



HELPDESK ADMINISTRATION AND USAGE

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.

Helpdesk Administration and Usage

[Web-Application](#) [Activation](#) [End-users Management](#) [Enrollment](#)

1. Overview

The purpose of this web application is to provide an easy-to-use interface for the most common “tier 1” support task, typically performed by a Help-Desk function in a company IT organization.

This Web application is designed for internal (corporate) use and includes several self-management features like:

- › Activate users for OpenOTP use
- › View and manage account information such as email, mobile phone numbers, etc...
- › Reset LDAP password
- › Send password reset or token registration links
- › Enroll, re-synchronize and test a Software / Hardware Token or Yubikey
- › Manage user certificates
- › Manage SSH keys (SpanKey)

Administration Help Desk web application must be installed on your WebADM server(s) and can be accessed through WAProxy or another reverse proxy configured with WebADM.

Please see the [Administration Helpdesk Installation and Configuration](#) for further details.

The **HelpDesk** application is accessible via the following address:

```
https://YOUR_WEBADM/webapps/helpdesk/login_uid.php
```

and through the WAProxy it is:


```
https://YOUR_WAPROXY/helpdesk/login_uid.php
```


2. Dashboard

Log in to the HelpDesk application.

Login

Please enter the required information to login.

 admin





Domain


Default

Login



Welcome to the HelpDesk Portal at *com*.



Select the user you want to manage the **User Profile**, **Security Tokens / Keys**, **SelfReg Link** and get an overview over the **Last User Activity**.

 **HELPDESK**

[Home](#) / [Dashboard](#)

You are logged on as **admin** |  |  Logout

Q USER SEARCH


Select the user you want to manage.

Login Name: CentOS8_57eypo4p
DN: cn=CentOS8_57eypo4p,o=R...
Full Name: CentOS8_57eypo4p
Domains: Default

Select

CentOS8_57eypo4p

Hello **admin**.
Welcome to the Helpdesk Portal at *com*.



DASHBOARD

OTP

FIDO

SSH

SSO

PKI

Home / Dashboard

DefaultCentOS8_57eypo4p

You are logged on as **admin** | | Logout

User Search

Select

USER PROFILE

DN: cn=CentOS8_57eypo4p,o=Root UID: CentOS8_57eypo4p

Full Name:

CentOS8_57eypo4p

WebADM Domains:

Default

LDAP Groups:

cn=group_linux_rpm,o=root

Blocking Status:

✔ Account active

Last login:

2021-05-27 15:41:51

Mobile Number:

Email Address:

loic@rcdevs.com

Language:

EN

Password:

.....

Deactivate

Primary OTP Method
 TOKEN

Fallback OTP Method
 MAIL

Push Enabled
 YES

1

Tokens

1

Login count

0

Reject count

USER SECURITY TOKENS / KEYS

TOTP

Software

Add a Token

LAST USER ACTIVITY

Display 10 records

Search:

Date	Client	Source	Host	Session
2021-05-27 15:41:51	SelfDesk	10.2.3.2	192.168.4.200	Z7XSVW4D
2021-05-27 15:41:51	SelfDesk	10.2.3.2	192.168.4.200	Z7XSVW4D
2021-05-27 15:41:42	SelfDesk	10.2.3.2	192.168.4.200	Z7XSVW4D
2021-05-27 15:41:42	SelfDesk	10.2.3.2	192.168.4.200	Z7XSVW4D

Showing 1 to 4 of 4 entries

Previous

1

Next

3. User Activation

Log in to the HelpDesk application.



Login

Please enter the required information to login.

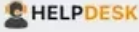
Domain

Login



Welcome to the HelpDesk Portal at *com.*



Select the user you want to **Activate**.



Home / Dashboard

You are logged on as **admin** |  |  Logout


Q USER SEARCH

Select the user you want to manage.


Login Name: test-user
DN: cn=test-user,o=Root
Full Name: test-user
Domains: Default

Select



Hello **admin**.
Welcome to the Helpdesk Portal at *com.*



Please **Activate** the selected user if not already done previously.



Home / Dashboard

You are logged on as **admin** |  |  Logout

User Search


Select

USER PROFILE

DN: cn=test-user,ou=Internal,o=Root

Activate

Under **Blocking Status**, the users account is now active.

 **HELPDESK**

DASHBOARD

OTP



FIDO

App Keys


SSH


SSO

PKI

Home / DashboardDefault\test-userYou are logged on as admin |  |  Logout

User SearchSelect

 **USER PROFILE**

 DN: cn=test-user,o=Root UID: test-user

Full Name:

test-user

WebADM Domains:

Default

LDAP Groups:


Blocking Status:

✔ Account active

Last login:


[Not Set]

Mobile Number:




Email Address:

loic@rcdevs.com





Language:

[Not Set]






Password:


.....

Deactivate

 **Primary OTP Method**
TOKEN

 **Fallback OTP Method**
[NOT SET]

 **Push Enabled**
NO

0


Tokens

0

Login count

0

Reject count

 **USER SECURITY TOKENS / KEYS**

4. Token Enrollment


4.1 Software Token Registration


4.1.1 Registration from Helpdesk page

Log in to the HelpDesk application.

Login

Please enter the required information to login.

 admin





Domain


Default

Login



Welcome to the HelpDesk Portal at *com*.



Select the user you want to register a **Software Token**.

 **HELPDESK**

Home / Dashboard

You are logged on as **admin** |  |  Logout

USER SEARCH


Select the user you want to manage.

Login Name: CentOS8_57eypo4p
DN: cn=CentOS8_57eypo4p,o=R...
Full Name: CentOS8_57eypo4p
Domains: Default

Select

CentOS8_57eypo4p

Hello **admin**.
Welcome to the Helpdesk Portal at *com*.



Go to the **OTP** tab. Choose your **Fallback OTP Methode**, **Enable Push Login** and **Emergency OTP**. At the bottom of the page, click **Add a Token**.

HELPDESK

DASHBOARD

OTP


FIDO

SSH

PKI

Home / Openotp

Default|CentOS8_57eypo4p

You are logged on as admin |  | [Logout](#)

MANAGE OTP AUTHENTICATION SETTINGS

← Back

Manage users hardware and software Tokens: register, deactivate, remove, test or resynchronize user devices.
Configure OTP authentication settings: primary OTP method, fallback OTP method, challenge session timeout or enable push login notification.

Primary OTP Method:

Token

✕

Fallback OTP Method:

Mail

✕

OTP Challenge Timeout:

1 minute 30 seconds

✕

Enable Push Login:

☒ Yes ☐ No

✕

Emergency OTP:

✎

Test user authentication

Token

⌵

Submit SelfReg link

Mail

⌵

Primary Token

⌵

USER SECURITY TOKENS / KEYS

Add a Token

On the next page, click under **Software Token** [Add Token](#) .

HELPDESK

DASHBOARD

OTP


FIDO

SSH

PKI

Home / Openotp / Register

Default|CentOS8_57eypo4p

You are logged on as admin |  | [Logout](#)


REGISTER A NEW TOKEN

← Back

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

Hardware Token


Token Inventoried



Add Token

Software Token


QRCode-based Authenticator



Add Token

Yubikey


Inventoried & YubiCloud



Add Token

Another Token

Manual Registration



Add Token

Then scan the QRCODE to register your **Software Token**.

RCDevs

DASHBOARD

OTP

FIDO

App Keys

SSH

SSO

PKI

+


REGISTER A NEW TOKEN

You must first register your Software or Hardware Token to start using it.

The registration consists in synchronizing a Secret Key and an initial Token state.

Software Token

QRCode-based Authenticator



Cancel

+

INSTRUCTIONS TO REGISTER A QR CODE-BASED SOFTWARE TOKEN

1. Install the Software Token on your mobile device.


2. Start your software Token and Scan the QRCode displayed below.

3. You need to enter the OTP displayed on your Token in order to register. If you use RCDevs Push Token, the registration will auto-complete after scanning.

It's possible to download QRCode to register a distant device. Configure expiration time, set a PIN code, and click download. To finish registration, scan QRCode and enter PIN code in OpenOTP Token mobile application. QRCode will be unavailable after expiration time.

HOTP

TOTP



(Enlarge)

☐ Disable push

Receiving Mobile response

Enter OTP

Register

Download QRcode

Expiration Time

30 minutes

PIN Code

Enter PIN Code

Gen

PIN will be automatically sent by mail and SMS

Download

Send e-mail

Finally, you will see the **Software Token** that you have just registered in the user's **OTP** tab.

RCDevs

DASHBOARD

OTP

FIDO

App Keys


SSH

SSO

PKI

Home / Openotp

Demos\Loic

You are logged on as Loic |  | [Logout](#)

MANAGE OTP AUTHENTICATION SETTINGS

Manage users hardware and software Tokens: register, deactivate, remove, test or resynchronize user devices.

Configure OTP authentication settings: primary OTP method, fallback OTP method, challenge session timeout or enable push login notification.

Primary OTP Method:

Token

Fallback OTP Method:

Mail

OTP Challenge Timeout:

1 minute 30 seconds

Enable Push Login:

☒ Yes ☐ No

Test user authentication

Token


Submit SelfReg link

Mail

Primary 1

TOTP

iPhone11,8



Type: OATH Time-based (160 bits)


Add a Token


4.1.2 Submit a SelfReg link to the end user

Log in to the HelpDesk application.

Login

Please enter the required information to login.

 admin





Domain


Default

Login



Welcome to the HelpDesk Portal at *com*.



Select the user you want to submit a **SelfReg Link** via Mail / SMS.

 **HELPDESK**

Home / Dashboard

You are logged on as **admin** |  |  Logout

Q USER SEARCH


Select the user you want to manage.

