HID® Origo™ Management Portal Organization Administrator

User Guide

PLT-07733, Rev. A.2
January 2026

Copyright

© 2024 - 2026 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

This document may not be reproduced, disseminated, or republished in any form without the prior written permission of HID Global Corporation.

Trademarks

HID GLOBAL, HID, the HID Brick logo, and HID Origo are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

Contacts

For technical support, please visit: **https://support.hidglobal.com**.

What's new

Date	Description	Revision
January 2026	• Section 2.1. Updated section for completing account registration. • Section 2.4. Updated section for the Portal Help Center feature. • Section 3.4. New section added for user search and filtering functionality. • Section 3.6. Updated content for issuing a Pass to Wallet. • Section 3.9. Updated section for export users file. • Section 4 Credential Management. Updated section for Pass Design functionality. • Section 5.12 Create and manage System Accounts. Updated section for Public Key Infrastructure (PKI) based authentication for System Accounts. • Section 6 Report Management. Updated the section for new report information layout and for pre-paid subscription reports for Wallet and Bridge.	A.2

A complete list of revisions is available in **Revision history**.

About this document 1
1.1 Purpose 2
1.2 Intended audience 2
1.3 Information statements 2
1.4 Typographical conventions 2
HID Origo Management Portal Onboarding and Account Setup 3
2.1 Organization and Administrator Onboarding 4
2.2 Migration to new Portal (Wallet customers only) 9
HID Origo Management Portal Overview 10
3.1 Organization Administration Home page 11
3.1.1 Portal header bar 12
3.1.2 Portal navigation pane 12
3.1.3 Portal Home page widgets 13
3.1.4 Get Acquainted with the Origo Portal 14
3.1.5 Pass Template 15
3.1.6 Shortcuts 16
3.2 My Account management 17
3.2.1 My Account General settings 17
3.2.2 My Account Security settings 19
3.3 Portal Help Center 20
User Management 21
4.1 User management overview 22
4.2 Enroll new Users 23
4.2.1 Enroll a single user 23
4.2.2 Enroll multiple users 27
4.3 User profile management 29
4.3.1 Manage Administrator Roles 31
4.4 User search and filtering 32
4.4.1 User search 32
4.4.2 Filter users 33
4.5 User Pass management 34
4.6 User Pass provisioning via Single Sign On (SSO) 37
4.6.1 Add Pass to Google Wallet using SSO 37
4.6.2 Add Pass to Apple Wallet using SSO 39
4.7 Delete a User 41
4.8 View file imports 42
4.9 Export Users 44
4.9.1 Export user details 44

4.9.2 Export all user details ... 46
Credential Management ... 48
5.1 Credential management overview ... 49
5.2 Create a Pass Design ... 50
5.2.1 Manage Pass Designs ... 59
5.2.2 Manage Assets ... 60
5.3 Create and manage Pass Templates ... 61
5.3.1 Create a new Pass Template ... 62
5.3.2 View Pass Template details ... 67
5.3.3 Edit Pass Template ... 68
5.3.4 Change Pass Design ... 69
5.3.5 Delete Pass Template ... 70
5.4 View Credential Templates ... 71
5.5 View Keysets ... 72
Organization Management ... 73
6.1 Organization management overview ... 74
6.2 Edit Organization details ... 75
6.3 View Subscription details ... 76
6.4 Manage Administrators ... 77
6.4.1 Assign new Administrator ... 77
6.4.2 Manage existing Administrators ... 79
6.5 View Roles and Permissions ... 80
6.6 Configure enrollment details ... 81
6.7 Configure notifications ... 82
6.8 Customize or edit E-Mail templates ... 83
6.9 Export settings ... 84
6.10 Mobile App settings ... 85
6.11 Configure Single Sign On settings ... 86
6.11.1 SAML 2.0 configuration ... 87
6.11.2 OpenID Connect configuration ... 88
6.12 Create and manage System Accounts ... 89
6.12.1 Add a system account ... 89
6.12.2 Edit a system account ... 91
6.12.3 Delete a system account ... 93
Report Management ... 94
7.1 License Usage & Reports ... 95
7.1.1 License Usage & Reports page widgets ... 96
7.1.2 Subscription Usage ... 96

7.1.3 Tech Giant Wallet Fee Activations 97
7.1.4 User Activity 98
7.2 Export License Usage data 99

Section 01

About this document

1.1 Purpose

This document provides information on the tools and services offered within the HID Origo Management Portal and how you can use these to support your organization for Mobile Access Control.

1.2 Intended audience

This document is intended for HID Origo Management Portal users who are assigned the roles of:

- Organization Administrators
- Pass Service Administrators
- Pass Service Operators

1.3 Information statements

The following information statements are used in this document to alert the reader to important information.

Important: This notice is used to highlight important information about hazards or actions that could potentially impact service performance, application functionality or successful feature configuration.

Note: This note is used to highlight information of interest that needs to be brought to the reader's attention.

1.4 Typographical conventions

Typographical conventions used in this document are described in the following table:

Appearance	Description
Bold	Used to highlight GUI items such as menus, menu selections, window and dialog names, soft keys, file names, and directory names when they are used in a procedure or user action. For example: File > Exit C:\Program Files\HID Global\
Italics	Used to refer to document titles and references, for example: *HID Origo™ Management Portal Organization Administrator User Guide*.

`Monospaced`	Used for code fragments, for example:
	`"permanentlyDeleteCredential":false,`
	`"deleteCredentialState":"inactive"`

<Italics>	Angle brackets surrounding user supplied required values, for example: *<Server name>*
[text]	Square brackets surrounding user supplied optional values, for example: [your site location name]

Section 02

HID Origo Management Portal Onboarding and Account Setup

2.1 Organization and Administrator Onboarding

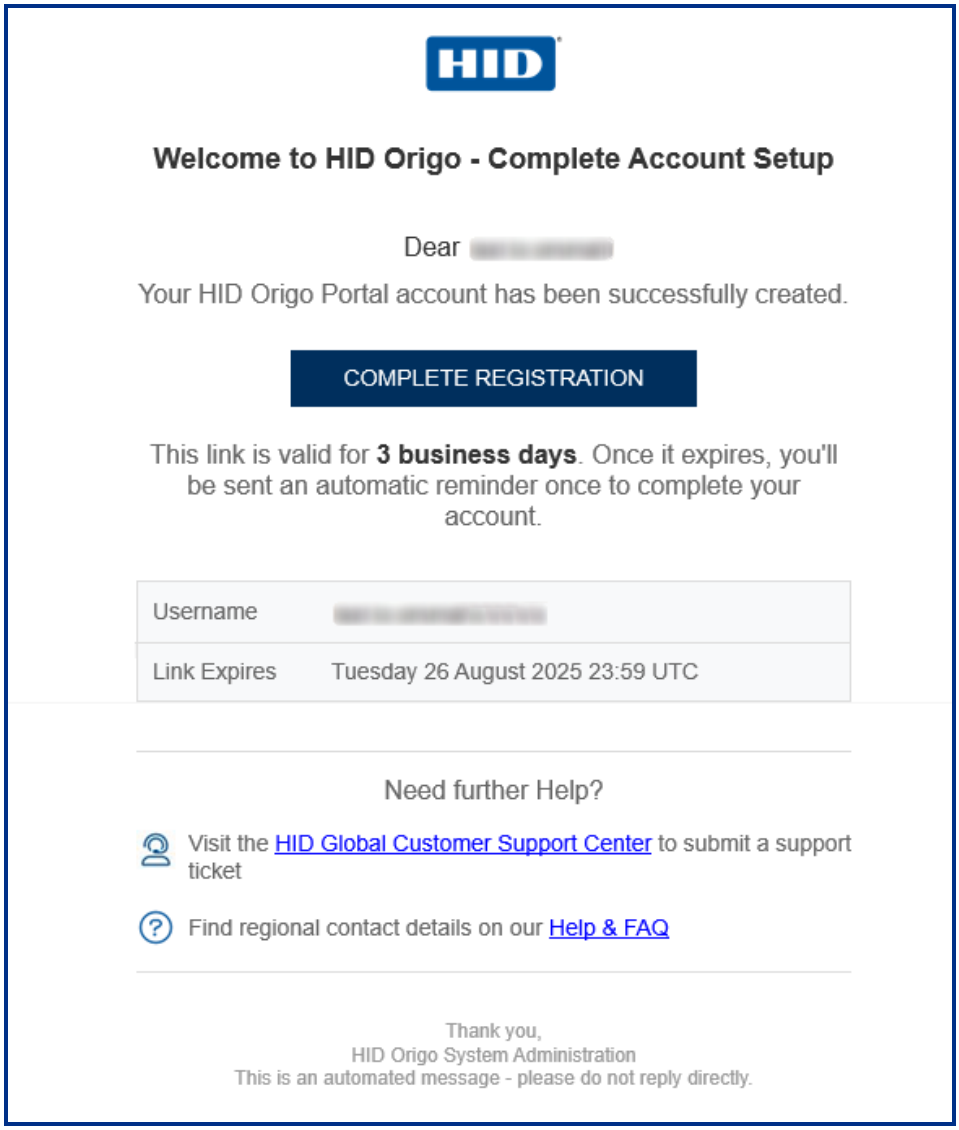
Currently customers are required to complete a manual Managed Onboarding registration process for an Organization account on the HID Origo Management Portal. If you have not yet created an account by working with your HID team, please contact your HID Representative to discuss the process to sign up for Mobile Access and get access to your Origo Portal.

> **Note:** For Organization setup within the HID Origo Management Portal an E-Mail address and Organization Code are mandatory.

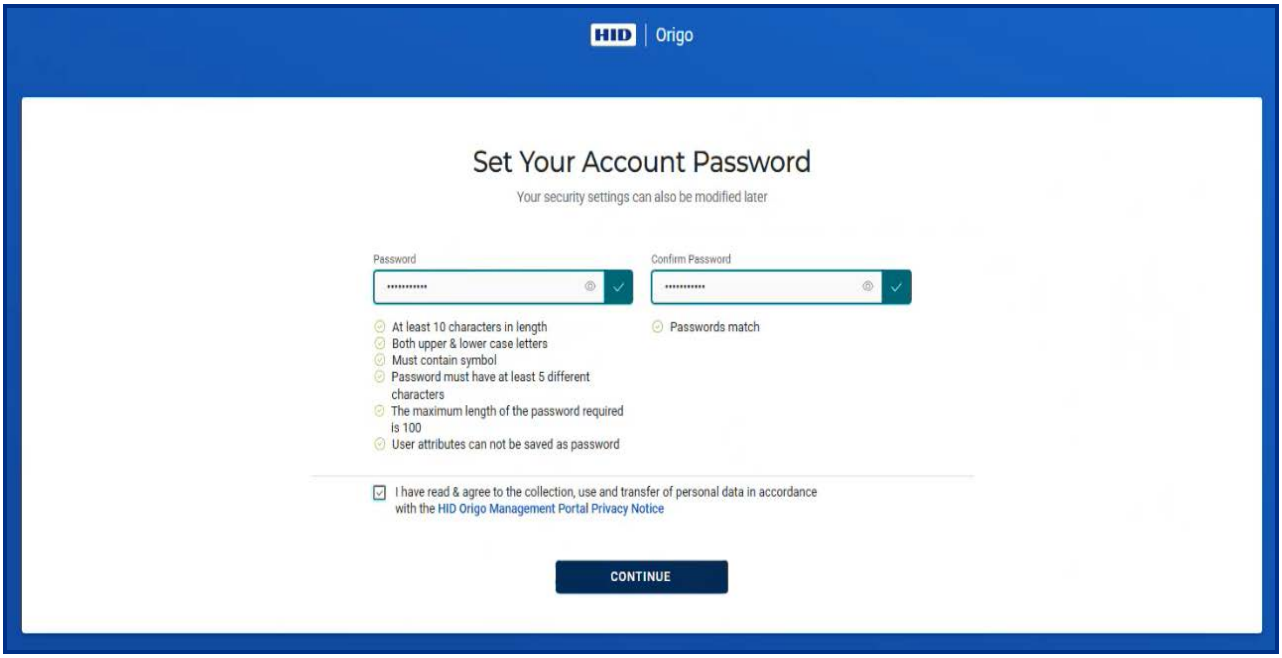
Once an Organization account has been created, an account registration notification is triggered and sent to the nominated Organization administrator.

1. In the **Complete Account Setup** notification, click **COMPLETE REGISTRATION**.

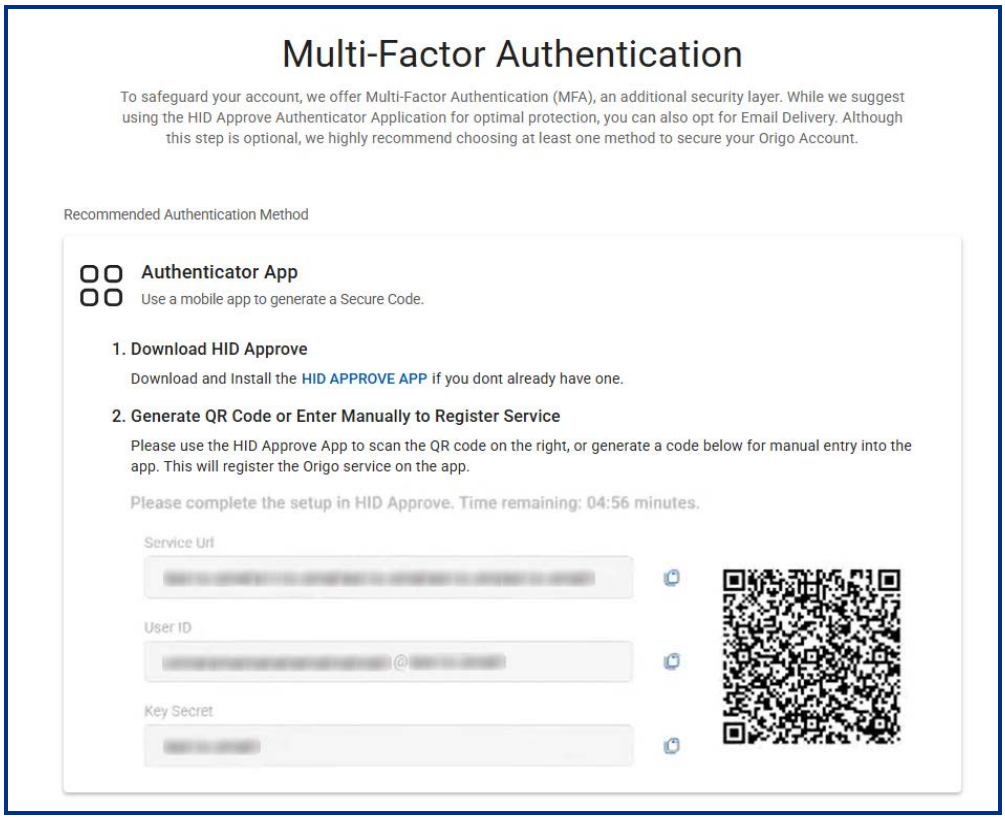
   > **Note:** The link in the account registration notification is valid for three days. After this period the system will automatically send an account registration reminder.



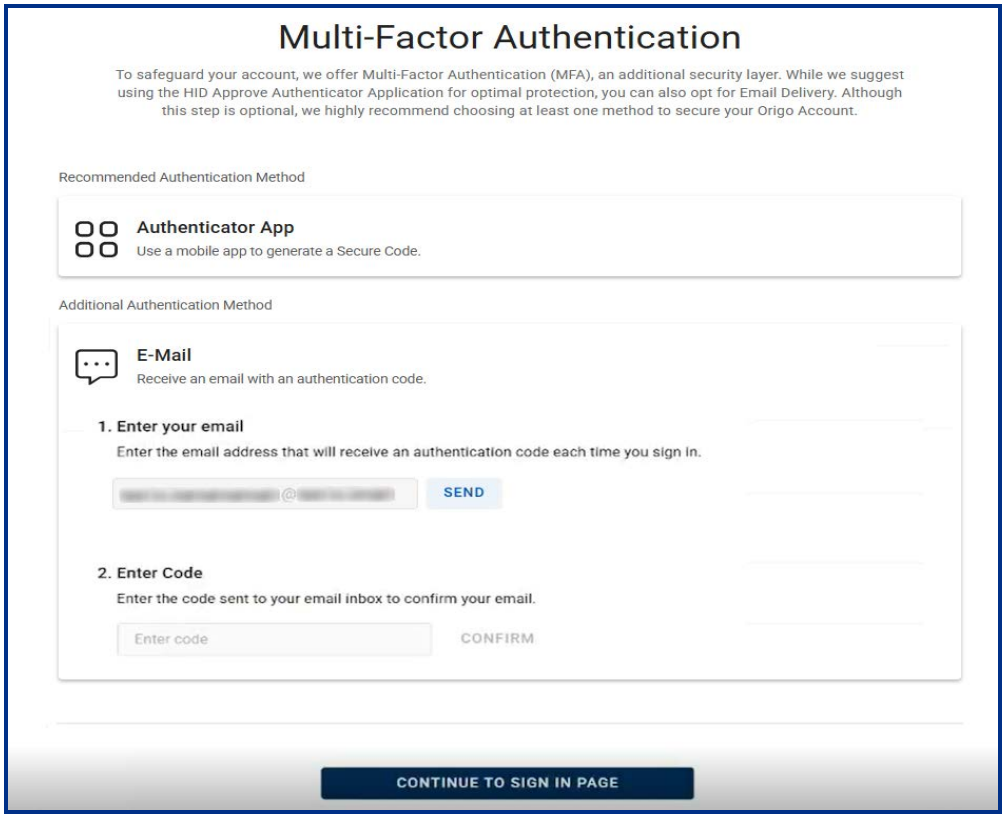
2. Set an account password, observing the displayed password requirements. Check the **HID Origo Management Portal Privacy Notice** option and click **CONTINUE**.



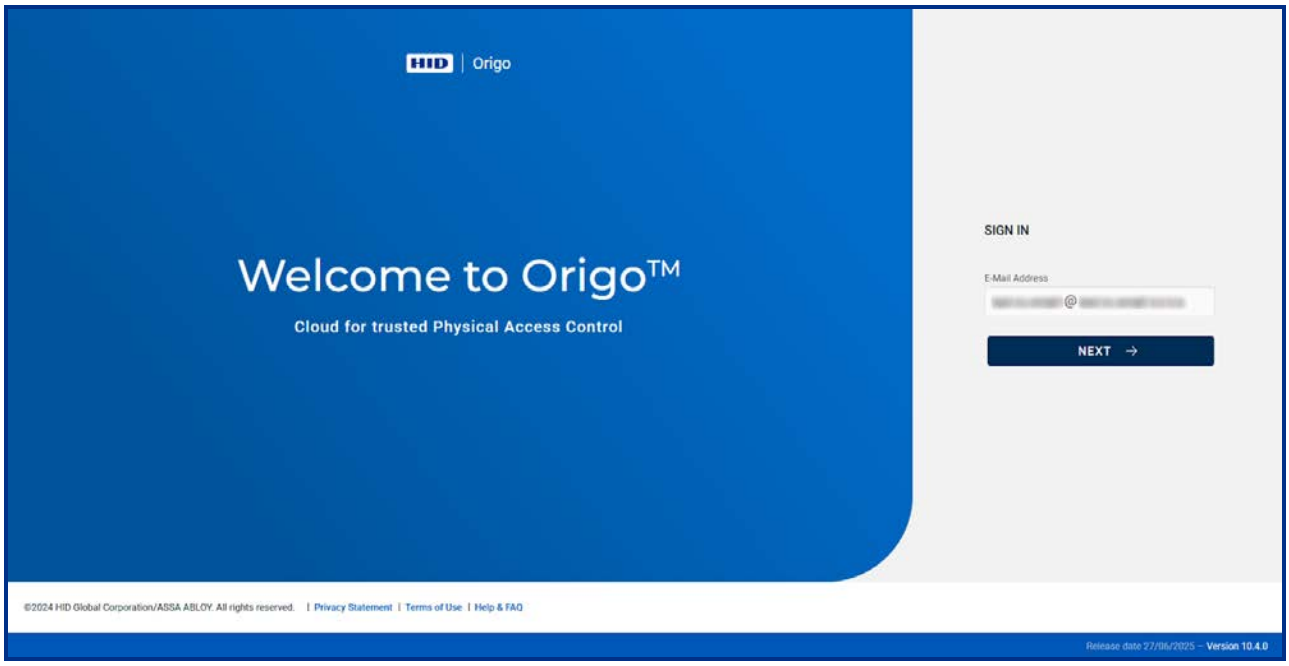
3. For additional security it is recommended that Multi-Factor Authentication (MFA) via the HID Approver App is enabled. On the **Multi-Factor Authentication** screen, under the **Authenticator App** section, click **GENERATE**. Use the HID Approve App to scan the displayed QR code or manually enter the displayed information in the Approve App to register the Origo Service on the App.



