NITROKEY - PIV

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.

Nitrokey - PIV

Nitrokey PIV PIVKey SSH Hardware Tokens

Authentication with a Nitrokey / PIV

In this How-To we will configure a user in WebADM for using a PIV key. We need a WebADM server already configured.

1. Import the Inventory

We need to create an inventory file like this:

```
"Type","Reference","Description","DN","Data","Status"
"PIV Device","<ID1>","PIV Nitrokey","","PublicKey=<pub_key1>","Valid"
"PIV Device","<ID2>","PIV Nitrokey","","PublicKey=<pub_key2>","Valid"
"PIV Device","<ID3>","PIV Nitrokey","","PublicKey=<pub_key3>","Valid"
```

For my test, I have a Nitrokey Start with a PIV certificate and I use `gpg2 --card-edit` for the management of the Nitrokey. Please follow this documentation Nitrokey - Installation.

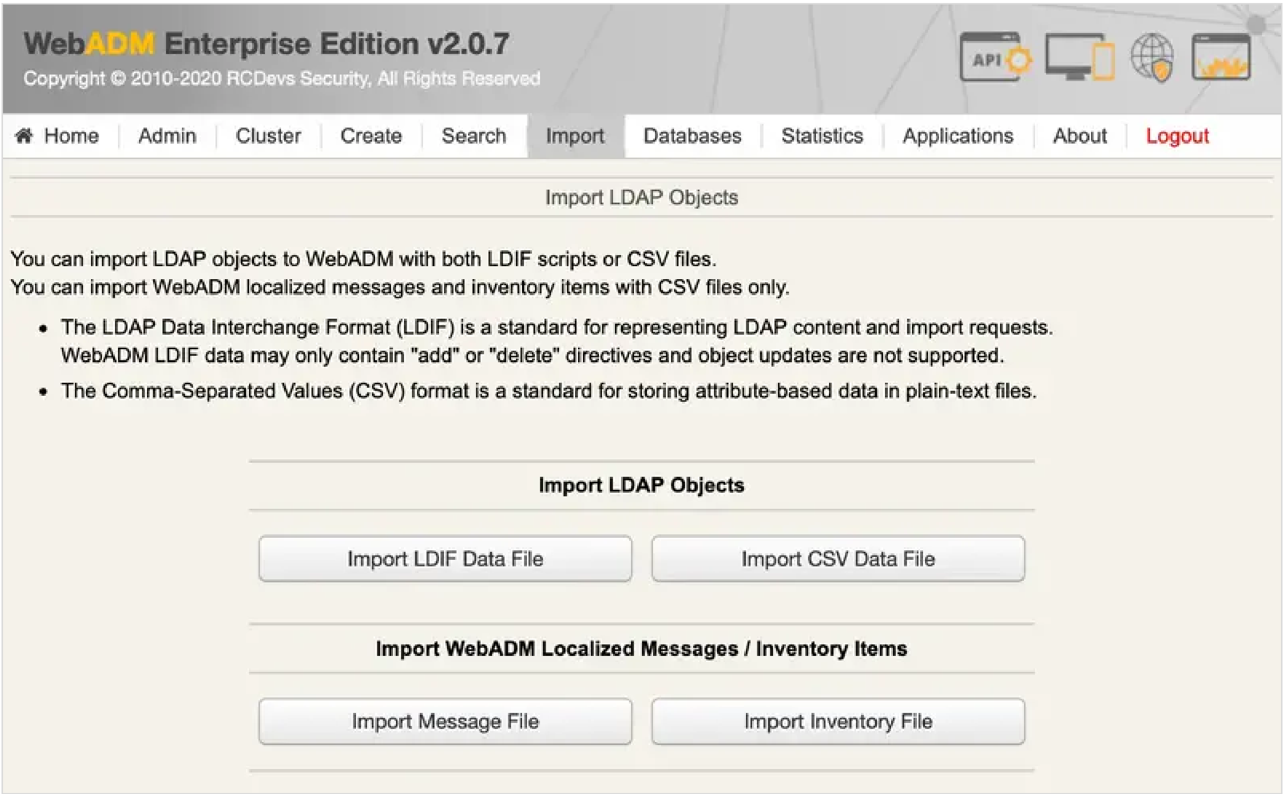
We need to extract the public key. I do it with `pkcs15-tool`:

```
-bash-4.2# pkcs15-tool --read-public-key 03
Using reader with a card: Nitrokey Start
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwiBZ8g4yHliKPSr/Kg4E
cAJLHch+Kh6w6emzn9ZRxSfrBofSO45x17oi7UsG8OIrBRMIVTgXOzqMbTwnnPjk
pep9dKe4FHEMaPEvNYhAwHDMGVhbYBcf7Ru3CsCM9NPqmbjeV/+zGsMxq8XbZLKP
doW4EjtneTpqD8ummip1ZBTuaFXGi3D/SDxAWTy3DlA+QtU5E2HpU7tZghi5ygiy
9przQct/pMCNX8WJgkLC58g/UtnVeClkh2GGalFrODR2hY0lhWQYhzNH5FzIBmEE
NcPucSwB7/r0abV9hdW52qWXECGBIjKAXrA16n/4QsFJNlPJaysl5Pv4ZBqM86jo
gwIDAQAB
-----END PUBLIC KEY-----
```

We can create a file called `nitrokey.csv` with the serial number as ID and the right public key:

```
"Type","Reference","Description","DN","Data","Status"
"PIV Device","67090940","PIV
NitroKey","","PublicKey=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwiBZ8g4yHliKPSr/Kg4EcAJLH
```

We import the file. Under the `Import` tab, we click on `Import Inventory File`:


