 Data (Software encryption)		Valid
□	OTP Token	8671120	Yubikey OATH-HOTP	Link [NA]	Add [NA]	4 Data (Software encryption)		Valid

On my side, the reference is `8671120`.

Click now on a user account in the left tree, `MFA authentication Server`, `Register/Unregister OTP Tokens`. Register your Token and choose `Second Token`. Select the option `I use a Hardware Token (Inventoried)`. In the Token Serial field, put the reference previously copied.



Register / Unregister OTP Tokens for cn=test_user,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	YUBIKEY	Remove Disable Yubikey #8671120

Instructions to register an inventoried Hardware Token:

1. Type the serial number displayed on the back side of the Token.
2. Click the 'Register' button below.

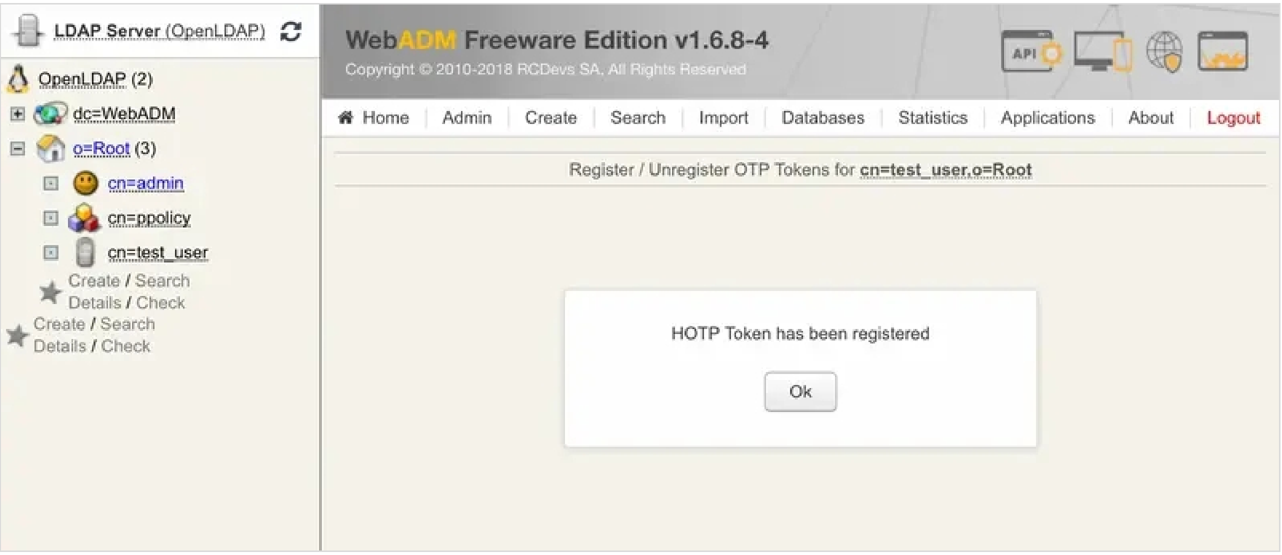
Register Token: Second Token

● 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 Serial: 8671120

Register Cancel

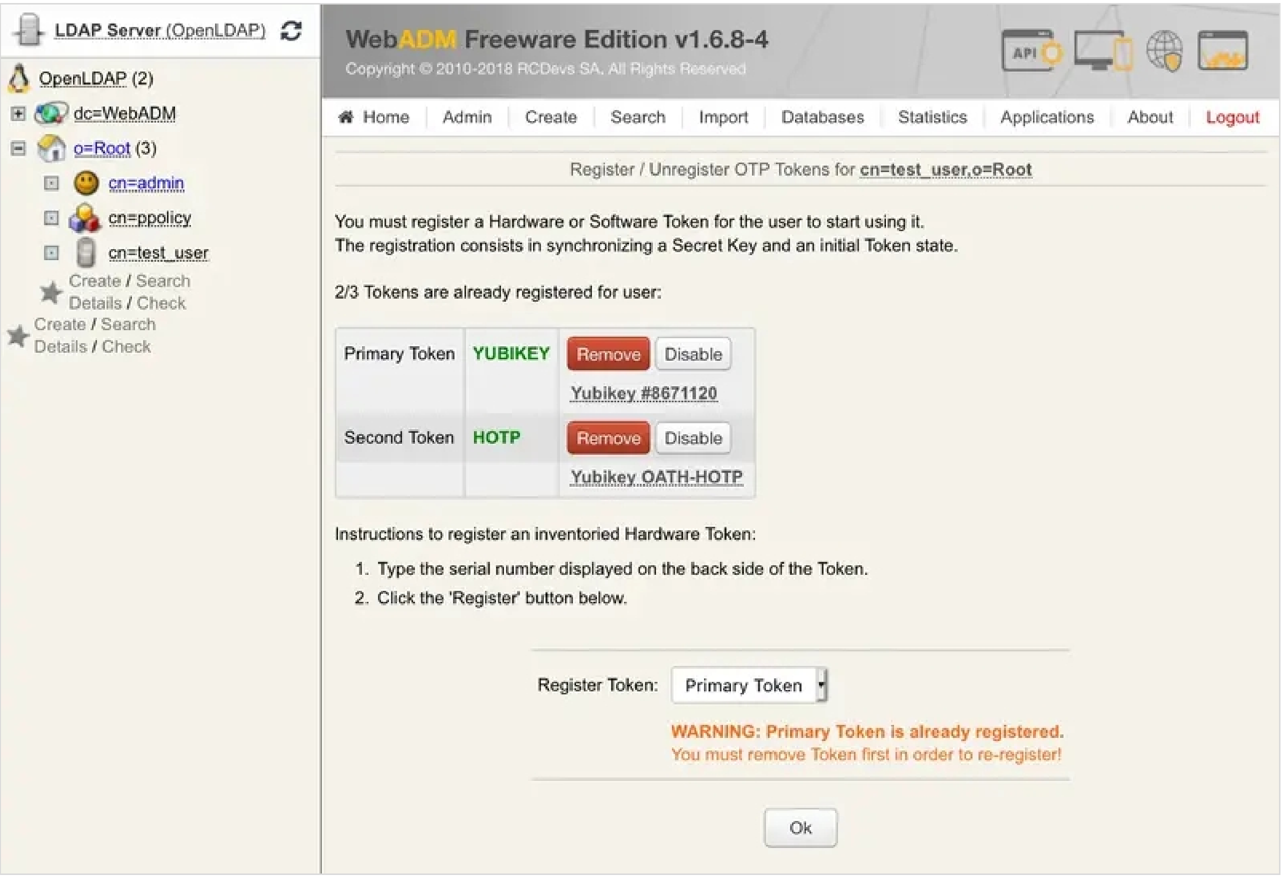
Click on `Register` and the Yubikey is now enrolled on your account.



Register / Unregister OTP Tokens for cn=test_user,o=Root

HOTP Token has been registered

Ok



Register / Unregister OTP Tokens for cn=test_user,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.

2/3 Tokens are already registered for user:

Primary Token	YUBIKEY	Yubikey #8671120
Second Token	HOTP	Yubikey OATH-HOTP

Instructions to register an inventoried Hardware Token:

