



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:

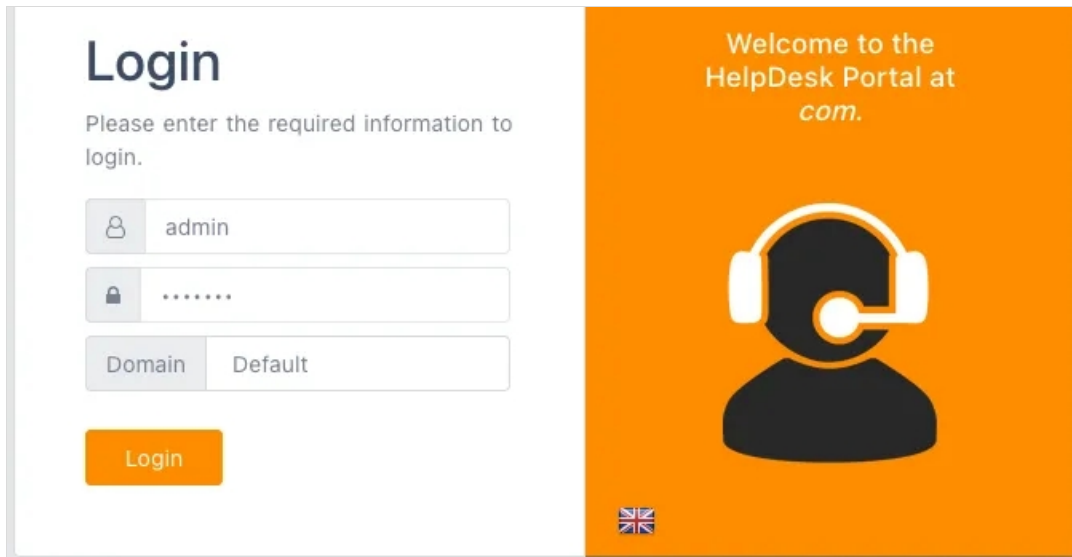
```
https://YOUR_WEBADM/webapps/helpdesk/login_uid.php
```

and through the WAProxy it is:

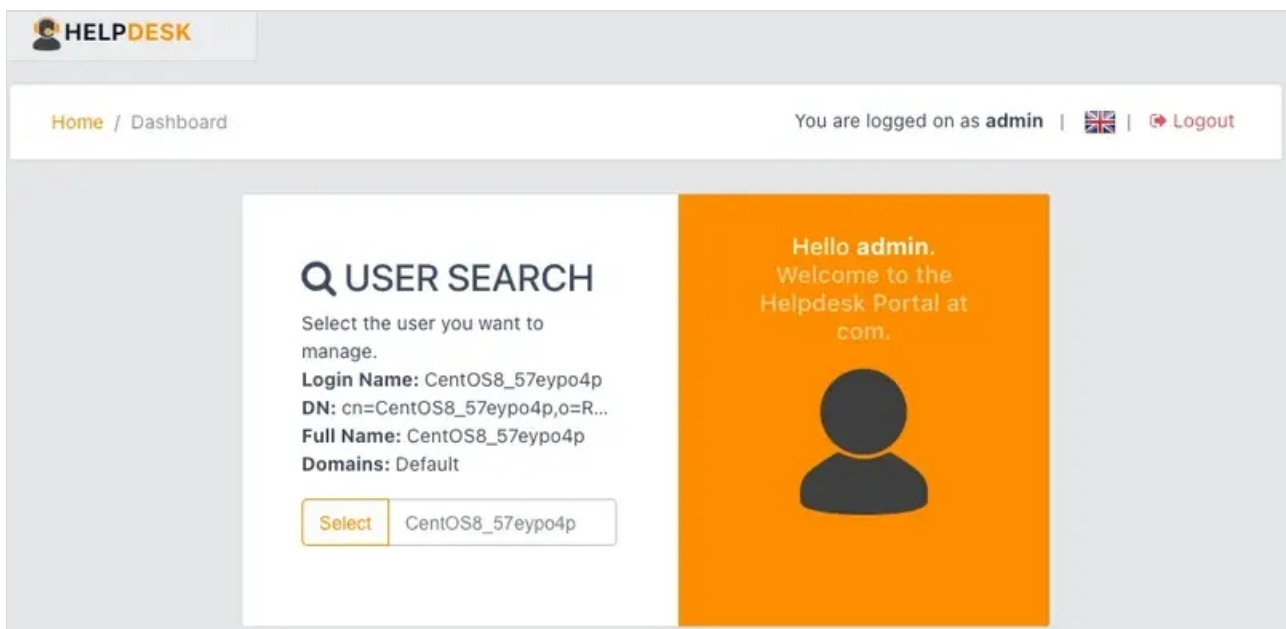
```
https://YOUR_WAPROXY/helpdesk/login_uid.php
```

2. Dashboard

Log in to the HelpDesk application.



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



HELPSDESK DASHBOARD OTP FIDO SSH SSO PKI

Home / Dashboard Default(CentOS8_57eypo4p) You are logged on as admin | | Logout

User Search

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:

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

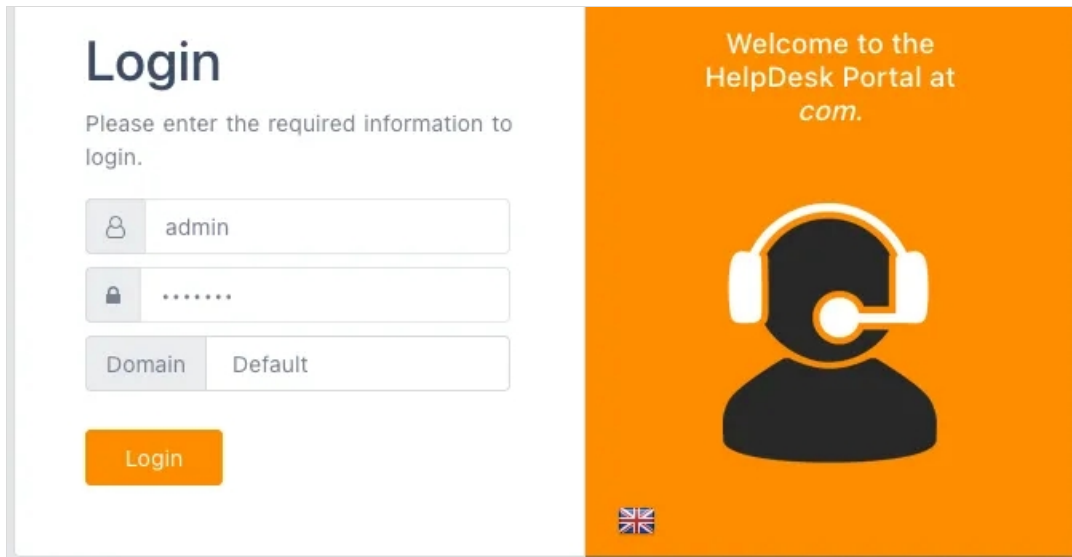
Display records Search:

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

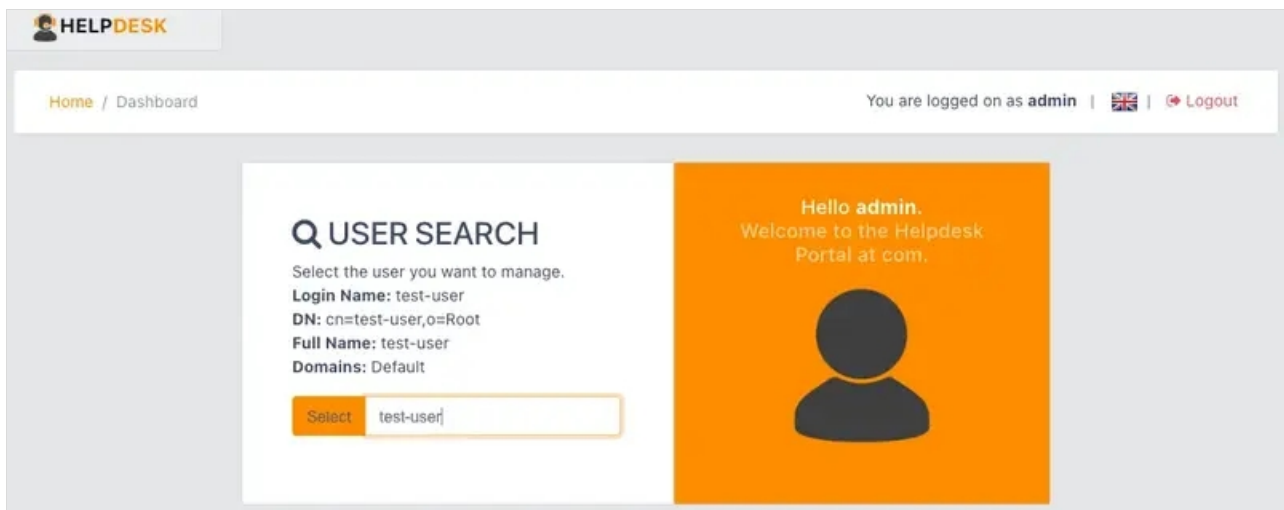
Showing 1 to 4 of 4 entries

3. User Activation

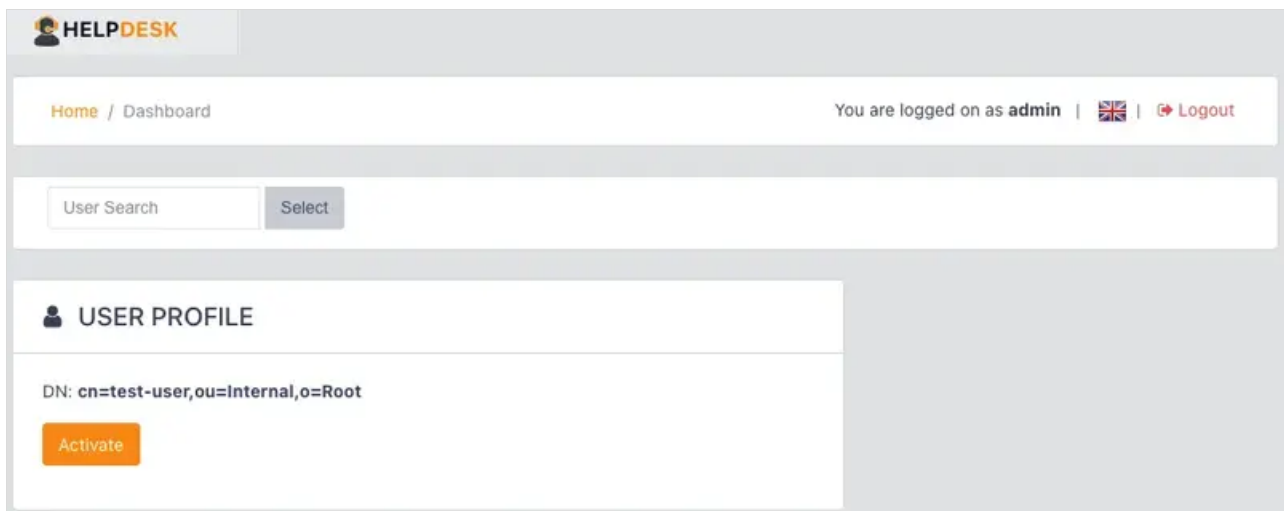
Log in to the HelpDesk application.