Login Name: test-user
DN: cn=test-user,o=Root
Full Name: test-user
Domains: Default


Select

test-user

Hello **admin**.
Welcome to the Helpdesk Portal at *com*.



The user must have set an email or mobile number. Go to the **Primary OTP Method** tab.

 **HELPDESK**

DASHBOARD

OTP



FIDO

App Keys


SSH


SSO

PKI

Home / DashboardDefault\test-userYou are logged on as admin |  |  Logout

User SearchSelect

 **USER PROFILE**

 DN: cn=test-user,o=Root UID: test-user

Full Name:

test-user

WebADM Domains:

Default

LDAP Groups:


Blocking Status:

✔ Account active

Last login:


[Not Set]

Mobile Number:




Email Address:

loic@rcdevs.com





Language:

[Not Set]




Password:

.....


 


Deactivate



Primary OTP Method


TOKEN





Fallback OTP Method

[NOT SET]



Push Enabled

NO

0


Tokens

0

Login count

0

Reject count

 **USER SECURITY TOKENS / KEYS**

Choose your **Fallback OTP Methode**, **Enable Push Login** and **Emergency OTP**. At the bottom of the page, click **Submit SelfReg Link** via Mail / SMS.

HELPDESK

DASHBOARD

OTP

FIDO

App Keys

Helpdesk success1s X

Home / OpenotpDefault\test-userYou are logged in as test-user

Self Registration link sent

+ MANAGE OTP AUTHENTICATION SETTINGS

Manage users hardware and software Tokens: register, deactivate, remove, test or resynchronize user devices.
Configure OTP authentication settings: primary OTP method, fallback OTP method, challenge session timeout or enable push login notification.

Primary OTP Method:

Token

X

Fallback OTP Method:

X

OTP Challenge Timeout:

1 minute 30 seconds

X

Enable Push Login:

☐ Yes ☒ No

X

Emergency OTP:

[Not Set]

Test user authentication

Token

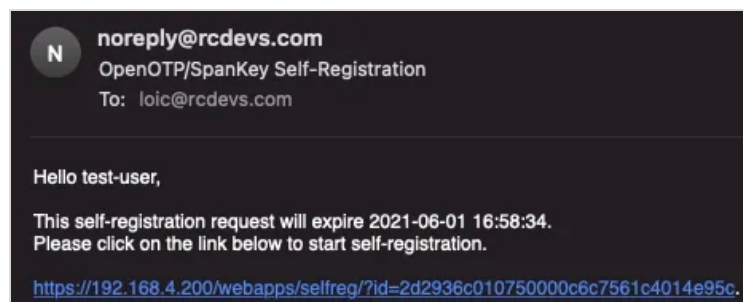
Submit SelfReg link

Mail

Primary Token

USER SECURITY TOKENS / KEYS

The SelfReg email has been sent. The user must click on the SelfReg link and enroll the token.



User Self-Registration

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

Instructions to register a QRCode-based Software Token:

1. [Install the Software Token](#) on your mobile device.
2. Start your software Token and Scan the QRCode displayed below.
3. Click the 'Register' button below after scanning.



☐ I use a Hardware Token (Inventoried)

☐ I use a Yubikey Token (Inventoried / YubiCloud)

☒ I use a QRCode-based Authenticator (Time-based)

☐ I use a QRCode-based Authenticator (Event-based)

☐ I use another Token (Manual Registration) [i](#)

Register As:

Primary Token

QRCode:
([Enlarge](#))



[i](#)

Enter OTP:

.....

[i](#)

Register

Cancel




Provided by [RCDevs Security SA](#)

User Self-Registration

Your Primary Token has been registered

Ok



Provided by [RCDevs Security SA](#)

Finally, you will see that the user has enrolled the token.

DN: cn=test-user,o=Root

UID: test-user

Full Name:

test-user

WebADM Domains:

Default

LDAP Groups:

Blocking Status:

✔ Account active

Last login:

[Not Set]

Mobile Number:

Email Address:

loic@rcdevs.com

Language:

[Not Set]

Password:

.....

Deactivate

✔

Fallback OTP Method

[NOT SET]

📱

Push Enabled

NO

1

Tokens

0

Login count


0

Reject count

🔑 USER SECURITY TOKENS / KEYS

TOTP

Software



✔

🗑️

🔄

+

Add a Token

4.1.3 Submit QRCode/PIN by Mail/SMS to the end user

It's possible to download the **QRCode** to register a distant device.


⚠ IMPORTANT NOTE


This is only available with enabled **Push** feature. Please see the [Configure Push Login with OpenOTP](#) for further details.

Log in to the HelpDesk application.

Login

Please enter the required information to login.

 admin





Domain


Default

Login



Welcome to the HelpDesk Portal at *com*.



Select the user you want to register a **Software Token** with the **Push** feature.

 **HELPDESK**

Home / Dashboard

You are logged on as **admin** |  |  Logout

USER SEARCH


Select the user you want to manage.

Login Name: CentOS8_57eypo4p
DN: cn=CentOS8_57eypo4p,o=R...
Full Name: CentOS8_57eypo4p
Domains: Default

Select

CentOS8_57eypo4p

Hello **admin**.
Welcome to the Helpdesk Portal at *com*.



Go to the **OTP** tab. At the bottom of the page, click **Add a Token**.

← Back

Set the **Expiration Time** and must generate a **PIN Code** . Finally, click **Download / Send E-mail** .

DOWNLOAD QR CODE

Expiration Time

1 week



PIN Code

728164

Gen



PIN will be automatically sent by mail

 Download

 Send e-mail


4.2 Hardware Token Registration


4.2.1 Token Registration based on Serial Number (inventoried devices)

Log in to the HelpDesk application.

Login

Please enter the required information to login.