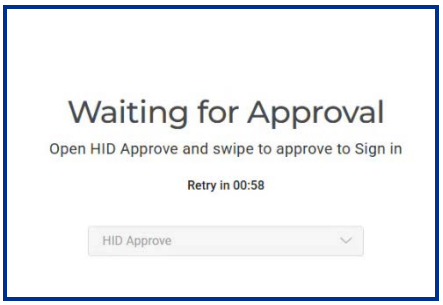
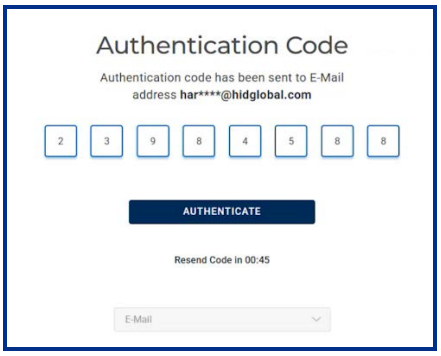
4. Also, as an option, an additional authentication method can be enabled whereby a code is sent by email. On the **Multi-Factor Authentication** screen, under the **E-Mail** section click the plus icon [⊕], enter the email address that will receive the code and click **SEND**. From the generated email, enter the code and click **CONFIRM**.
5. Once the authentication method(s) have been selected, click **CONTINUE TO SIGN IN PAGE**.



6. The Organization administrator can sign in to the [HID Origo Management Portal] as an Org Admin.

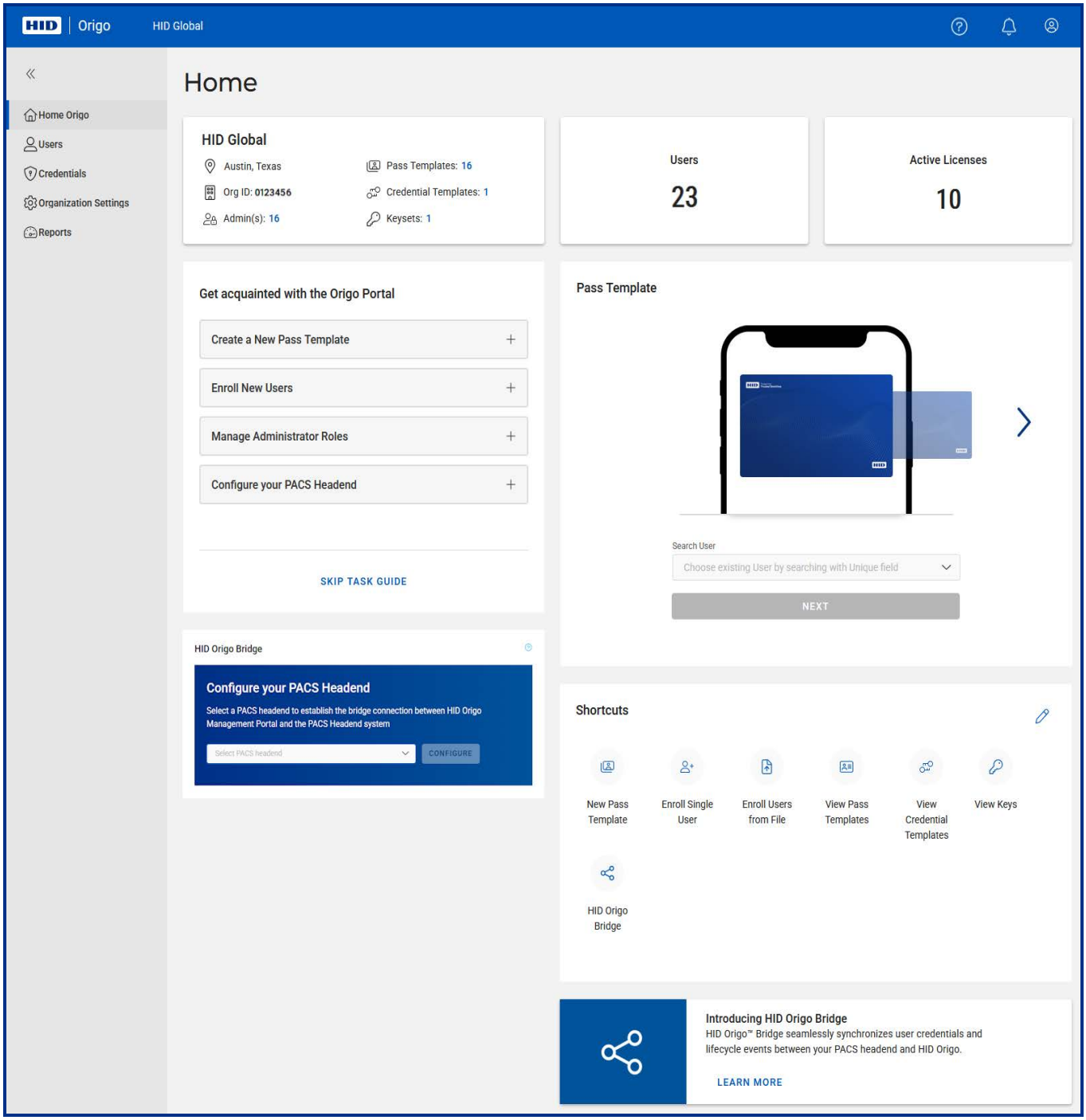


7. When Multi-Factor Authentication is enabled, approve the sign-in request via the HID Approve App or by entering the security code sent by E-Mail.

For Authentication via the HID Approve App	Open the HID Approve App and approve the sign-in request in the App.	
For Authentication via E-Mail	Enter the authentication code sent to the E-Mail address and click **AUTHENTICATE**.	

Note: For a first time Organization Onboarding the administrator must agree to the **HID Global Corporation Origo Terms of Service** before continuing to the HID Origo Management Portal.

8. After a successful authentication, the HID Origo Management Portal **Home** screen is displayed.



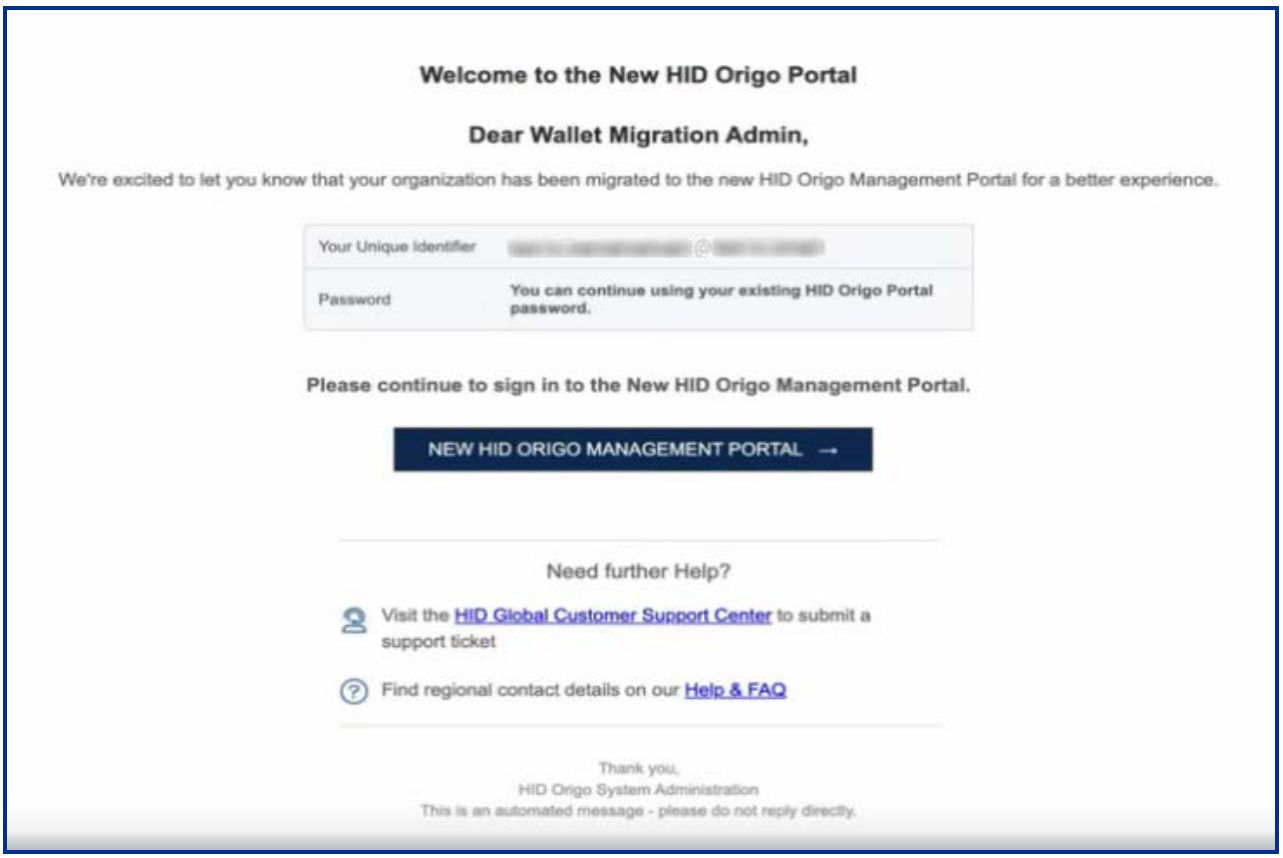
2.2 Migration to new Portal (Wallet customers only)

When existing Wallet customers are migrated to the new HID Origo Management Portal, the following information is transferred:

- Customer Data (Organization information)
- User data
- System accounts
- Admin User accounts
- License information
- User License activity

Upon a successful Organization migration to the new HID Origo Management Portal, Organization Admins are sent a notification email, directing them to sign in to the new Portal using their existing credentials (username and password). In the notification email, click the **NEW HID ORIGO MANAGEMENT PORTAL** link.

> **Note:** After migration, Organization Admins are blocked from accessing the old Portal and will be re-directed to sign in to the new Portal.

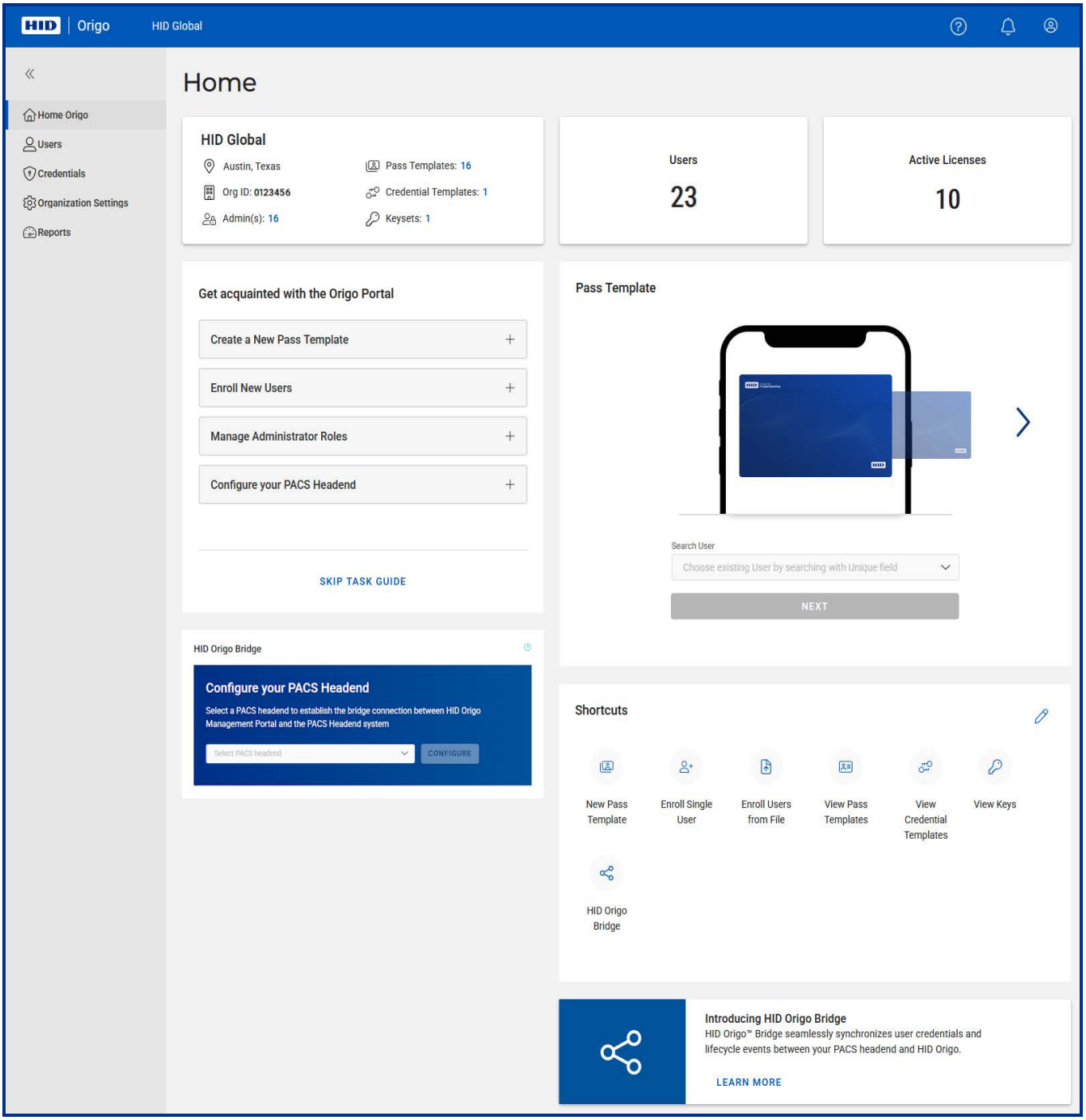


Section 03

HID Origo Management Portal Overview

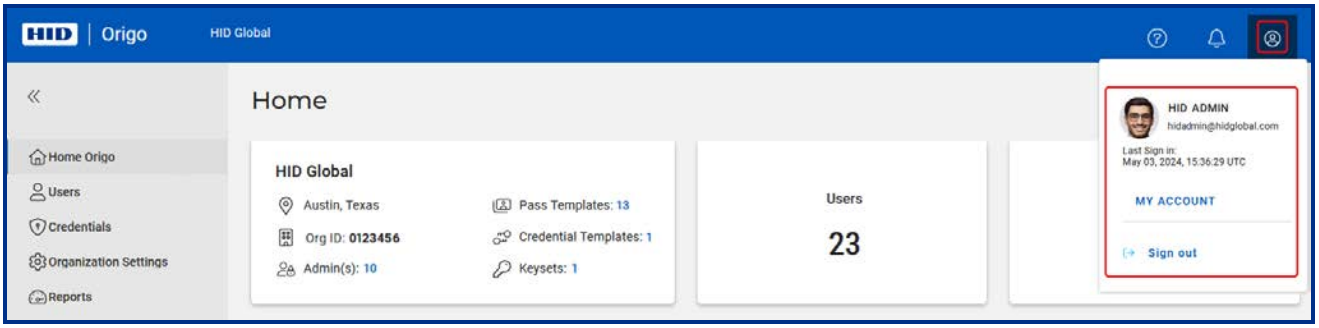
3.1 Organization Administration Home page

This section provides an overview of the Organization Administration **Home** page and navigation bar. The **Home** page allows an Organization Administrator to conduct specific tasks based on the services they have enrolled in. The navigation bar options can be used to access administration tasks relating to user, credential management, and organization settings.



3.1.1 Portal header bar

The HID Origo Management Portal header bar displays the name of the Organization, and on right side, provides a user icon [ ] menu containing user details, last sign-in information, a **My Account** link for access to user configuration settings, and a link to **Sign out** of your account. For more information see the **My Account management** section.

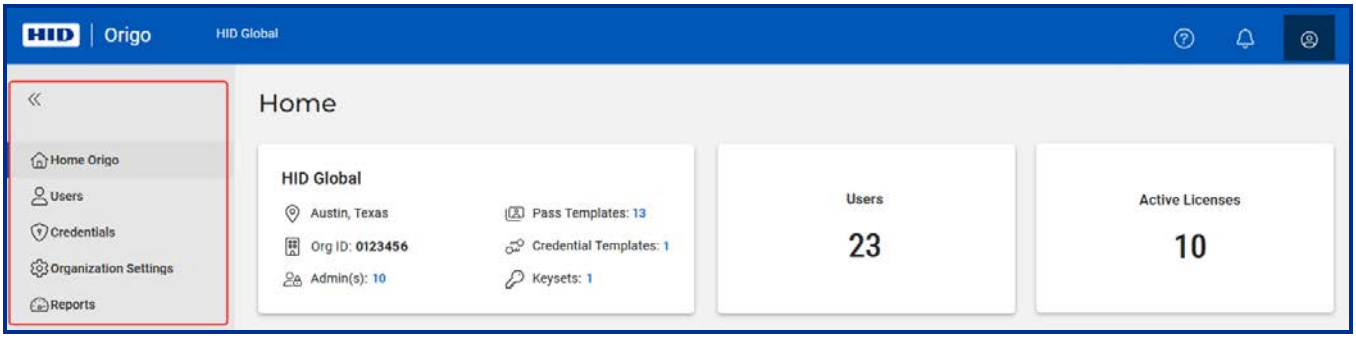


3.1.2 Portal navigation pane

The HID Origo Management Portal navigation pane, located on the left-hand side of the screen, provides quick navigation to the following sections:

- **Home Origo**: Navigation back to the HID Origo Management Portal **Home** page.
- **Users**: Provides access to the User Management section. This section lists current users, with associated user information, and allows administrators to create, manage, and delete Users. For more information see the **User Management** section.
- **Credentials**: Provides access to the Credential Management section. This section allows administrators to view and manage Pass Templates, Credential Templates, and Keysets. For more information see the **Credential Management** section.
- **Organization Settings**: Provides access to the Organization Settings section. This section allows administrators to view and edit Organization details, configure Single Sign On (SSO) settings, view Subscription plan and License information, assign new Administrators and manage existing Administrators, view User roles and permissions, and manage system accounts. For more information see the **Organization Management** section.
- **Reports**: Provides access to information related to HID Mobile Access usage, including license data and user activity. For more information see the **Report Management** section.

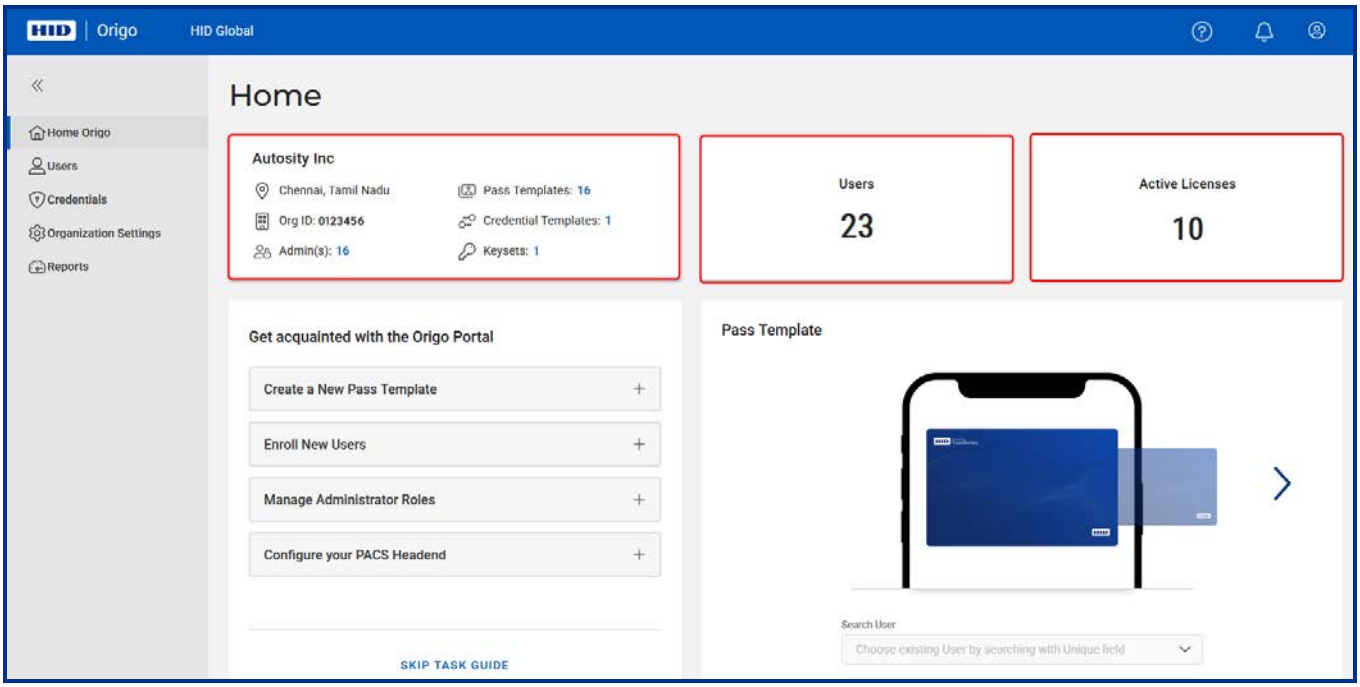
Note:
- Click the double-arrow icon in the navigation pane, to expand/collapse the navigation pane area.
- The items listed on the navigation pane will vary depending on the services your Organization has enrolled in.