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



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



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

HELPSDESK DASHBOARD OTP FIDO App Keys SSH SSO PKI

Home / Dashboard Default\test-user You are logged on as admin | | Logout

User Search Select

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

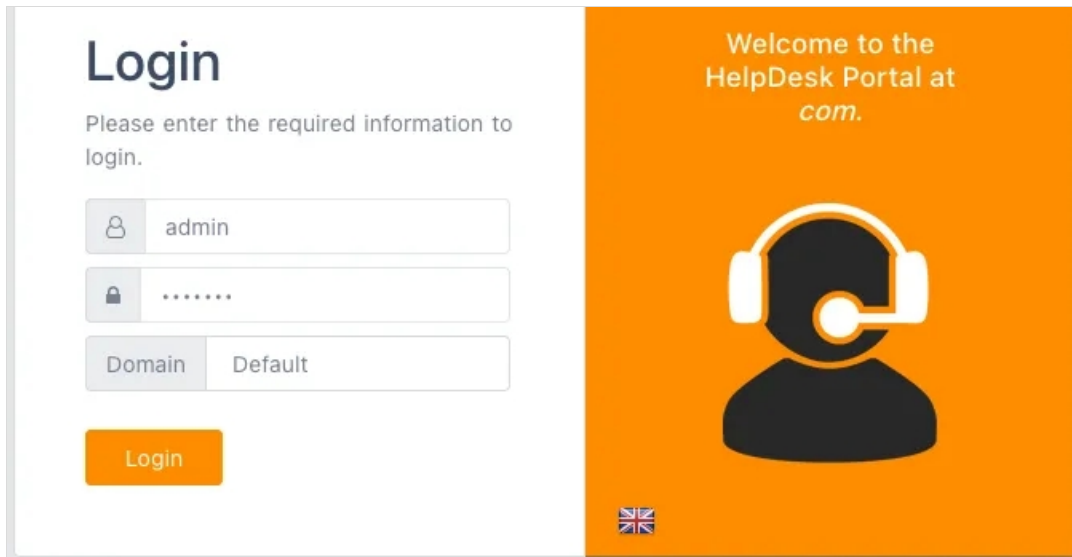
USER SECURITY TOKENS / KEYS

4. Token Enrollment

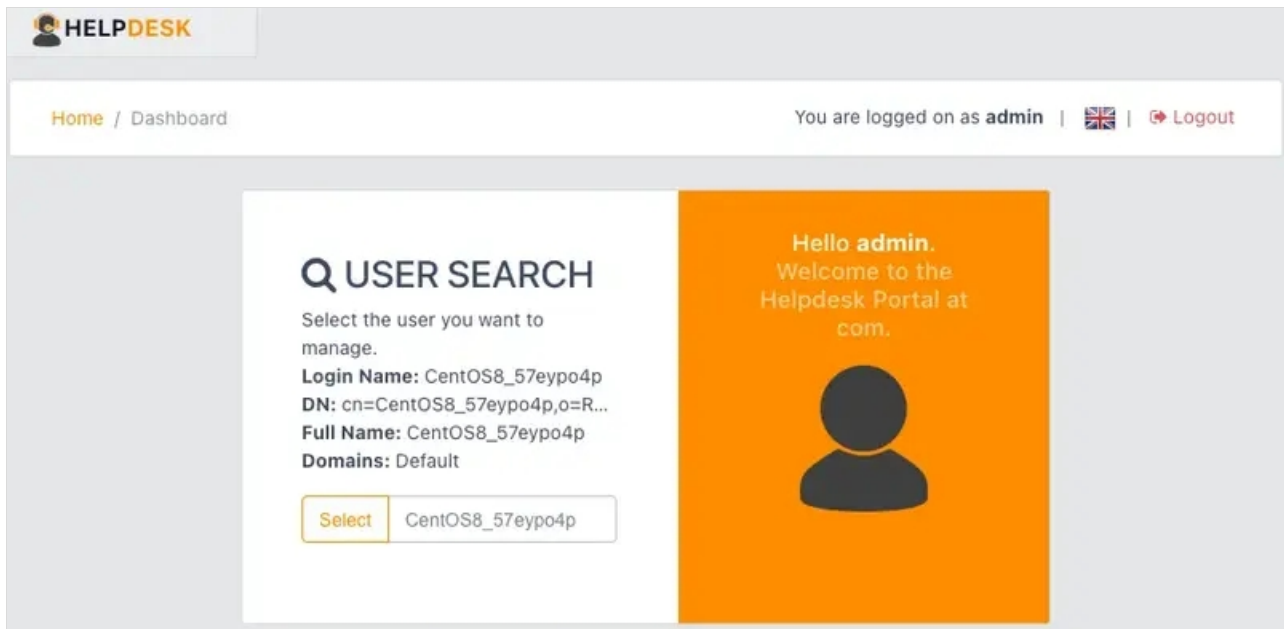
4.1 Software Token Registration

4.1.1 Registration from Helpdesk page

Log in to the HelpDesk application.



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



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**.

HELPSDESK | 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:

Fallback OTP Method:

OTP Challenge Timeout:


Enable Push Login: Yes No

Emergency OTP:

[Test user authentication](#)

[Submit SelfReg link](#)

🔑 USER SECURITY TOKENS / KEYS



Add a Token





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

HELPSDESK | 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.

<p>Hardware Token</p> <p>Token Inventoried</p>  <p>Add Token</p>	<p>Software Token</p> <p>QRCode-based Authenticator</p>  <p>Add Token</p>	<p>Yubikey</p> <p>Inventoried & YubiCloud</p>  <p>Add Token</p>	<p>Another Token</p> <p>Manual Registration</p>  <p>Add Token</p>
--	---	---	---

Then scan the QR CODE to register your **Software Token**.

+ 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.

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 QR CODE

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 [← 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: 

Fallback OTP Method: 


OTP Challenge Timeout: 

Enable Push Login: Yes No 


[Test user authentication](#) 


[Submit SelfReg link](#)  



USER SECURITY TOKENS / KEYS

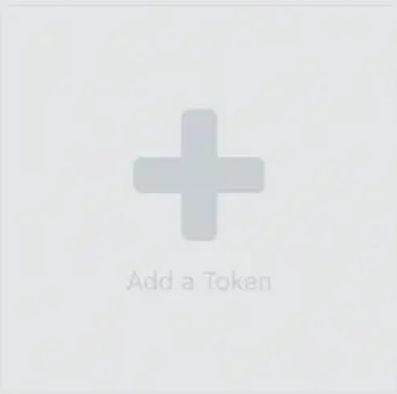
TOTP 

iPhone11,8



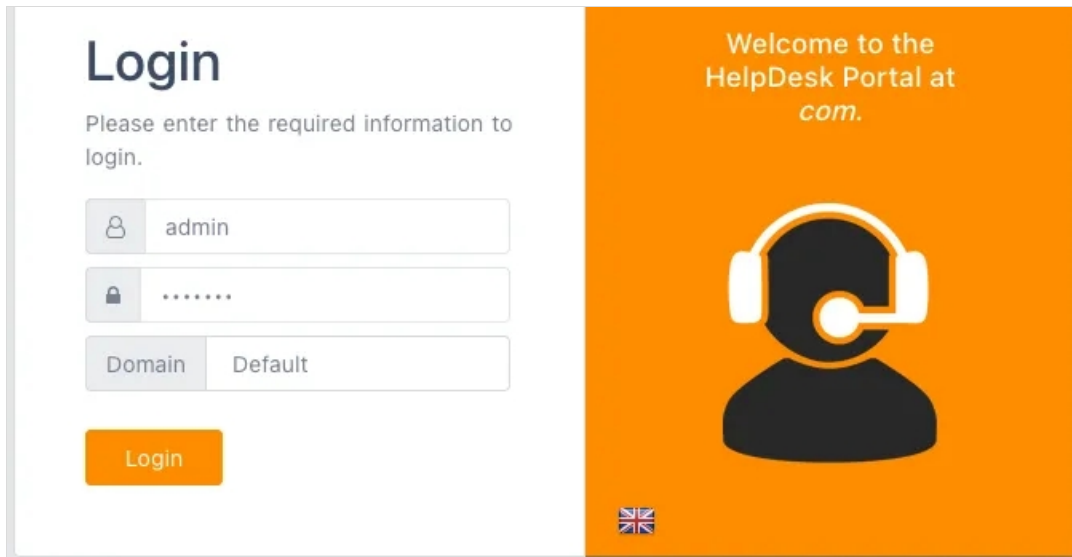
Type: OATH Time-based (160 bits) 

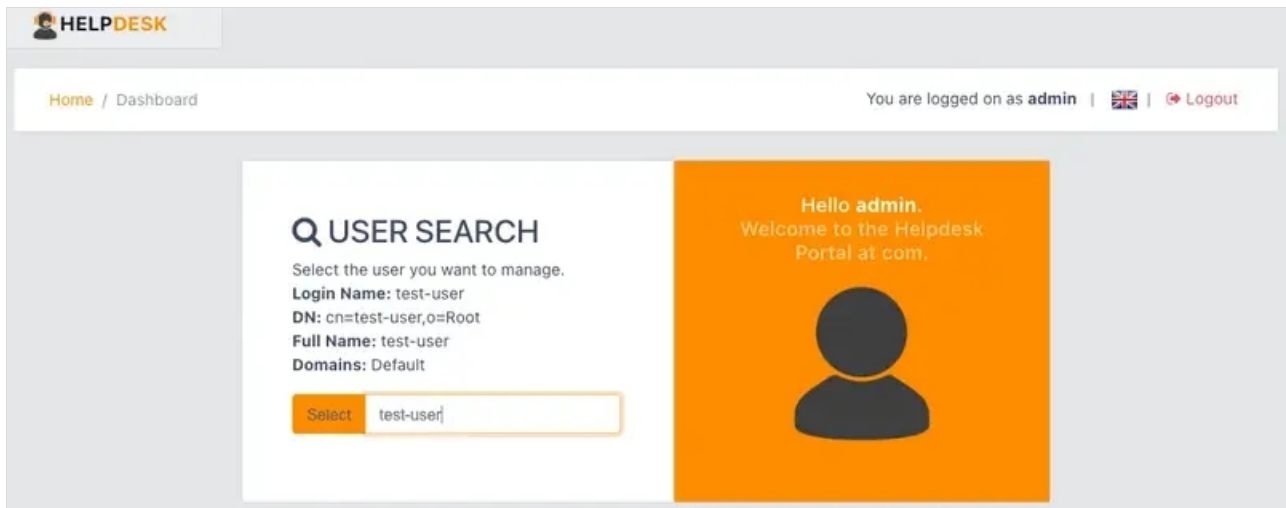


4.1.2 Submit a SelfReg link to the end user

Log in to the HelpDesk application.