1. Type the serial number displayed on the back side of the Token.
2. Click the 'Register' button below.

Register Token: Primary Token

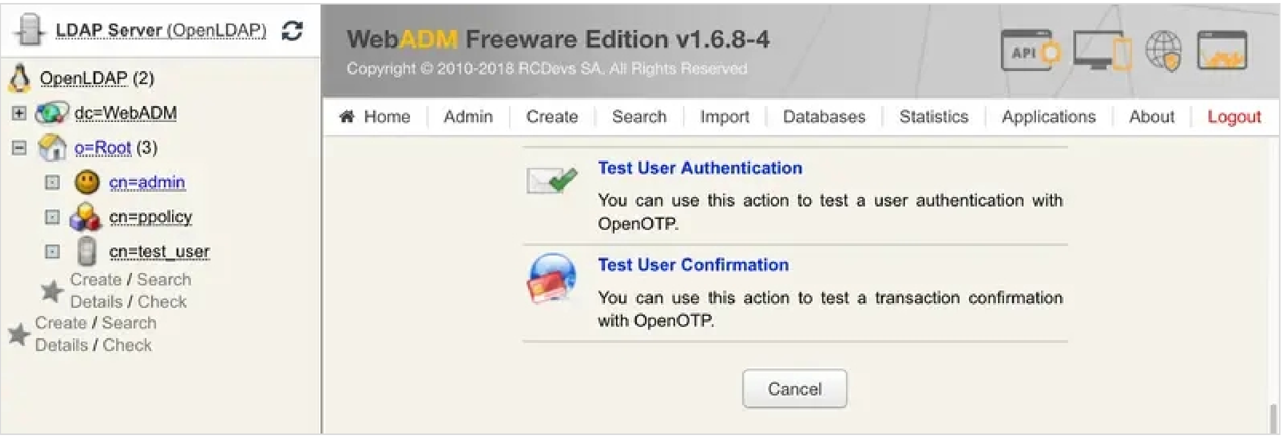
WARNING: Primary Token is already registered.
You must remove Token first in order to re-register!

⚠ Important Note

If you have chosen 8 digits OTP length, you will have to configure the OpenOTP to work with 8 digits OTP Token in the default configuration or through a client policy. Default OpenOTP configuration cannot work with 6 and 8 digits at the same time. This setting can be found under the graphical OpenOTP configuration: `OTP Password Length`.

7. Test OATH-HOTP Authentication

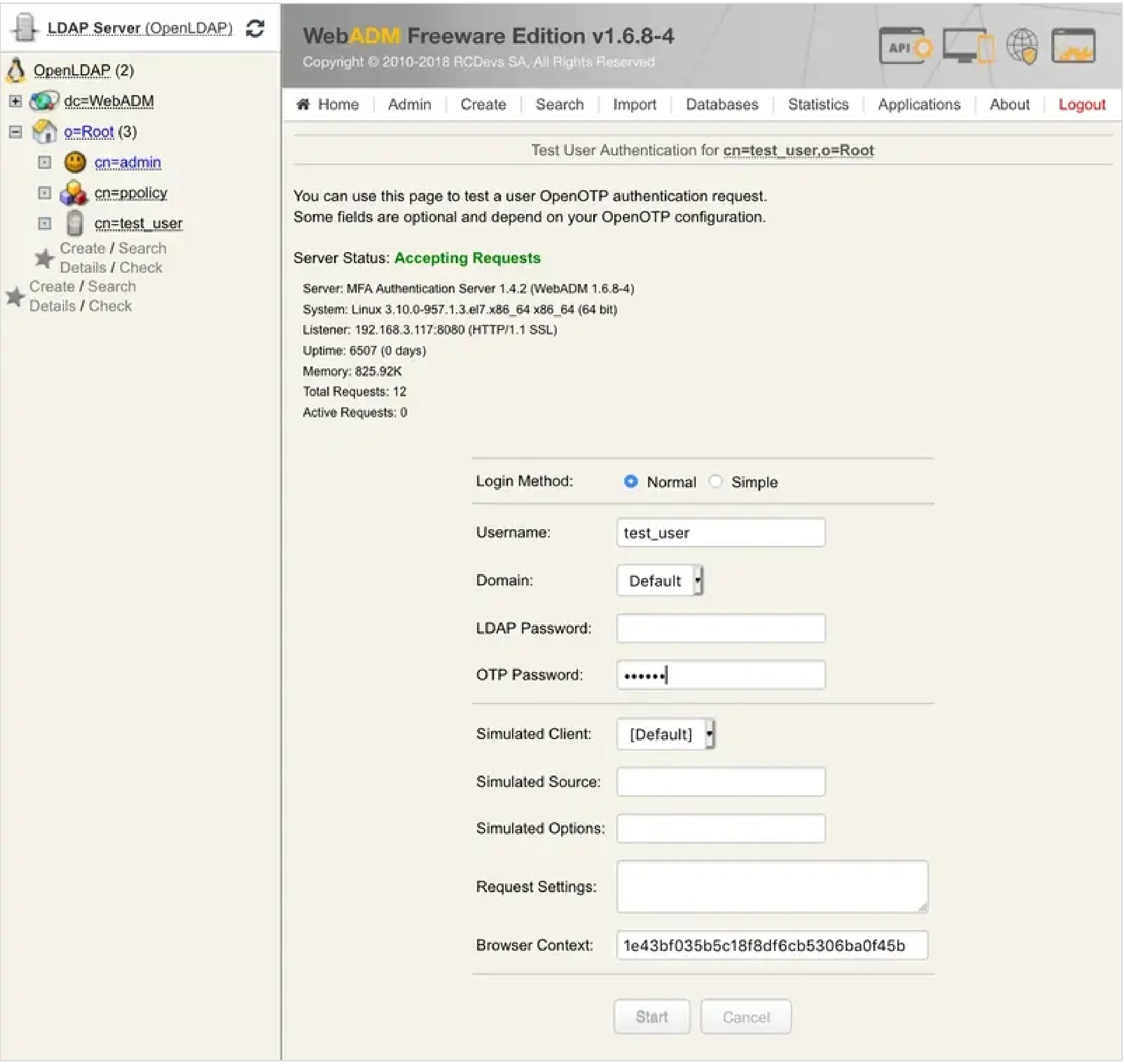
Let's try a `Test User Authentication`. Return to the `MFA Authentication Server` in the Application Actions box for the user and click the `Test User Authentication` action.