3.1.3 Portal Home page widgets

The top of the HID Origo Management **Home** page area contains several widgets that display information relating to the Organization, Users, and Active Licenses:

- **Organization**: This widget displays information about your Organization, including Address, Organization ID, number of Admins, Pass Templates, Credential Templates, and Keysets. Use the hyperlinked items to directly access that item.
- **Users**: This widget displays the total number of users created for your Organization.
- **Active Licenses**: This widget displays the total number of licenses your Organization has consumed for Mobile Access.

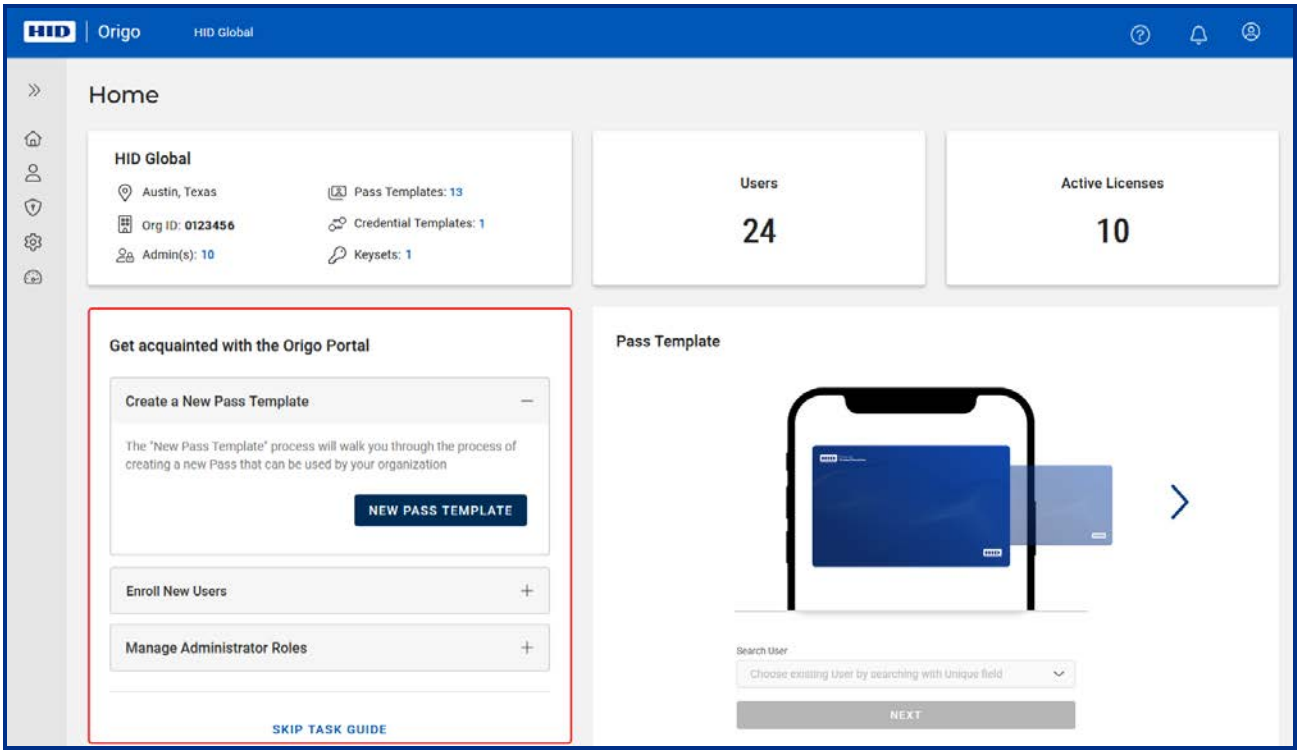


3.1.4 Get Acquainted with the Origo Portal

The **Get Acquainted with the Origo Portal** section includes several common actions that an administrator would conduct as part of their daily activities.

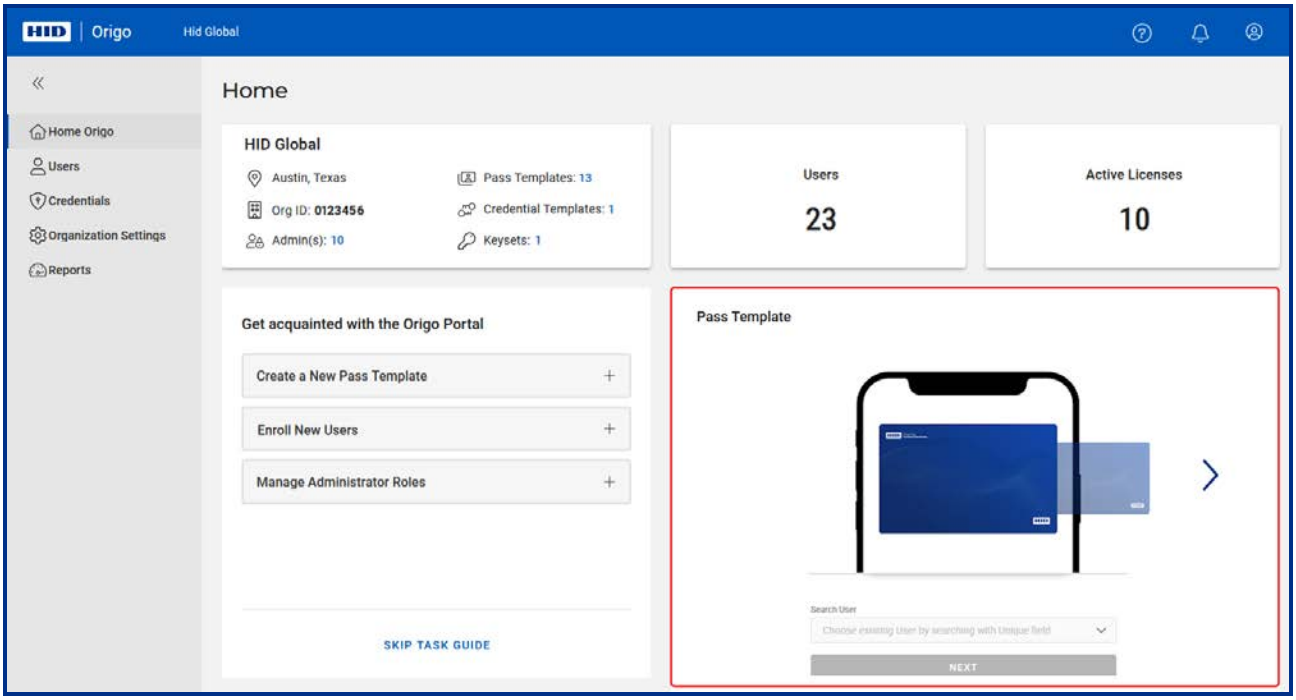
For any displayed action, click the plus icon [+] to expand the action. You can then click the included action link to access the associated process.

> **Note:** Click **SKIP TASK GUIDE** to hide the **Get Acquainted with the Origo Portal** section. The section will reappear when the Portal is reloaded in the browser.

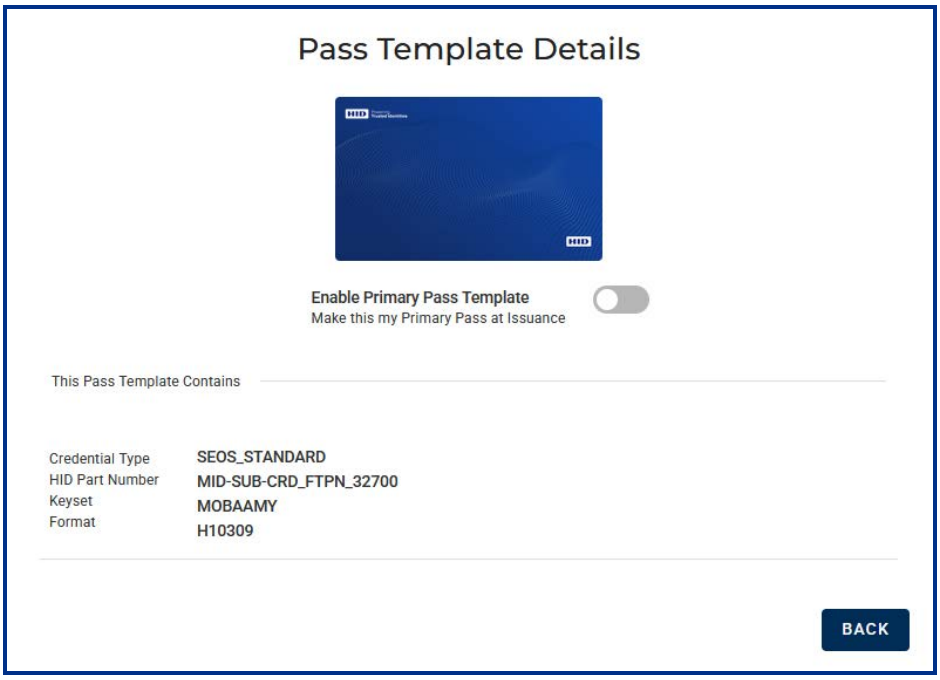


3.1.5 Pass Template

The **Pass Template** section displays all the Pass Templates associated with your Organization. If there are multiple Passes, use the arrow icons to scroll through and display the various Pass Templates.



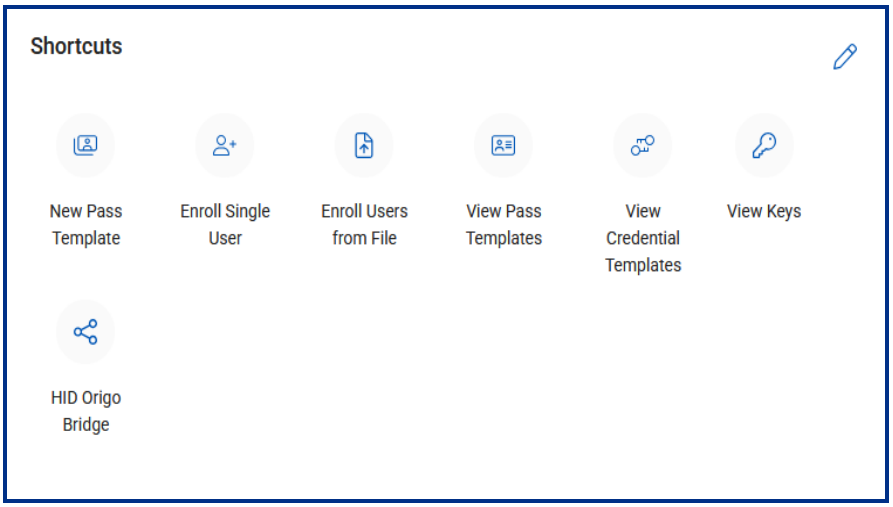
Hover over a Pass and click **View** to display information associated with the Pass as well as the credentials contained within the Pass. There is also an **Enable Primary Pass** option to make this Pass the primary Pass at issuance.



3.1.6 Shortcuts

The **Shortcuts** section contains shortcut icons that take you directly to specific areas within the portal.

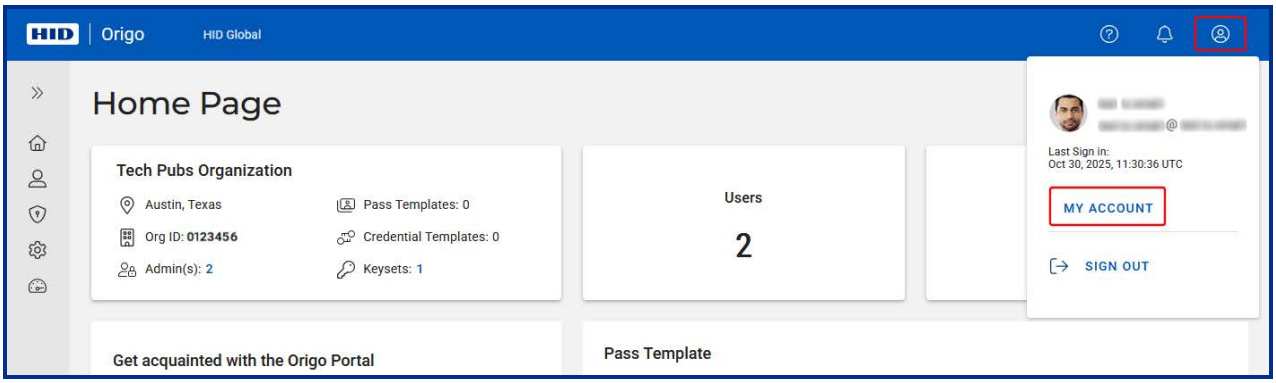
The shortcuts in this section can be customized to add, remove, and order shortcuts based on the different actions taken for your organization. Click the customize shortcuts icon [✎] to manage your shortcuts in this section.



3.2 My Account management

In the top right corner of the HID Origo Management Portal **Home** page click on the user icon [] to view user and last sign-in information. Also provided is a **My Account** link for access to user configuration settings and a link to **Sign out** of your account.

Select the **MY ACCOUNT** link to access account configuration settings.

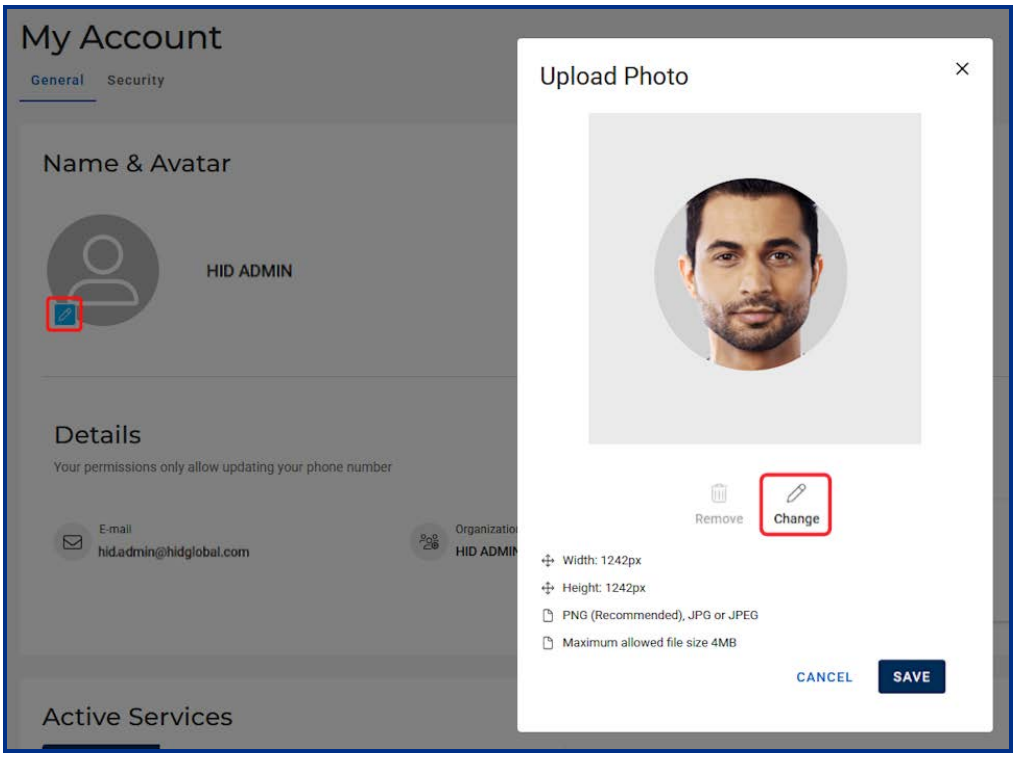


3.2.1 My Account General settings

Name & Avatar

In the **Name & Avatar** section you can update your avatar by selecting the edit avatar icon []. Click **Change** and navigate to a photo to upload. You also have the option to remove the photo that was uploaded.

> **Note:** The photo image must meet the listed dimensions, file size, and file format specification.



Details

In the **Details** section you will be able to view your email address and your Organization Role. You can also edit your phone number and country code by clicking on the edit icon [✎].



Active Services

The **Active Services** section displays the services that your Organization is enrolled in.



Time Zone

In the **Time Zone** section, search for your specific time zone and save the selection by clicking on **UPDATE TIME ZONE**.



Privacy Agreement

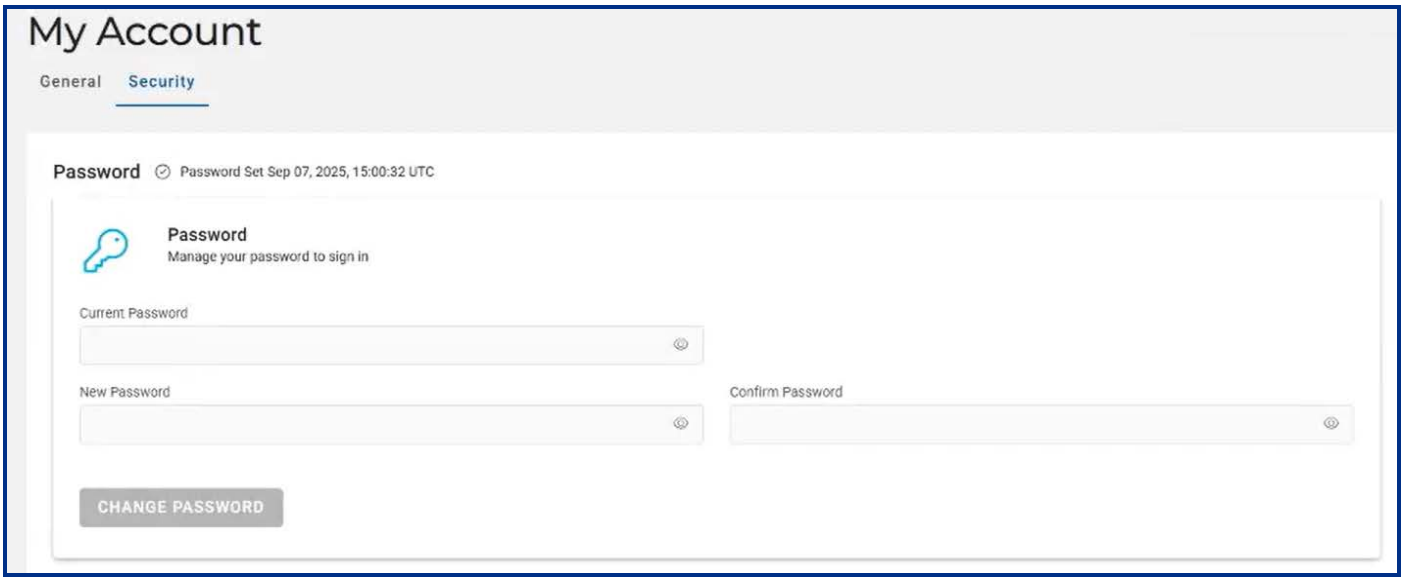
In the **Privacy Agreement** section, click on the link to access the HID Global Privacy Notice.



3.2.2 My Account Security settings

Password

In the **Password** section you can change the password used to sign-in to the Portal.



Multi-Factor Authentication

In the **Multi-Factor Authentication** section, authentication via the HID Approve App or authentication via a security code sent by E-Mail can be enabled or disabled.

> **Note:** For an additional layer of security on your account it is recommended that Multi-Factor Authentication (MFA) via the HID Approve App is enabled.

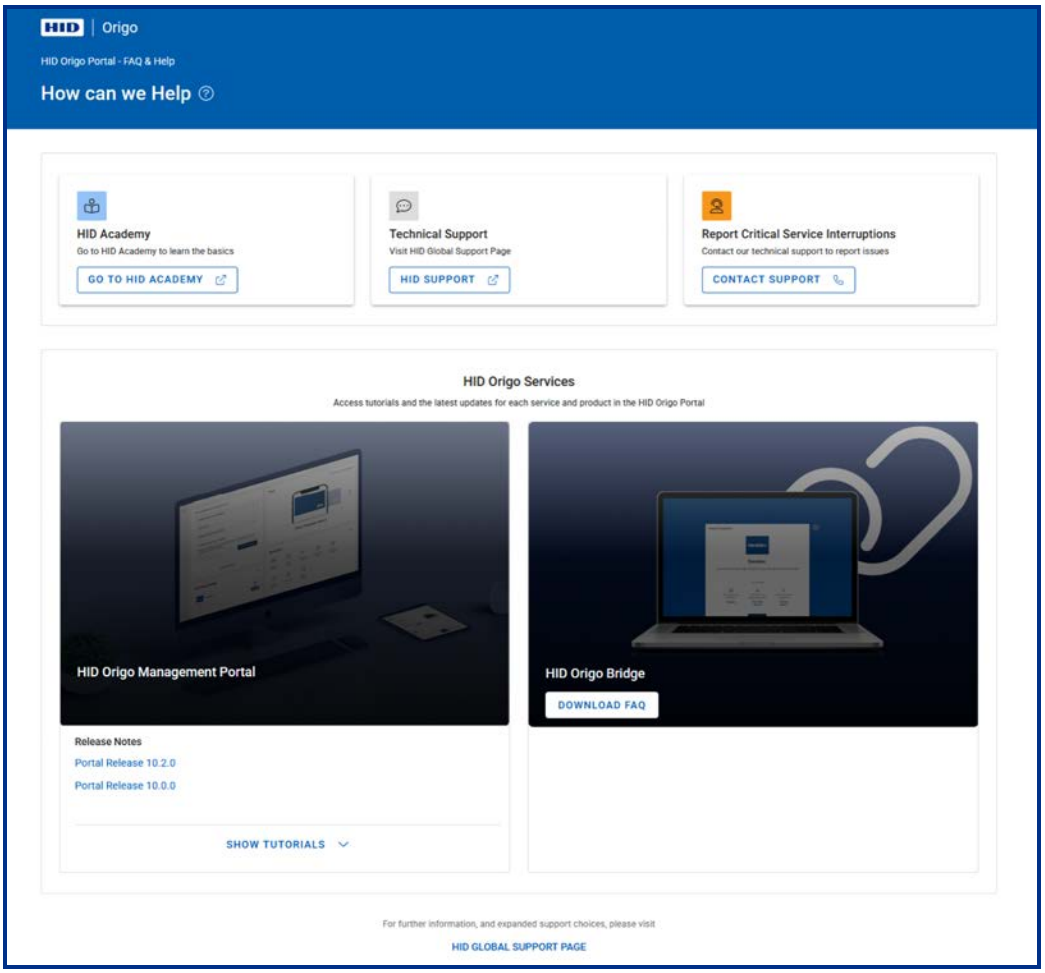


3.3 Portal Help Center

To access the Help Center, at the bottom of the HID Origo Management Portal login page, click the **Help & FAQ** link. The Help Center can also be accessed from Portal screens by clicking on the Help Center icon [?] in a screen header.