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



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

HELPSDESK DASHBOARD OTP FIDO App Keys SSH SSO PKI

Home / Dashboard Default\test-user You are logged on as admin | | Logout

User Search

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:

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.

HELPSDESK DASHBOARD OTP FIDO App Keys

Home / Openotp Default\test-user You are here

Helpdesk success 1s X

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.

N noreply@rcdevs.com
OpenOTP/SpanKey Self-Registration
To: loic@rcdevs.com

Hello test-user,

This self-registration request will expire 2021-06-01 16:58:34.
Please click on the link below to start self-registration.

<https://192.168.4.200/webapps/selfreg/?id=2d2936c010750000c6c7561c4014e95c>.

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) ⓘ

Register As:


QRCode: [\(Enlarge\)](#)

Enter OTP: ⓘ


 Provided by [RCDevs Security SA](#)






User Self-Registration

Your Primary Token has been registered

 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

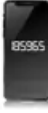
0

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.


Domain

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

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



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

HELPSDESK 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:

Fallback OTP Method:

OTP Challenge Timeout:


Enable Push Login: Yes No

Emergency OTP:

[Test user authentication](#)

[Submit SelfReg link](#)

🔑 USER SECURITY TOKENS / KEYS



Add a Token

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

HELPSDESK 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](#)

+ 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.

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

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

 **DOWNLOAD QR CODE**

Expiration Time 

PIN Code 

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

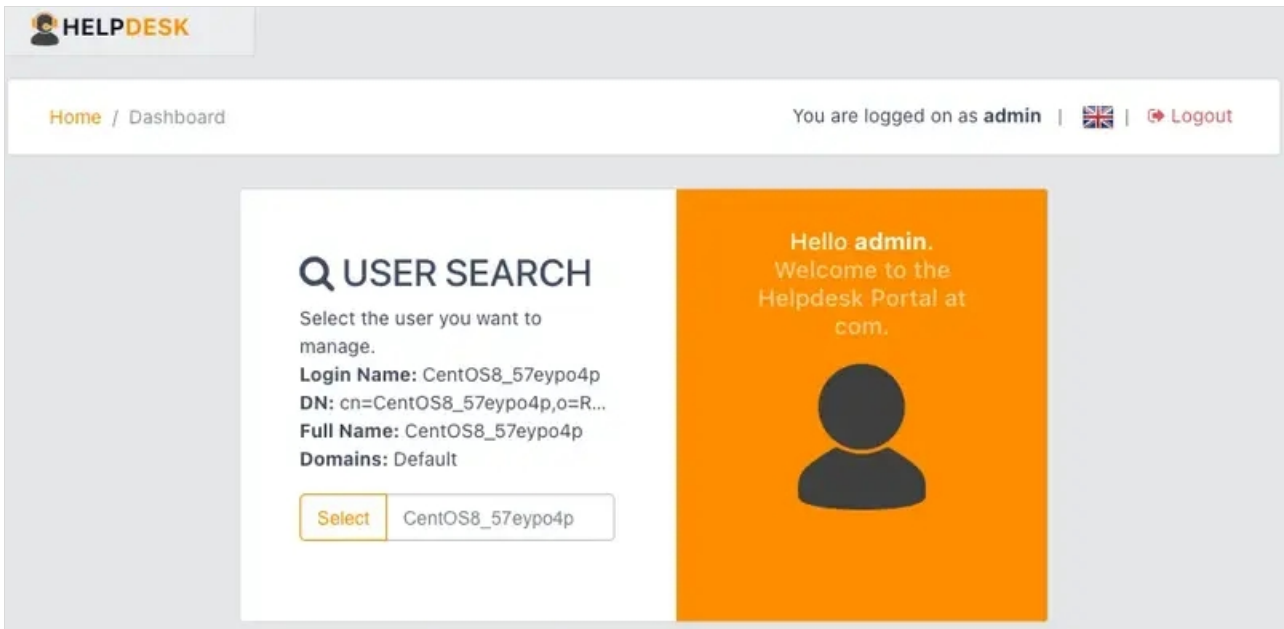
Please enter the required information to login.

Domain

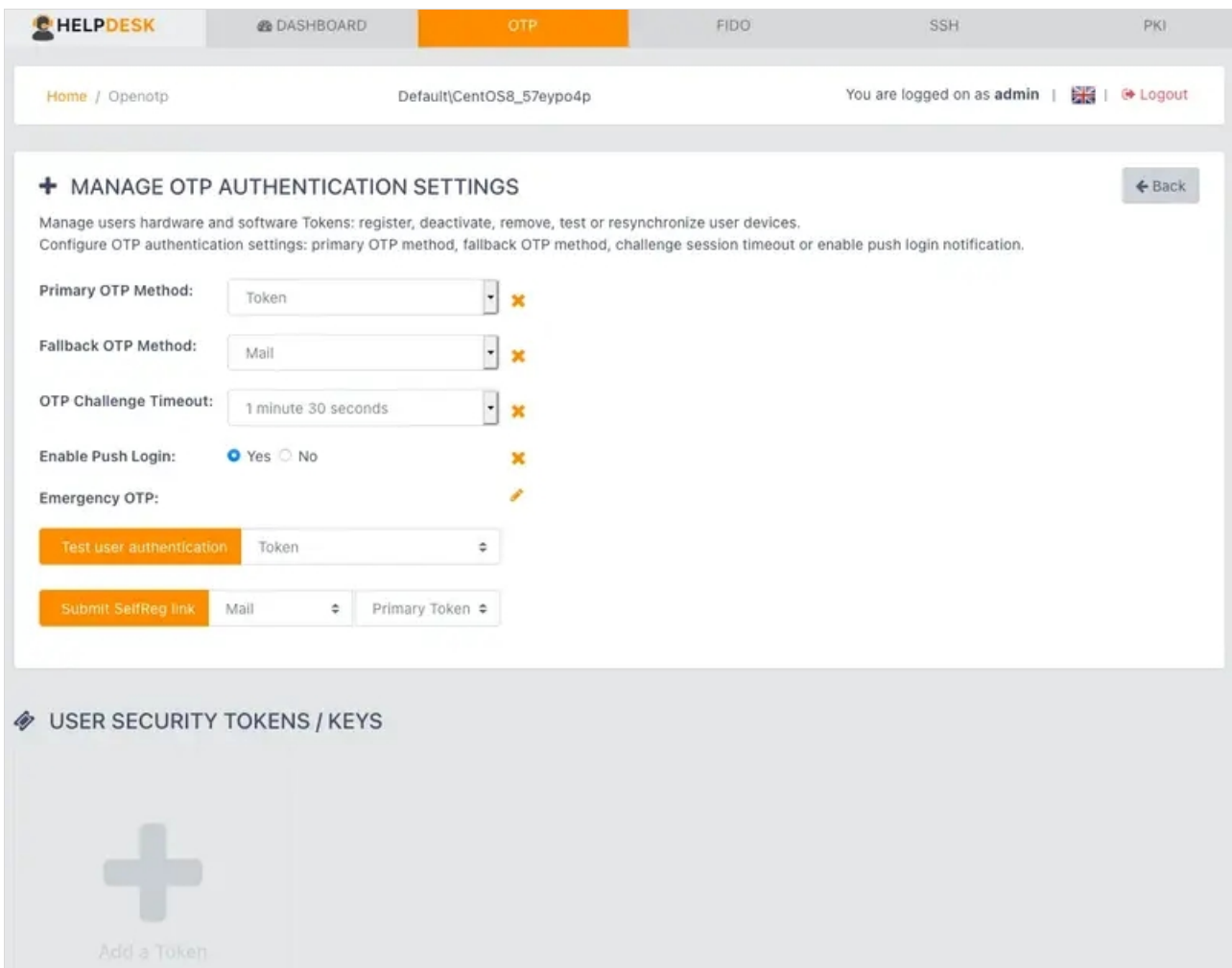
Welcome to the
HelpDesk Portal at
com.



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**.

HELPSDESK 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 enter the serial of your inventoried **Token** and click on [Register](#) .

+ 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.

Hardware Token

Token Inventoried



[Cancel](#)

+ INSTRUCTIONS TO REGISTER YOUR HARDWARE TOKEN

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

[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

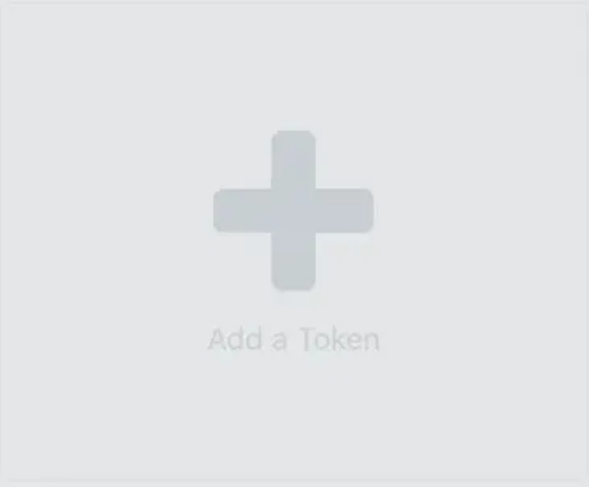
TOTP

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.