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

Import LDAP Objects

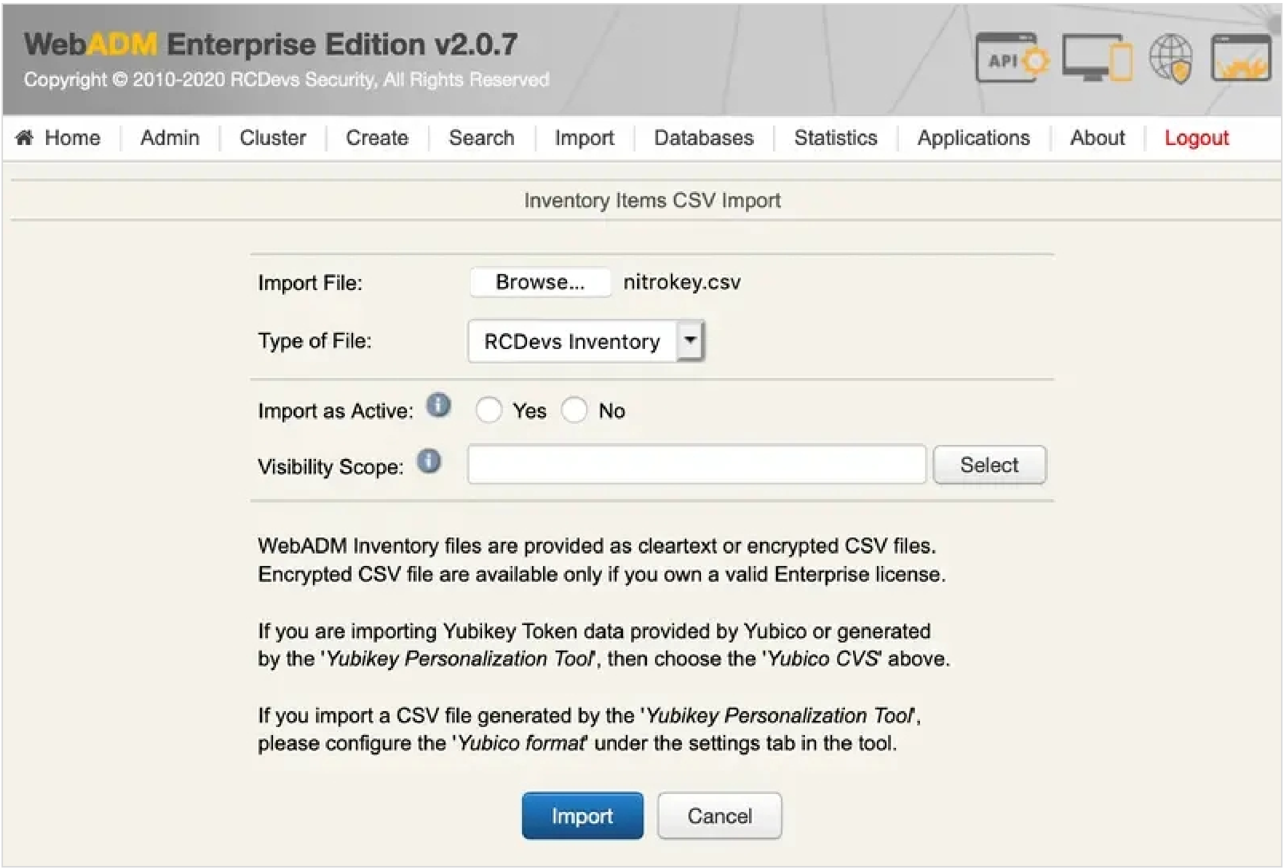
You can import LDAP objects to WebADM with both LDIF scripts or CSV files.
You can import WebADM localized messages and inventory items with CSV files only.

- 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 WebADM Localized Messages / Inventory Items

We choose the `nitrokey.csv` file and click on `Import`:


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

Inventory Items CSV Import

Import File: Browse... nitrokey.csv

Type of File: RCDevs Inventory

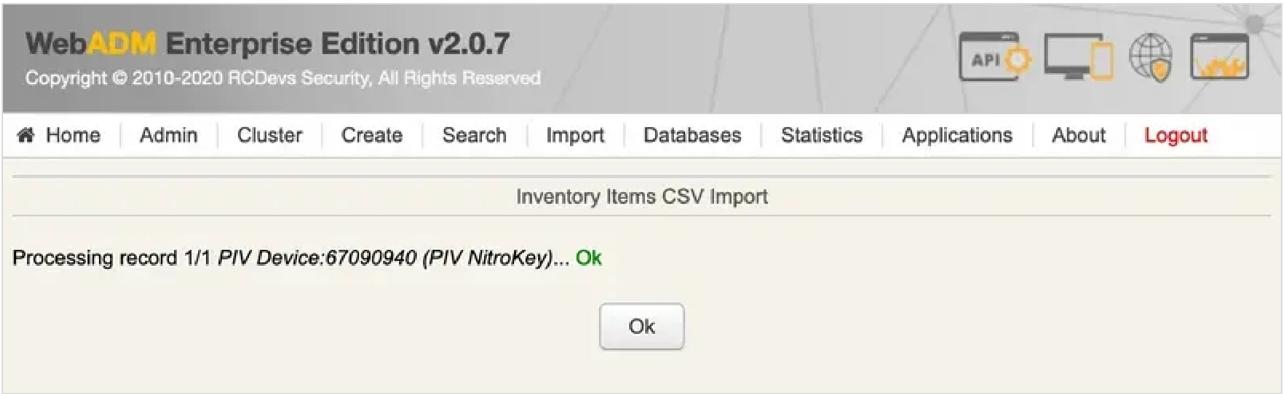
Import as Active: ○ Yes ○ No

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.