 admin





Domain

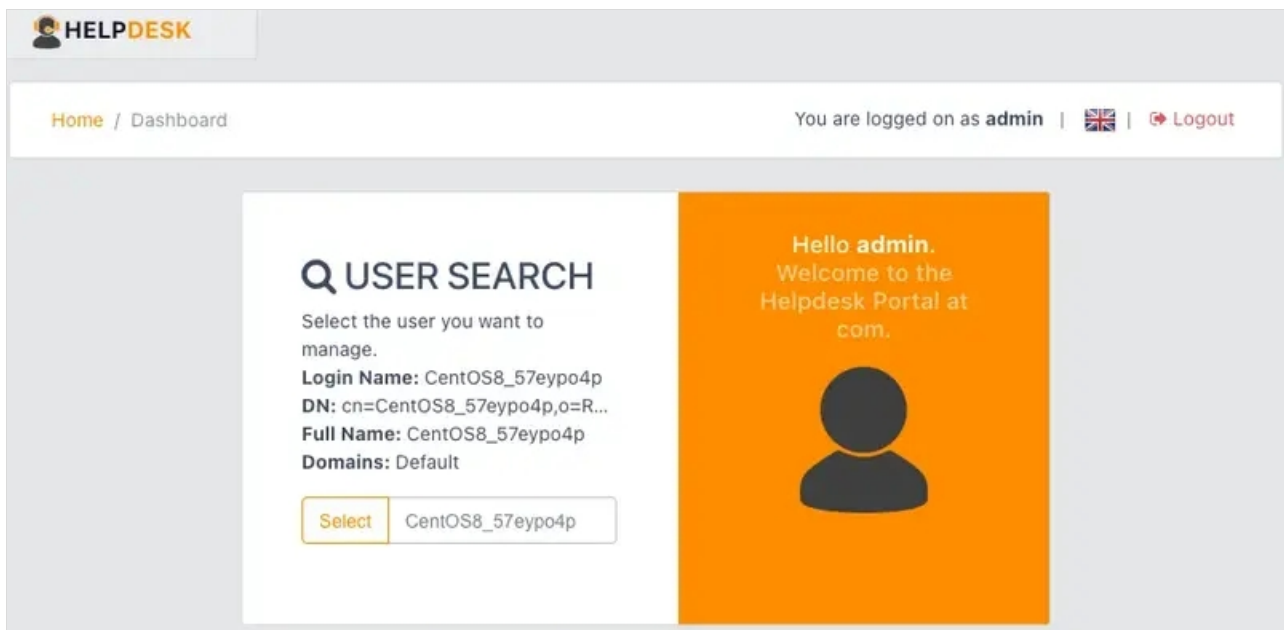
Default

Login

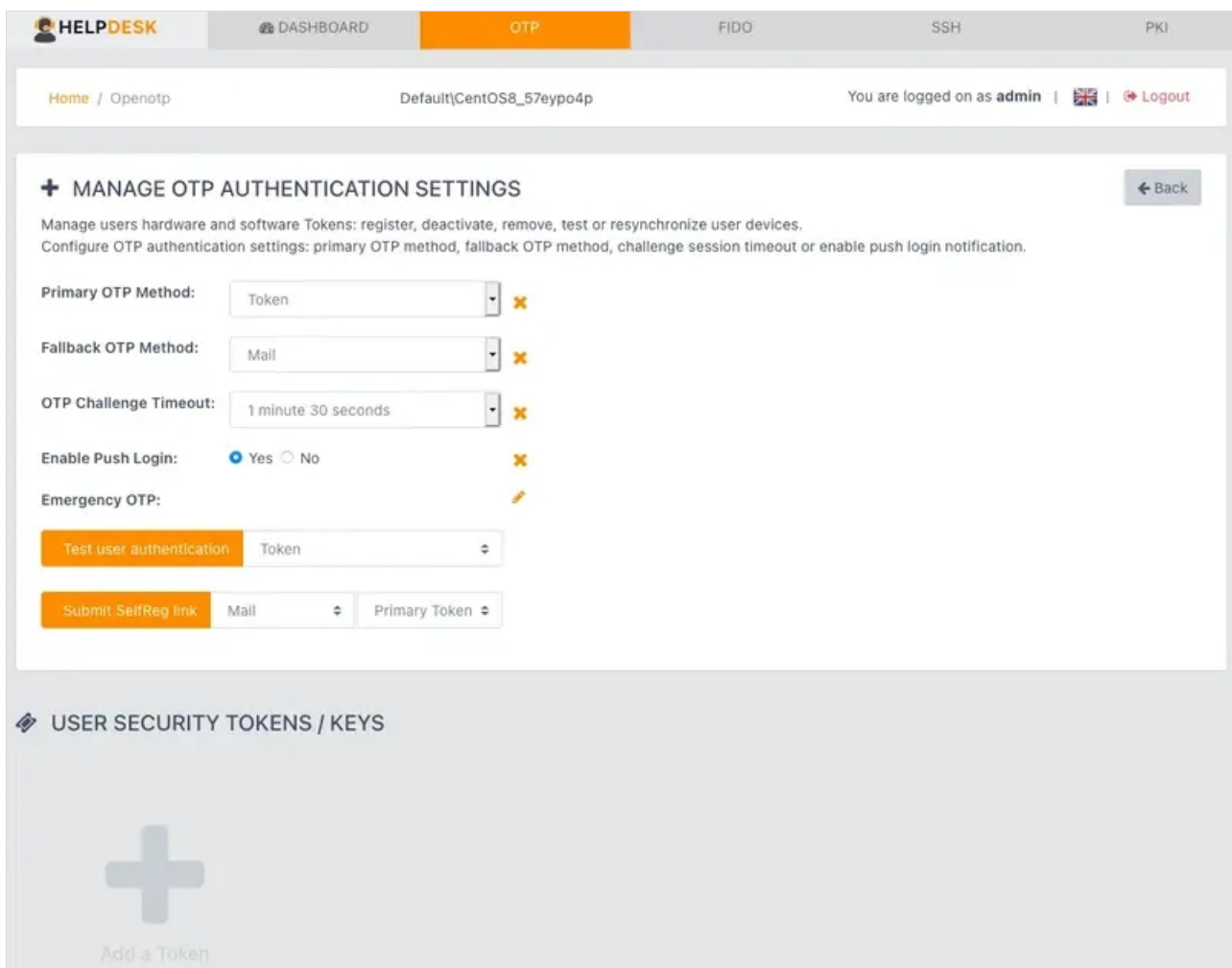
Welcome to the
HelpDesk Portal at
com.



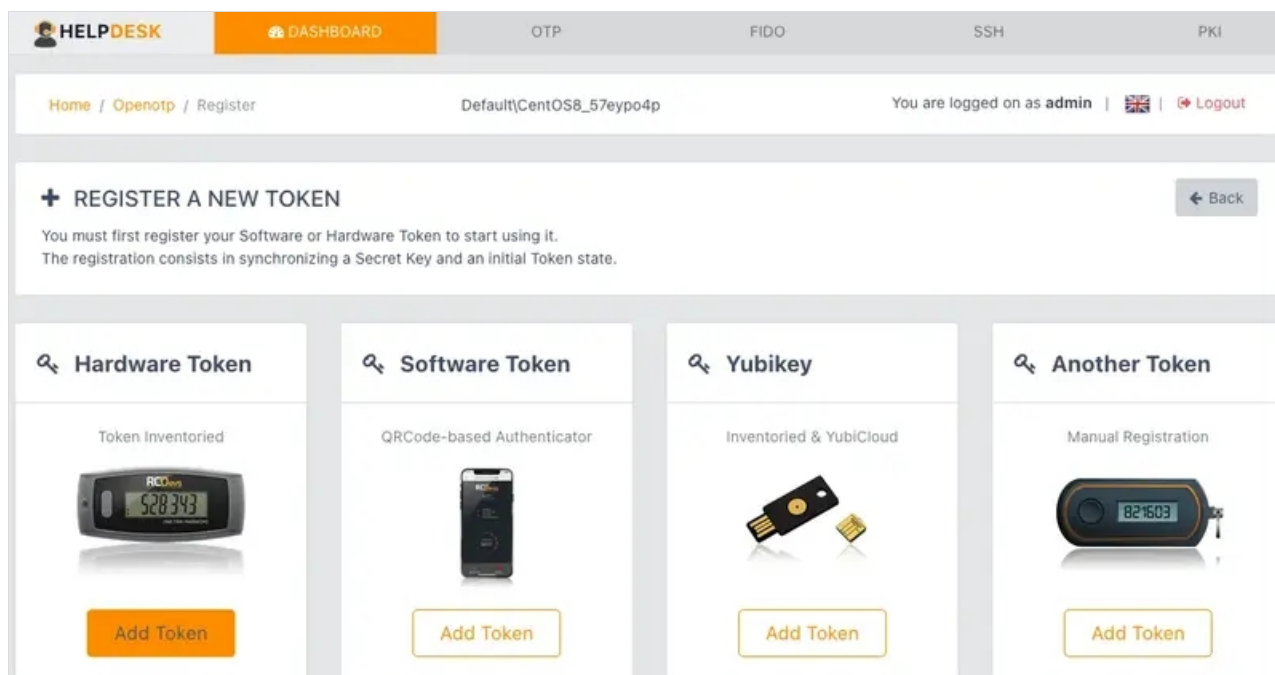
Select the user you want to register a **Hardware Token**.



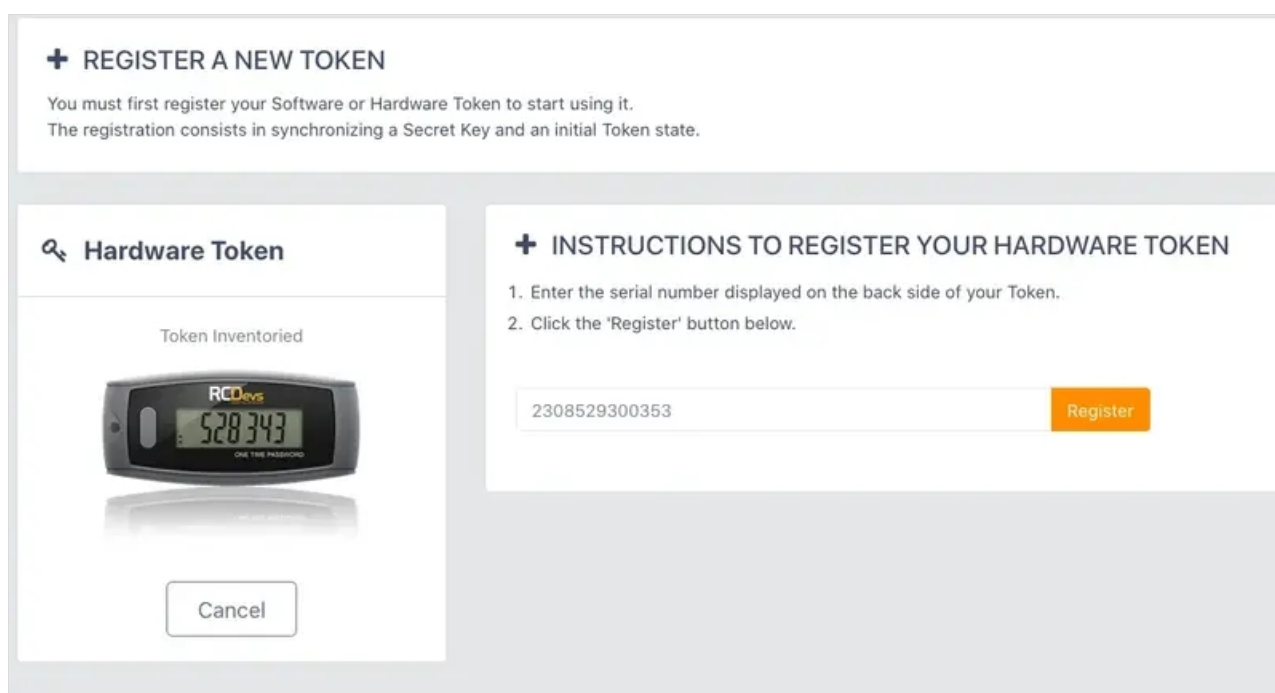
Go to the **OTP** tab. At the bottom of the page, click **Add a Token**.



On the next page, click under **Hardware Token** **Add Token**.



Then enter the serial of your inventoried **Token** and click on **Register**.



Finally, you will see the **Hardware Token** that you have just registered in the user's **OTP** tab.

HELPSDESK

DASHBOARD

OTP

FIDO

token

×

Fallback OTP Method:

×

OTP Challenge Timeout:

1 minute 30 seconds

×

Enable Push Login:

☒ Yes ☐ No

×

Test user authentication

Token

⇅

Submit SelfReg link

Mail

⇅

Primary Token

⇅

USER SECURITY TOKENS / KEYS

TOTP

RCDevs RC200-T6 2308529300353



Type: OATH Time-based (160 bits) ▼

☒ ☐ ☐

+


Add a Token


4.2.2 YubiKey Registration

Log in to the HelpDesk application.

Login

Please enter the required information to login.

 admin





Domain


Default

Login



Welcome to the HelpDesk Portal at *com*.



Select the user you want to register a **YubiKey**.

 **HELPDESK**

[Home](#) / [Dashboard](#)

You are logged on as **admin** |  |  Logout

USER SEARCH


Select the user you want to manage.

Login Name: CentOS8_57eypo4p
DN: cn=CentOS8_57eypo4p,o=R...
Full Name: CentOS8_57eypo4p
Domains: Default

Select

CentOS8_57eypo4p

Hello **admin**.
Welcome to the Helpdesk Portal at *com*.



Go to the **OTP** tab. At the bottom of the page, click **Add a Token**.