The Origo Portal Help Center provides links to the HID Training Academy and Technical Support, as well as a reporting mechanism if you experience issues or problems. The Help Center also provides Origo Portal service- related resources such as documentation, release notes, and tutorials.



Section 04

User Management

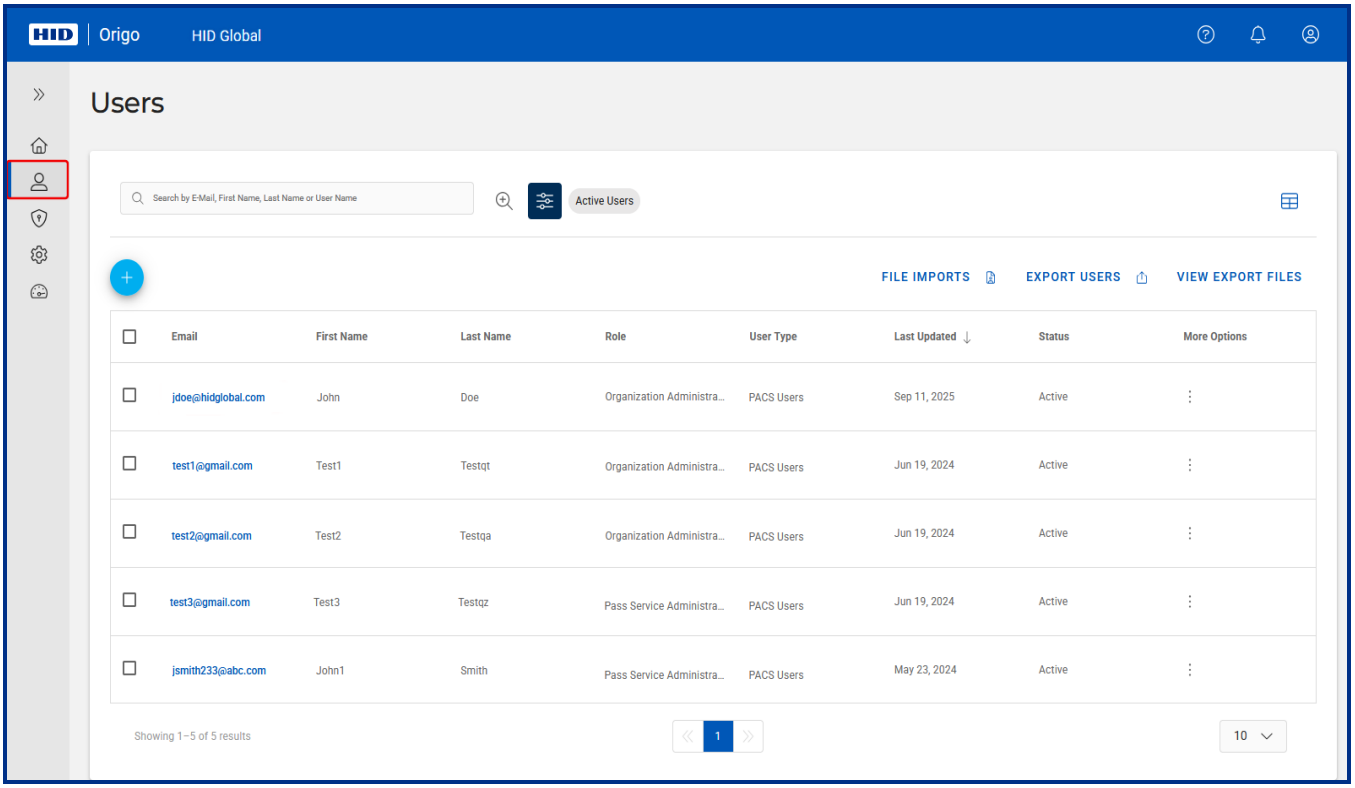
4.1 User management overview

On the Organization **Home** screen, from the left navigation menu, select the **Users** option. The **Users** screen displays a list of users and associated user information such as **Name**, **Email**, **User ID**, **Role**, **User Type**, and **Last Updated**. The **Users** screen also provides administrators with options to:

- Create new users. See the **Enroll new Users** section.
- View and edit user details and profile information. See the **User profile management** section.
- Search and filter users based on selectable parameters, see the **User search and filtering** section.
- View and manage user Passes. See the **User Pass management** section.
- Delete users. See the **Delete a User** section.
- View previously imported files. See the **View file imports** section.
- Export user records. See the **Export Users** section.

The user information grid can be customized by clicking on the customize user grid icon [ ], selecting the user details to display in the grid, and clicking **SAVE AND APPLY**. Information displayed under each column can be ranked in ascending or descending order by selecting the ranking icon [ ] associated with a column heading.

On the **Users** page you can also search for users and filter displayed users based on selectable parameters, see the **User search and filtering** section.



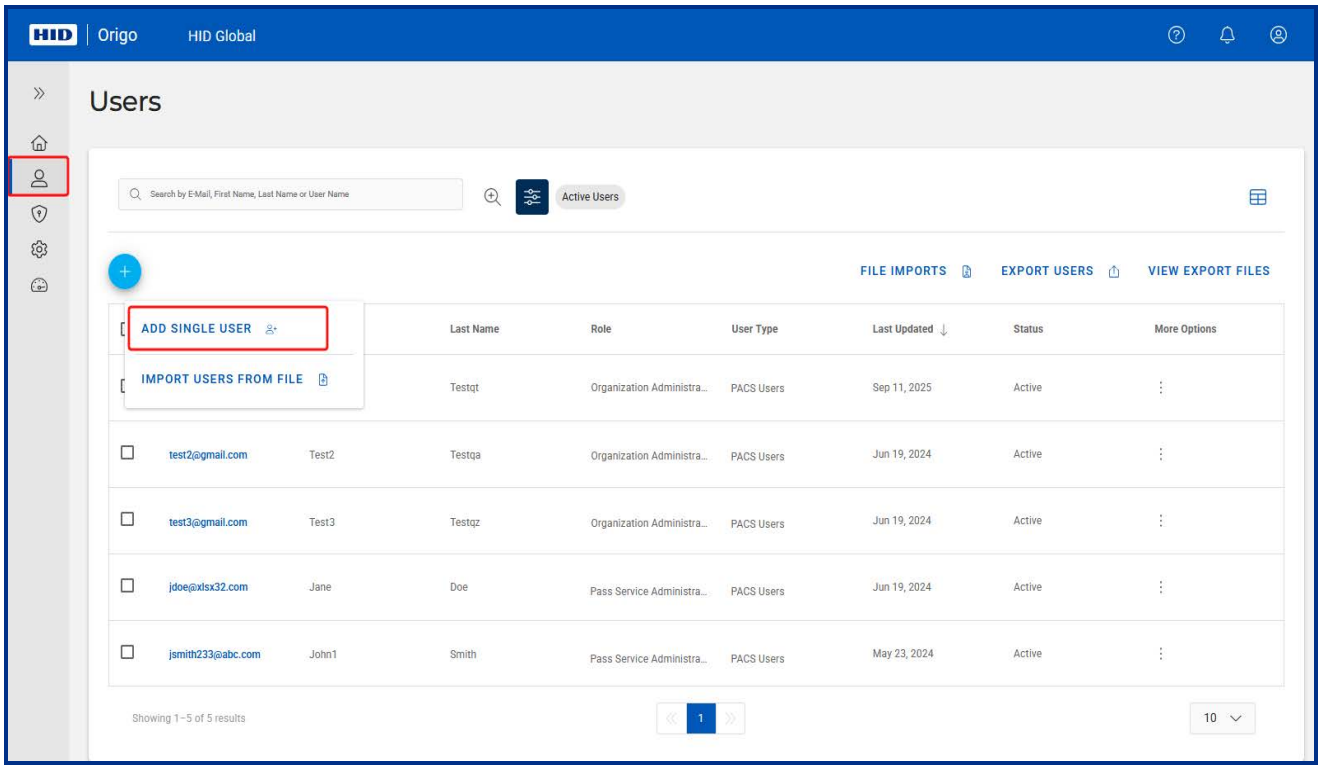
4.2 Enroll new Users

Users can be enrolled and issued a pass individually or a file can be used to bulk enroll multiple users.

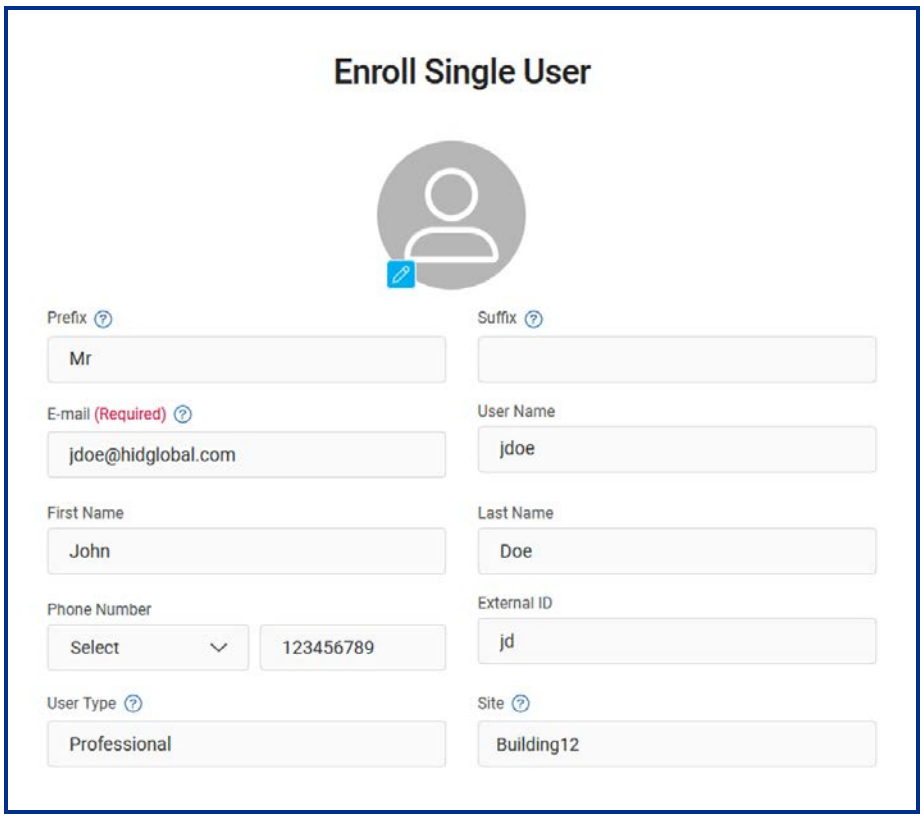
4.2.1 Enroll a single user

1. From the left navigation panel select the **Users** option.
2. On the **User** screen, click the enroll user icon [+] and select **ADD SINGLE USER**.

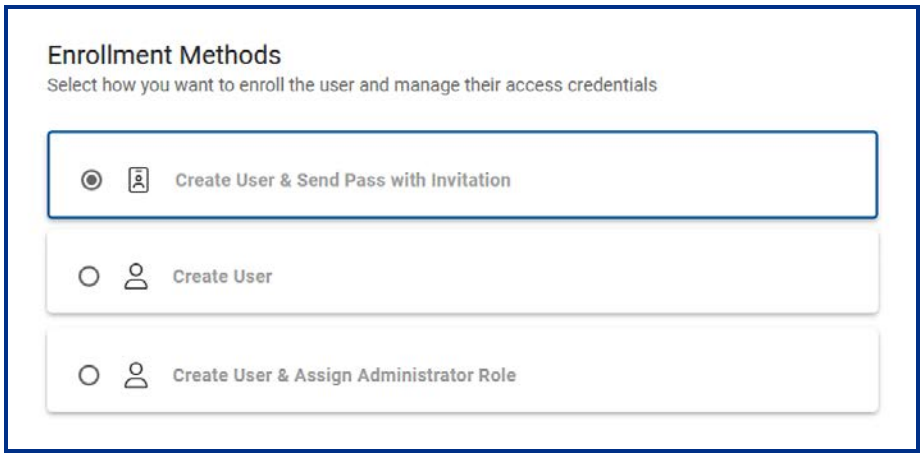
> **Note:**
> Alternatively single users can be enrolled from the Portal **Home** screen:
> - In the **Get acquainted with the Origo Portal** section, click **Enroll New Users** > **Single User**.
> - In the **Shortcuts** section, click **Enroll Single User**.



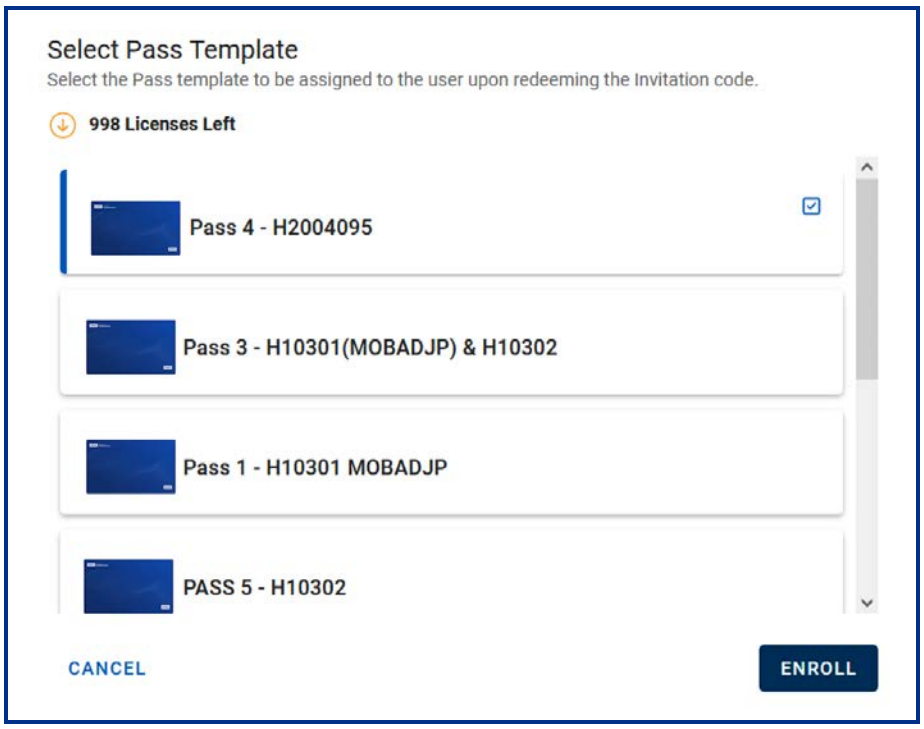
3. In the **Enroll Single User** screen:
   - Upload a user photo by selecting the edit icon [ ]. In the **Upload Photo** dialog, click **Change** and navigate to a photo to upload (the photo image must meet the listed dimensions, file size, and file format specification).
   - Enter the new user details in the displayed fields.



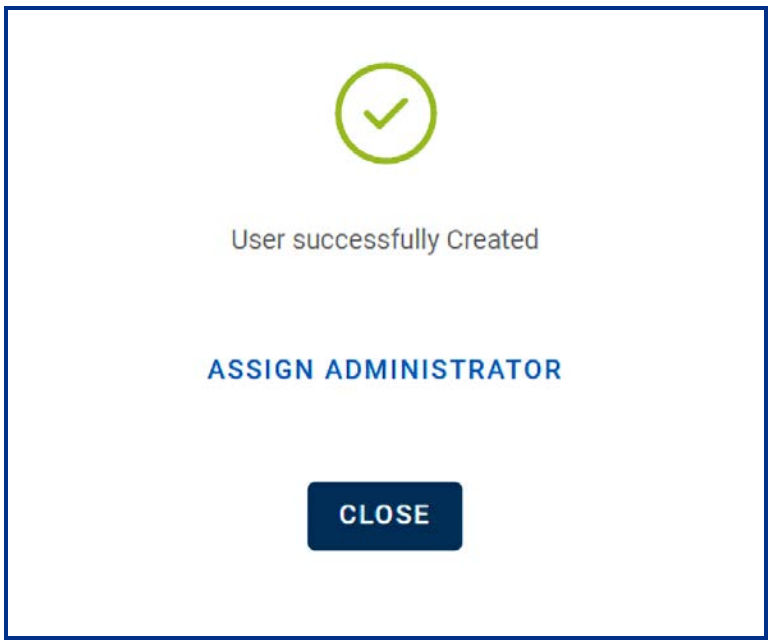
4. In the **Enrollment Methods** section, select an option for how to enroll the user and manage their access credentials.



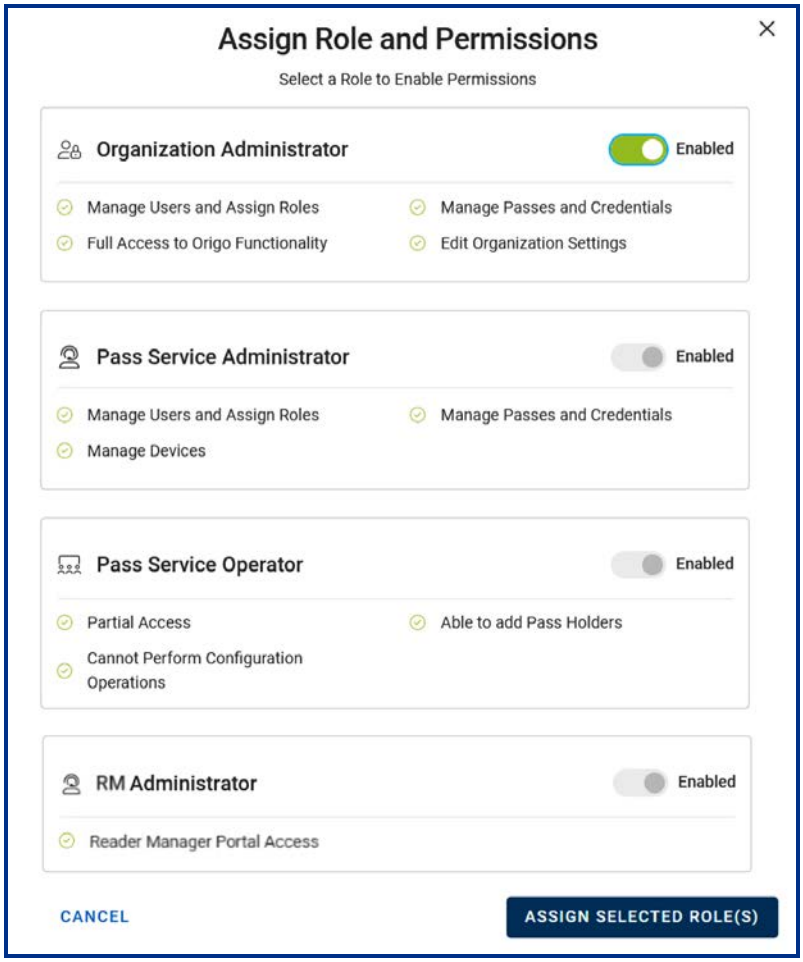
5. In the **Select Pass Template** section, select the Pass Template to be assigned to the user when the invitation code is redeemed and click **ENROLL**.



6. The user has now been created, click **CLOSE** to go back to **User** screen, or click **ASSIGN ADMINISTRATOR** to make this user an administrator.



7. On the **Assign Role and Permissions** screen, enable the required role and associated permissions for the user and click **ASSIGN SELECTED ROLE(S)**.