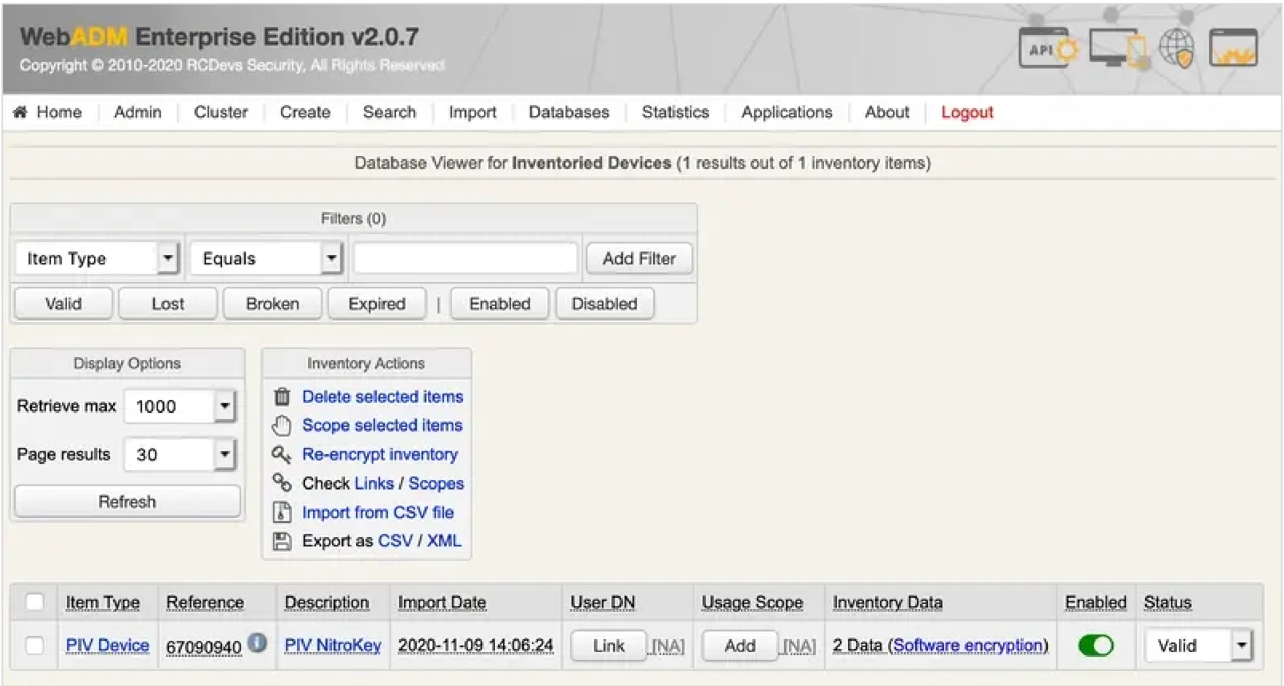
If you import a CSV file generated by the '*Yubikey Personalization Tool*', please configure the '*Yubico format*' under the settings tab in the tool.


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
Ok

Inventory Items CSV Import

Processing record 1/1 *PIV Device:67090940 (PIV NitroKey)*... Ok

Now, the PIV key is present in the inventory:



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

Item Type | Equals

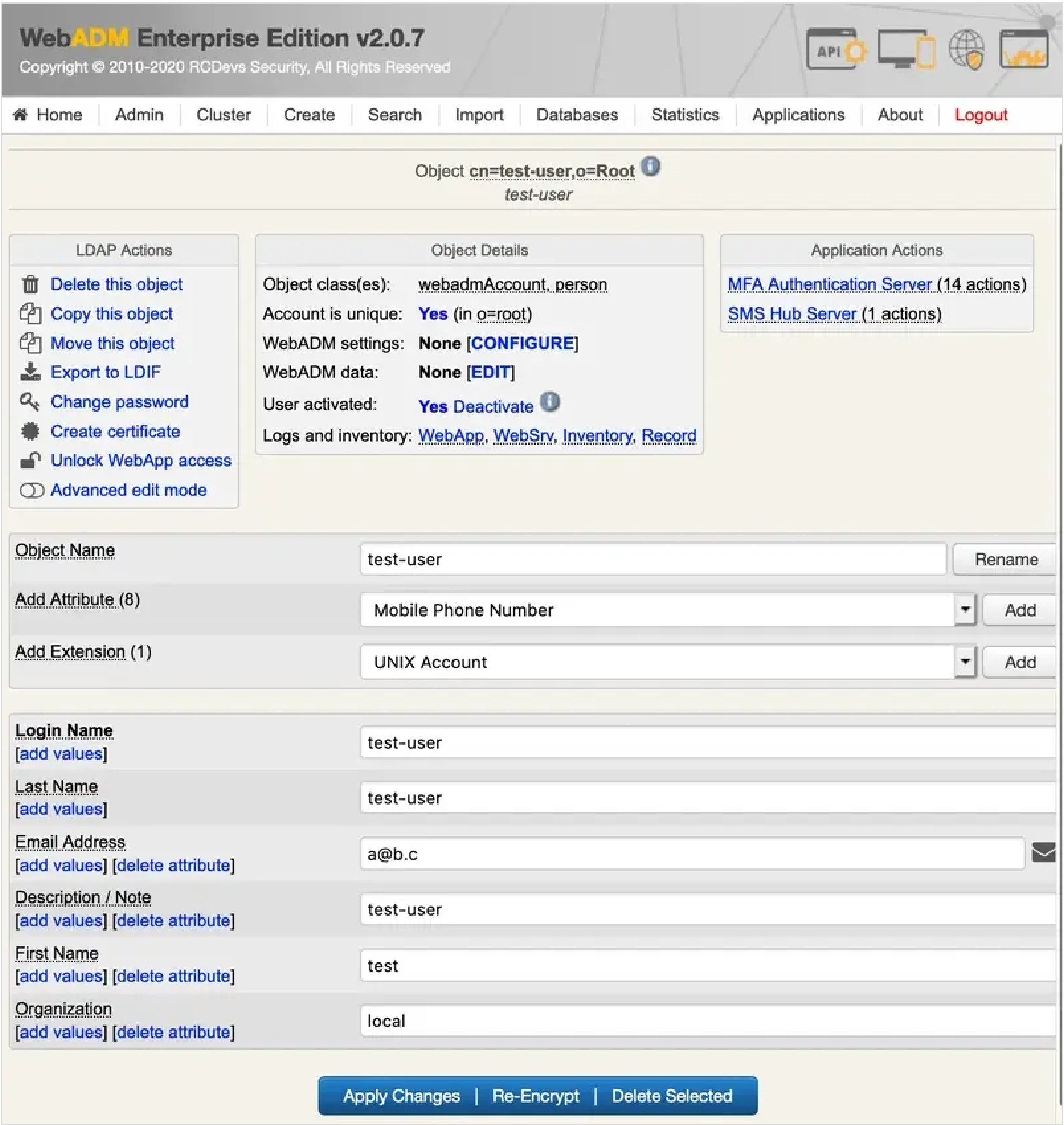
Retrieve max: 1000

Page results: 30

□	Item Type	Reference	Description	Import Date	User DN	Usage Scope	Inventory Data	Enabled	Status
□	PIV Device	67090940	PIV NitroKey	2020-11-09 14:06:24	Link [NA]	Add [NA]	2 Data (Software encryption)	●	Valid

