

SMART CARD - 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.

Authentication with a Yubikey Smart Card / 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 Yubikey","", "PublicKey=<pub_key1>","Valid"
"PIV Device","<ID2>","PIV Yubikey","", "PublicKey=<pub_key2>","Valid"
"PIV Device","<ID3>","PIV Yubikey","", "PublicKey=<pub_key3>","Valid"
```

For my test, I have a Yubikey Nano with a PIV certificate and I use [yubico-piv-tool](#) for the management of the Yubikey, but it can work with other PIV keys.

We need to extract the public key. I do it with `yubico-piv-tool` and `openssl`:

```
[john@Mac-mini ~]$ yubico-piv-tool -aread-cert -s9a | openssl x509 -pubkey -noout
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwjYEZhuhF9rrxHdCDstG
J2ibVVrJhrZIfz4wwjrXtwEACJP2wWRe9dvNw5h3CrbguSc1l8mkKrfNwxAkGMOp
MIx5KgNBaDMcOggmjjFTOBIK4muJjdUZKhR3oFwBD/jjR7O1lGinYK873lYz01aS
nf7j00wgTI4kU3V+sJEbl9t3cQHfE6DMMWeG8w3Q03z+fVkNN9f30TvvBDua95Qg
G9m5eMtGqlrnPuovErHagfg8kd5IZFkYOakaoAhbOW6oQ8s8YKzCP1evcjfLYe/o
8K4br8vwp0jnBaKNKbVpO8iAn1A0UTXWaKUytb3cYqMvzp9UYh5Vyfl4MtMh8ULP
wwIDAQAB
-----END PUBLIC KEY-----
```

Another way that works with other keys/cards (Feitian, electronic ID, ...) is to do this with `opensc` and `pcsc-lite`. Once they are installed, you need to run these commands:

```
[root@fedora28 ~]# pkcs15-tool --list-key
Using reader with a card: Yubico Yubikey 4 OTP+CCID 00 00
Private RSA Key [PIV AUTH key]
Object Flags : [0x1], private
Usage       : [0x2E], decrypt, sign, signRecover, unwrap
Access Flags : [0x1D], sensitive, alwaysSensitive, neverExtract, local
ModLength   : 2048
Key ref     : 154 (0x9A)
Native      : yes
Auth ID     : 01
ID          : 01
```

```
[root@fedora28 ~]# pkcs15-tool --read-public-key 1
Using reader with a card: Yubico Yubikey 4 OTP+CCID 00 00
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwjYEZhuhF9rrxHdCDstG
J2ibVVrJhrZlfz4wwjrXtwEACJP2wWRe9dvNw5h3CrbguSc1l8mkKrfNwxAkGMOp
MIx5KgNBaDMcOggmjjFTOBIK4muJjdUZKhr3oFwBD/jjR7O1lGinYK873IYz01aS
nf7j00wgTI4kU3V+sJEbl9t3cQHfE6DMMWeG8w3Q03z+fVkJNN9f30TvvBDua95Qg
G9m5eMtGqlrnPuovErHagfg8kd5lZFkYOakaoAhbOW6oQ8s8YKzCP1evcjfLYe/o
8K4br8vwp0jnBaKNKbVpO8iAn1A0UTXWaKUytb3cYqMvzp9UYh5Vyfl4MtMh8ULP
wwIDAQAB
-----END PUBLIC KEY-----
```

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