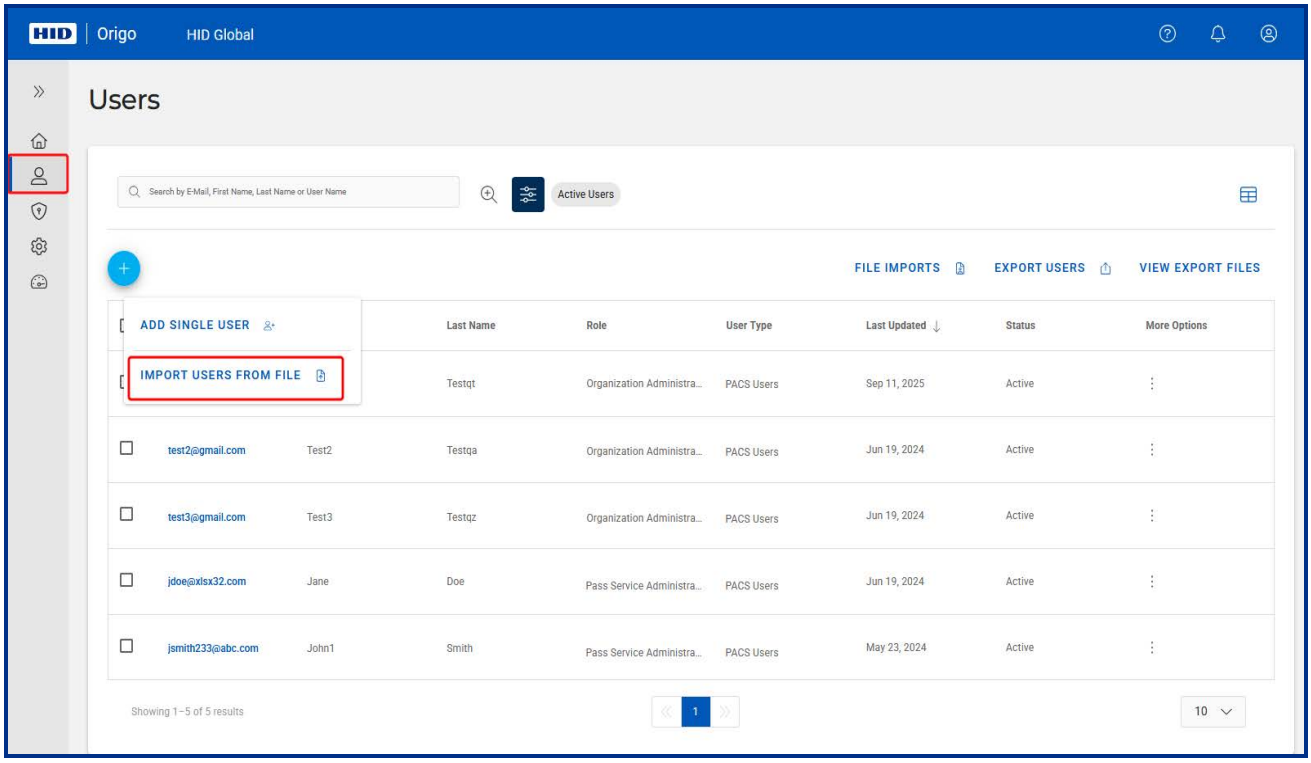
Role	Permission
Organization Admin	• Manage Users and Assign Roles • Manage Passes and Credentials • Full Access to Origo Functionality • Edit Organization Settings
Pass Service Administrator	• Manage Users and Assign Roles • Manage Passes and Credentials • Manage Devices
Pass Service Operator	• Partial Access • Able to add Pass Holders • Cannot Perform Configuration Operations
RM Administrator	• Reader Manager Portal Access

Note: Roles are hierarchical, therefore if you enable Organization Administrator, you will also have Pass Service Administrator and Pass Service Operator enabled. If you enable Pass Service Administrator, you will also have Pass Service Operator enabled.

4.2.2 Enroll multiple users

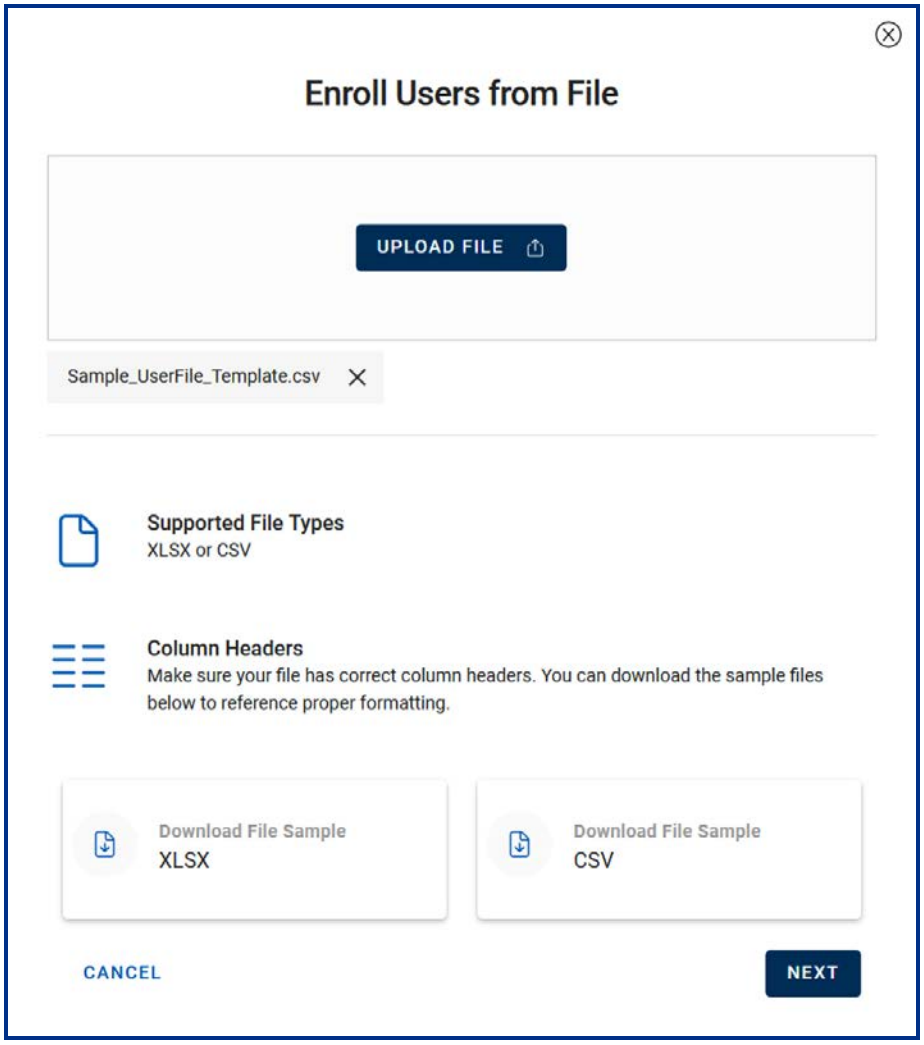
1. From the left navigation panel select the **Users** option.
2. On the **User** screen, click the enroll user icon [+] and select **IMPORT USERS FROM FILE**.

> **Note:**
> Alternatively single users can be enrolled from the Portal **Home** screen:
> - In the **Get acquainted with the Origo Portal** section, click **Enroll New Users** > **Import from file**.
> - In the **Shortcuts** section, click **Enroll Users from File**.



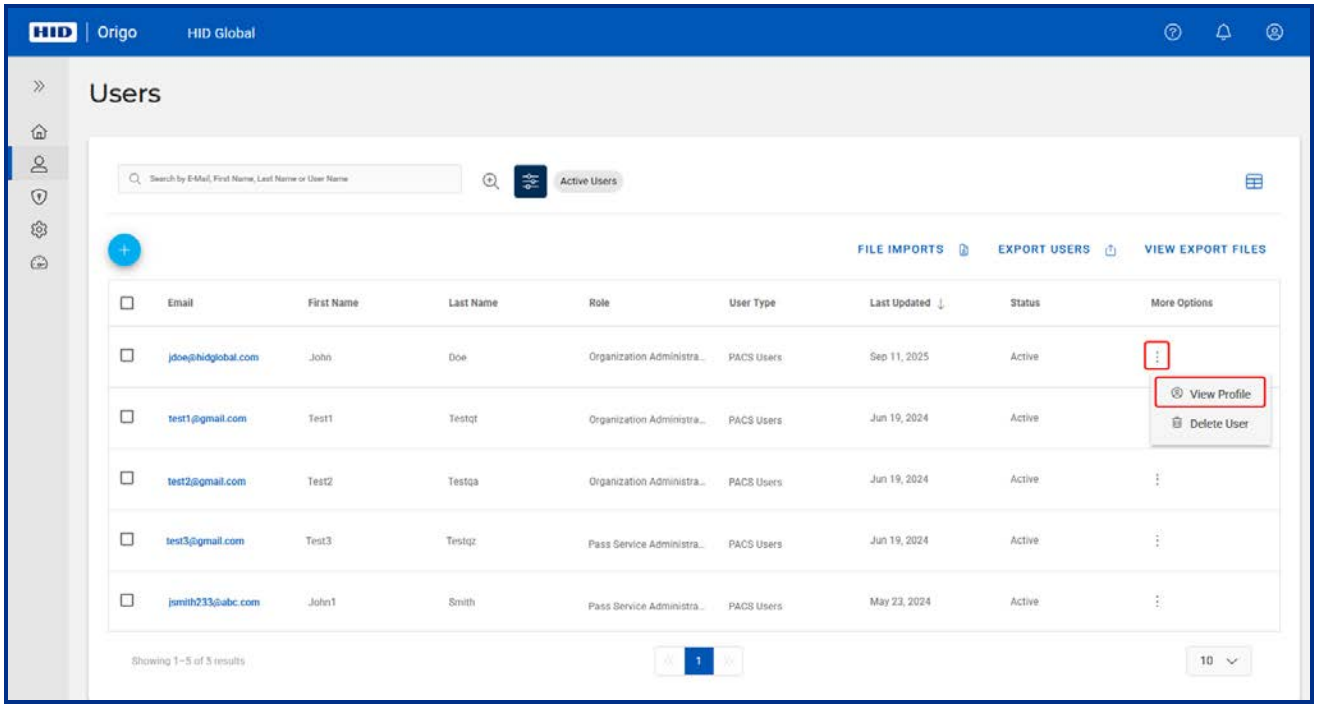
3. In the **Enroll Users from File** screen, click **UPLOAD FILE** and select your user file to upload. Supported file formats are **.xlsx** or **.csv**.

> **Note:** From the **Enroll Users from File** screen you can download sample **.xlsx** or **.csv**. files that contain the correct column headers. These can be used to enter your user details and upload.

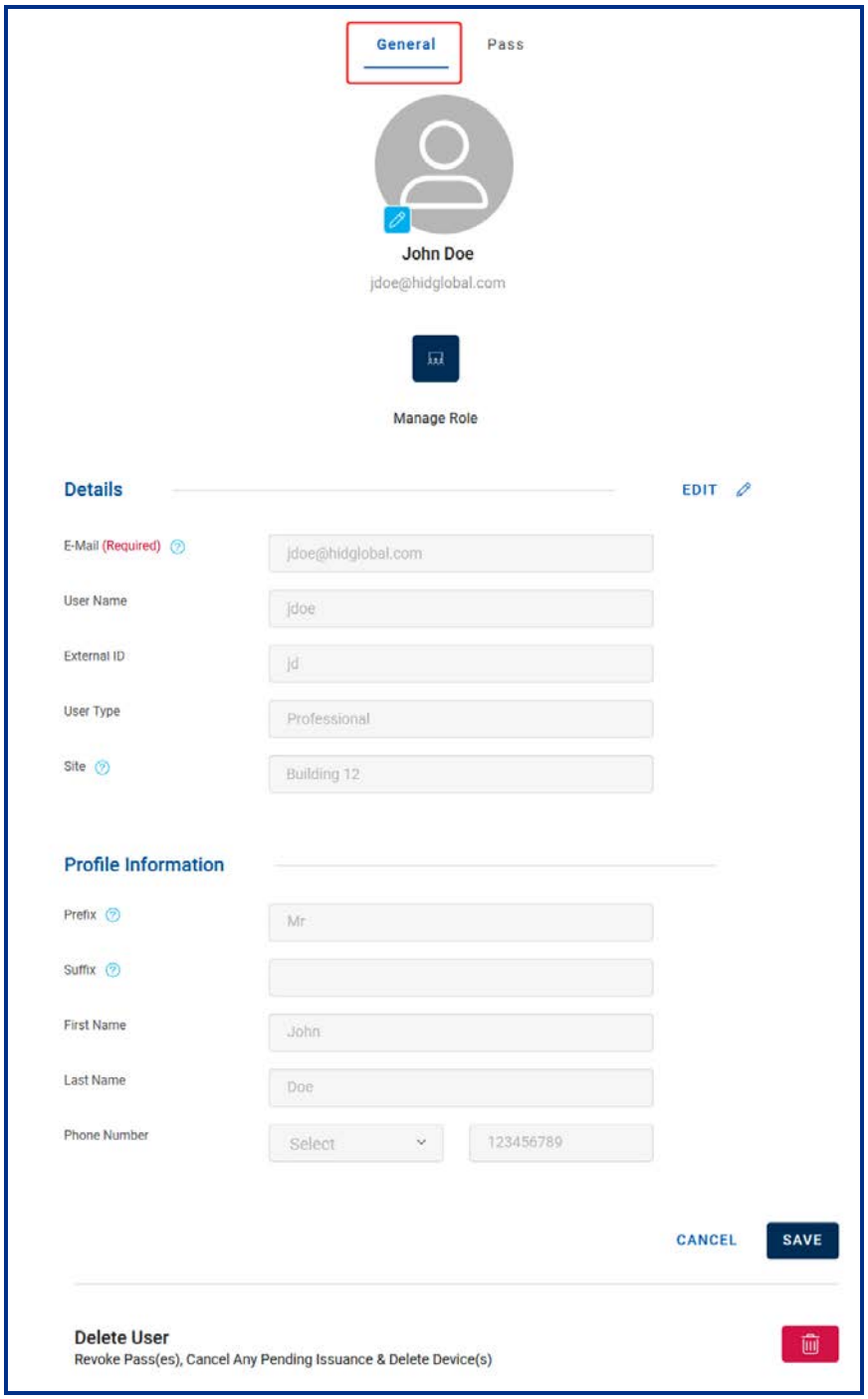


4.3 User profile management

1. On the **Users** screen, click on an email hyperlink from the **Email** column or click the ellipses icon [⋮] associated with a displayed user and select the **View Profile** option.



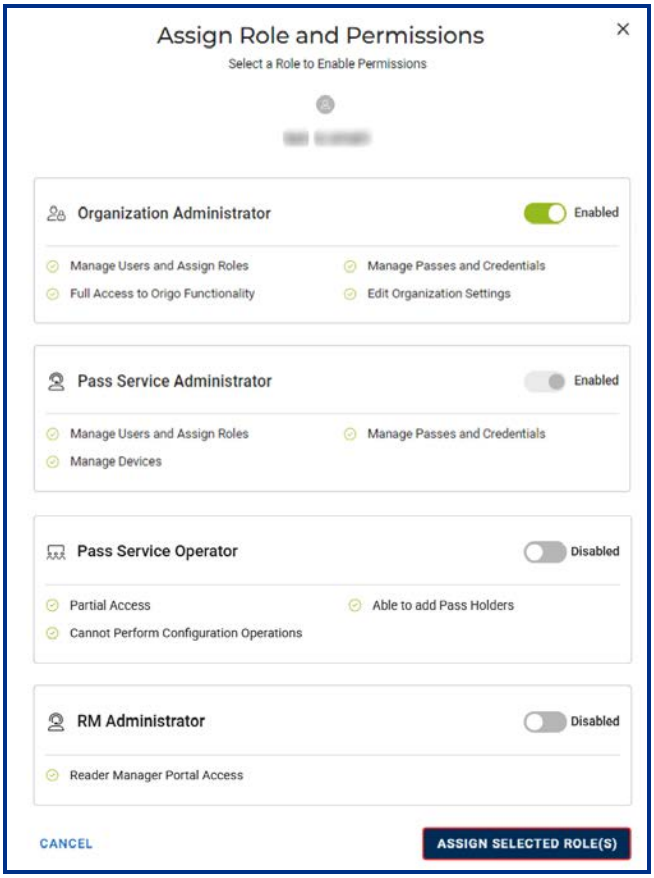
2. Select the **General** option to view or edit user details and profile information.
   - Click the Upload Photo icon [✎] to upload a user photo (the photo image must meet the listed dimensions, file size, and file format specification).
   - Select **Manage Role** to assign a selected role or roles for the user, see **Manage Administrator Roles**.
   - Click **EDIT** to edit details and profile information associated with the user. Click **SAVE** to save any edits.
   - Click the **Delete User** icon [🗑] to delete the user.



4.3.1 Manage Administrator Roles

Enable the required roles and associated permissions for the user and click **ASSIGN SELECTED ROLE(S)**.

Note: Enable a role to select the associated permissions.



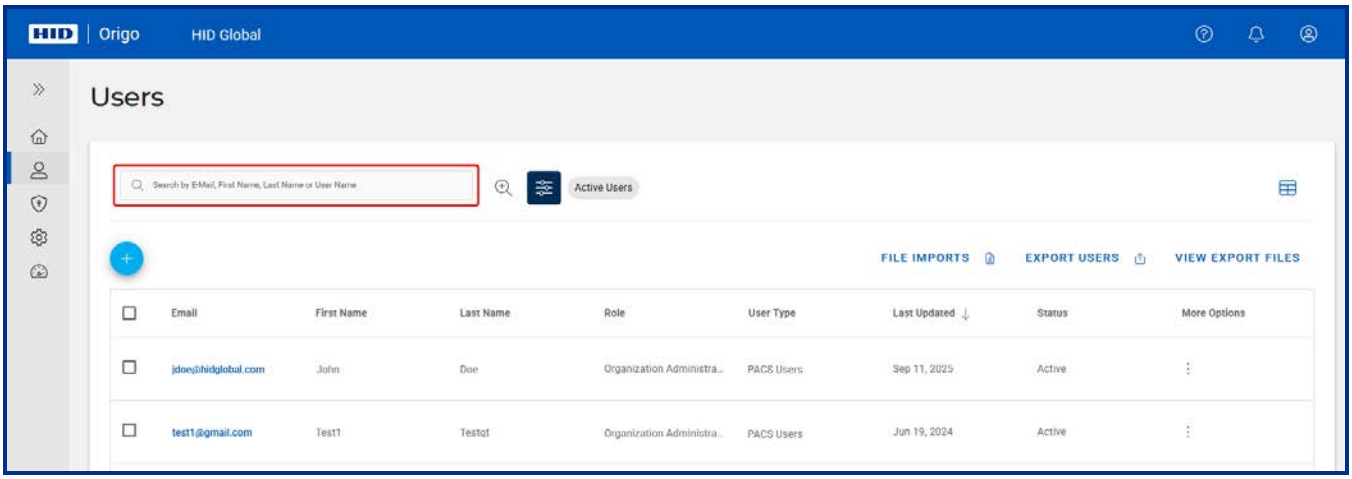
Role	Permission
Organization Admin	• Manage Users and Assign Roles • Manage Passes and Credentials • Full Access to Origo Functionality • Edit Organization Settings
Pass Service Administrator	• Manage Users and Assign Roles • Manage Passes and Credentials • Manage Devices
Pass Service Operator	• Partial Access • Able to add Users
RM Administrator	• Reader Manager Portal Access

Note: Roles are hierarchical, therefore, if you enable Organization Administrator, you will also have Pass Service Administrator and Pass Service Operator enabled. If you enable Pass Service Administrator, you will also have Pass Service Operator enabled.

4.4 User search and filtering

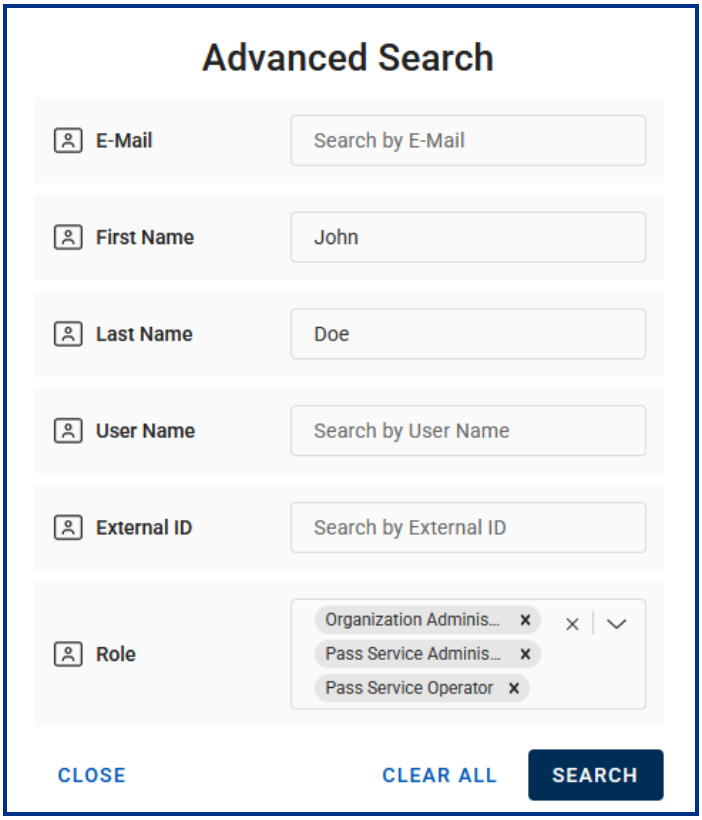
4.4.1 User search

On the **Users** screen, enter a user **E-Mail**, **First Name**, **Last Name**, or **User Name** in the search field to display users based on the entered search option.