2. Assign the Nitrokey

We select the user in the LDAP tree on the left and add a `UNIX Account` extension:



Object cn=test-user,o=Root
test-user

Object Details

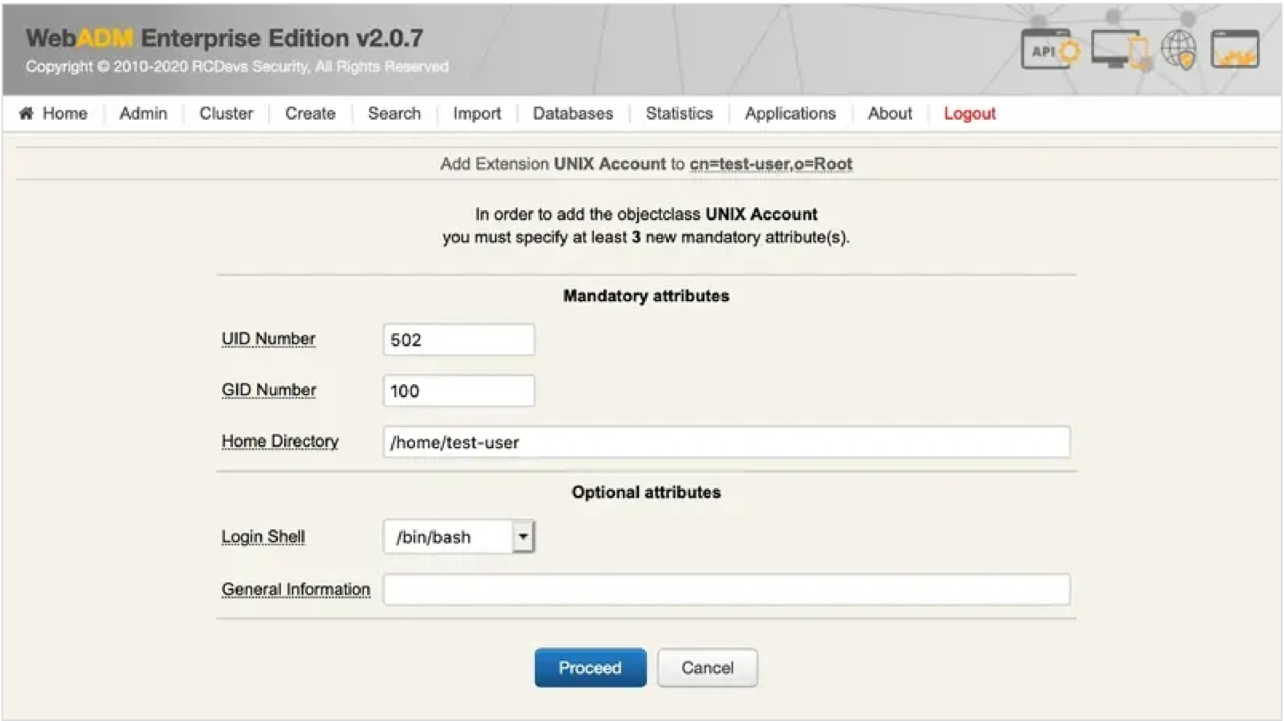
Object class(es):	webadmAccount, person
Account is unique:	Yes (in o=root)
WebADM settings:	None [CONFIGURE]
WebADM data:	None [EDIT]
User activated:	Yes Deactivate
Logs and inventory:	WebApp, WebSrv, Inventory, Record

MFA Authentication Server (14 actions)
SMS Hub Server (1 actions)

Object Name	test-user
Add Attribute (8)	Mobile Phone Number
Add Extension (1)	UNIX Account

Login Name [add values]	test-user
Last Name [add values]	test-user
Email Address [add values] [delete attribute]	a@b.c
Description / Note [add values] [delete attribute]	test-user
First Name [add values] [delete attribute]	test
Organization [add values] [delete attribute]	local

We click on `Proceed`:


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

Add Extension **UNIX Account** to cn=test-user,o=Root

In order to add the objectclass **UNIX Account**
you must specify at least **3** new mandatory attribute(s).