```
"Type","Reference","Description","DN","Data","Status"
"PIV Device","8671120","PIV
Yubikey","", "PublicKey=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwjYEZhuhF9rrxHdCDstGJ2ibV
```

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

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

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

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: piv.csv

Type of File:

Import as Active: ☐ Yes ☐ No

Visibility Scope:

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

API

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

Inventory Items CSV Import

Processing record 1/1 PIV Device:8671120 (PIV Yubikey)... **Ok**

Now, the PIV key is present in the inventory:

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

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

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"/>	PIV Device	8671120	PIV Yubikey	2020-11-09 14:49:23	Link [NA]	Add [NA]	2 Data (Software encryption)	<input checked="" type="checkbox"/>	Valid

2. Assign the Yubikey

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

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

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

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)

Object Name

test-user

Rename

Add Attribute (8)

Mobile Phone Number

Add

Add Extension (1)

UNIX Account

Add

Login Name

test-user

[add values]

Last Name

test-user

[add values]

Email Address

a@b.c

[add values] [delete attribute]

Description / Note

test-user

[add values] [delete attribute]

First Name

test

[add values] [delete attribute]

Organization

local

[add values] [delete attribute]

Apply Changes

Re-Encrypt

Delete Selected

We click on **Proceed**:

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

API

HomeAdminClusterCreateSearchImportDatabasesStatisticsApplicationsAboutLogout

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

Proceed

Cancel

We **Extend Object**:

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

API

HomeAdminClusterCreateSearchImportDatabasesStatisticsApplicationsAboutLogout

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

Extend Object

Cancel

We click on **SSH Public key server**:

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

HomeAdminClusterCreateSearchImportDatabasesStatisticsApplicationsAboutLogout