[DASHBOARD](#)
[OTP](#)
[FIDO](#)
[SSH](#)
[PKI](#)

[Home](#) / [Openotp](#)
Default|CentOS8_57eypo4p
You are logged on as **admin** | | [Logout](#)

+ MANAGE OTP AUTHENTICATION SETTINGS

[← Back](#)

Manage users hardware and software Tokens: register, deactivate, remove, test or resynchronize user devices.
Configure OTP authentication settings: primary OTP method, fallback OTP method, challenge session timeout or enable push login notification.

Primary OTP Method: Token

Fallback OTP Method: Mail

OTP Challenge Timeout: 1 minute 30 seconds

Enable Push Login: ☒ Yes ☐ No

Emergency OTP:

[Test user authentication](#) Token

[Submit SelfReg link](#) Mail Primary Token

USER SECURITY TOKENS / KEYS

Add a Token

On the next page, click under **YubiKey** [Add Token](#).

[DASHBOARD](#)
[OTP](#)
[FIDO](#)
[SSH](#)
[PKI](#)

[Home](#) / [Openotp](#) / [Register](#)
Default|CentOS8_57eypo4p
You are logged on as **admin** | | [Logout](#)

+ REGISTER A NEW TOKEN

[← Back](#)

You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an Initial Token state.

Hardware Token

Token Inventoried

[Add Token](#)

Software Token

QRCode-based Authenticator

[Add Token](#)

Yubikey

Inventoried & YubiCloud

[Add Token](#)

Another Token

Manual Registration

[Add Token](#)

Plug the YubiKey in a USB port on your computer. Then press the button of the inventoried **YubiKey** to finish the registration.

HELPDESK

DASHBOARD

OTP


FIDO

SSH

PKI

Home / Openotp / Register

DefaultCentOS8_57eypo4p

You are logged on as admin |  | [Logout](#)


REGISTER A NEW TOKEN

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

[← Back](#)

Yubikey


Inventoried & YubiCloud



Cancel

INSTRUCTIONS TO REGISTER YOUR YUBIKEY TOKEN

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



Finally, you will see the **YubiKey** that you have just registered in the user's **OTP** tab.

RCDevs

DASHBOARD

OTP

FIDO

App Keys



SSH

SSO

PKI

Home / Openotp

Demos\Loic

You are logged on as Loic |  |  Logout

+

MANAGE OTP AUTHENTICATION SETTINGS

Manage users hardware and software Tokens: register, deactivate, remove, test or resynchronize user devices.

Configure OTP authentication settings: primary OTP method, fallback OTP method, challenge session timeout or enable push login notification.

Primary OTP Method:

Token

✕

Fallback OTP Method:

Mail

✕

OTP Challenge Timeout:

1 minute 30 seconds

✕

Enable Push Login:

☒ Yes ☐ No

✕

Test user authentication

Token

⬆

Submit SelfReg link

Mail


⬆

Primary 1


⬆


YUBIKEY


Yubikey YubiCloud 2573110



Type: YubiKey (YubiCloud)







+

Add a Token

4.2.3 FIDO Registration

Log in to the HelpDesk application.



Login

Please enter the required information to login.

Domain Default

Login


Welcome to the HelpDesk Portal at *com*.

Select the user you want to manage the **FIDO** devices settings.

HELPDESK

Home / Dashboard

You are logged on as Admin BERCDEVS |  | Logout


Q USER SEARCH

Select the user you want to manage.

Login Name: testuser1
DN: CN=Test User Un,OU=Users,OU=BENOIT,OU=WebADMs,DC=su...
Full Name: Test User Un
Domains: Default

Select testuser1

Hello Admin BERCDEVS.
Welcome to the Helpdesk Portal at webadmb.support.rcdevs.com.




Go to the **FIDO** tab.

HELPDESK

DASHBOARD
OTP
FIDO
App Keys
SSH
SSO
PKI

Home / U2F


Default(testuser1)

You are logged on as Admin BERCDEVS |  | Logout

MANAGE FIDO DEVICES SETTINGS


Back

You must first register your FIDO Device or Token to start using it.
If any of the checks below fails then the registration cannot be done.

Your Web browser supports FIDO: Yes 
URL is enabled for FIDO: Yes

Instructions to register your FIDO Device:


- Plug the FIDO Device in a USB port on the computer.
- Click the blinking message below (or press Enter) to initiate the registration.
- When the device starts blinking, press the button to proceed the registration.

Friendly Name: fido 2 token 

Device Type:
☐ U2F
☒ FIDO2

Registered UserID: testuser1

Registered Domain: Default



fido

[Click Here or Press Enter]

Plug the **FIDO** device in a USB port on your computer. Choose a **Friendly Name** and **Device Type: FIDO2**.

[Click Here or Press Enter] to finish the registration.

HELPDESK

DASHBOARD

OTP

Home / U2F

MANAGE FIDO DEVICES SETTINGS

You must first register your FIDO Device or Token to start using it.
If any of the checks below fails then the registration cannot be done.

Your Web browser supports FIDO: Yes
URL is enabled for FIDO: Yes

Instructions to register your FIDO Device:


- Plug the FIDO Device in a USB port on the computer.
- Click the blinking message below (or press Enter) to initiate the registration.
- When the device starts blinking, press the button to proceed the registration.

Friendly Name:

Device Type: ☐ U2F ☒ FIDO2

Registered UserID:

Registered Domain:


[Press your FIDO Device]

Verify your identity with rcdevs.com

Pick an option

USB security key

This device

Cancel

HELPDESK

DASHBOARD

OTP

Home / U2F

MANAGE FIDO DEVICES SETTINGS

You must first register your FIDO Device or Token to start using it.
If any of the checks below fails then the registration cannot be done.

Your Web browser supports FIDO: Yes
URL is enabled for FIDO: Yes

Instructions to register your FIDO Device:


- Plug the FIDO Device in a USB port on the computer.
- Click the blinking message below (or press Enter) to initiate the registration.
- When the device starts blinking, press the button to proceed the registration.

Friendly Name:

Device Type: ☐ U2F ☒ FIDO2

Registered UserID:

Registered Domain:


[Press your FIDO Device]

PIN required

Enter the PIN for your security key

PIN

Cancel

Next

HELPDESK

DASHBOARD

OTP

Home / U2F

MANAGE FIDO DEVICES SETTINGS

You must first register your FIDO Device or Token to start using it.
If any of the checks below fails then the registration cannot be done.

Your Web browser supports FIDO: **Yes**
URL is enabled for FIDO: **Yes**

Instructions to register your FIDO Device:

- Plug the FIDO Device in a USB port on the computer.
- Click the blinking message below (or press Enter) to initiate the registration.
- When the device starts blinking, press the button to proceed the registration.

Friendly Name:

fido 2 token

Device Type:


☐ U2F ☒ FIDO2

Registered UserID:

testuser1

Registered Domain:

Default


[Press your FIDO Device]

Use your security key with rcodevs.com

Touch your security key again to complete the request.

Cancel

HELPDESK

DASHBOARD

OTP

Home / U2F

MANAGE FIDO DEVICES SETTINGS

You must first register your FIDO Device or Token to start using it.
If any of the checks below fails then the registration cannot be done.

Your Web browser supports FIDO: **Yes**
URL is enabled for FIDO: **Yes**

Instructions to register your FIDO Device:

- Plug the FIDO Device in a USB port on the computer.
- Click the blinking message below (or press Enter) to initiate the registration.
- When the device starts blinking, press the button to proceed the registration.

Friendly Name:

fido 2 token

Device Type:


☐ U2F ☒ FIDO2

Registered UserID:

testuser1

Registered Domain:

Default



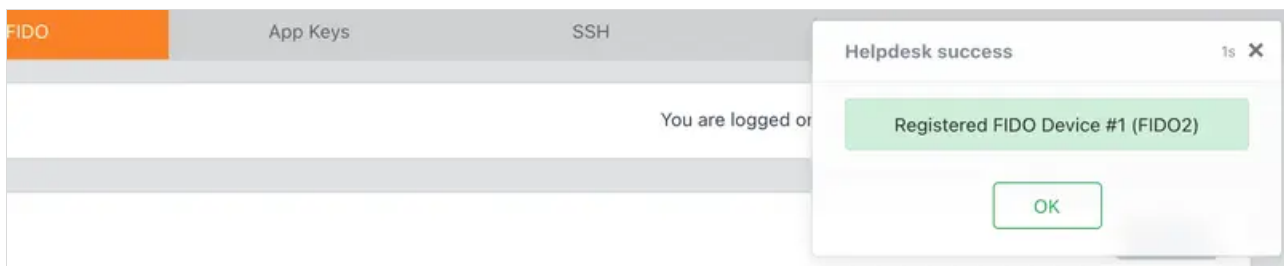
Allow this site to see your security key?