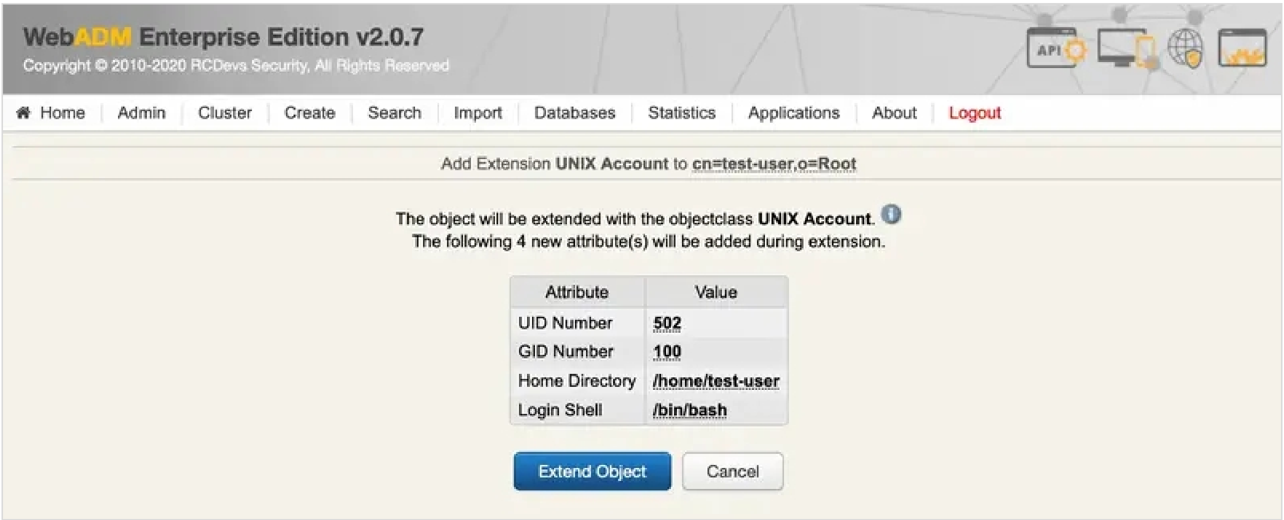
Mandatory attributes

UID Number	502
GID Number	100
Home Directory	/home/test-user

Optional attributes

Login Shell	/bin/bash
General Information	

We `Extend Object`:

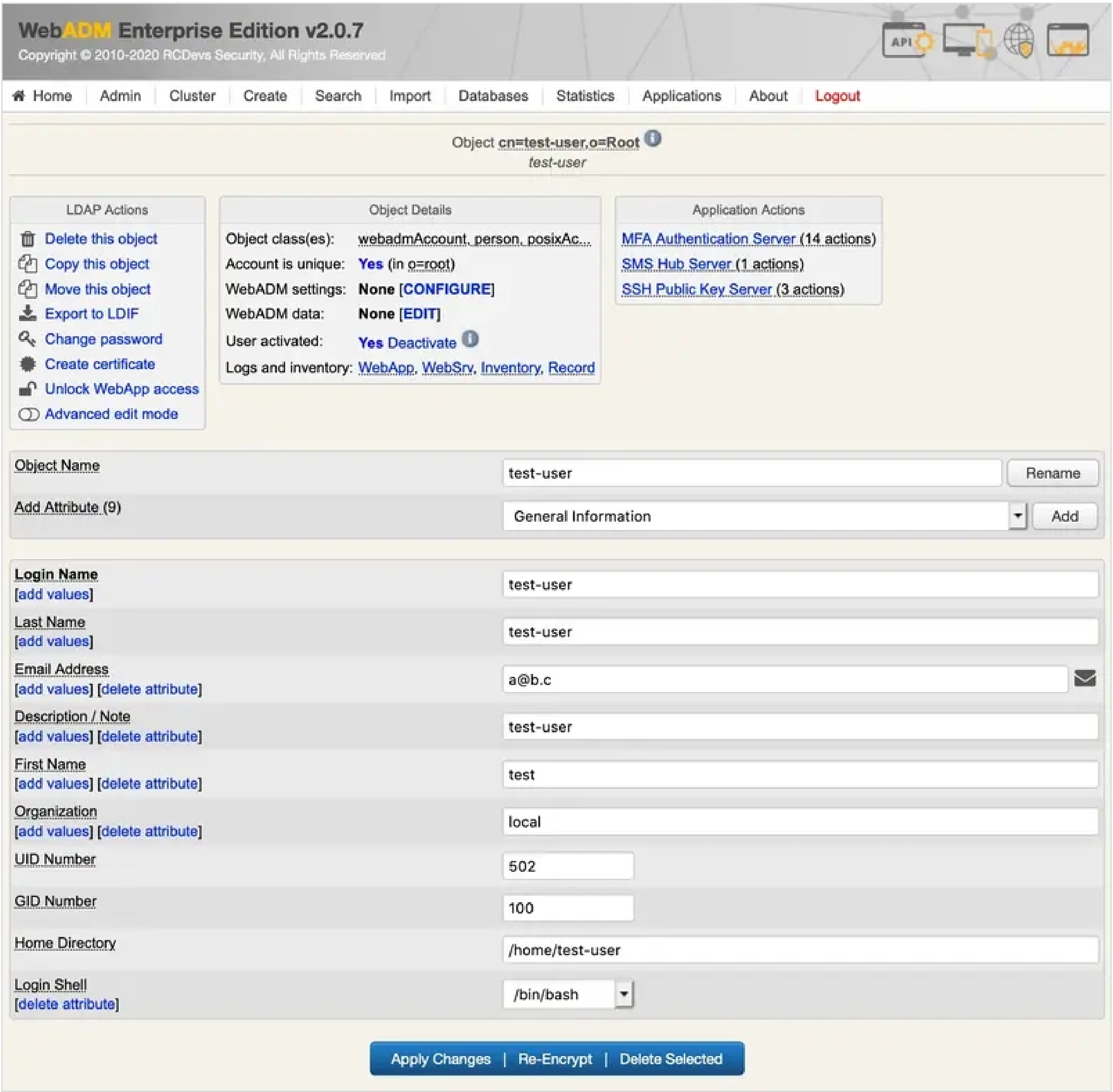

WebADM Enterprise Edition v2.0.7
Copyright © 2010-2020 RCDevs Security, All Rights Reserved
Home | Admin | Cluster | Create | Search | Import | Databases | Statistics | Applications | About | Logout

Add Extension **UNIX Account** to cn=test-user,o=Root

The object will be extended with the objectclass **UNIX Account**.
The following **4** new attribute(s) will be added during extension.