Test User Authentication
You can use this action to test a user authentication with OpenOTP.

Test User Confirmation
You can use this action to test a transaction confirmation with OpenOTP.

Put the cursor in the OTP Password field and long touch your Yubikey for activating Slot 2.



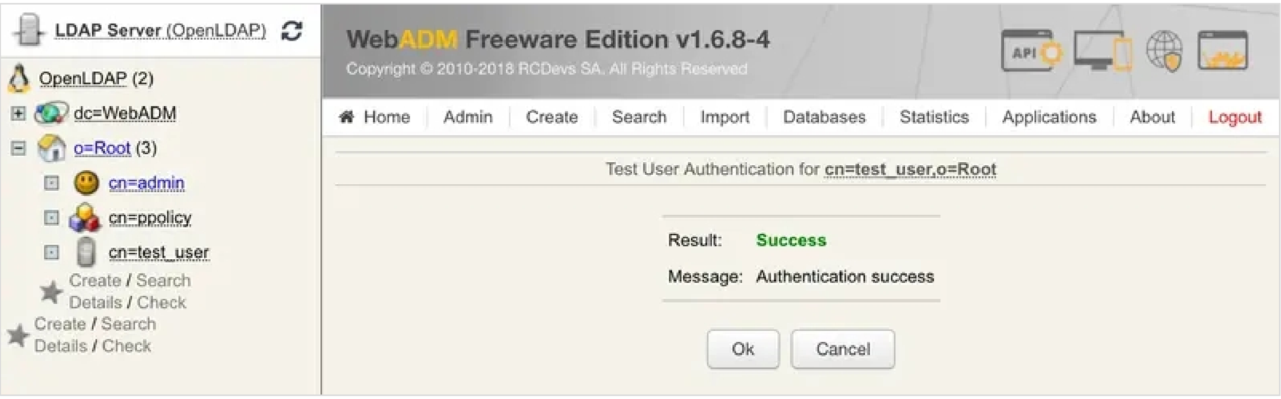
Test User Authentication for cn=test_user,o=Root

You can use this page to test a user OpenOTP authentication request.
Some fields are optional and depend on your OpenOTP configuration.