rcodevs.com wants to see the make and model of your security key

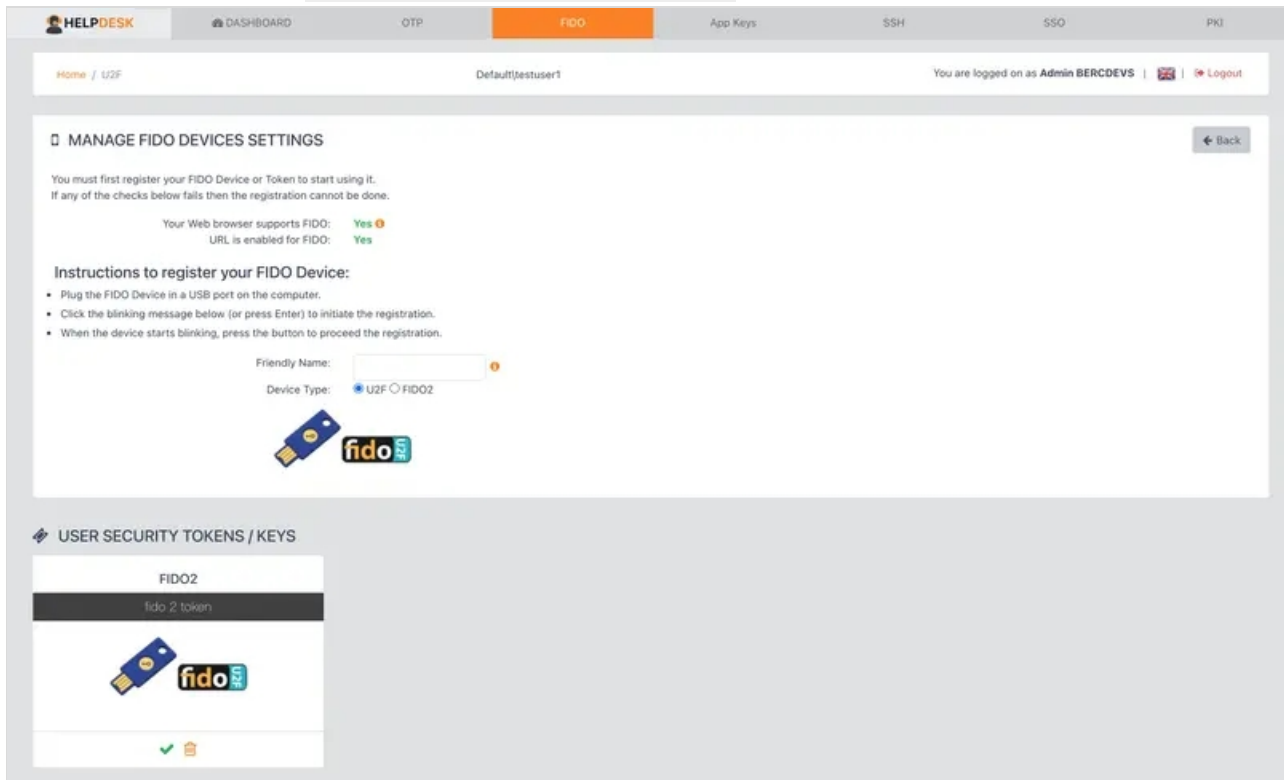
Skip

Allow

The **FIDO** Device has been successfully registered.

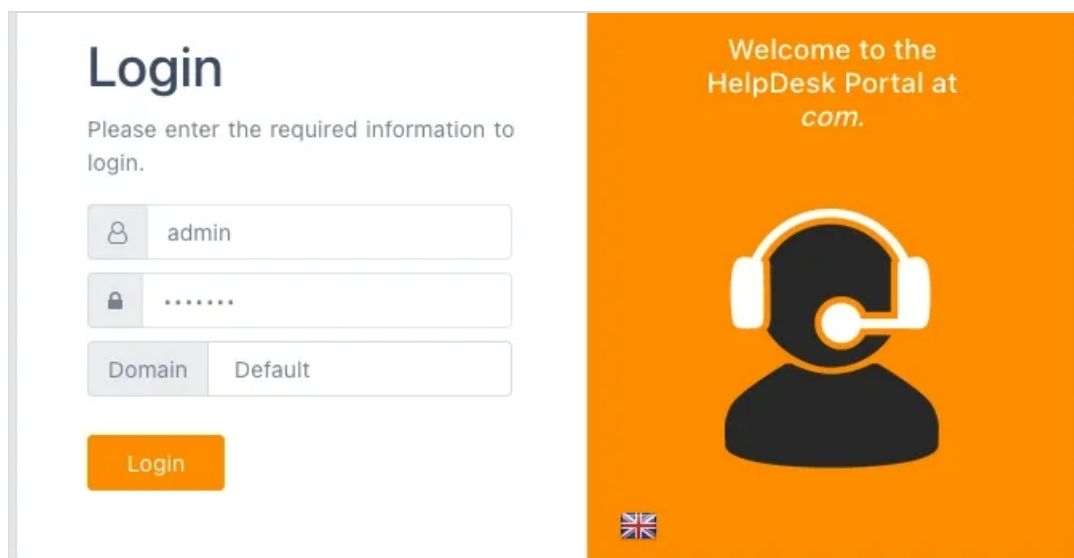


At the bottom of the page under **User Security Tokens / Keys** you will see the enrolled **FIDO** key.



5. Build OTP List

Log in to the HelpDesk application.



Select the user you want to build an **OTP List**.

The screenshot shows the Helpdesk Dashboard. At the top, there's a header with the Helpdesk logo and a navigation bar. The main content area is divided into two columns. The left column contains a 'USER SEARCH' section with a search bar and a list of users. The right column contains a welcome message for the user 'admin' and a profile picture placeholder.

HELPDESK

Home / Dashboard

You are logged on as **admin** | | Logout

USER SEARCH

Select the user you want to manage.

Login Name: CentOS8_57eypo4p
DN: cn=CentOS8_57eypo4p,o=R...
Full Name: CentOS8_57eypo4p
Domains: Default

Select CentOS8_57eypo4p

Hello **admin**.
Welcome to the Helpdesk Portal at com.

Go to the **OTP** tab. At the bottom of the page, click **Build OTP List**.

The screenshot shows the Helpdesk Dashboard with the 'OTP' tab selected. The main content area is titled 'MANAGE OTP AUTHENTICATION SETTINGS'. It contains several configuration options for OTP authentication, including Primary OTP Method, Fallback OTP Method, OTP Challenge Timeout, and Enable Push Login. There are also buttons for 'Test user authentication' and 'Submit SelfReg link'. At the bottom, there's a section for 'USER SECURITY TOKENS / KEYS' with a large plus icon and the text 'Add a Token'.

HELPDESK DASHBOARD **OTP** FIDO SSH PKI

Home / Openotp Default\CentOS8_57eypo4p You are logged on as **admin** | | Logout

+ MANAGE OTP AUTHENTICATION SETTINGS

Manage users hardware and software Tokens: register, deactivate, remove, test or resynchronize user devices.
Configure OTP authentication settings: primary OTP method, fallback OTP method, challenge session timeout or enable push login notification.

Primary OTP Method: Token

Fallback OTP Method: Mail

OTP Challenge Timeout: 1 minute 30 seconds

Enable Push Login: ☒ Yes ☐ No

Emergency OTP:

Test user authentication Token

Submit SelfReg link Mail Primary Token

USER SECURITY TOKENS / KEYS

Add a Token

SMS OTP

OK

MAIL OTP

OK

OTP LIST

NOT OK

SMS OTP:

Delivery Mode:

☒ On demand
☐ Prefetch
☐ Mobile ID

Message Type:

☒ Normal
☐ Flash

Mail OTP:

loic@rcdevs.com

Delivery Mode:

☒ On demand
☐ Prefetch

Secure Mail:

☐ Yes
☒ No

List Size:

50 OTPs

Algorithm:

SHA1

Build OTP List

The OTP List has been generated. Click on [View or Download](#) to get the list.

SMS OTP

OK

MAIL OTP

OK

OTP LIST

OK

View or Download

Unregister

List Size:

50 OTPs (0 used)

List Type:

SHA1 (160 bits)

HELPDESK

DASHBOARD

OTP

FIDO

App Keys

SSH

SSO

PKI

Home / Openotp / Otp / List

Default\CentOS8_57eypo4p

You are logged on as admin | | Logout

Manage OTP List

OpenOTP Password List (50 OTPs)

Back


ID	OTP	ID	OTP	ID	OTP	ID	OTP	ID	OTP
1	236821	2	414967	3	955860	4	586808	5	544196
6	782852	7	400464	8	888487	9	015929	10	112665
11	936877	12	580456	13	715994	14	365707	15	717964
16	022043	17	759688	18	485442	19	254163	20	249730
21	011363	22	362485	23	108452	24	377531	25	005256
26	797377	27	183087	28	771661	29	746733	30	993481
31	496374	32	811962	33	535279	34	582729	35	495234
36	695904	37	790428	38	657667	39	003841	40	413175
41	527056	42	124394	43	552280	44	301142	45	773421
46	508128	47	900316	48	548562	49	806848	50	099520

6. App Keys Registration


Log in to the HelpDesk application.

Login

Please enter the required information to login.



admin





.....

Domain


Default

Login



Welcome to the HelpDesk Portal at *com*.



Select the user you want to manage the **Application Passwords**.

 **HELPDESK**

Home / Dashboard

You are logged on as **admin** |  |  Logout

USER SEARCH


Select the user you want to manage.

Login Name: CentOS8_57eypo4p
DN: cn=CentOS8_57eypo4p,o=R...
Full Name: CentOS8_57eypo4p
Domains: Default

Select

CentOS8_57eypo4p

Hello **admin**.
Welcome to the Helpdesk Portal at *com*.



Go to the **App Keys** tab.

HELPDESK

DASHBOARDOTPFIIDApp KeysSSHSSOPKI

Home / AppkeysDefault\CentOS8_57eypo4pYou are logged on as admin | | Logout

MANAGE APPLICATION PASSWORDS

Back

Application passwords can be used as a replacement to your OTP. They are useful for application like mail clients not supporting OTP.

Application	Password	Valid Until
OWA	[Not Set]	

Password Length:

10

Expires After:

1 day

Build

Remove

Create a new **Application Password**, click on **Build**.

HELPDESK

DASHBOARDOTPFIIDApp KeysSSHSSOPKI

Home / AppkeysYou are logged on as admin | | Logout

MANAGE APPLICATION

Back

Application passwords can be used as a replacement to your OTP. They are useful for application like mail clients not supporting OTP.