Attribute	Value
UID Number	502
GID Number	100
Home Directory	/home/test-user
Login Shell	/bin/bash

We click on `SSH Publick Key Server`:


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

Object cn=test-user,o=Root

test-user

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

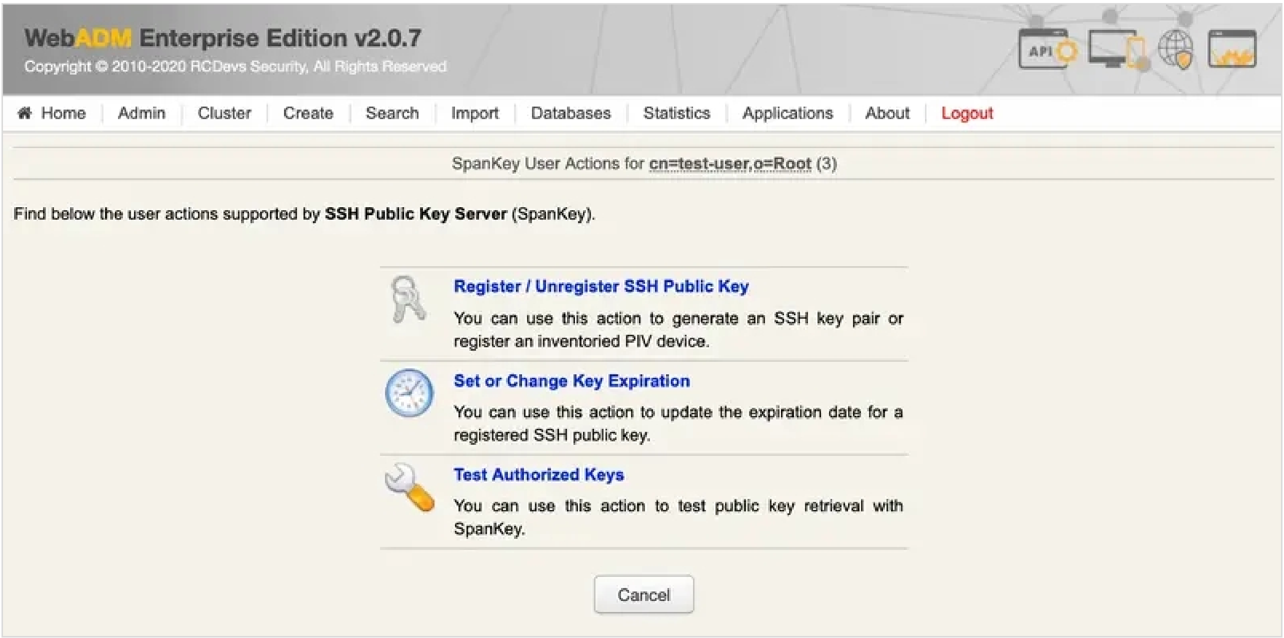
Object class(es):	webadmAccount, person, posixAc...
Account is unique:	**Yes** (in o=root)
WebADM settings:	**None [CONFIGURE]**
WebADM data:	**None [EDIT]**
User activated:	**Yes** Deactivate
Logs and inventory:	WebApp, WebSrv, Inventory, Record

Application Actions
MFA Authentication Server (14 actions)
SMS Hub Server (1 actions)
SSH Public Key Server (3 actions)

Object Name	test-user [Rename]
Add Attribute (9)	General Information [Add]

Login Name [add values]	test-user
Last Name [add values]	test-user
Email Address [add values] [delete attribute]	a@b.c
Description / Note [add values] [delete attribute]	test-user
First Name [add values] [delete attribute]	test
Organization [add values] [delete attribute]	local
UID Number	502
GID Number	100
Home Directory	/home/test-user
Login Shell [delete attribute]	/bin/bash

We click on `Register / Unregister SSH Key`:


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

SpanKey User Actions for cn=test-user,o=Root (3)

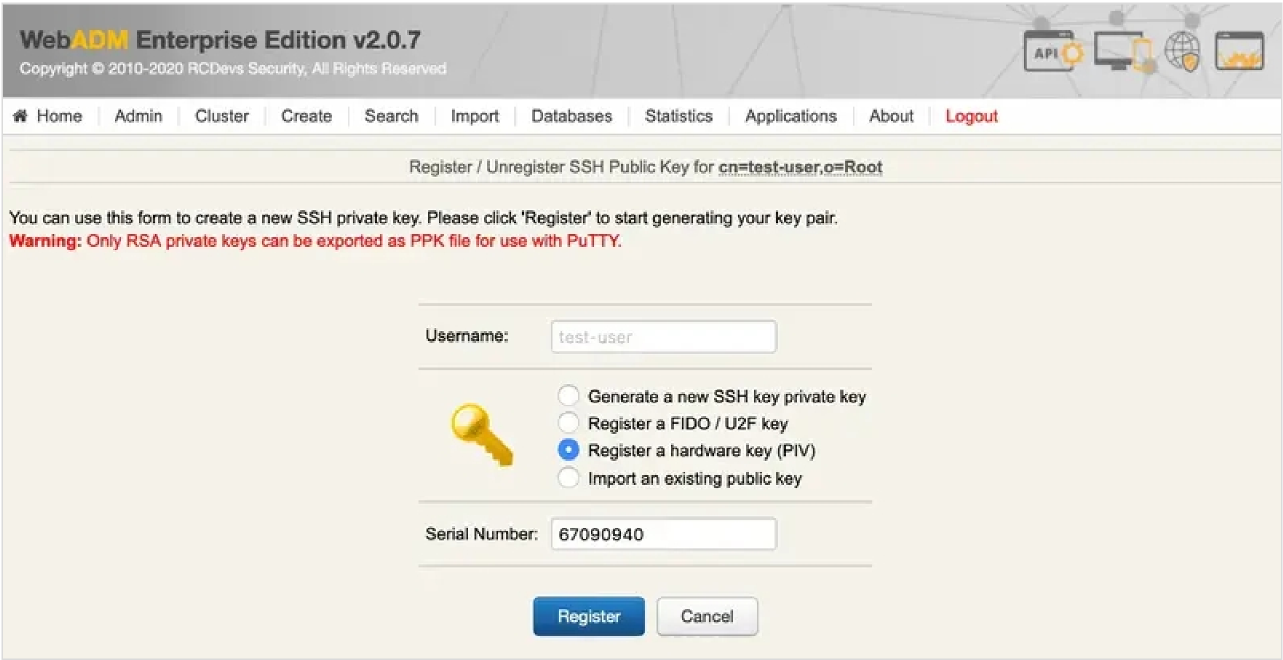
Find below the user actions supported by **SSH Public Key Server** (SpanKey).