Server Status: Accepting Requests

```
Server: MFA Authentication Server 1.4.2 (WebADM 1.6.8-4)
System: Linux 3.10.0-957.1.3.el7.x86_64 x86_64 (64 bit)
Listener: 192.168.3.117:8080 (HTTP/1.1 SSL)
Uptime: 6507 (0 days)
Memory: 825.92K
Total Requests: 12
Active Requests: 0
```

Login Method:	● Normal ○ Simple
Username:	test_user
Domain:	Default
LDAP Password:	
OTP Password:	••••••
Simulated Client:	[Default]
Simulated Source:	
Simulated Options:	
Request Settings:	
Browser Context:	1e43bf035b5c18f8df6cb5306ba0f45b



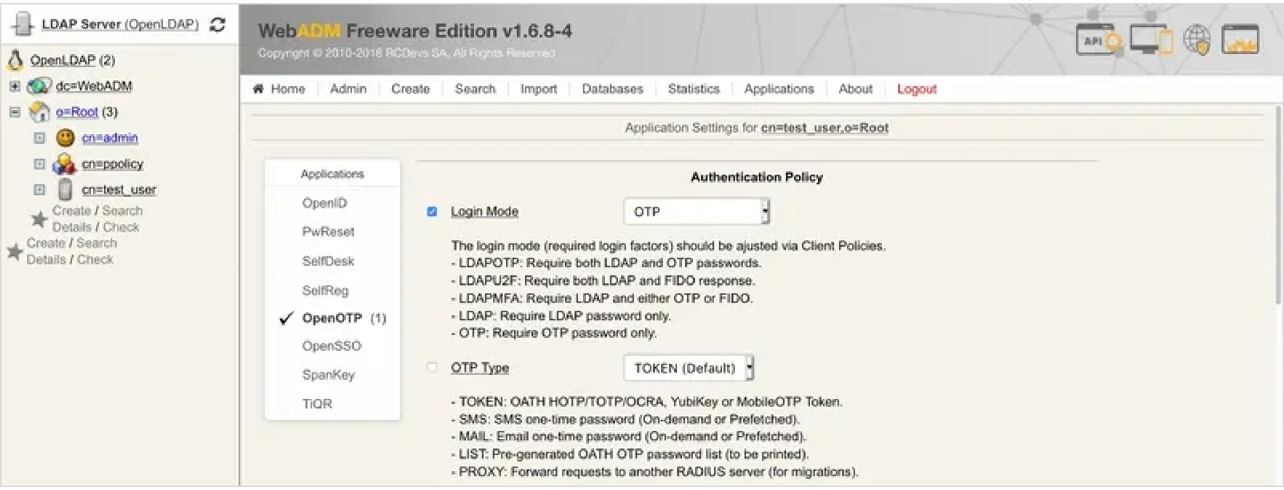
Test User Authentication for cn=test_user,o=Root

Result:	Success
Message:	Authentication success

You can now perform a login through OpenOTP with your Yubikey.

⚠ Important Note

We didn’t type in any LDAP Password because the Login Mode is OTP only. Therefore, select your user and click on `WebADM settings: CONFIGURE`. Then select `OpenOTP` and choose `Login Mode: OTP`.



Application Settings for cn=test_user,o=Root

Authentication Policy

☑ Login Mode: OTP

The login mode (required login factors) should be ajusted via Client Policies.
- LDAPOTP: Require both LDAP and OTP passwords.
- LDAPU2F: Require both LDAP and FIDO response.
- LDAPMFA: Require LDAP and either OTP or FIDO.
- LDAP: Require LDAP password only.
- OTP: Require OTP password only.

□ OTP Type: TOKEN (Default)

- TOKEN: OATH HOTP/TOTP/OCRA, YubiKey or MobileOTP Token.
- SMS: SMS one-time password (On-demand or Prefetched).
- MAIL: Email one-time password (On-demand or Prefetched).
- LIST: Pre-generated OATH OTP password list (to be printed).
- PROXY: Forward requests to another RADIUS server (for migrations).

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