Application	Password	Valid Until
OWA	[Not Set]	

Password Length:

10

Expires After:

1 day

Build

Remove


Rebuild application keys

×


Do you want to create application keys

Cancel

Confirm

 **HELPDESK**

DASHBOARDOTPApp KeysSSHSOPI

Home / AppkeysDefaultCentOS8_57eypo4pYou are logged on as **admin** |  | [Logout](#)

MANAGE APPLICATION PASSWORDS

← Back

Application passwords can be used as a replacement to your OTP. They are useful for application like mail clients not supporting OTP.

Application	Password	Valid Until
OWA	wKVNjLs5NG	2021-05-28 16:03:04

Password Length:

10

Expires After:

1 day

Build


Remove

7. SSH Key Registration


Log in to the HelpDesk application.

Login

Please enter the required information to login.



admin





Domain

Default

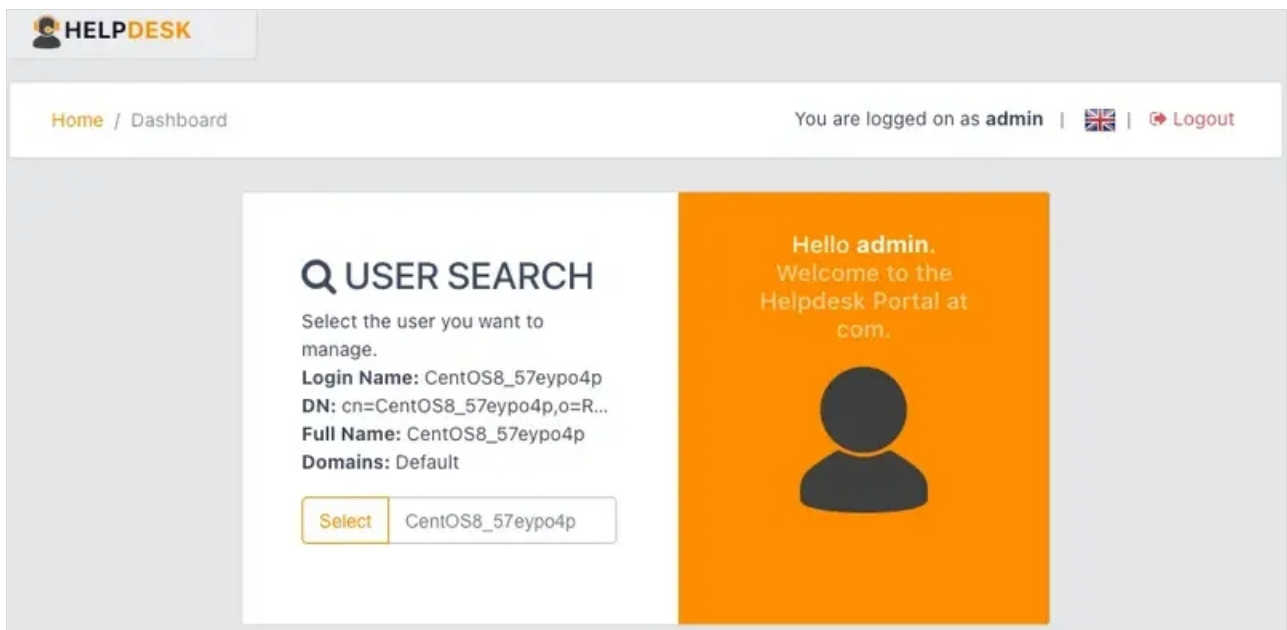
Login

Welcome to the
HelpDesk Portal at
com.

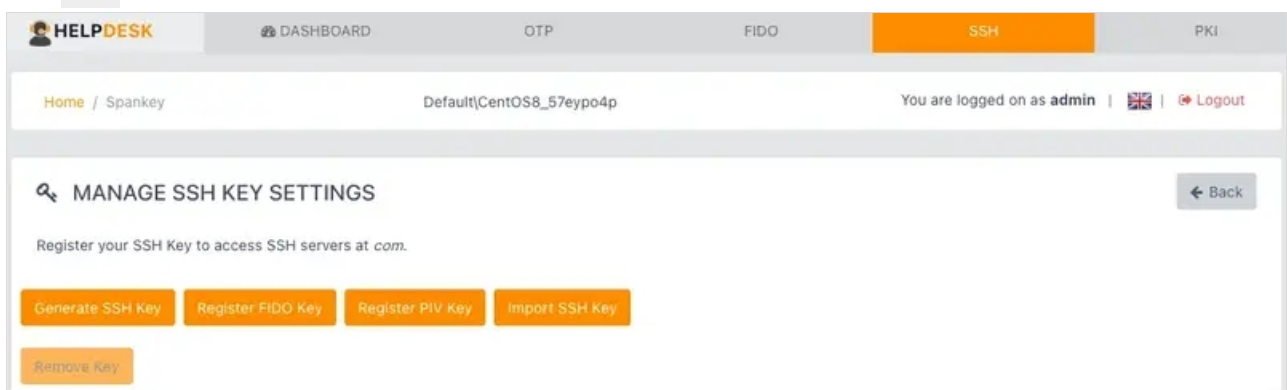




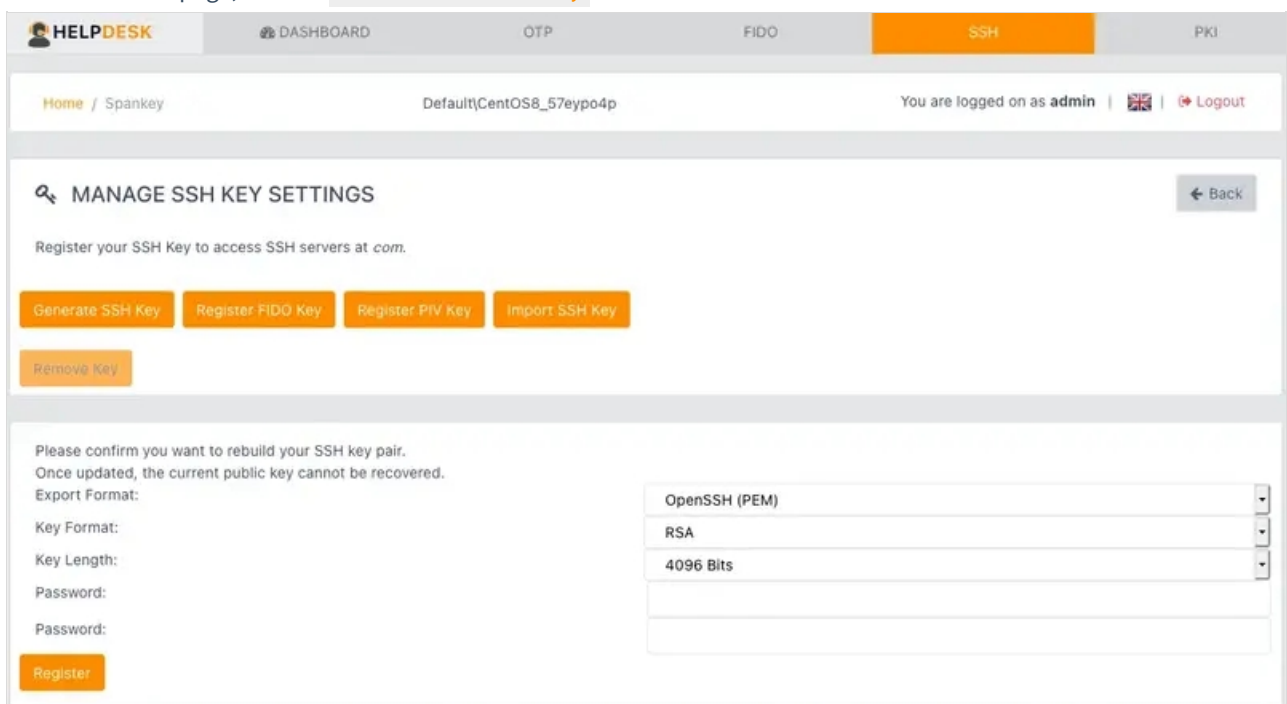
Select the user you want to register an **SSH Key**.



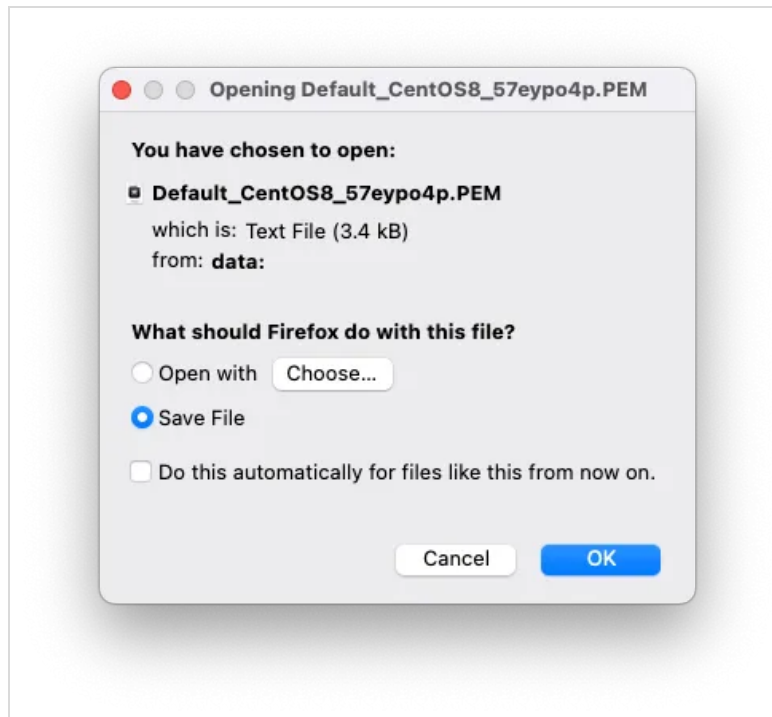
Go to the **SSH** tab.