To search and display users based on multiple criteria, click the advanced search icon [🔍], select required search options, and click **SEARCH**.

> **Note:** Click **CLEAR ALL** to clear all the selected search options.

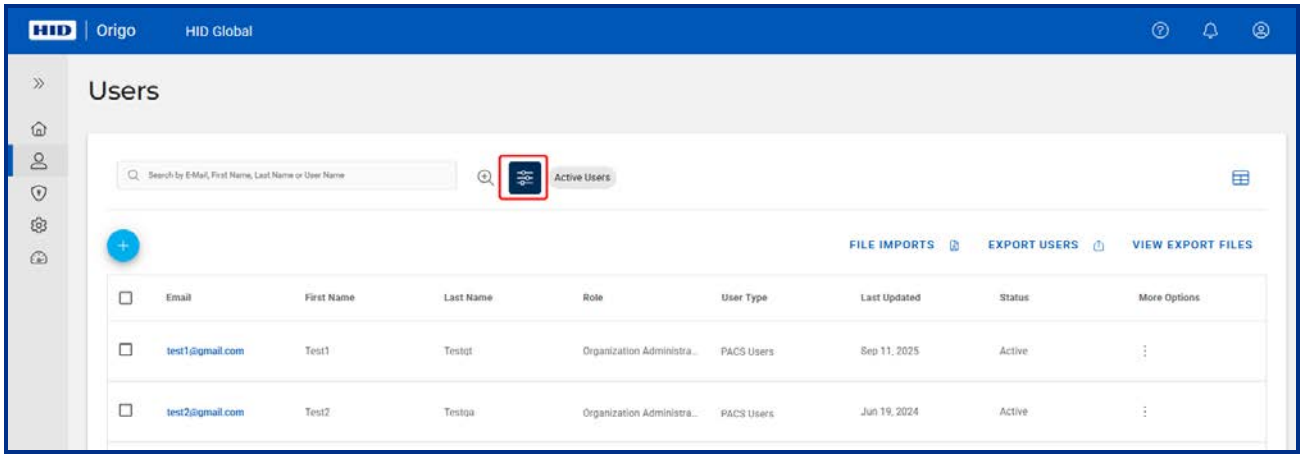


4.4.2 Filter users

Displayed users can be filtered based on **User Status** and/or **Pass Status**.

> **Note:** The search and filter functions can be used in combination to refine the displayed list of users.

1. Click on the user filter icon [ ].

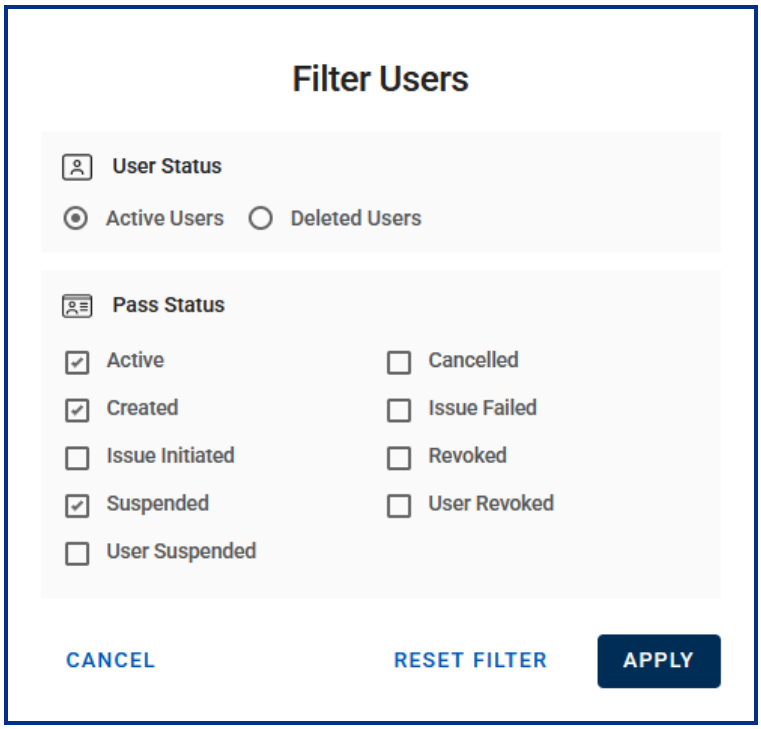


2. Select the required **User Status** (the default is **Active Users**) and the associated **Pass Status** options.

> **Note:** If **Active Users** is selected, all the **Pass Status** options are available. If **Deleted Users** is selected only the **Cancelled**, **Revoked**, and **User Revoked** options are available.

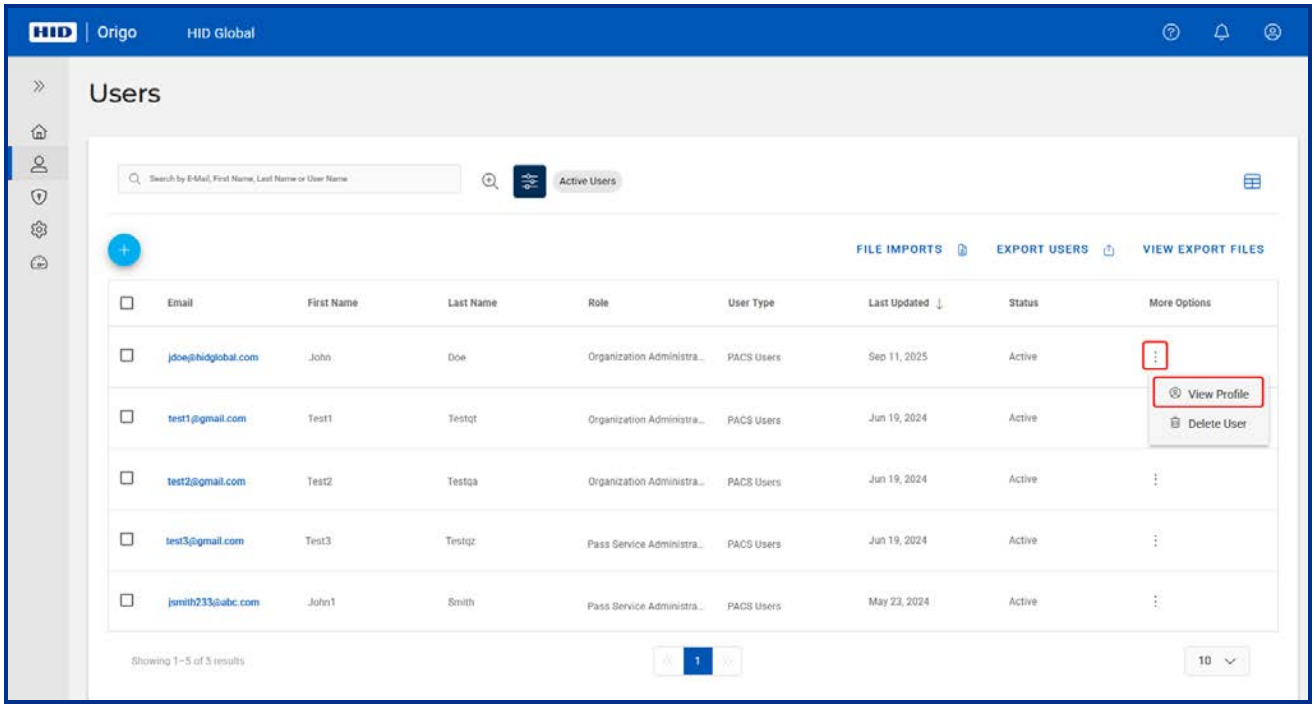
3. Click **APPLY** to list users with the selected filter parameters.

> **Note:** Click **RESET FILTER** to clear all the selected filter options.

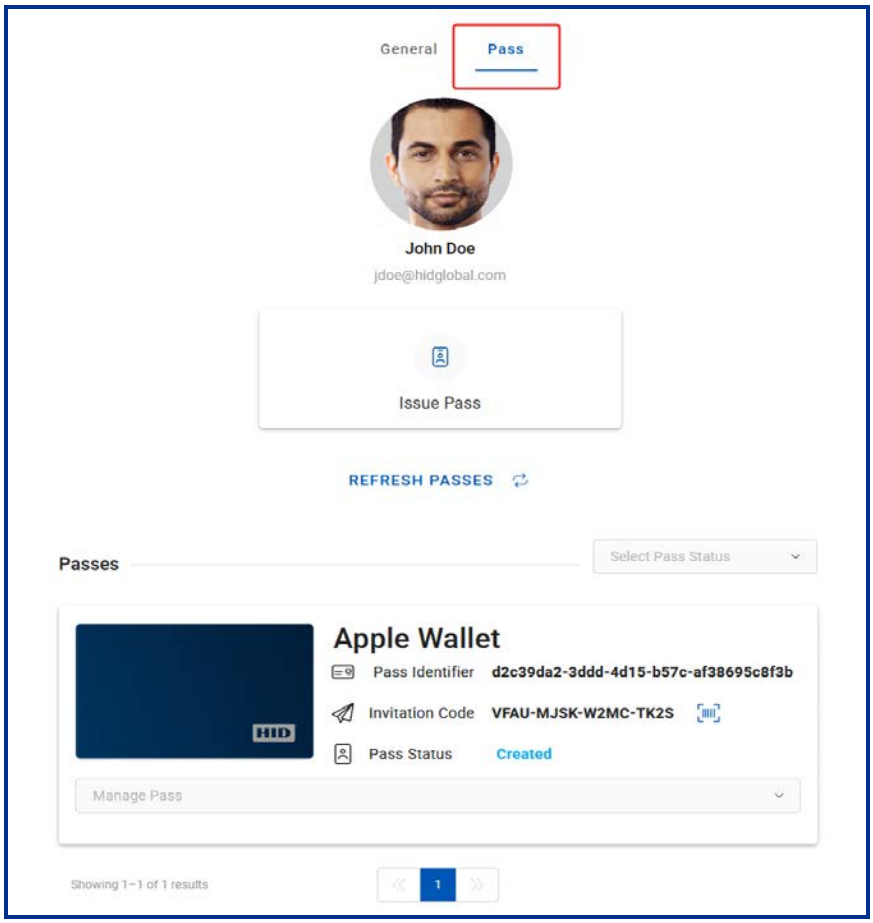


4.5 User Pass management

1. On the **Users** screen, click on an email hyperlink from the **E-mail** column or click the ellipses icon [⋮] associated with a displayed user.
2. Select the **View Profile** option.



3. Select the **Pass** option to view and manage the Passes associated with the user.
   - For a displayed pass click the associated QR code icon to generate an invitation QR code that can be scanned with the Mobile Access App.
   - Click **Select Pass status** and select a status option to filter displayed Passes based on the selected status.
   - Click **Manage Pass** and select a status option to apply the selected status to an issued Pass.

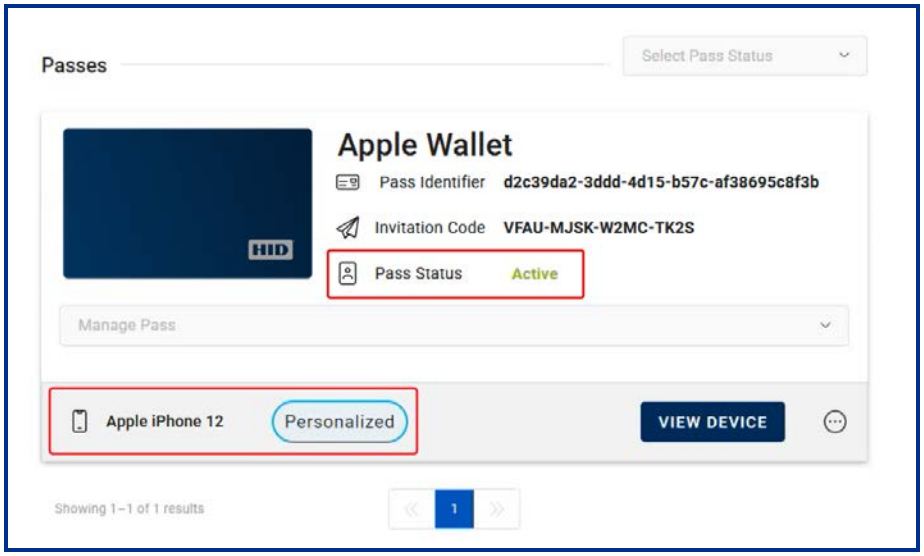


4. For a displayed Pass hover your cursor over a Pass image and click **View** to display information associated with the Pass as well as the credentials contained within the Pass.

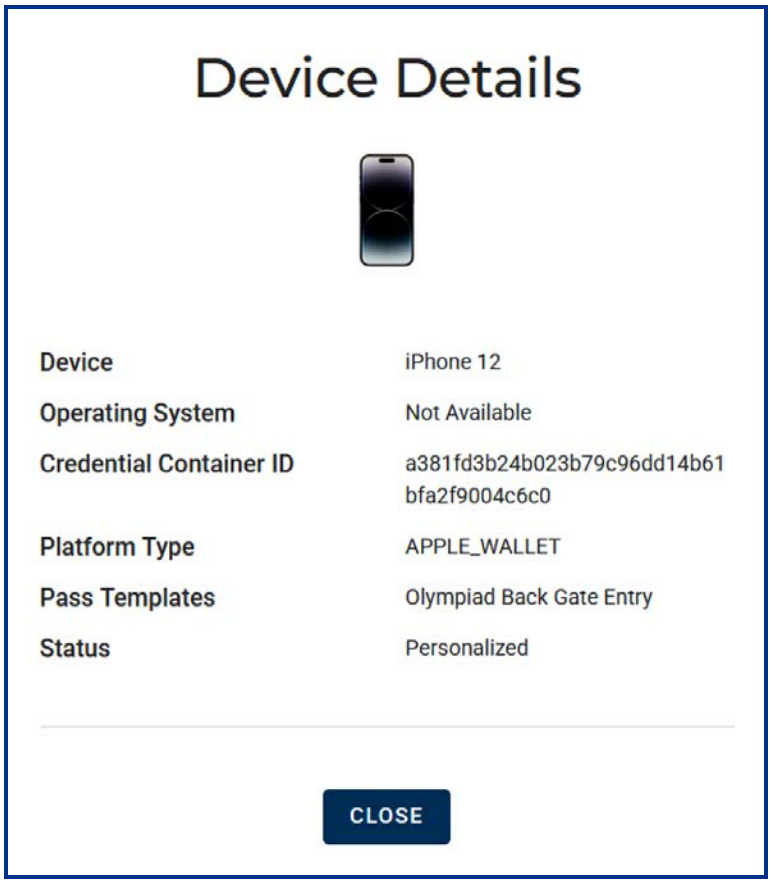


5. Once a Pass has been issued and redeemed by the end user in the Mobile Access App (refer to the **User Pass provisioning via Single Sign On (SSO)** section), the Pass status changes to **Active** and device information is displayed.

> **Note:** To delete the device, click the delete device ellipses icon [⋯] and select **Delete device**.



6. In the **Passes** section, click **VIEW DEVICE** to view device details.

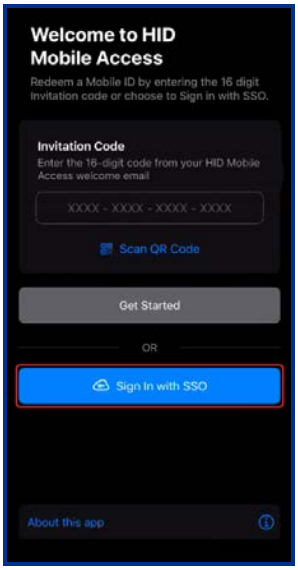


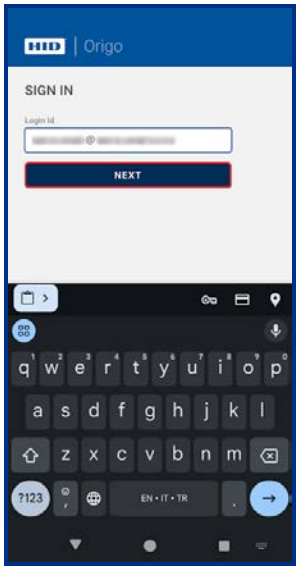
4.6 User Pass provisioning via Single Sign On (SSO)

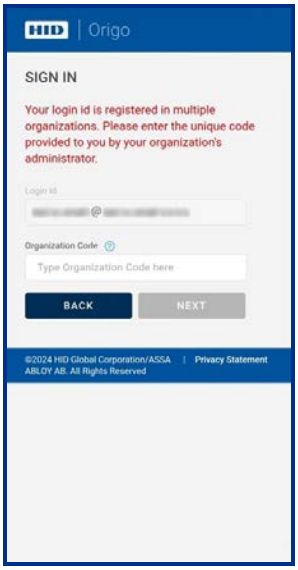
4.6.1 Add Pass to Google Wallet using SSO

1. Ensure the mobile device is connected to the internet (either via mobile data network or Wi-Fi).
2. Open the HID Mobile Access App.
3. On the **Welcome to HID Mobile Access** screen tap **Sign in with SSO**.
4. Enter your login email address and tap **NEXT**.

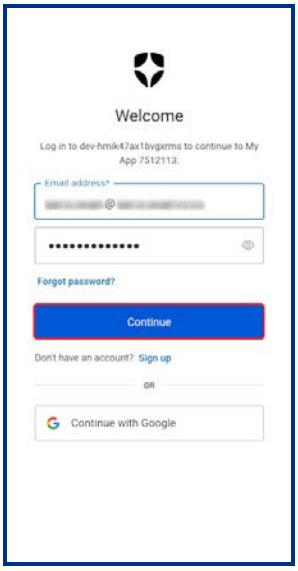
> **Note:** If, after entering your login id and tapping **NEXT**, a notification message is displayed regarding your login id is registered in multiple organizations, then contact your Organization administrator to obtain an Organization Code. This code is required to proceed with Pass provisioning.

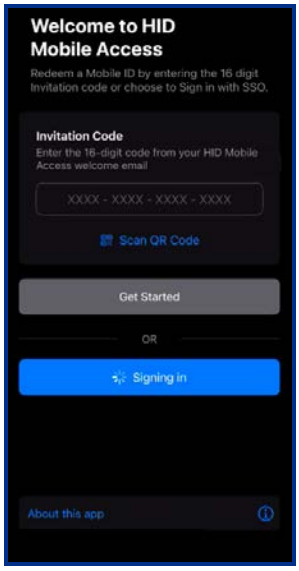




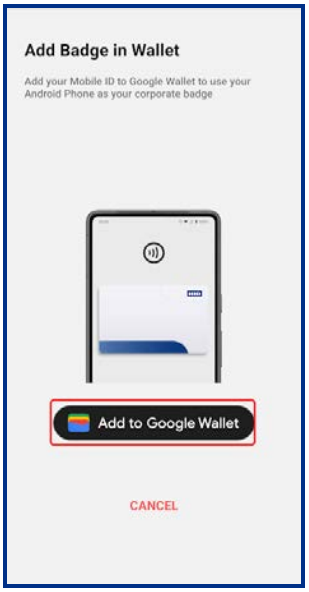


5. You are re-directed to your Identity Provider portal. Enter your credentials and tap **Continue**. If successful, the Pass issuance will re-trigger in the HID Mobile Access App.

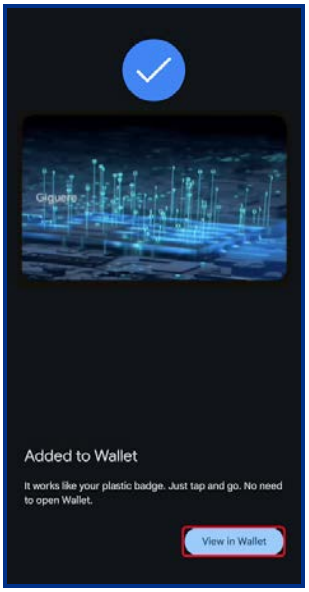




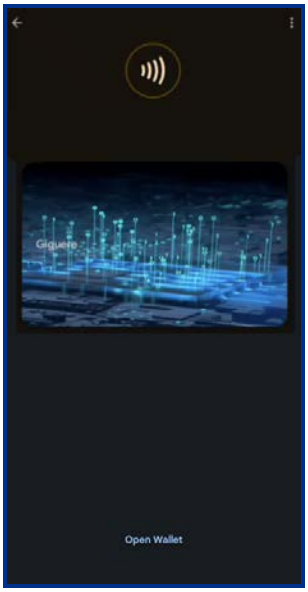
6. Once the Pass is redeemed, tap **Add to Google Wallet** to add the Pass to Wallet.
7. Tap **Accept & continue** to add the Pass to Wallet.







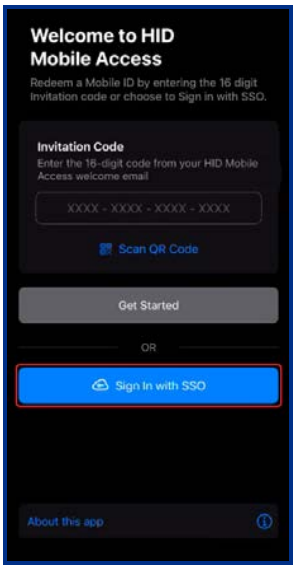
8. Tap **Open Wallet** to view the pass and user details.