Domain: Default

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

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



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

HELPSDESK | 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:

Fallback OTP Method:

OTP Challenge Timeout:


Enable Push Login: Yes No

Emergency OTP:

[Test user authentication](#)

[Submit SelfReg link](#)

🔑 USER SECURITY TOKENS / KEYS



Add a Token





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

HELPSDESK | 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	🔍 Software Token	🔍 Yubikey	🔍 Another Token
<p>Token inventoried</p>  <p>Add Token</p>	<p>QRCode-based Authenticator</p>  <p>Add Token</p>	<p>Inventoried & YubiCloud</p>  <p>Add Token</p>	<p>Manual Registration</p>  <p>Add Token</p>

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

HELPSDESK | DASHBOARD | OTP | FIDO | SSH | PKI

Home / Openotp / Register | Default\CentOS8_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 [← 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:

Fallback OTP Method:

OTP Challenge Timeout:

Enable Push Login: Yes No


Test user authentication:

Submit SelfReg link:

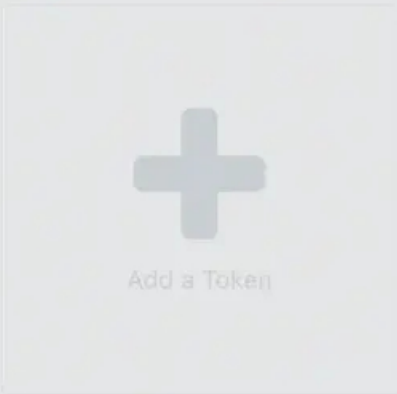
USER SECURITY TOKENS / KEYS

YUBIKEY

Yubikey YubiCloud 2573110

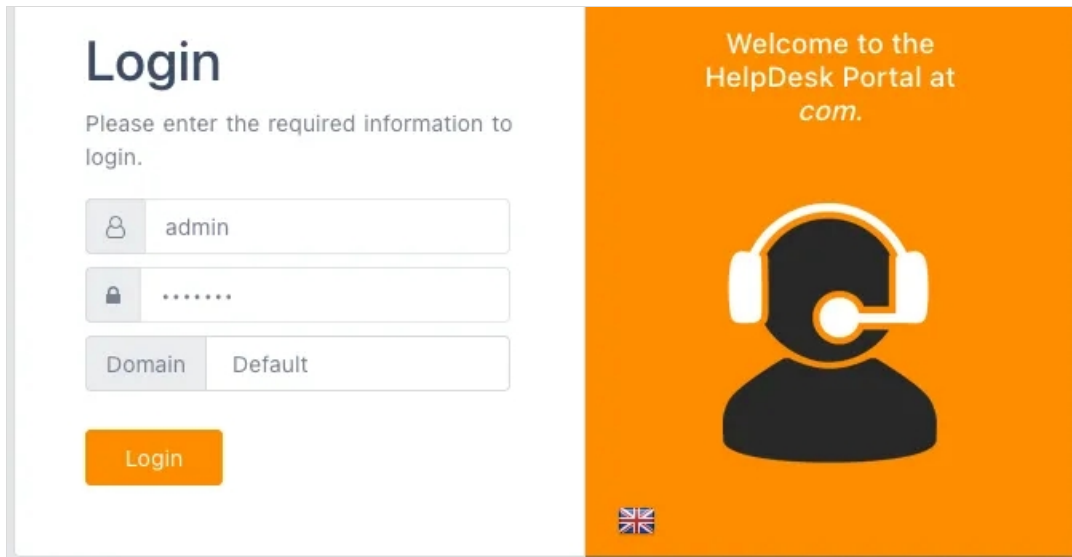


Type: YubiKey (YubiCloud)

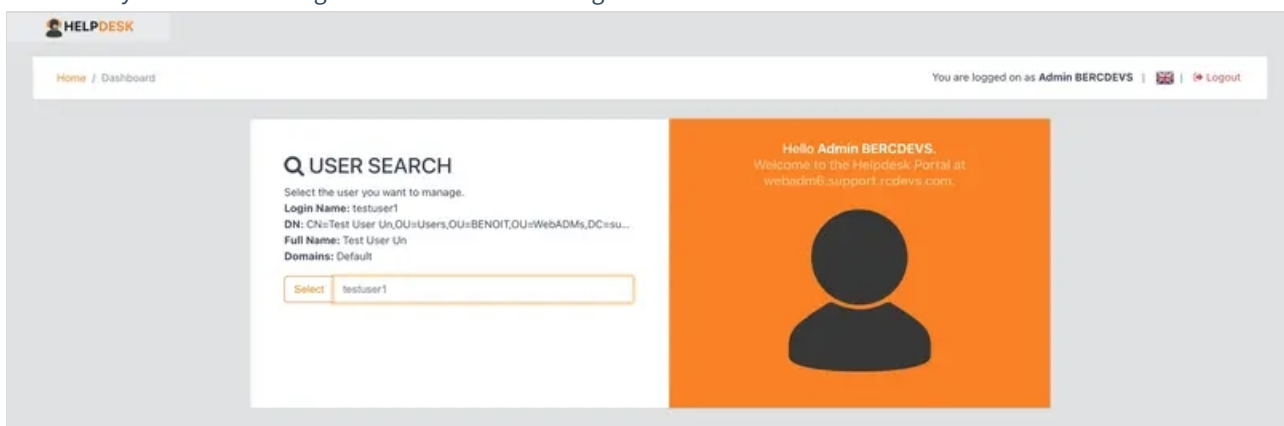


4.2.3 FIDO Registration

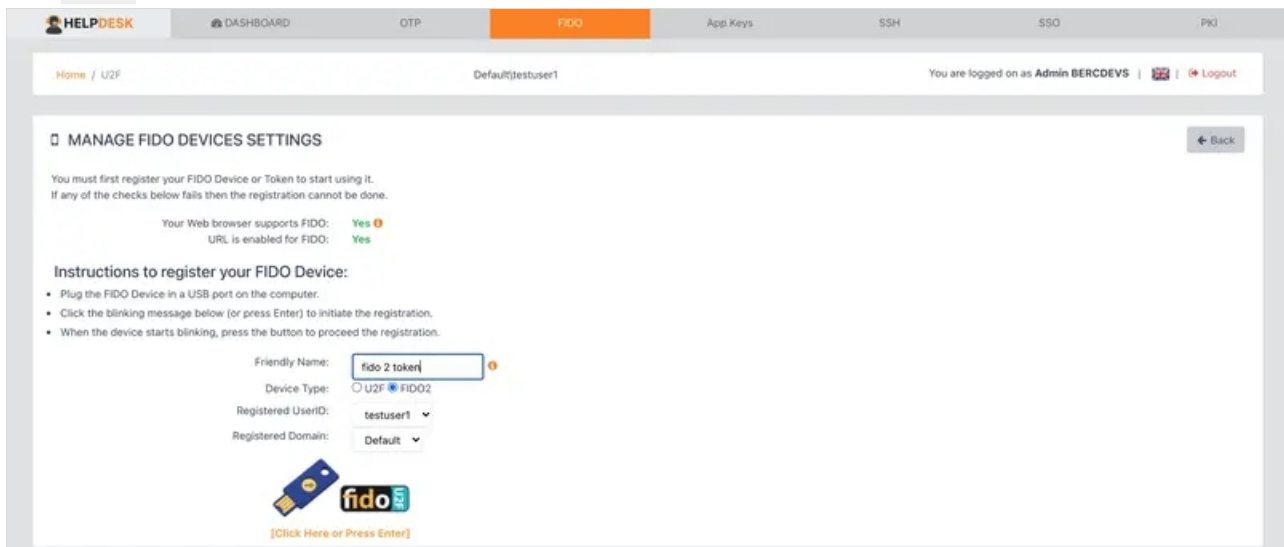
Log in to the HelpDesk application.



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



Go to the **FIDO** tab.



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.

HELPSDESK 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

HELPSDESK 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**

HELPSDESK 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]

Use your security key with rcodevs.com

Touch your security key again to complete the request.

Cancel

HELPSDESK 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: ▼



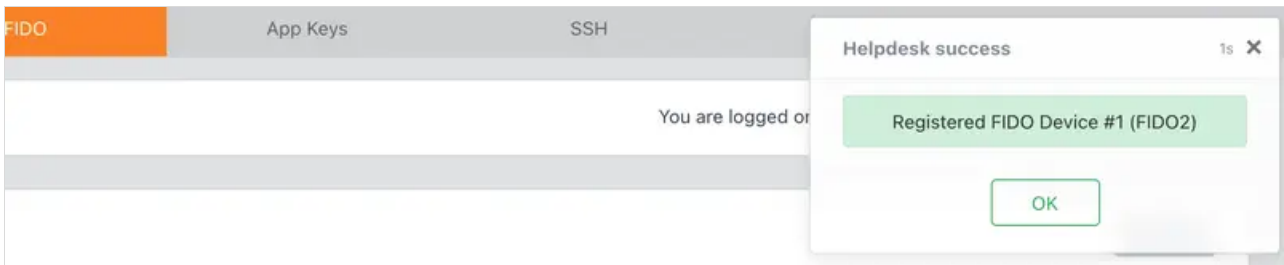
[Press your FIDO Device]

Allow this site to see your security key?