Register / Unregister SSH Public Key
You can use this action to generate an SSH key pair or register an inventoried PIV device.

Set or Change Key Expiration
You can use this action to update the expiration date for a registered SSH public key.

Test Authorized Keys
You can use this action to test public key retrieval with SpanKey.

We select `Register a hardware key (Inventoried)`, enter the `Serial Number` (Reference) and `Register`:


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

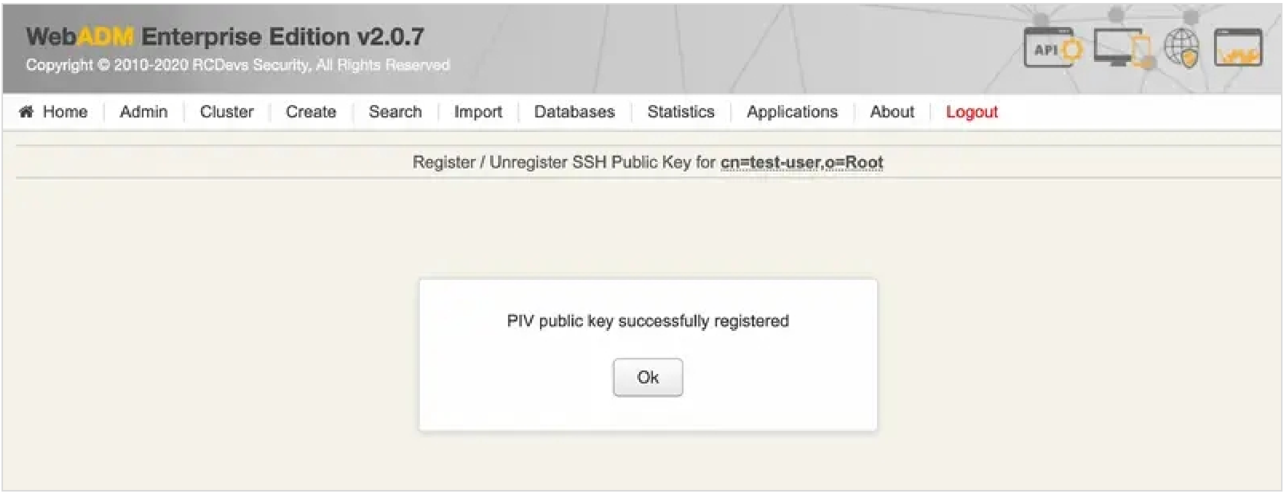
Register / Unregister SSH Public Key for cn=test-user,o=Root

You can use this form to create a new SSH private key. Please click 'Register' to start generating your key pair.
Warning: Only RSA private keys can be exported as PPK file for use with PuTTY.

Username: test-user

○ Generate a new SSH key private key
○ Register a FIDO / U2F key
● Register a hardware key (PIV)
○ Import an existing public key