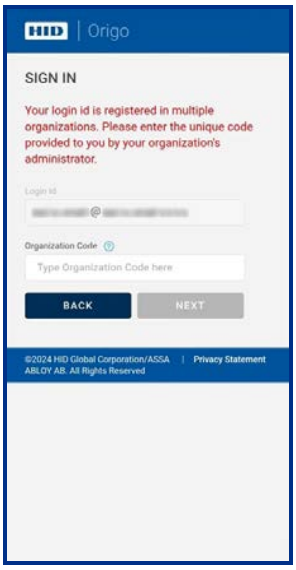
4.6.2 Add Pass to Apple Wallet using SSO

1. Ensure the mobile device is connected to the internet (either via mobile data network or Wi-Fi).
2. Open the HID Mobile Access App.
3. On the **Welcome to HID Mobile Access** screen tap **Sign in with SSO**.
4. Enter your login email address and tap **NEXT**.

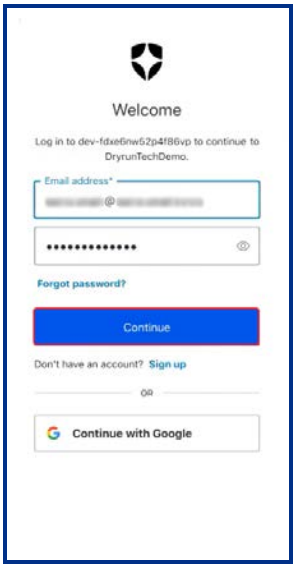
> **Note:** If, after entering your login id and tapping **NEXT**, a notification message is displayed regarding your login id is registered in multiple organizations, then contact your Organization administrator to obtain an Organization Code. This code is required to proceed with Pass provisioning.

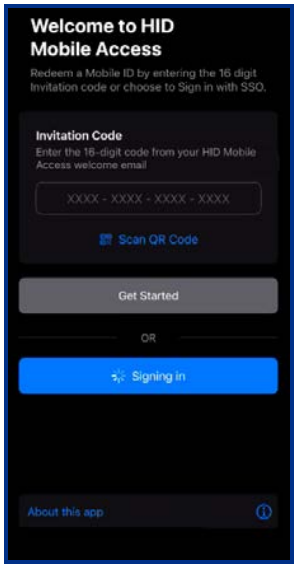






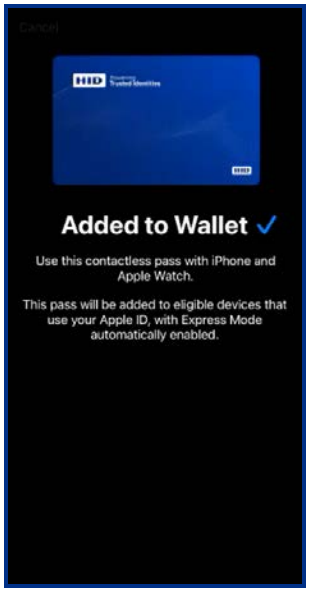
5. You are re-directed to your Identity Provider portal. Enter your credentials and tap **Continue**. If successful, the Pass issuance will re-trigger in the HID Mobile Access App.





6. Once the Pass is redeemed, tap **Add** to add the Pass to Wallet.

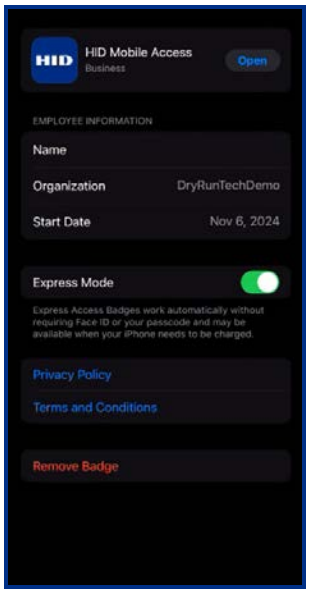






7. Tap **Open Apple Wallet** to view the pass and user details.



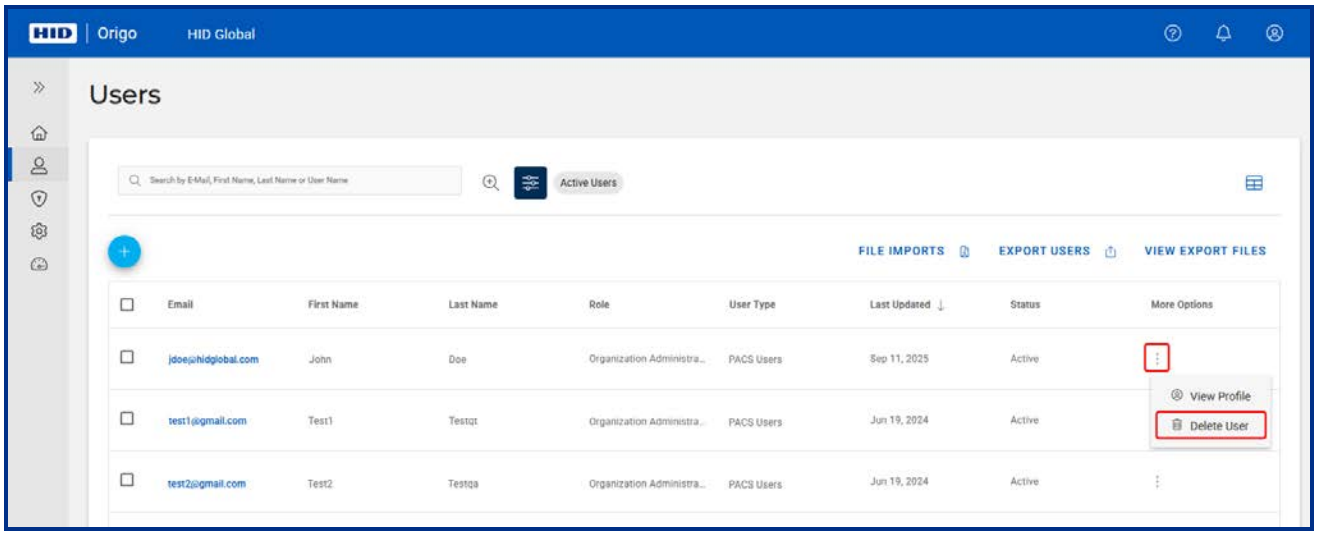


4.7 Delete a User

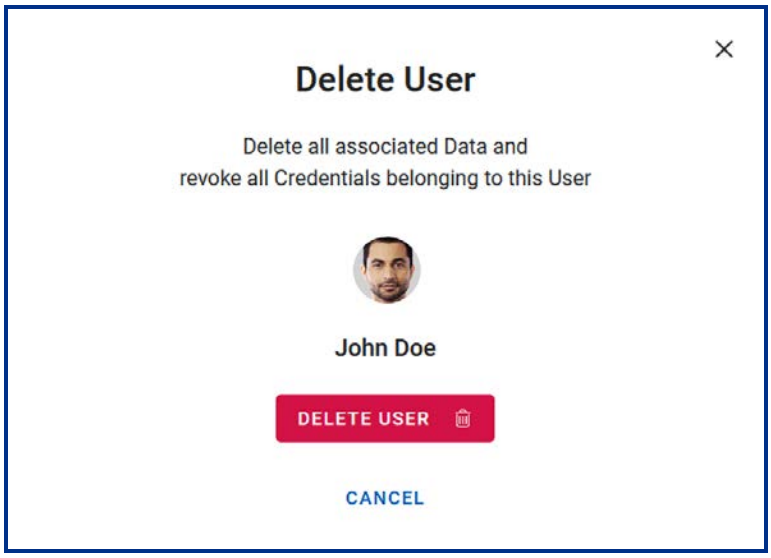
Note: The delete user action also revokes the user Pass, cancels any pending issuance, and deletes the associated device endpoint.

1. On the **Users** screen, click the ellipses icon [⋮] associated with a displayed user and select the **Delete User** option.

   Note: Alternatively select the **View Profile** option, and in the **General** section, click the delete user icon [🗑].

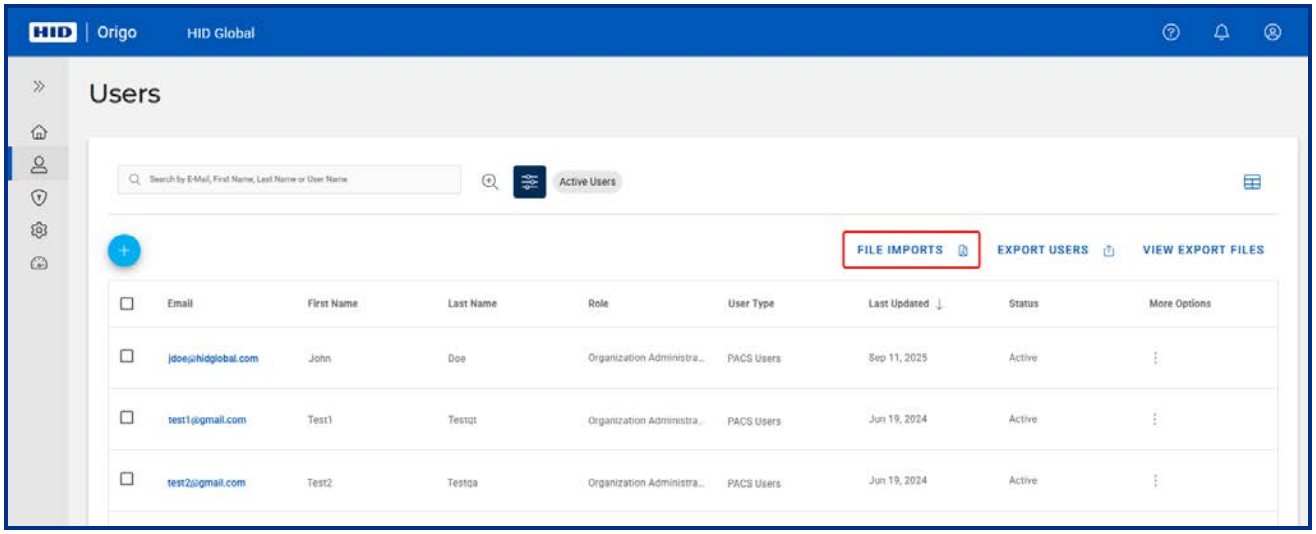


2. Click **DELETE USER** to confirm the action and delete the user.

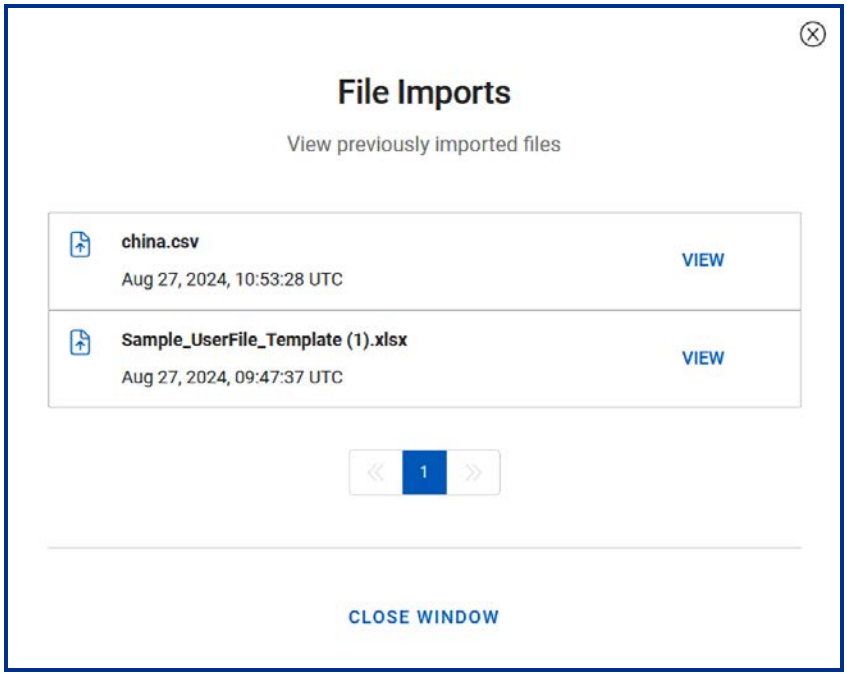


4.8 View file imports

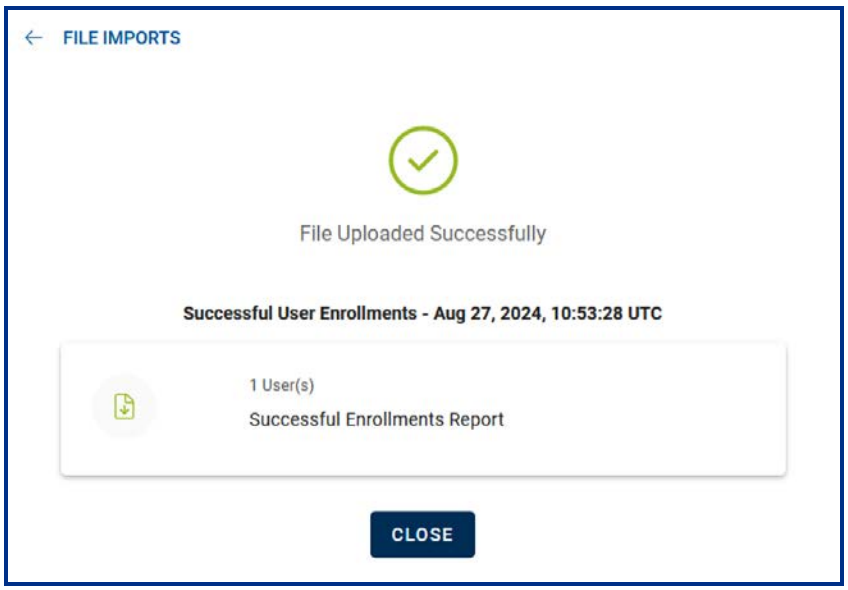
1. On the **Users** screen, select the **FILE IMPORTS** option.



2. The **File Imports** screen displays a list of previously imported files.



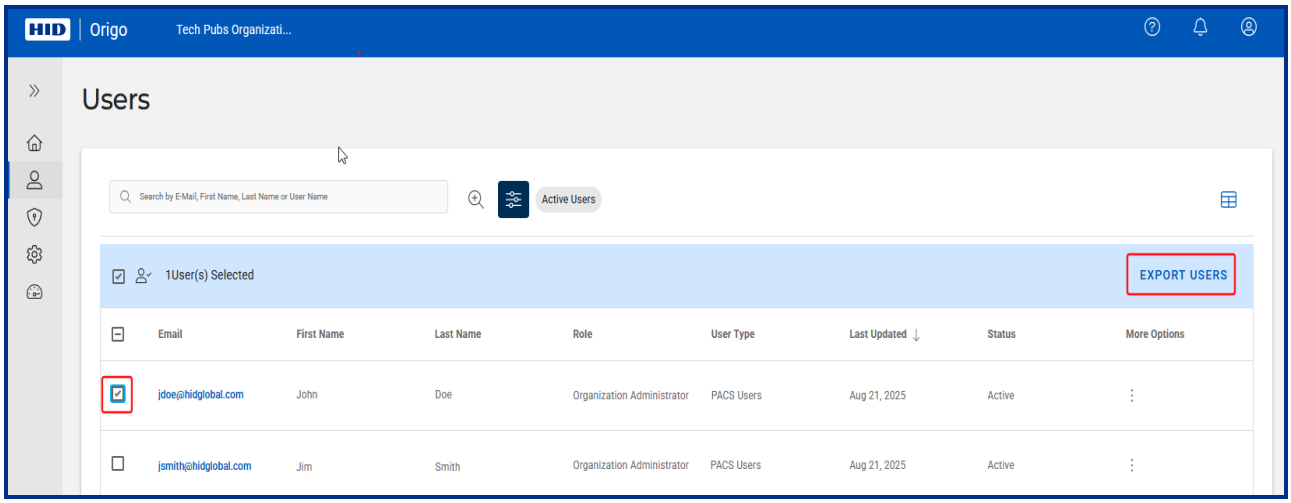
3. Click **VIEW** for an associated file to view the file import details.



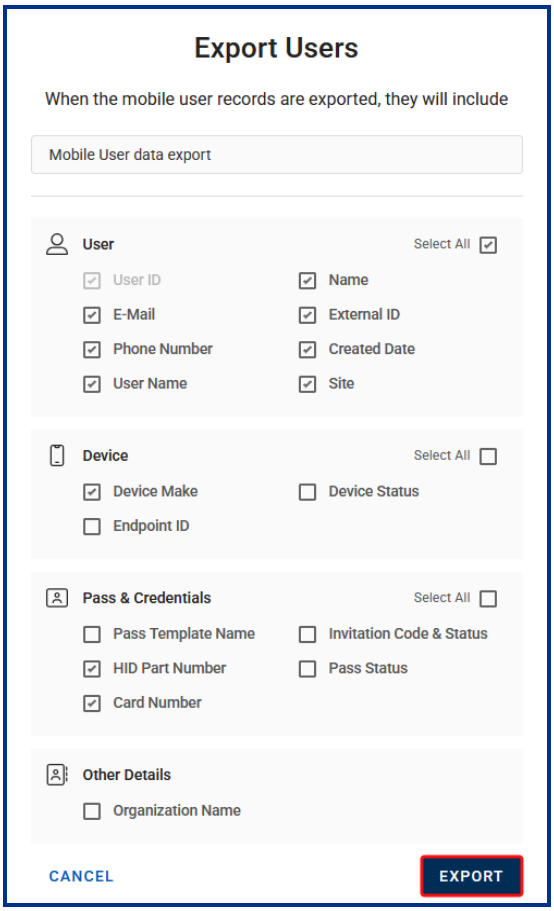
4.9 Export Users

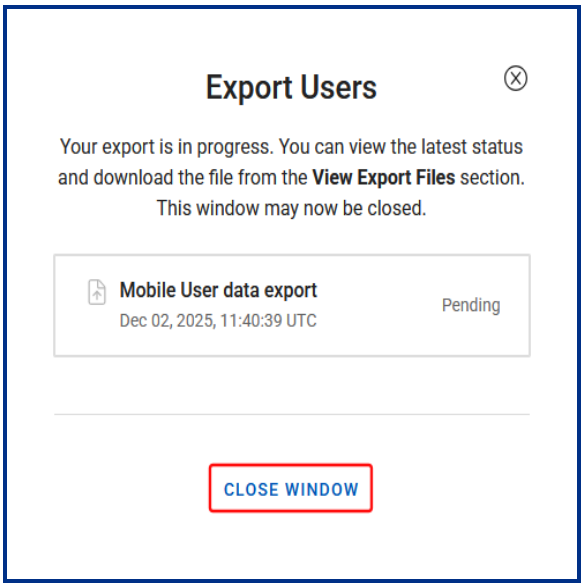
4.9.1 Export user details

1. On the **Users** screen, select a displayed user and click **EXPORT USERS**.

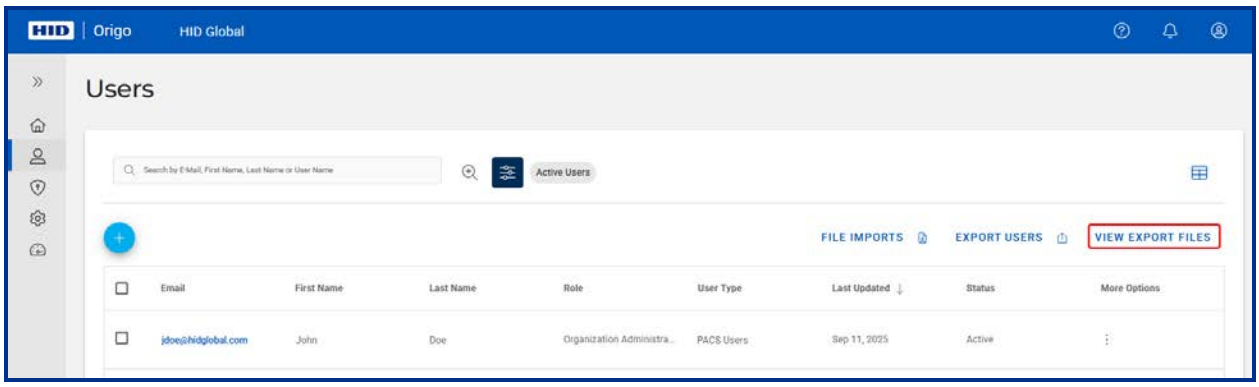


2. In the **Export Users** dialog box, enter a name for the export file. In each record item section either check the **Select All** box to include all the listed items in the report or individually select each required item.
3. Click **EXPORT** to save the export user file and close the **Export Users** window.