At the bottom of the page, click on **Generate SSH Key**.



Set the Key Format, Length and Password to protect your **Private Key**. Finally, click on **Register** and save your **Private Key**.



Now the **Public Key** is registered for that user.

HELPDESK

DASHBOARD

OTP

FIDO

SSH

PKI

Home / Spankey

Default(CentOS8_57eypo4p)

You are logged on as admin | | Logout

MANAGE SSH KEY SETTINGS

Back

The key does not have an expiration date and will not auto-expire!
The key does not have a maximum usage count!

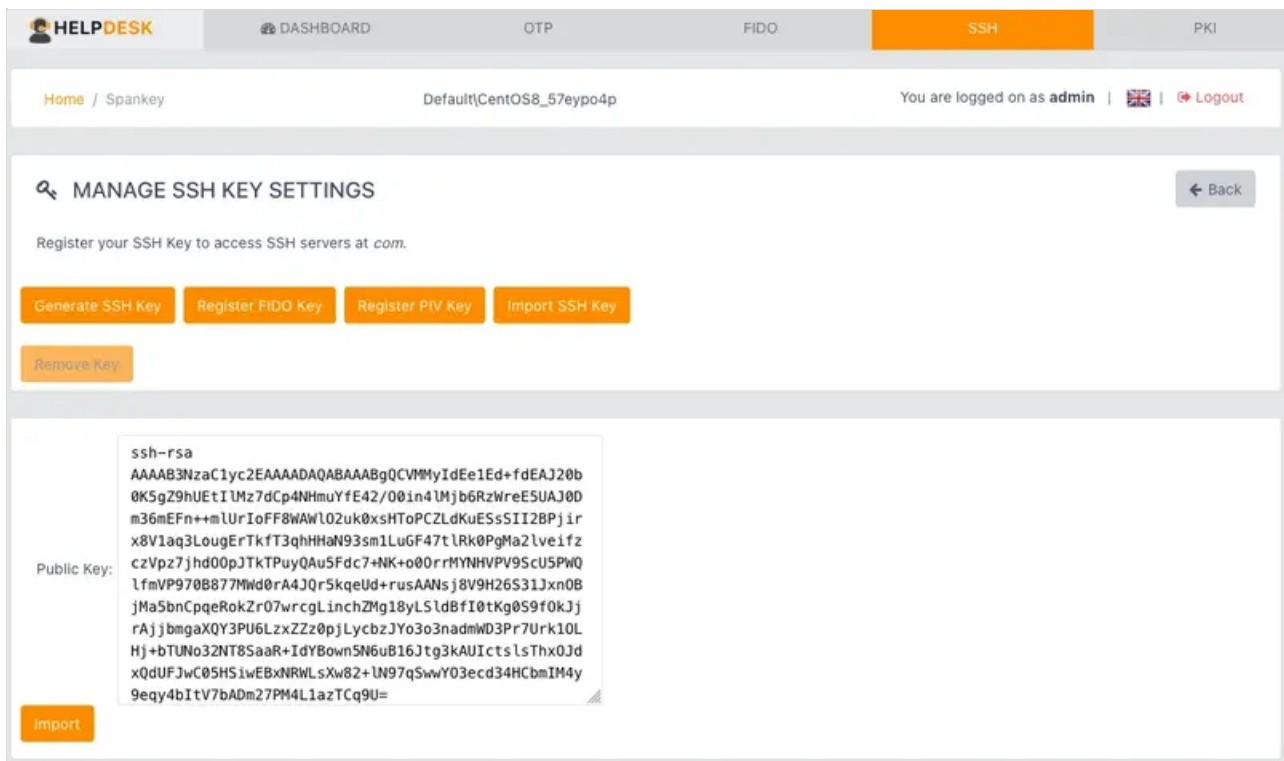
SSH Public Key:
(RSA 4096 Bits)
Copy

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCAwEgJmI+T1VZ1Ab8Dzr91CvQ0V6R5t2AejfG
FXVhwPF43MyglCYb3ip0jyMUP3qteIJ5bniEC3Q8Ja4qYI02bXv9M/AgVJFjqSU6u3nfZ6oQAAS
tJK0yW10VFaoJlJ6lTG
/GJw9WtBrh7dzJqKgQ1zQe9hmm66EjU+KC00SwYQueqpD9s86hI8a0E5kn6r/Xh9+X
/JxxFET0H0+APiJZGYwfc61RwUd8K6Hm1qLKDrMxhQzn1kwLQ+9yvvQNLopGltzLSG8p+2hxLnM
HZU5xh9kUYI9Yzsr+qWm6y10ymJcHScKENygd5jUhx2kVd9jgm4bkQWC9BHXSdo8XUnDUNICxb5
nvUtq24PGcxUa8wXmW41ro5FFJFRYzRKyo5twkksvM57R/qjWq1FIrdB0B
/Z2k0ZVeKlVI9rKLo0/BEbnOUdZ+t
/9G1c1sL6HJTU+xlW8YyAdm4maHQG+cpJrV61rREUNpT6EL24AXsRkUN
/G00hGnF8iYGrGrWB8MKm1aw0zG0p60/8fTtru1Q00Gt1jnFtm6794kXx/h4Mox6xwC8DvJy8D
/eKVMW55jHB9LPmzoMjz5muLQD/s0hndWqawydVQGRfdcaqPd5aHsHkvX4jCY
/2LejN37A1FrGv249tZd0ZNIbrHfgXB8Ma7+d1q0P9e0Rw== DefaultCentOS8_57eypo4p

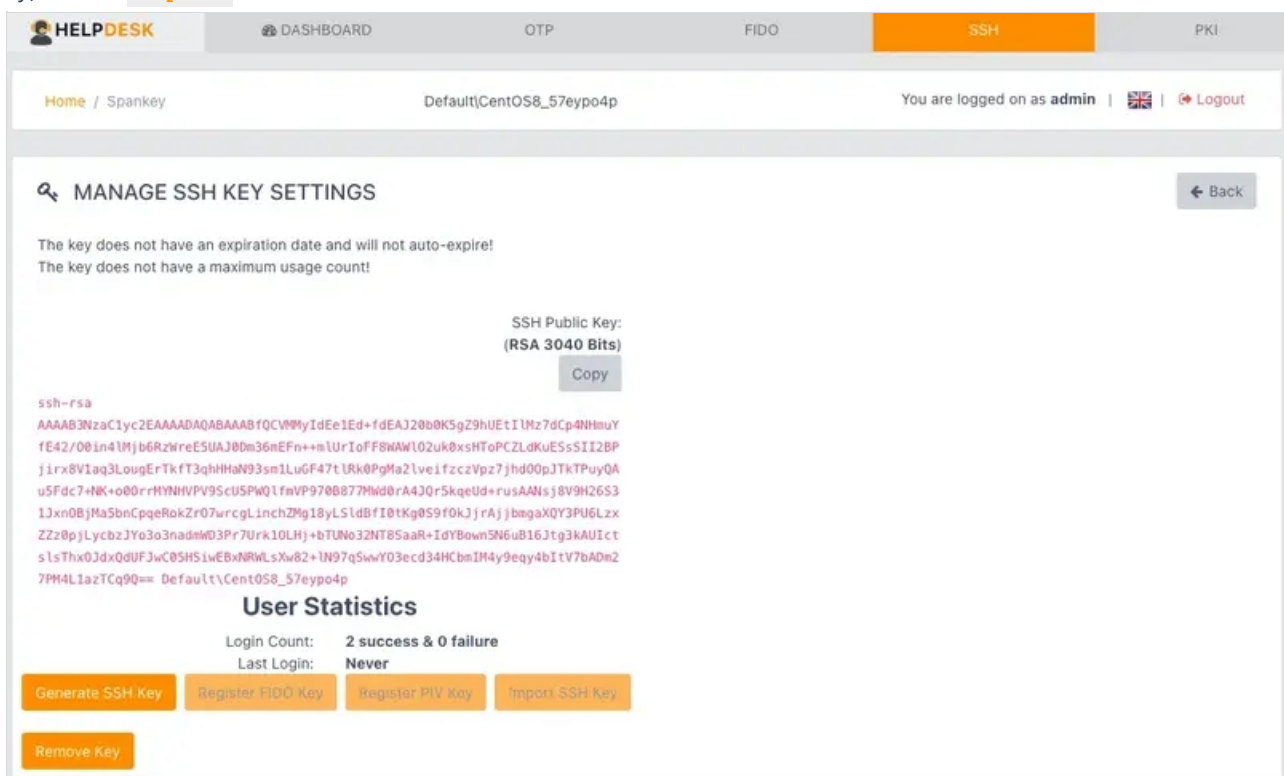
User Statistics
Login Count: 2 success & 0 failure
Last Login: Never

Generate SSH KeyRegister FIDO KeyRegister PIV KeyImport SSH KeyRemove Key

To import an SSH Key, click on **Import SSH Key**. Copy and paste your **Public Key** into the Field.



Finally, click on **Import**.



8. SSO Customizations

Log in to the HelpDesk application.



Login

Please enter the required information to login.

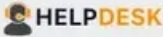
Domain

Login


Welcome to the HelpDesk Portal at *com*.



Select the user you want to manage the **SSO** Portal.



Home / Dashboard

You are logged on as **admin** |  | [Logout](#)


USER SEARCH

Select the user you want to manage.


Login Name: CentOS8_57eypo4p
DN: cn=CentOS8_57eypo4p,o=R...
Full Name: CentOS8_57eypo4p
Domains: Default

[Select](#) CentOS8_57eypo4p

Hello **admin**.
Welcome to the Helpdesk Portal at *com*.