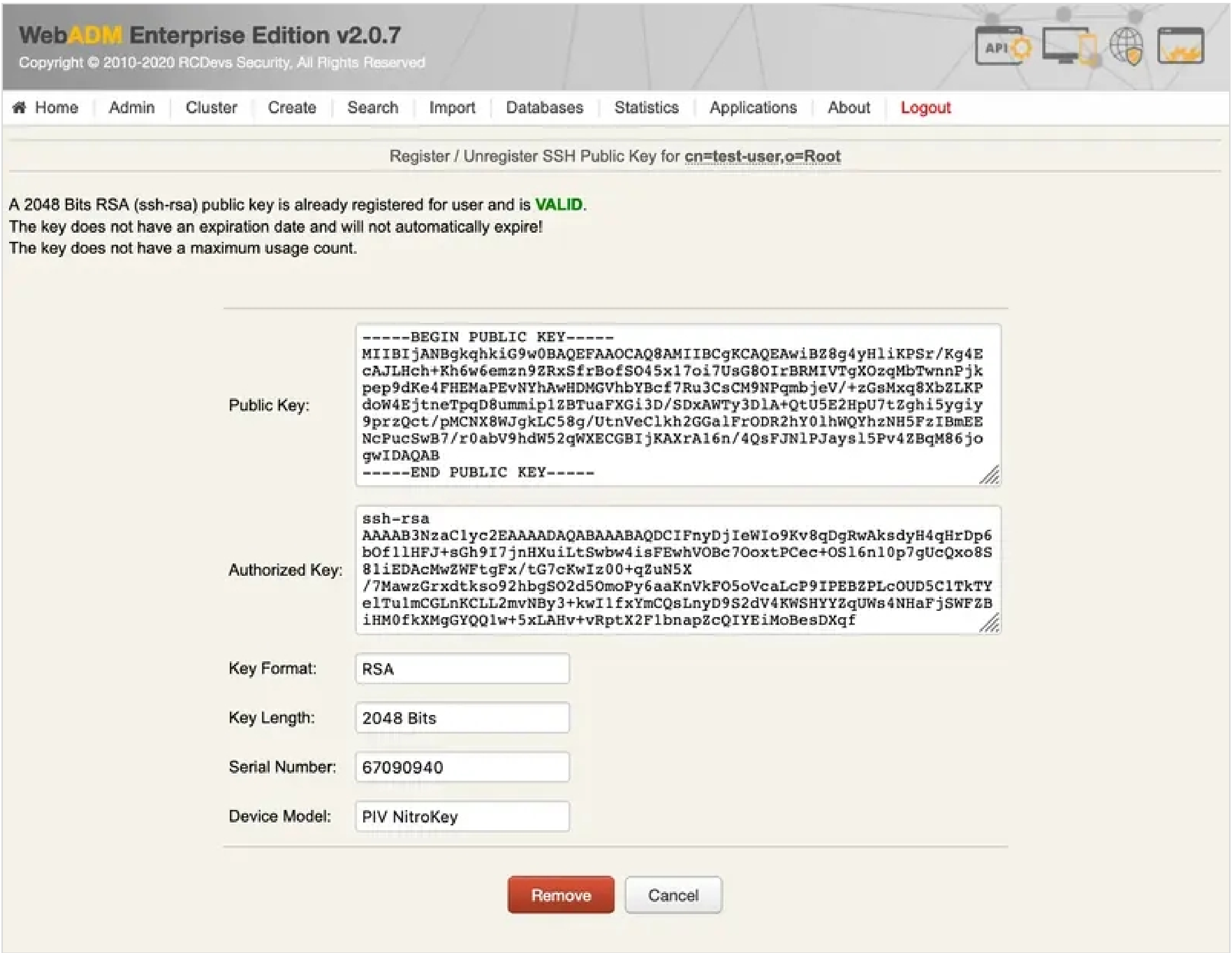
Serial Number: 67090940


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

Register / Unregister SSH Public Key for cn=test-user,o=Root

PIV public key successfully registered

Now, the PIV key is well registered.


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 SSH Public Key for cn=test-user,o=Root

A 2048 Bits RSA (ssh-rsa) public key is already registered for user and is VALID.
The key does not have an expiration date and will not automatically expire!
The key does not have a maximum usage count.

Public Key:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwiBZ8g4yHliKPSr/Kg4E
cAJLHch+Kh6w6emzn9ZRxSfrBofSO45x17oi7UsG8OIrBRMIVTgXOzqMbTwnnPjk
pep9dKe4FHEMaPEvNYhAwHDMGVhbYBcf7Ru3CsCM9NPqmbjeV/+zGsMxq8XbZLKP
doW4EjtneTpqD8ummip1ZBTuaFXGi3D/SDxAWTy3D1A+QtU5E2HpU7tZghi5ygiy
9przQct/pMCNX8WJgkLC58g/UtnVeClkh2GGalFrODR2hY0lhWQYhzNH5FzIBmEE
NcPucSwB7/r0abV9hdW52qWXECGBIjKAXrA16n/4QsFJNlPJays15Pv4ZBqM86jo
gwIDAQAB
-----END PUBLIC KEY-----
```

Authorized Key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDCIFnyDjIeWIo9Kv8qDgRwAksdyH4qHrDp6
bOfllHFJ+sGh9I7jnHXuiLtSwbw4isFEwhVOBc7OoxtPCec+OSl6nl0p7gUcQxo8S
8liEDAcMwZWFtgFx/tG7cKwIz00+qZuN5X
/7MawzGrxdtkso92hbgSO2d5OmoPy6aaKnVkFO5oVcaLcP9IPEBZPLcOUD5C1TkTY
elTulmCGLnKCLL2mvNBy3+kwIlfxYmCQsLnyD9S2dV4KWSHYYZqUWs4NHaFjSWFZB
iHM0fkXMgGYQQlw+5xLAHv+vRptX2FlbnapZcQIYEiMoBesDXqf
```

Key Format: RSA

Key Length: 2048 Bits

Serial Number: 67090940

Device Model: PIV NitroKey

Remove Cancel

3. Test with SSH

We’ll try with a CentOS 7 as an ssh server.

We install and configure `spankey_client` on it:

```
[root@centos7-client ~]# yum install https://repos.rcdevs.com/redhat/base/rcdevs_release-1.1.1-1.noarch.rpm
[root@centos7-client ~]# yum clean all
[root@centos7-client ~]# yum install spankey_client -y
[root@centos7-client ~]# /opt/spankey/bin/setup
Enter one of your running WebADM node IP or hostname []: 192.168.3.236
Do you want to enable SpanKey Client for OpenSSH server (y/n)? [N]: y
Do you want to enable SpanKey Client NSS plugin (y/n)? [Y]:
Do you want to register SpanKey Client logrotate script (y/n)? [Y]:
Do you want SpanKey Client to be automatically started at boot (y/n)? [Y]:

    Primary OpenOTP service URL is: 'https://192.168.3.236:8443/spankey/'
    Secondary OpenOTP service URL is: 'NONE'
    Enable SpanKey Client for OpenSSH server: 'YES'
    Enable SpanKey Client NSS plugin: 'YES'
    Register SpanKey Client logrotate script: 'YES'
    SpanKey Client must be automatically started at boot: 'YES'

Do you confirm (y/n)?: y

Applying SpanKey Client settings from default configuration files... Ok
Retrieving WebADM CA certificate from host '192.168.3.236'... Ok
The setup needs now to request a signed 'SpanKey' client certificate.
This request should show up as pending in your WebADM interface and an administrator must accept it.
Waiting for approbation... Ok
Updating entry 'client_id' in file '/opt/spankey/conf/spankey.conf'... Ok
Updating file '/etc/ssh/sshd_config'... Ok
Updating file '/etc/nsswitch.conf'... Ok
Updating file '/etc/pam.d/password-auth'... Ok
Registering SpanKey Client service...
Registering SpanKey Client service... Ok
Adding logrotate script... Ok

SpanKey Client has successfully been setup.

IMPORTANT: Do not forget to perform the following actions before you exit this session:
 - Start SpanKey (/opt/spankey/bin/spankey start)
 - Restart 'sshd'
 - Restart 'nscd'

[root@centos7-client ~]#
```

For the ssh client, we use a Mac mini. We configure it for using the smartcard:

```
[LO@Mac-mini ~]$ brew install opensc
```

We try the authentication:

```
[LO@Mac-mini ~]$ ssh -I opensc-pkcs11.so test-user@192.168.3.120
Enter PIN for 'User PIN (OpenPGP card)':


Session recording is disabled.
Audit logs recording is disabled.
Session lock is disabled.
Session's max duration is unlimited.

[test-user@centos7-client ~]$ pwd
/home/test-user
[test-user@centos7-client ~]$ exit
exit

>>>> Session's duration was aprox 42 seconds <<<<

Connection to 192.168.3.120 closed.
```

I’m connected to the server with a user from the LDAP database and authenticated with my PIV key.

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