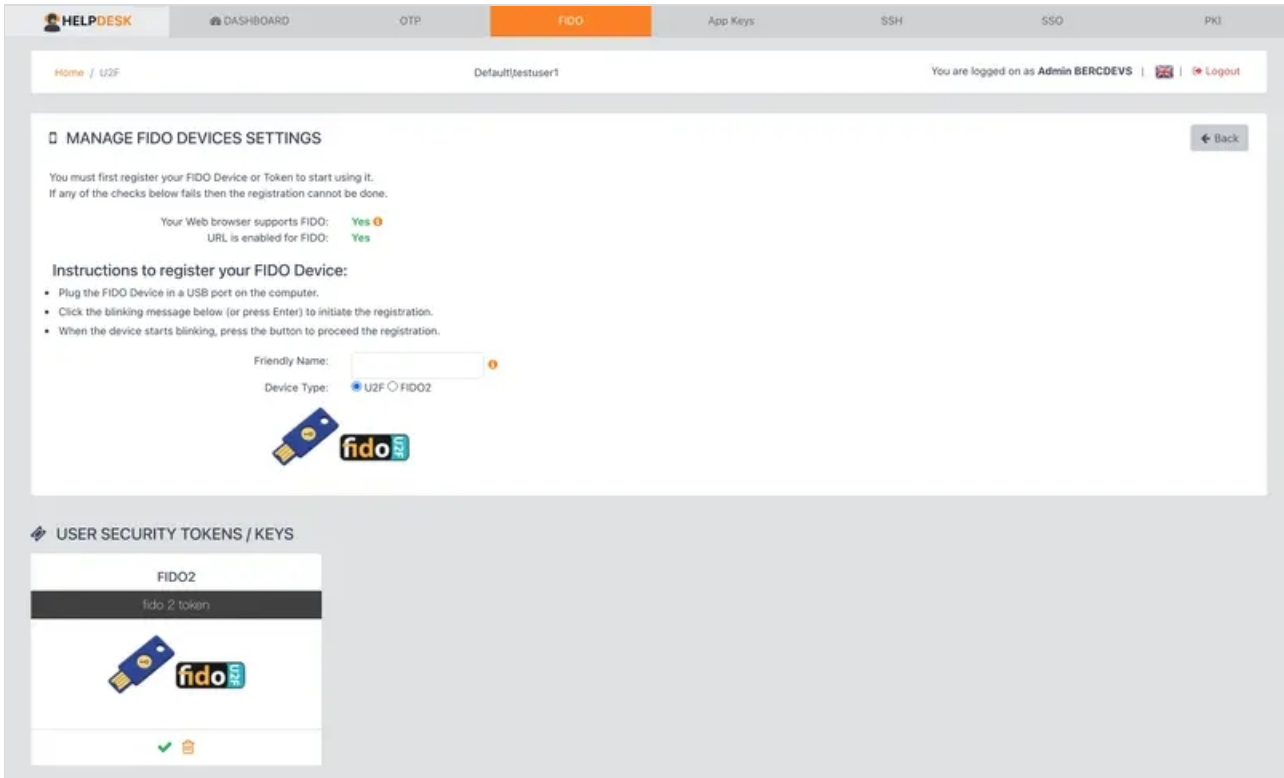
rcodevs.com wants to see the make and model of your security key

Skip

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

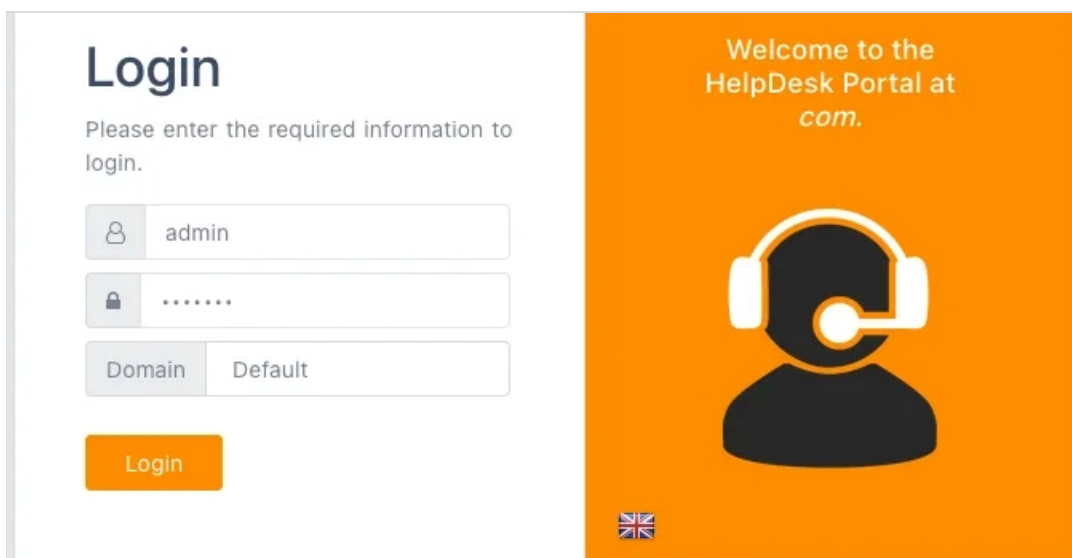


At the bottom of the page under **User Security Tokens / Keys** you will see the enrolled **FIDO** key.

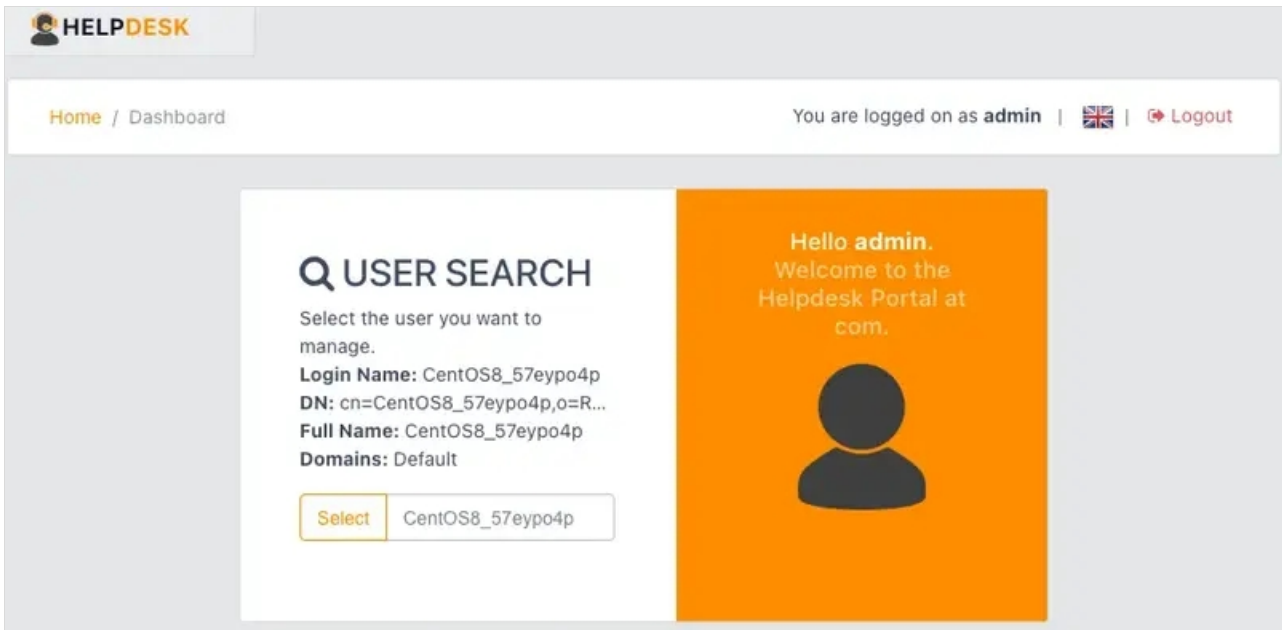


5. Build OTP List

Log in to the HelpDesk application.

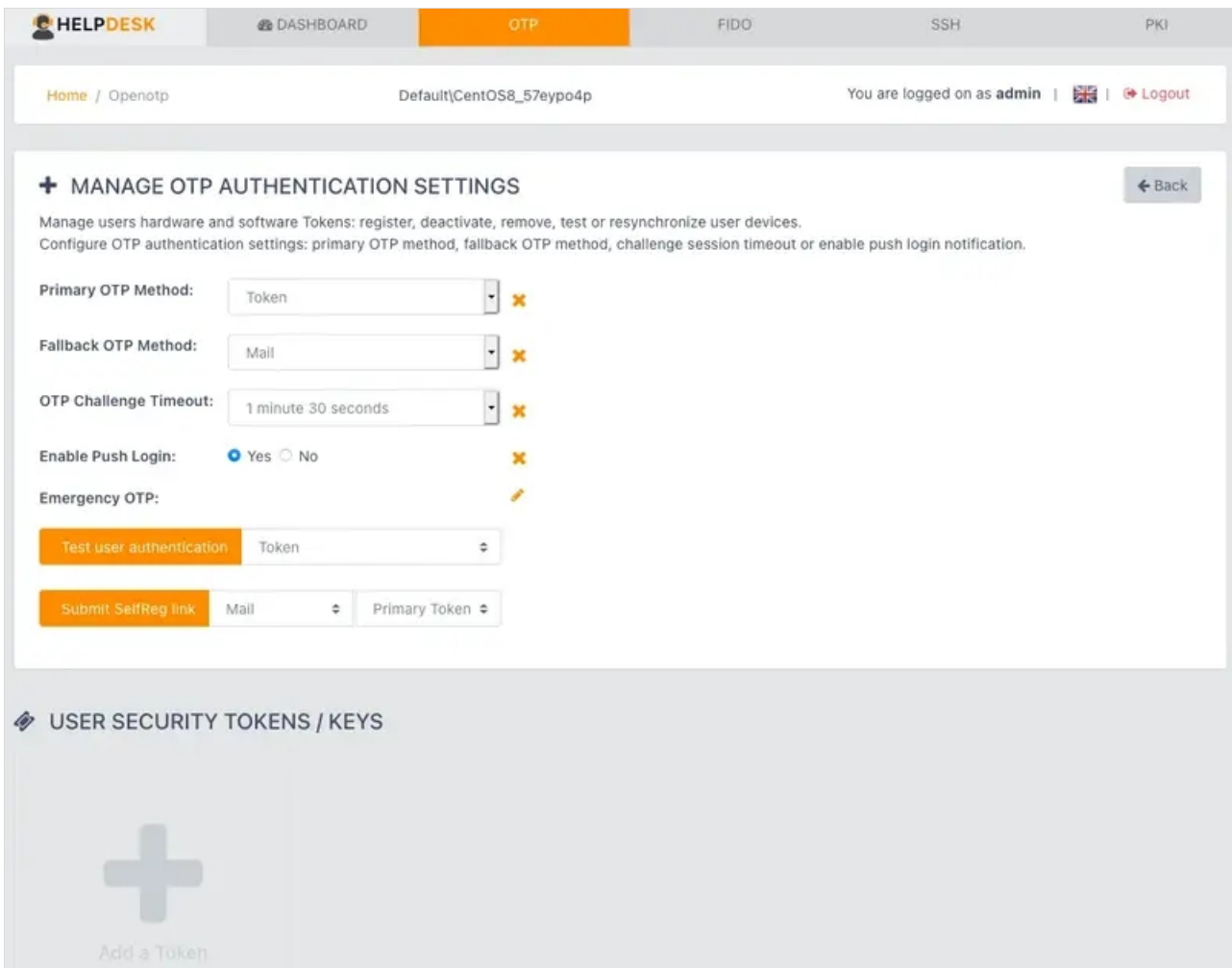


Select the user you want to build an **OTP List**.