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]

Description / Note
[add values] [delete attribute]

First Name
[add values] [delete attribute]

Organization
[add values] [delete attribute]

UID Number

GID Number

Home Directory

Login Shell
[delete attribute]

Apply Changes | Re-Encrypt | Delete Selected

We click on **Register/Unregister SSH key** :

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

HomeAdminClusterCreateSearchImportDatabasesStatisticsApplicationsAboutLogout

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

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

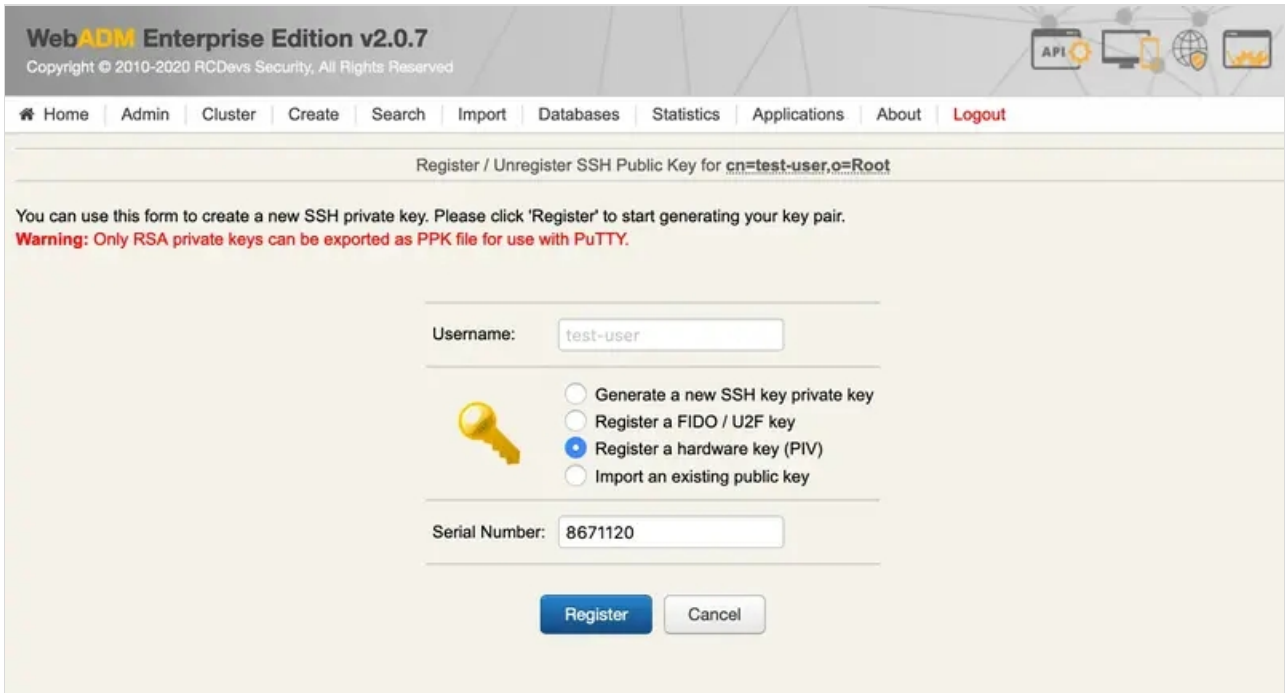
Register / Unregister SSH Public Key
You can use this action to generate an SSH key pair or register an inventoried PIV device.

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.

Cancel

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

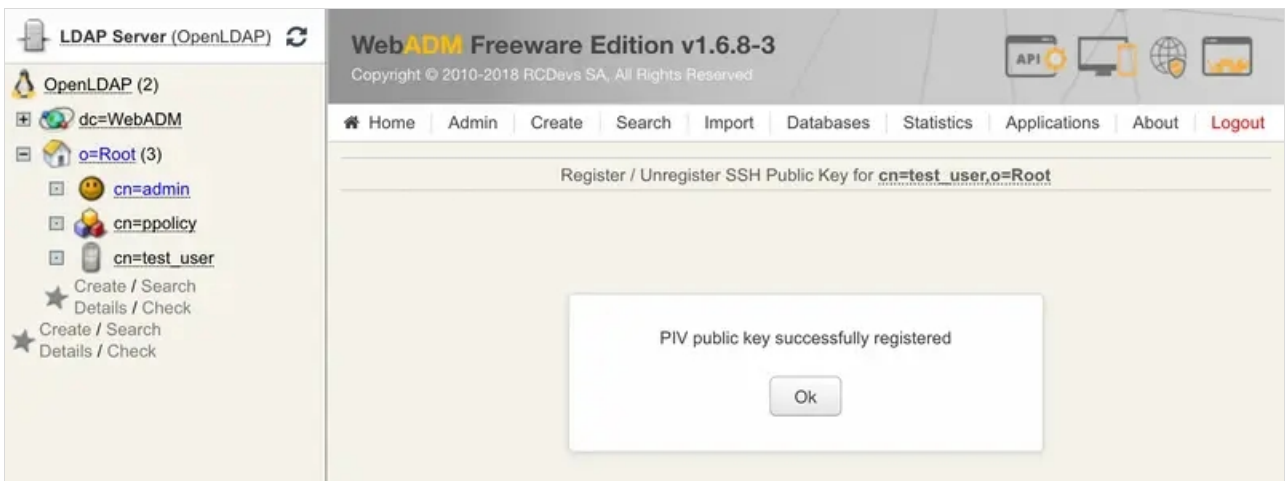
Register / Unregister SSH Public Key for **cn=test-user,o=Root**

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:

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

Serial Number:



LDAP Server (OpenLDAP)

- OpenLDAP (2)
 - dc=WebADM
 - o=Root (3)
 - cn=admin
 - cn=ppolicy
 - cn=test_user
 - Create / Search
 - Details / Check

WebADM Freeware Edition v1.6.8-3
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

Home Admin 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.

LDAP Server (OpenLDAP) ↻

OpenLDAP (2)

dc=WebADM

o=Root (3)

cn=admin

cn=ppolicy

cn=test_user

Create / Search Details / Check

Create / Search Details / Check

WebADM Freeware Edition v1.6.8-3

Copyright © 2010-2018 RCDevs SA, All Rights Reserved

Home

Admin

Create

Search

Import

Databases

Statistics

Applications

About

Logout

Register / Unregister SSH Public Key for cn=test_user,o=Root

An SSH public key is already registered for user and is **VALID**.

The key does not have an expiration date and will not automatically expire!

Public Key:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwjYEZhuhF9rrxHdCDstGJ
2ibVVRJhrZIfz4wwjrxTWEACJP2wRe9dvNw5h3CrbguSc118mkKrfNwxAKGMOpMI
x5KgNBaDMcOggmjFTOBIK4muJjdUZKhR3oFwBD/jjR7011GinYK8731Yz01aSnf7
j00wgT14kU3V+sJebI9t3cQHE6DMMWeG8w3Q03z+fVKN9f30TvvBDua95QgG9m5
eMtGqlrnPuovErHagfg8kd51ZFkYOakaoAhhOW6oQ8s8YKzCP1evcjfLYe
/o8K4br8vwp0jnBaKNKbVpO8iAn1A0UTXWaKUYtb3cYqMvzp9UYh5Vyf14MtMh8UL
PwIDAQAB
-----END PUBLIC KEY-----
```

