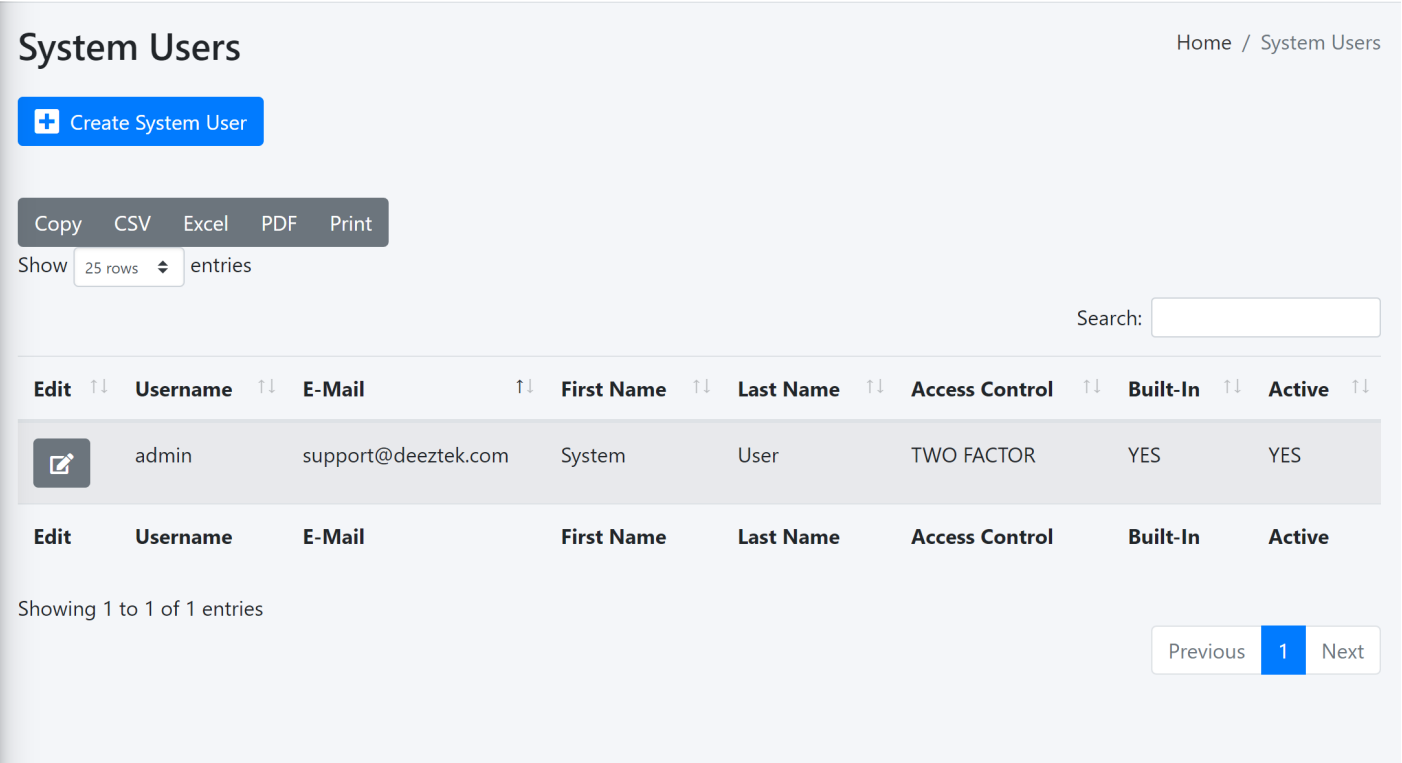


System Users

The **System Users** screen allows you to create, add and delete System Users (**Figure 1**).

Figure 1



By default, Hermes SEG comes pre-configured with the the **System User** account with the following default credentials:

- **Username:** admin
- **Password:** ChangeMe2!


Create System User

If you wish to create a new System User, click the **Create System User** button on top of the screen (**Figure 2**).

Figure 2

System Users


Home / System Users

 Create System User

Copy CSV Excel PDF Print

Show 25 rows entries

Search:

Edit	Username	E-Mail	First Name	Last Name	Access Control	Built-In	Active
	admin	support@deeztek.com	System	User	TWO FACTOR	YES	YES

Edit	Username	E-Mail	First Name	Last Name	Access Control	Built-In	Active
------	----------	--------	------------	-----------	----------------	----------	--------

Showing 1 to 1 of 1 entries

Previous 1 Next

You will be directed to the **Edit System User** screen where the system has already pre-filled the **Username**, **E-Mail Address**, **First Name** and **Last Name** fields. The **Access Control Policy** field has been set to **One Factor**, the **Set User Password** field has been set to **YES** and the **Check Password Against haveibeenpwned.com** has been set to **YES**. Adjust fields as necessary, enter a password in the **User Password** field and click the **Submit** button (**Figure 3**).