The screenshot shows the 'HELPDESK' user search interface. At the top, there is a navigation bar with 'Home / Dashboard' and 'You are logged on as admin | [UK Flag] | Logout'. The main content area is split into two panels. The left panel, titled 'USER SEARCH', contains the text: 'Select the user you want to manage.', 'Login Name: CentOS8_57eypo4p', 'DN: cn=CentOS8_57eypo4p,o=R...', 'Full Name: CentOS8_57eypo4p', and 'Domains: Default'. Below this is a 'Select' button and a text input field containing 'CentOS8_57eypo4p'. The right panel is orange and features a user silhouette icon with the text: '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 displays the 'HELPDESK' 'MANAGE OTP AUTHENTICATION SETTINGS' page. The top navigation bar includes 'DASHBOARD', 'OTP' (highlighted), 'FIDO', 'SSH', and 'PKI'. The breadcrumb is 'Home / Openotp' and the user is logged in as 'admin'. The page title is 'Default\CentOS8_57eypo4p'. A '+ Back' button is in the top right. The main content area is titled '+ MANAGE OTP AUTHENTICATION SETTINGS' and includes the following settings: 'Primary OTP Method: Token', 'Fallback OTP Method: Mail', 'OTP Challenge Timeout: 1 minute 30 seconds', and 'Enable Push Login: Yes (selected) No'. There is an 'Emergency OTP:' section with an edit icon. Below these are two buttons: 'Test user authentication' with a dropdown set to 'Token', and 'Submit SelfReg link' with dropdowns for 'Mail' and 'Primary Token'. At the bottom, there is a section for 'USER SECURITY TOKENS / KEYS' with a large plus icon and the text 'Add a Token'.

SMS OTP OK

SMS OTP: ✎

Delivery Mode: On demand ✖
 Prefetch
 Mobile ID

Message Type: Normal Flash ✖

MAIL OTP OK

Mail OTP: loic@rcdevs.com ✎

Delivery Mode: On demand ✖
 Prefetch

Secure Mail: Yes No ✖

OTP LIST NOT OK

List Size:

Algorithm:

[Build OTP List](#)

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

SMS OTP OK

SMS OTP: ✎

Delivery Mode: On demand ✖
 Prefetch
 Mobile ID

Message Type: Normal Flash ✖

MAIL OTP OK

Mail OTP: loic@rcdevs.com ✎

Delivery Mode: On demand ✖
 Prefetch

Secure Mail: Yes No ✖

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](#)

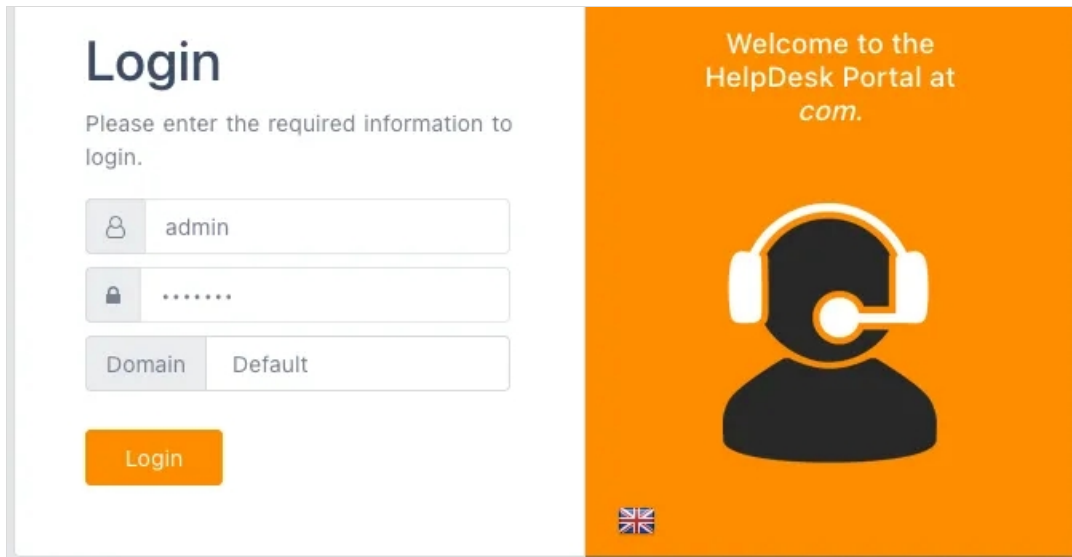
+ Manage OTP List [← Back](#)

OpenOTP Password List (50 OTPs)

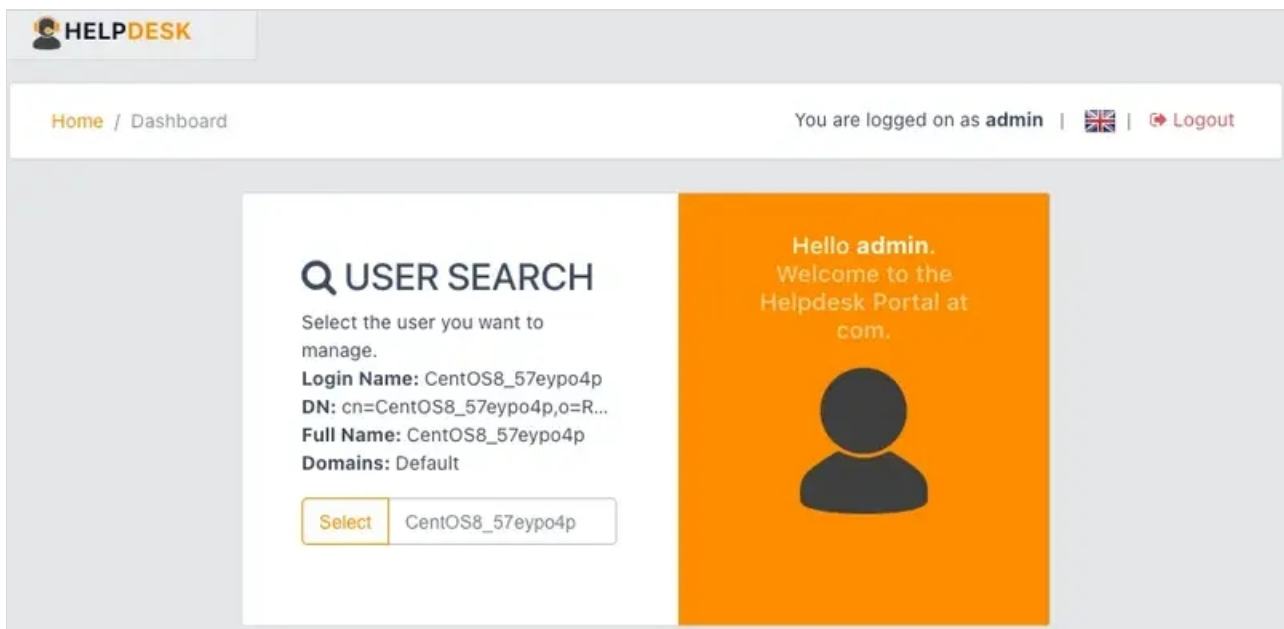
ID	OTP	ID	OTP	ID	OTP	ID	OTP	ID	OTP
1	236821	2	414967	3	955860	4	586808	5	544196
6	782852	7	400464	8	888487	9	015929	10	112665
11	936877	12	580456	13	715994	14	365707	15	717964
16	022043	17	759688	18	485442	19	254163	20	249730
21	011363	22	362485	23	108452	24	377531	25	005256
26	797377	27	183087	28	771661	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.



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



Go to the **App Keys** tab.

HELPCESK DASHBOARD OTP FIDO App Keys SSH SSO PKI

Home / Appkeys Default\CentOS8_57eypo4p You 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:

Expires After:

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

HELPCESK DASHBOARD OTP FIDO App Keys SSH SSO PKI

Home / Appkeys You 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:

Expires After:

Rebuild application keys ×

Do you want to create application keys

HELPDESK DASHBOARD OTP FIDO App Keys SSH SSO PKI

Home / Appkeys Default|CentOS8_57eypo4p You are logged on as admin |  |  Logout

MANAGE APPLICATION PASSWORDS

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:

Expires After:

7. SSH Key Registration



Log in to the HelpDesk application.

Login

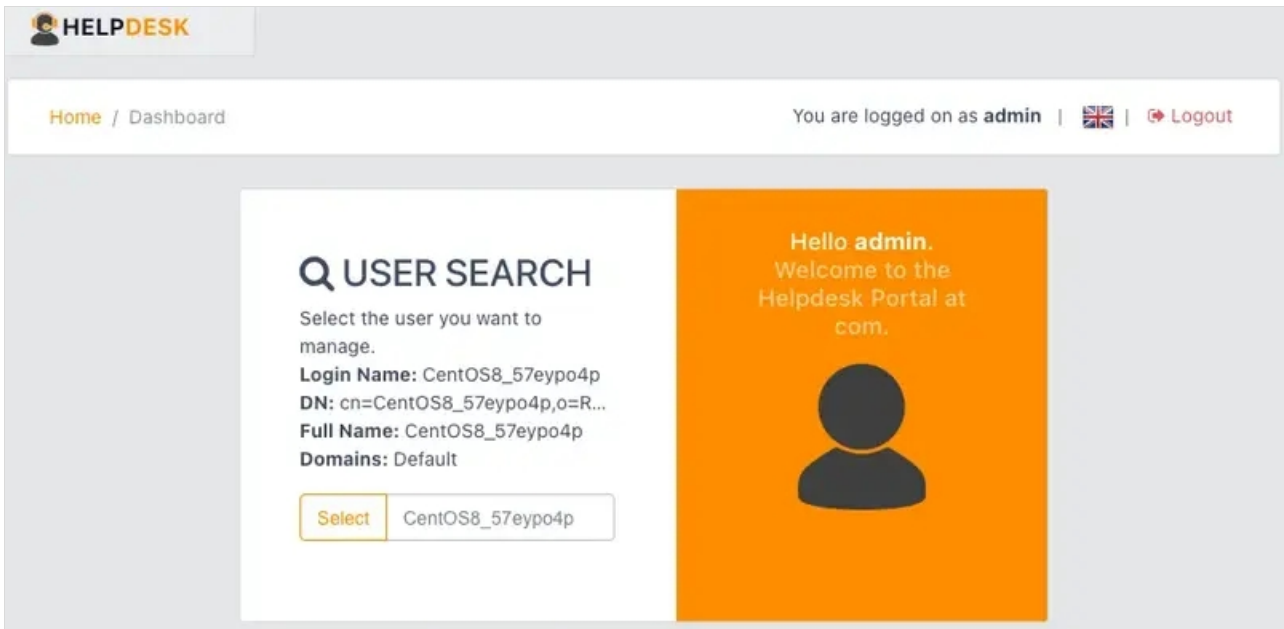
Please enter the required information to login.