Authorized Key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDCNgRmG6EX2uvEd0IOy0YnaJtVWsmGtKh/P
jDCote3AQAIk
/bBZF71283DmHcKtuC5JzWXyaQgt83DECQYw6kwjHkqA0FoMxw6CCA0MVM4Egria4
mN1RkqFHegXAEp+ONHs7WUaKdgrzveVjPTVpKd
/uPTTCBOXiRTdX6yMRsj23dxAd8ToMwxZ4bzDdDTfp59WQ031
/fRO+8EO5r31CAB2b14y0aqWuc+6i8SsdqB+DyR3mVkwRg5qRggCFs5bqhDyzxgrM
T/uA9vM8+h7+wrhuv/CnS0cF00ntWk7utCfiIDPMdZ0nPK1udviox
```

Key Format:

RSA

Key Length:

2048 Bits

Serial Number:

8671120

Device Model:

PIV Yubikey

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@test_vm ~]$ yum install https://repos.rcdevs.com/redhat/base/rcdevs_release-1.1.1-1.noarch.rpm
[root@test_vm ~]$ yum clean all
[root@test_vm ~]$ yum install spankey_client -y
[root@test_vm ~]$ spankey_setup
This is the configuration tool for RCDevs SpanKey Agent.
It will configure SpanKey Server URL(s), SSH helper and NSS.
```

```
Do you have a WebADM cluster or standalone server (c/s)? s
Enter hostname or address for SpanKey server: my_webadm
Do you want to enable SpanKey for OpenSSH server (y/n)? y
Do you want SpanKey agent to auto-create home directories (y/n)? y
Do you want to enable SSH session management options (y/n)? y
Do you want to enable SpanKey NSS plugin (y/n)? y
SpanKey Agent for SpanKey standalone Server
Server URL: https://192.168.3.202:8443/spankey/ (Server Ok)
Enable SpanKey for OpenSSH server: Yes
Auto-create home directories: Yes
SSH session management options: Yes
Enable SpanKey NSS plugin: Yes
```

```
Do you confirm (y/n)? y
```

```
Updating /etc/spankey/spankey.conf... Ok
Updating /etc/ssh/sshd_config... Ok
Updating /etc/nsswitch.conf... Ok
Updating /etc/pam.d/password-auth... Ok
Created symlink from /etc/systemd/system/multi-user.target.wants/nscd.service to
/usr/lib/systemd/system/nscd.service.
Created symlink from /etc/systemd/system/sockets.target.wants/nscd.socket to
/usr/lib/systemd/system/nscd.socket.
```

SpanKey Agent has been successfully configured.

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

```
[John@Mac-mini ~]$ brew install opensc
[John@Mac-mini ~]$ export OPENSC_LIBS=$(brew --prefix opensc)/lib
```

We try the authentication:

```
[John@Mac-mini ~]$ ssh -I $OPENSC_LIBS/opensc-pkcs11.so John@test_vm
Enter PIN for 'PIV Card Holder pin (../piv_II)':
bash-4.2$
```

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