Go to the **SSO** tab.

 DASHBOARD OTP FIDO SSH **SSO** PKI

Home / Spankey

DefaultCentOS8_57eypo4p

You are logged on as **admin** |  | [Logout](#)

MANAGE SSO PORTAL

[← Back](#)

Single Sign-On Settings

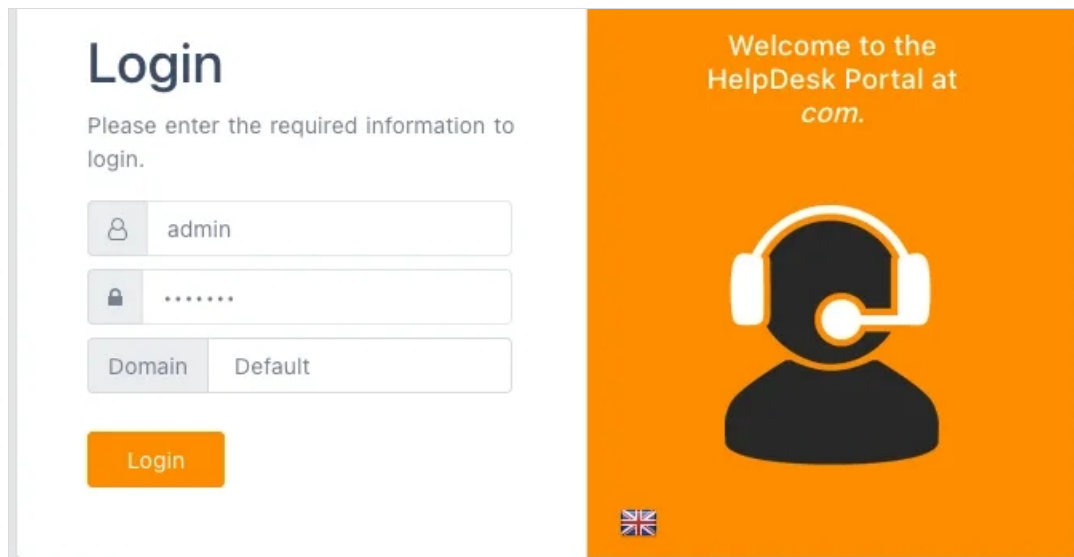
Enable SAML Usage: ☒ Yes ☐ No [×](#)

Enable OpenID Usage: ☒ Yes ☐ No [×](#)

SSO Session Time: [×](#)

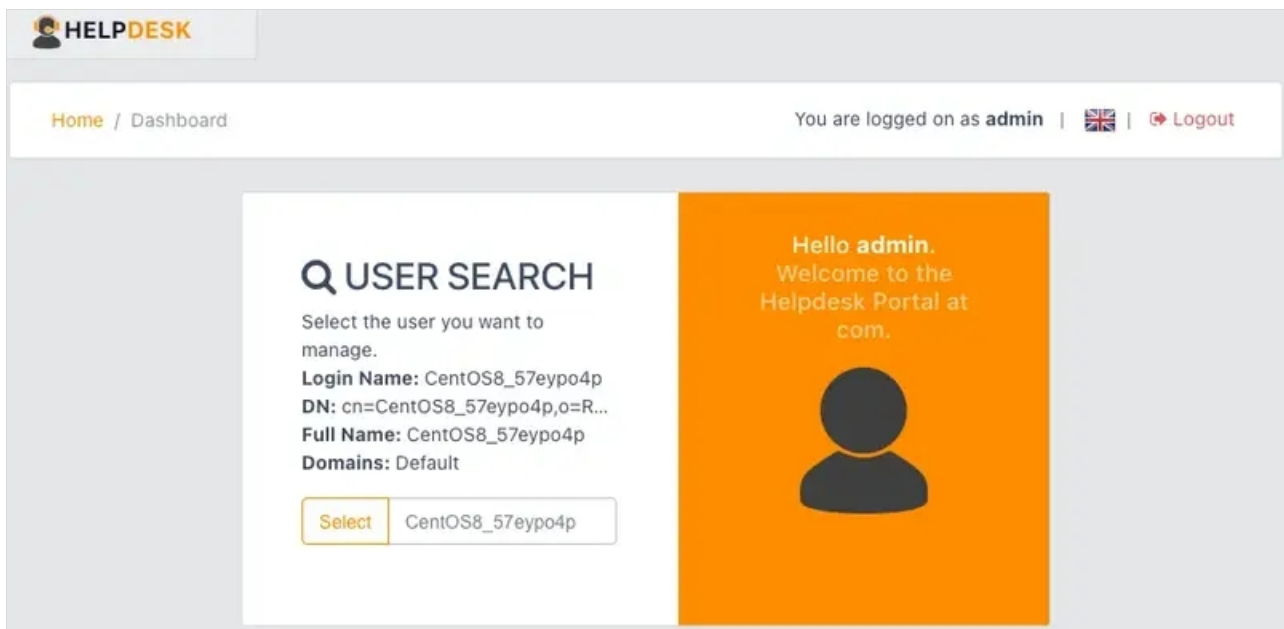
9. User certificate enrollment

Log in to the HelpDesk application.



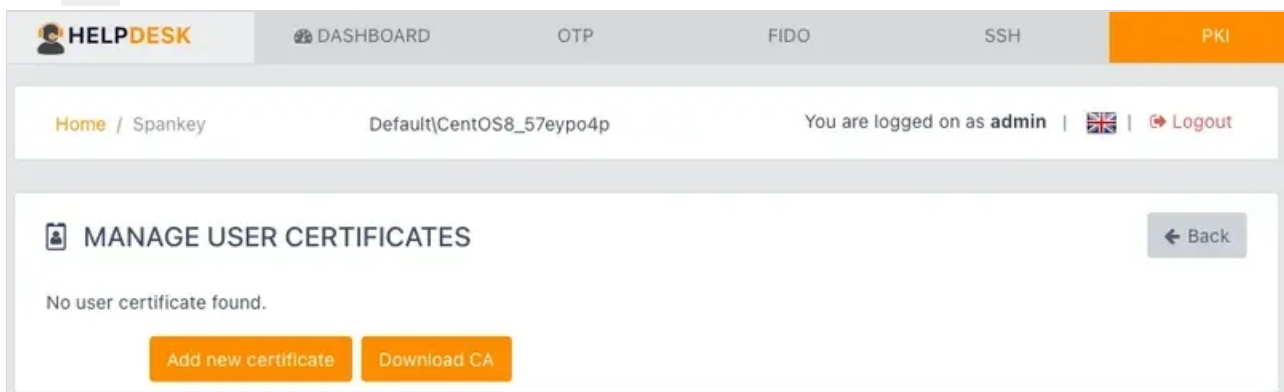
The login page features a white sidebar on the left with the title "Login" and a prompt: "Please enter the required information to login." Below this are three input fields: a username field containing "admin", a password field with masked characters "*****", and a domain dropdown menu set to "Default". An orange "Login" button is positioned below the domain field. The main content area has an orange background with the text "Welcome to the HelpDesk Portal at *com*." and a large icon of a person wearing a headset. A small UK flag icon is located at the bottom left of the orange area.

Select the user you want to add a new **Certificate**.



The dashboard shows the user is logged in as "admin". The main section is titled "USER SEARCH" and includes the instruction "Select the user you want to manage." It displays user details for "CentOS8_57eypo4p":
Login Name: CentOS8_57eypo4p
DN: cn=CentOS8_57eypo4p,o=R...
Full Name: CentOS8_57eypo4p
Domains: Default
A "Select" button is next to the user name in a search bar.

Go to the **PKI** tab.



The PKI tab is active, showing the "MANAGE USER CERTIFICATES" section. It states "No user certificate found." and provides two orange buttons: "Add new certificate" and "Download CA". A "Back" button is in the top right corner. The breadcrumb trail shows "Home / Spankey" and the user is logged in as "admin".

At the bottom of the page, click on **Add new certificate** and save your **Certificate**.

HELPDESK

DASHBOARD

OTP

FIDO

SSH

PKI

Home / Spankey

Default\CentOS8_57eypo4p

You are logged on as admin | | [Logout](#)

MANAGE USER CERTIFICATES

Click the actions in the table below to download, renew or delete your certificates.

Serial	Name	Valid From	Valid To	Status	Actions
27	Default\CentOS8_57eypo4p	26/05/2021	26/05/2022	valid	

Password: 4YrdkpmJ

Add new certificate

Download CA

Opening Default_CentOS8_57eypo4p.p12

You have chosen to open:

Default_CentOS8_57eypo4p.p12

which is: Text File (2.4 kB)

from: data:

What should Firefox do with this file?

Open with

Choose...

☒ Save File

☐ Do this automatically for files like this from now on.

Cancel

OK

The user certificate can be used to log in on WebADM web applications requiring PKI login.

You can click on [Download CA](#) to download the CA certificate of WebADM if you need it for specific purposes.

HELPDESK

DASHBOARD

OTP

FIDO

SSH

PKI

Home / Spankey

Default\CentOS8_57eypo4p

You are logged on as admin | | [Logout](#)

MANAGE USER CERTIFICATES

Click the actions in the table below to download, renew or delete your certificates.

Serial	Name	Valid From	Valid To	Status	Actions
27	Default\CentOS8_57eypo4p	26/05/2021	26/05/2022	valid	

Add new certificate

Download CA

Opening ca.crt

You have chosen to open:

ca.crt

which is: CRT file (889 bytes)

from: https://192.168.4.200

What should Firefox do with this file?

Open with

Keychain Access (default)

☒ Save File

☐ Do this automatically for files like this from now on.

Cancel

OK

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