Domain

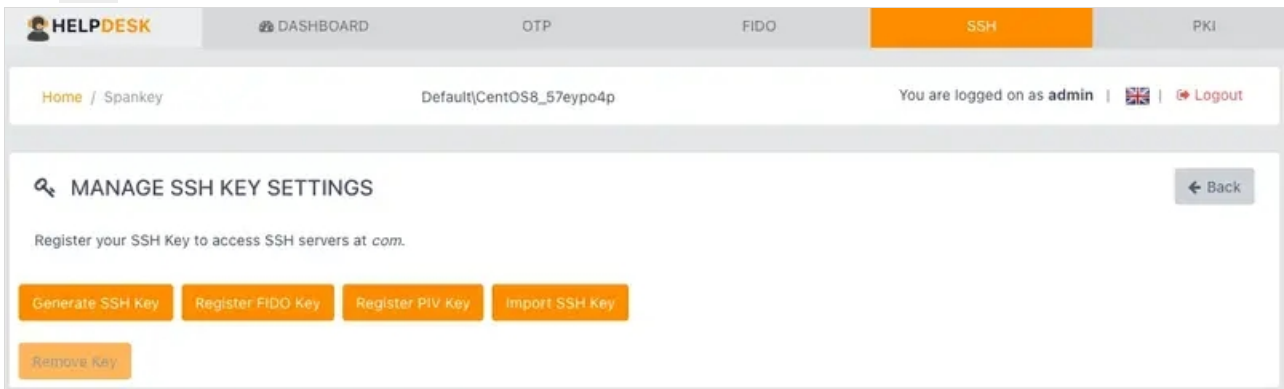
Welcome to the HelpDesk Portal at *com*.



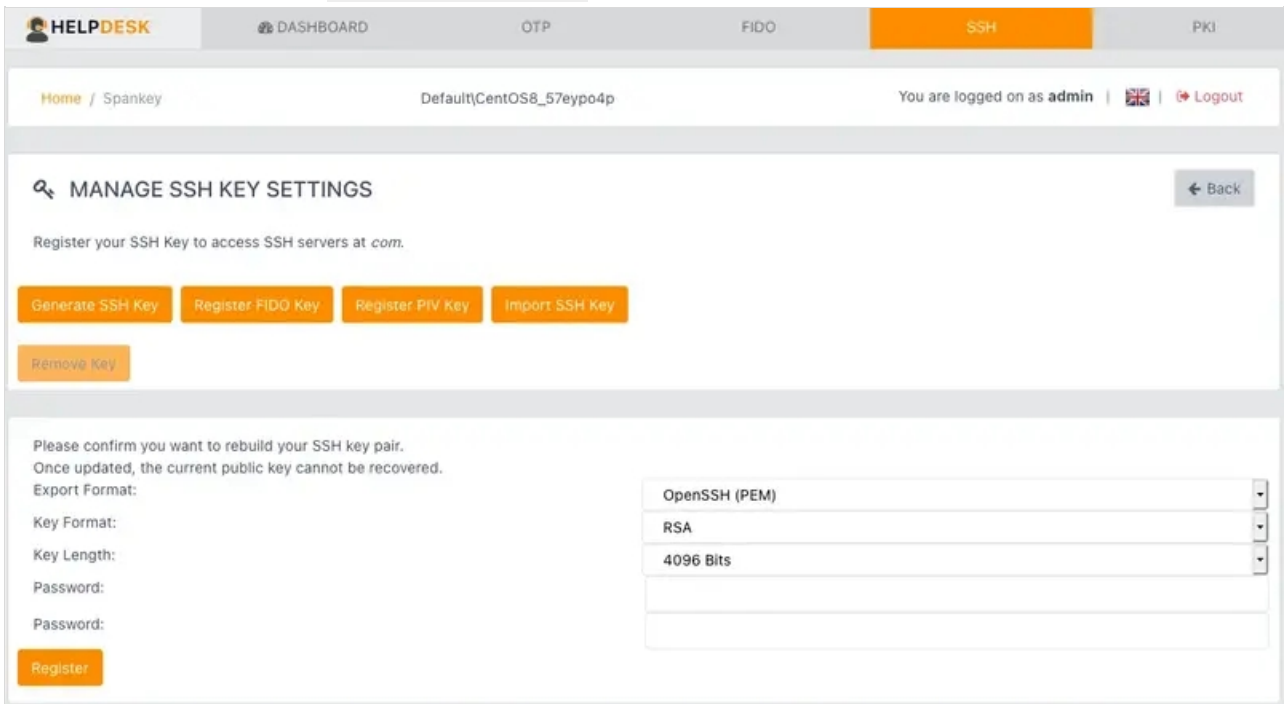
Select the user you want to register an **SSH Key**.



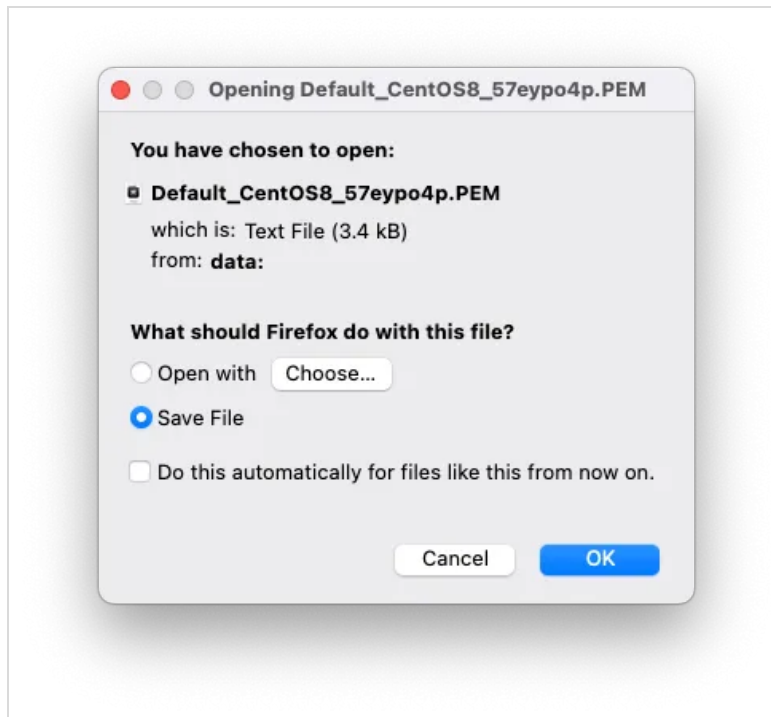
Go to the **SSH** tab.



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.

HELPSDESK DASHBOARD OTP FIDO **SSH** PKI

Home / Spankey Default(CentOS8_57eypo4p) You are logged on as admin | | Logout

MANAGE SSH KEY SETTINGS

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
AAAAB3NzaC1yc2EAAAADAQABAAQACw3aESJNC8LhJfnI+T1VZiAb8Dzr91Cv0QV6R5t2AejfG
FXVhwPF43HyglCYb3ip0jyMUP3qteIJSbniEC3Q8Ja4qYI02bXv9M/AgVJFjqSU6u3nfZ6oAAS
tJK8yW10VFaoJlJ6lTG
/GJw9WtB8rh7dzJqKq01zQe9hmm66EjU+KC00SvYQ0eqpD9s86h18a0E5kn6r/Xh9+X
/JxxFET0HD+APljZGYvfc61RwUd8K6Hm1qLKDnMxhQzn1kwLQ+9yvqONLopGltzLSG8p+2hxLnM
HZU5xh9kUYI9Yzsr+qWm6y10ymJcHScKENy05jUhx2kVd9jgm4bk0WC9BHXSdo8XUnDUNIcXbS
nvUtq24PGcxUa8wXmW41ro5FFJFRYzRKyo5twWkksvM57R/qjWq1FIrdB0B
/Z2k0ZVeKlVI9rKLoD/BEbnOUdz+t
/9G1c1sL6HJTU+Xw8YyAdm4maH0G+cpJrV61rREiNpT6EL24AXsRkUN
/G00hGnF81YGrGrWB8MKm1aw0zGDp60/8fTTru1Q00GtLjnfTm6794kXx/h4Mox6xwC80vJy8D
/eKVMW55jHB9LPmzoMjz5muLQD/s0hndWqawydV0GRfdcaqPd5aNsHkvX4jCY
/2LejN37A1frGv249tZd0ZNIarHfgXBMMa7+d1q0P9e0Rw== Default\CentOS8_57eypo4p
```

User Statistics

Login Count: **2 success & 0 failure**
Last Login: **Never**

[Generate SSH Key](#) [Register FIDO key](#) [Register PIV Key](#) [Import SSH Key](#)

[Remove Key](#)

To import an SSH Key, click on [Import SSH Key](#). Copy and paste your **Public Key** into the Field.

HELPSDESK | DASHBOARD | OTP | FIDO | **SSH** | PKI

Home / Spankey | Default(CentOS8_57eypo4p) | You are logged on as admin | | Logout

MANAGE SSH KEY SETTINGS

Register your SSH Key to access SSH servers at com.

[Generate SSH Key](#)
[Register FIDO Key](#)
[Register PIV Key](#)
[Import SSH Key](#)

[Remove Key](#)

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGCVMMyIdEe1Ed+fdEAJ20b
0K5gZ9hUEtI1Mz7dCp4NHmuYfE42/00in41Mjb6RzWreE5UAJ0D
m36mEFn++m1UrIoFF8WAWL02uk0xSHToPCZLdKuESsSII2BPjir
x8V1aq3LougErTktfT3qhHhA93sm1LuGF47tLRk0PgMa2lveifz
czVpz7jhd00pJTktPuyQAu5Fdc7+nK+o00rrMYNHVPV9ScU5PWQ
lfmVP970B877Mwd0rA4JQr5kqeUd+rusAANsj8V9H26S31Jxn0B
jMa5bnCpqeRokZr07wrcgLinchZMg18yLSldBfI0tKg0S9f0kJj
rAjJbmgaxQY3PU6LzXZZz0pjLycbzJYo3o3nadmD3Pr7UrK10L
Hj+bTUNo32NT8SaaR+IdYBown5N6uB16Jtg3KAUIctslsThx0Jd
xQdUFJwC05HSiwEBxNRWLSxw82+1N97qSwY03ecd34HCbmIM4y
9eqy4bItv7bAdm27PM4L1azTCq9U=
```

[Import](#)

Finally, click on [Import](#).