Figure 3

Edit System User

Home / Edit System User

Back to System Users

Delete User

Username

user_25

E-Mail Address

someone_25@domain.tld

First Name

System

Last Name

User_25

Access Control Policy

Warning!

Before setting **Access Control Policy** to **Two Factor** ensure you first read the [Access Control Policy Documentation](#), ensure e-mail delivery works as expected, the e-mail addresses for this System User is correct and you have an authenticator app such as [FreeOTP](#), [Google Authenticator](#), [Authy](#) etc installed on your mobile device

One Factor

Set User Password

YES

Check Password Against haveibeenpwned.com

YES

User Password

Enter the password for Username above

Submit

Access Control Policy

The Access Control Policy field allows you to switch between **One Factor** Authentication (1FA) which consists of Username and Password authentication (Default) OR **Two Factor** Authentication (2FA) which consists of Username and Password AND an additional **Timed One Time Password** (TOTP) generated on your mobile device for additional security.

Two Factor requires the following pre-requisites before enabling:

- Hermes SEG Outbound E-mail Flow must be working correctly
- The System User Account you enable Two Factor authentication must have a valid e-mail address.
- You must have an Authenticator app installed on your mobile device such as [FreeOTP](#), [Google Authenticator](#), [Authy](#) etc.

Once you set the **Access Control Policy** to **Two Factor** and click the **Submit** button, logout and then log back in with the same System User you enabled Two Factor authentication. After successfully authenticating, the system will prompt to register your mobile device. Click the **Register device** link on the One-Time Password screen (**Figure 4**).

Figure 4



Hi Ehsan

[LOGOUT](#) | [METHODS](#)

One-Time Password




The resource you're attempting to access
requires two-factor authentication.
Register your first device by clicking on the
link below.

[Register device](#)

Powered by Authelia

The system will display **An email has been sent to your address to complete the process** on the upper right-hand corner of the screen (**Figure 5**).

Figure 5

 An email has been sent to your address to complete the process.



Hi, [John Smith](#)

[LOGOUT](#) | [METHODS](#)

One-Time Password



The resource you're attempting to access
requires two-factor authentication.
Register your first device by clicking on the
[link below.](#)

[Register device](#)

Powered by Authelia


Check the mailbox of the e-mail address associated with your account and look for an e-mail that contains the subject **Register your mobile** and click the **Register** button at the bottom of the e-mail (**Figure 6**).

Figure 6



no-reply@hermes-seg.com | 1-800-555-1234

[Hermes SEG] Register your mobile

 If there are problems with how this message is displayed, click [here](#) to view it in a web browser.



Register your mobile

This email has been sent to you in order to validate your identity. If you did not initiate the process your credentials might have been compromised. You should reset your password and contact an administrator.



Please contact an administrator if you did not initiate the process.

You will be taken to the **Scan QR Code** page. Using the Authenticator app you previously downloaded and installed on your mobile device, scan the QR Code from the page and click the **DONE** button (**Figure 7**).

Figure 8



Scan QR Code

Need Google Authenticator?



Secret

otpauth://totp/Example:john.doe@gmail.com



DONE

On the following **One-Time Password** screen enter the passcode generated by your authenticator app (**Figure 9**).

Figure 9



Hi [User Name]



[LOGOUT](#) | [METHODS](#)

One-Time Password



1	2	3			
---	---	---	--	--	--

Enter one-time password

[Lost your device?](#)

Powered by Authelia

If everything goes well and you typed in the correct passcode within the allotted time, you should be able to successfully login to **Hermes SEG Administration Console**.

If you run into a problem and the Two Factor authentication did not work for any reason, you can reset authentication back to One Factor by running the following script from the console with root privileges:

```
/opt/hermes/scripts/disable_authelia_2fa.sh
```

Passwords

Hermes SEG implements the following [NIST 800-63](#) Password Guidelines:

- 8 character minimum password.
- 64 character maximum password.
- Able to check against known breached passwords via the use of the haveibeenpwned.com API.

- Implementation of Multifactor Authentication via the use of [Time-Based One-Time Password \(TOTP\)](#) , [Duo Security](#) and [Webauthn](#) Security Keys.
- Passwords are hashed with the [Argon2 KDF](#).

Revision #15

Created 19 November 2021 21:32:27 by Dino Edwards

Updated 11 June 2023 14:18:14 by Dino Edwards