HELPSDESK | DASHBOARD | OTP | FIDO | **SSH** | PKI

Home / Spankey | Default(CentOS8_57eypo4p) | You are logged on as admin | | Logout

MANAGE SSH KEY SETTINGS

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 3040 Bits)

[Copy](#)

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGCVMMyIdEe1Ed+fdEAJ20b0K5gZ9hUEtI1Mz7dCp4NHmuY
fE42/00in41Mjb6RzWreE5UAJ0Dm36mEFn++m1UrIoFF8WAWL02uk0xSHToPCZLdKuESsSII2BP
jirx8V1aq3LougErTktfT3qhHhA93sm1LuGF47tLRk0PgMa2lveifzczVpz7jhd00pJTktPuyQA
u5Fdc7+nK+o00rrMYNHVPV9ScU5PWQlfmVP970B877Mwd0rA4JQr5kqeUd+rusAANsj8V9H26S3
1Jxn0BjMa5bnCpqeRokZr07wrcgLinchZMg18yLSldBfI0tKg0S9f0kJj rAjJbmgaxQY3PU6LzX
ZZz0pjLycbzJYo3o3nadmD3Pr7UrK10LHj+bTUNo32NT8SaaR+IdYBown5N6uB16Jtg3KAUIctsls
Thx0JdxQdUFJwC05HSiwEBxNRWLSxw82+1N97qSwY03ecd34HCbmIM4y9eqy4bItv7bAdm2
7PM4L1azTCq9U= Default\CentOS8_57eypo4p
```

User Statistics

Login Count: **2 success & 0 failure**
Last Login: **Never**

[Generate SSH Key](#)
[Register FIDO Key](#)
[Register PIV Key](#)
[Import SSH Key](#)

[Remove Key](#)



8. SSO Customizations

Log in to the HelpDesk application.

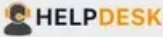
Login


Please enter the required information to 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

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

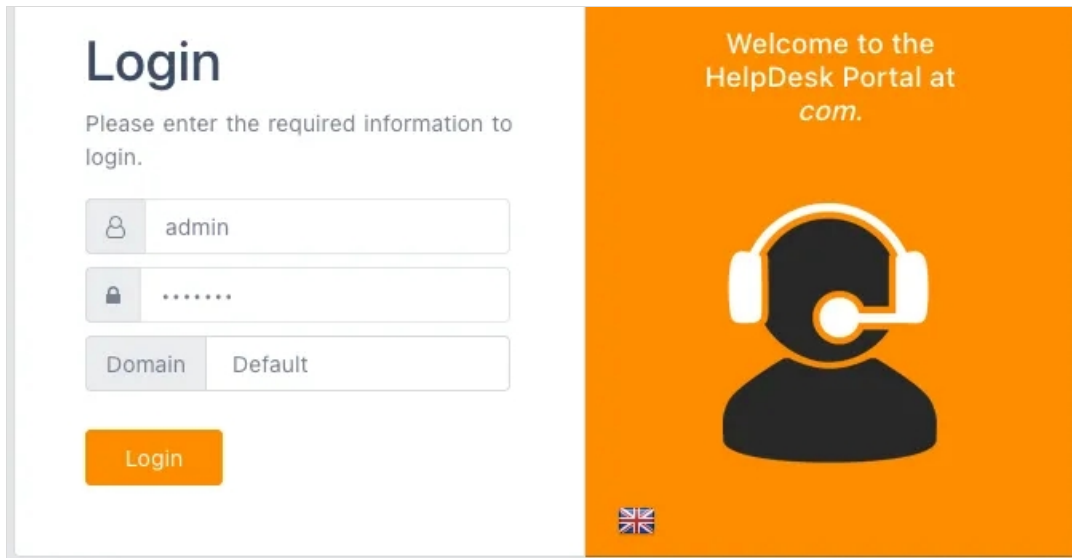
Enable SAML Usage: Yes No ✕

Enable OpenID Usage: Yes No ✕

SSO Session Time: ✕

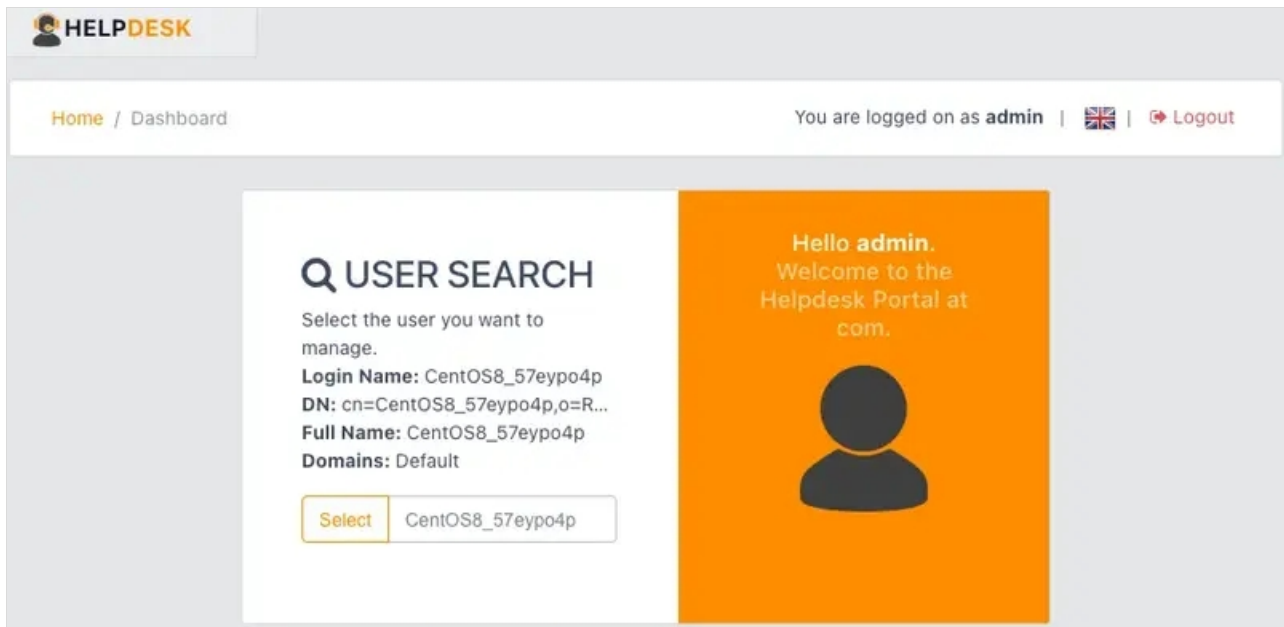
9. User certificate enrollment

Log in to the HelpDesk application.



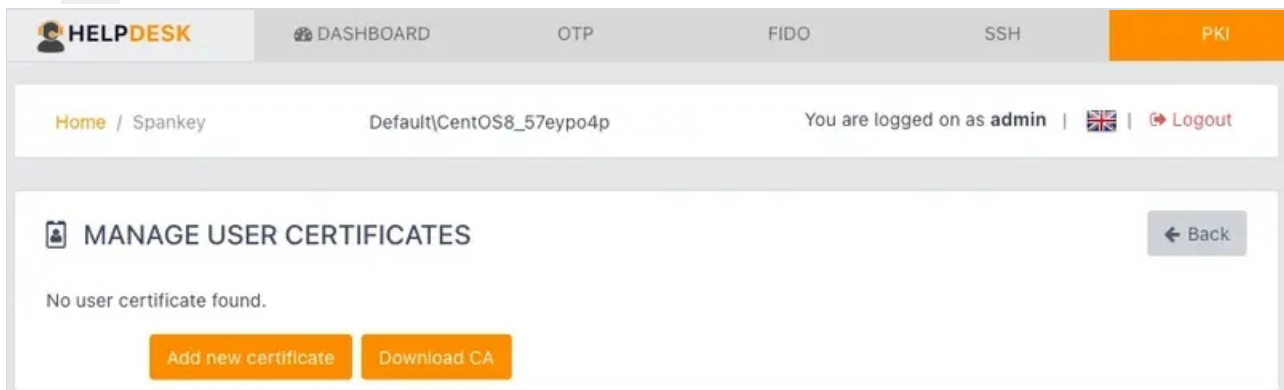
The login page features a white sidebar on the left with the title "Login" and instructions: "Please enter the required information to login." Below this are three input fields: a username field containing "admin", a password field with masked characters "*****", and a domain dropdown menu set to "Default". An orange "Login" button is positioned below the fields. The main content area has an orange background with the text "Welcome to the HelpDesk Portal at com." and a white headset icon. 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 header includes the "HELPDESK" logo, a breadcrumb "Home / Dashboard", and a user status "You are logged on as admin" with a UK flag and a "Logout" link. The main content is split into two panels. The left panel, titled "USER SEARCH", contains the text "Select the user you want to manage." and lists user details: "Login Name: CentOS8_57eypo4p", "DN: cn=CentOS8_57eypo4p,o=R...", "Full Name: CentOS8_57eypo4p", and "Domains: Default". A "Select" button is next to a dropdown menu showing "CentOS8_57eypo4p". The right panel has an orange background with "Hello admin. Welcome to the Helpdesk Portal at com." and a white user silhouette icon.

Go to the **PKI** tab.



The PKI tab header shows "HELPDESK" and navigation tabs for "DASHBOARD", "OTP", "FIDO", "SSH", and "PKI". The breadcrumb is "Home / Spankey" and the user status is "Default\CentOS8_57eypo4p" with "You are logged on as admin" and a "Logout" link. The main content area is titled "MANAGE USER CERTIFICATES" and includes a "Back" button. Below the title, it states "No user certificate found." and features two orange buttons: "Add new certificate" and "Download CA".

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

HELPSDESK | 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.

HELPSDESK | 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