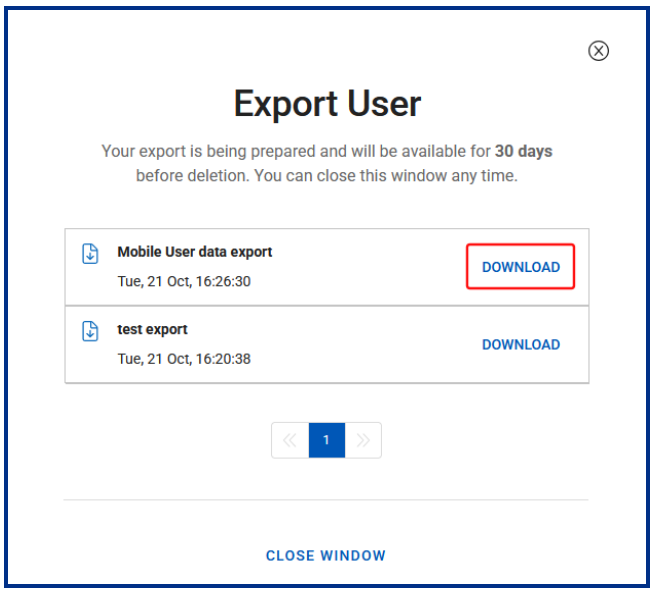




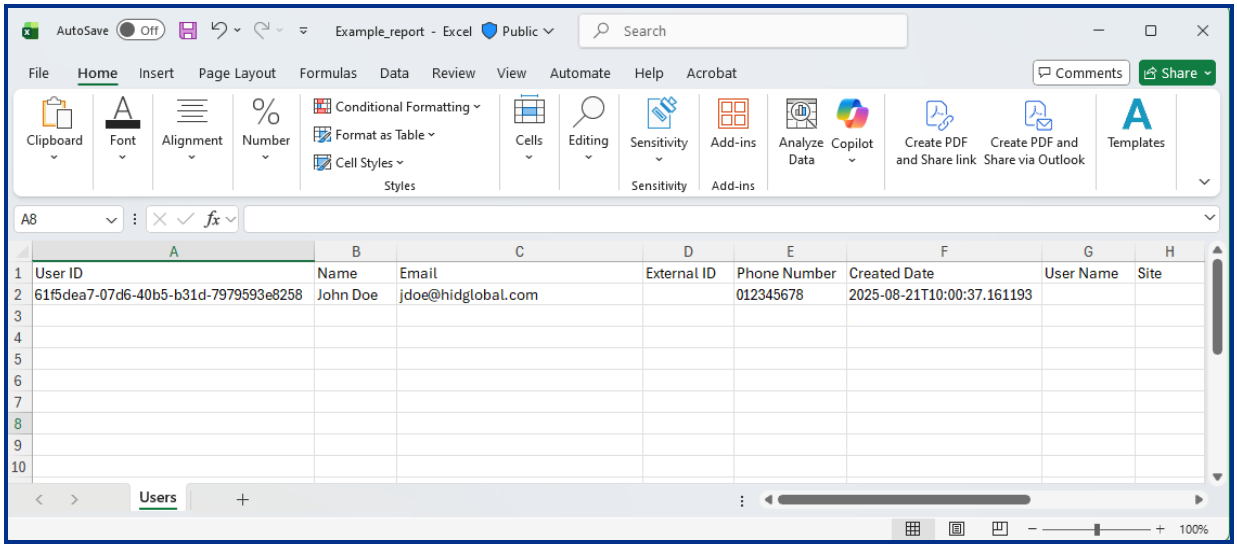
4. Back on the **Users** screen, select the **VIEW EXPORT FILES** option.



5. Click **DOWNLOAD** for the export file you wish to download, select a location, and click **Save**.

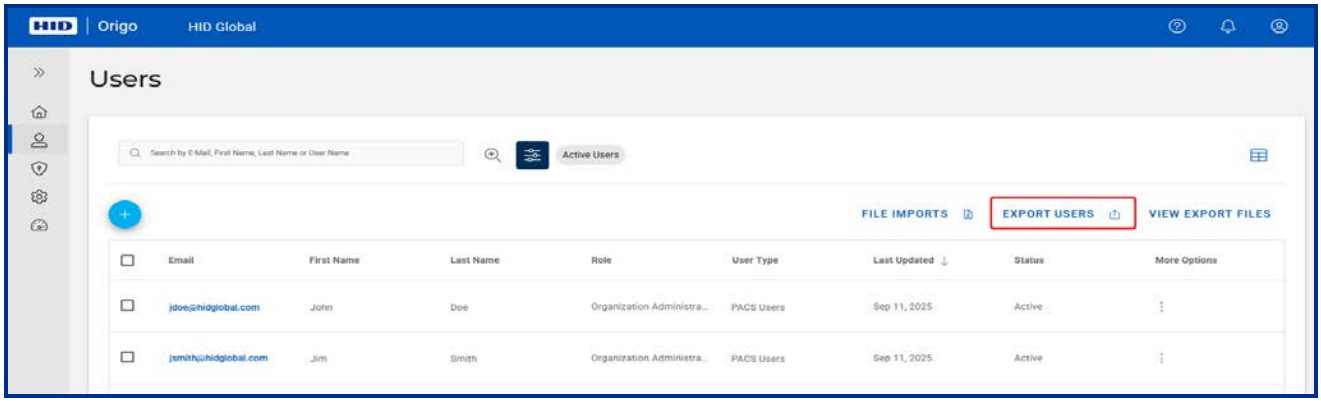


6. Navigate to the export file download folder and open the **.xls** file to view the exported user details.

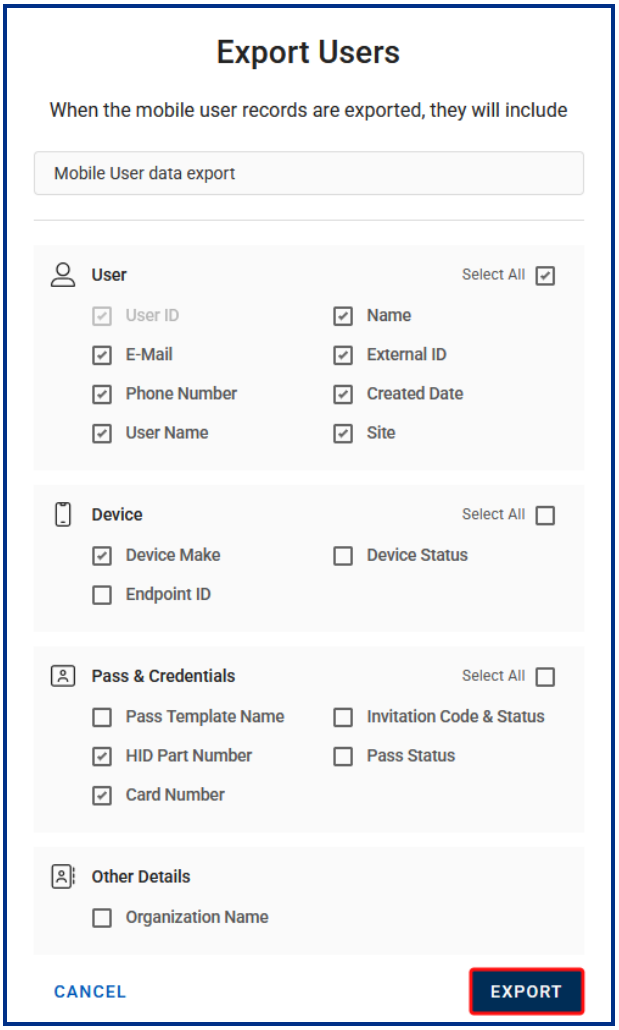


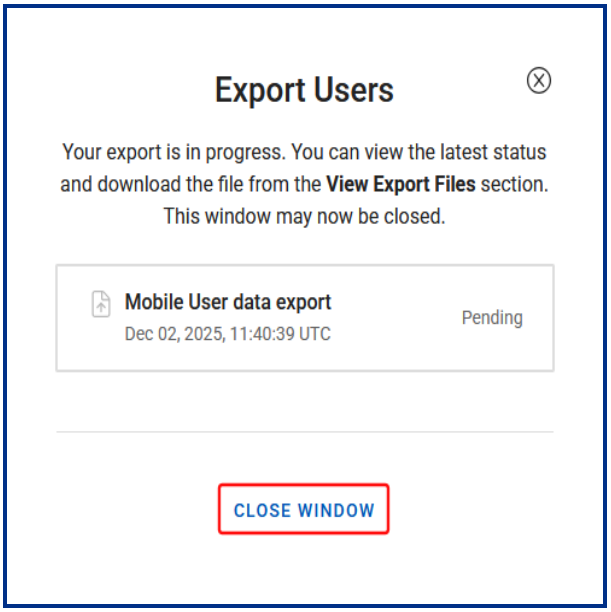
4.9.2 Export all user details

1. On the **Users** screen, select the **EXPORT USERS** option.

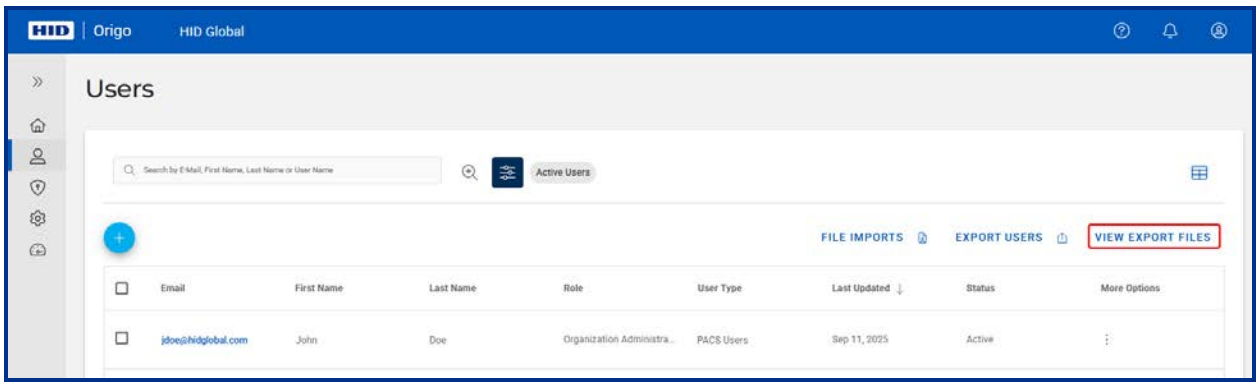


2. In the **Export Users** dialog box, enter a name for the export file. In each record item section either check the **Select All** box to include all the listed items in the report or individually select each required item.
3. Click **EXPORT** to save the export user file and close the **Export Users** window.

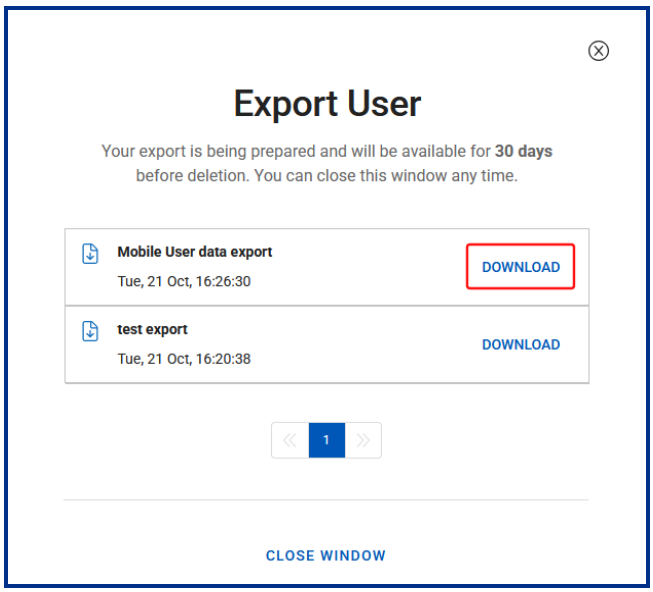




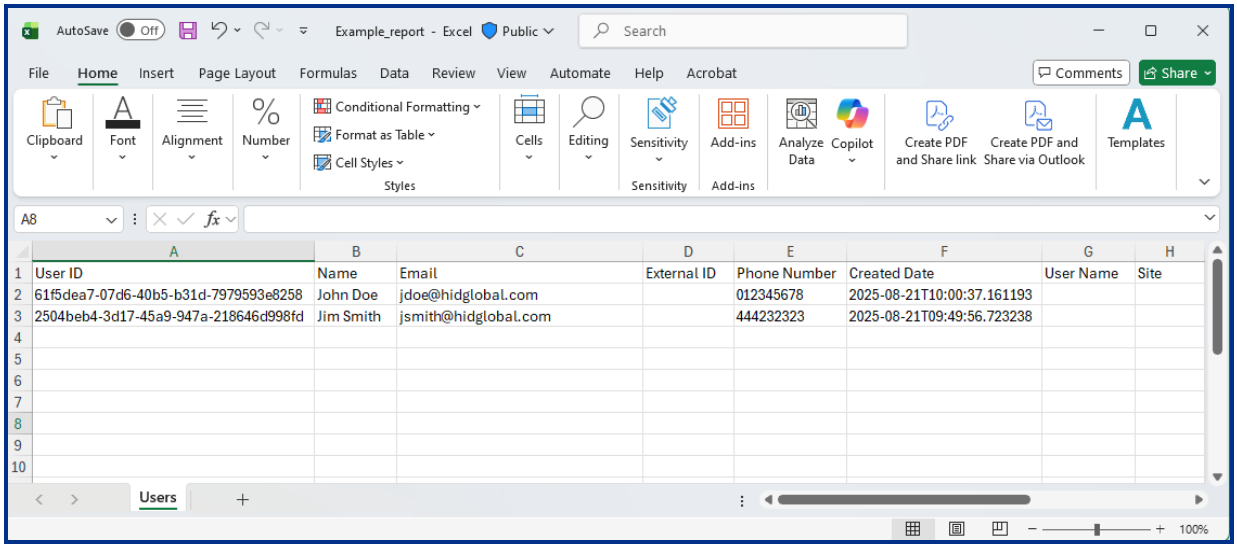
4. Back on the **Users** screen, select the **VIEW EXPORT FILES** option.



5. Click **DOWNLOAD** for the export file you wish to download, select a location, and click **Save**.



6. Navigate to the export file download folder and open the **.xls** file to view the exported user details.



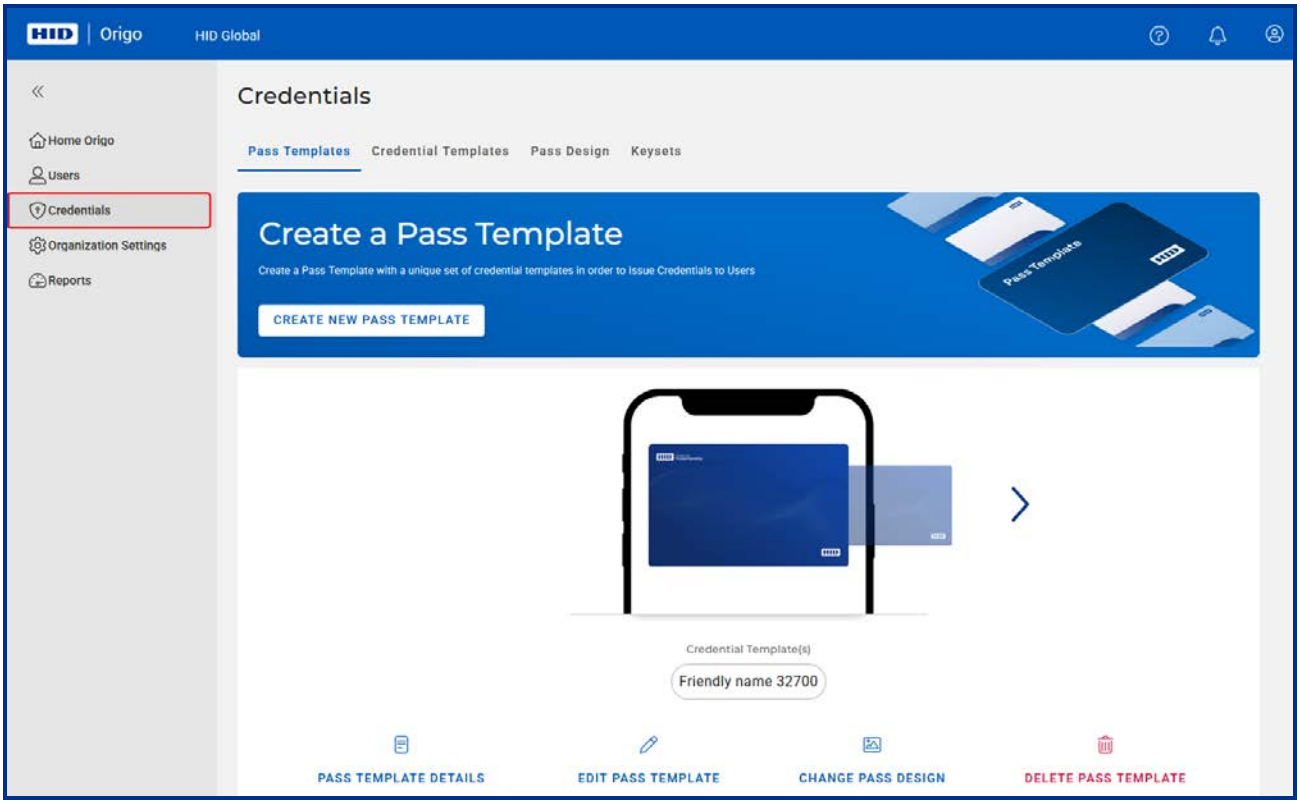
Section 05

Credential Management

5.1 Credential management overview

On the Organization **Home** screen, from the left navigation menu, select the **Credentials** option. The **Credentials** screen provides administrators with options to:

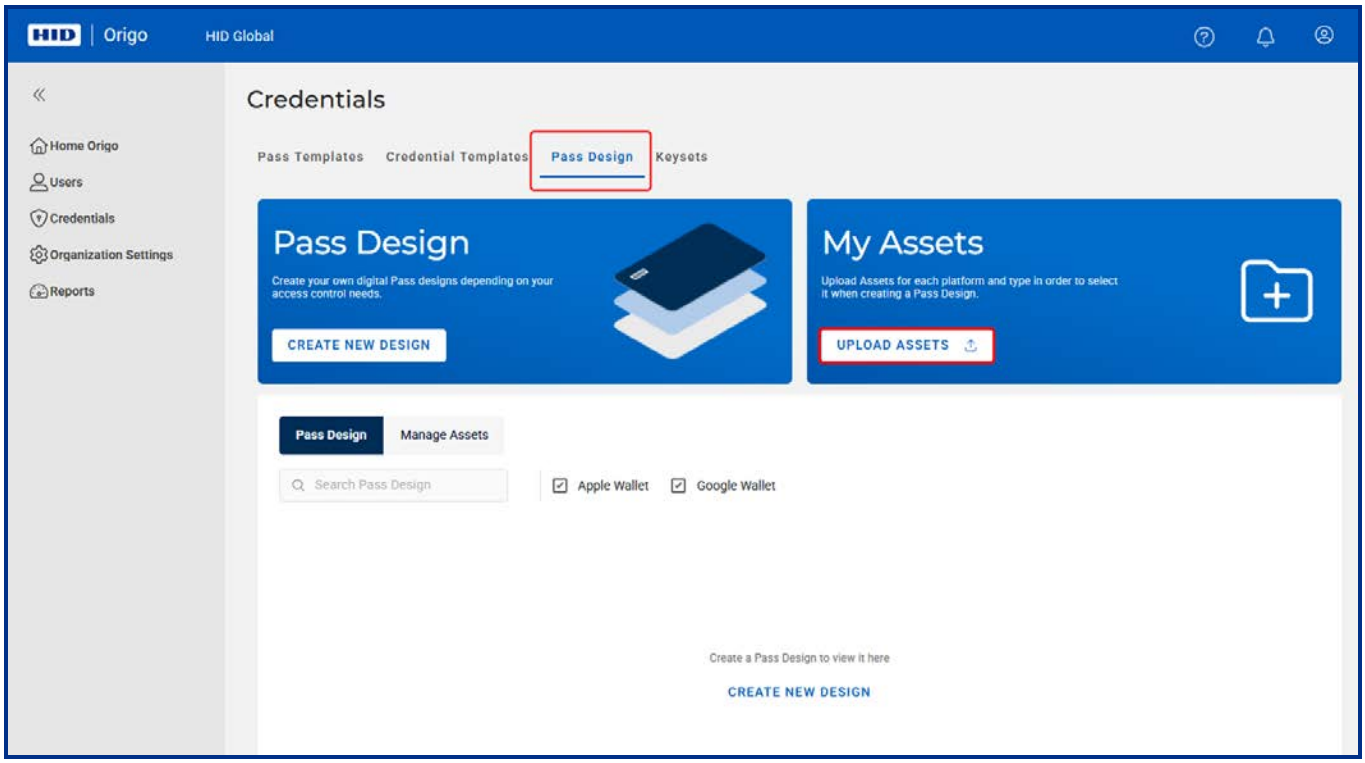
- Create Pass Designs. See the **Create a Pass Design** section.
- Create a new Pass Template and manage existing Templates. See the **Create and manage Pass Templates** section.
- View and edit Credential Templates. See the **View Credential Templates** section.
- View Keysets associated with your Organization. See the **View Keysets** section.



5.2 Create a Pass Design

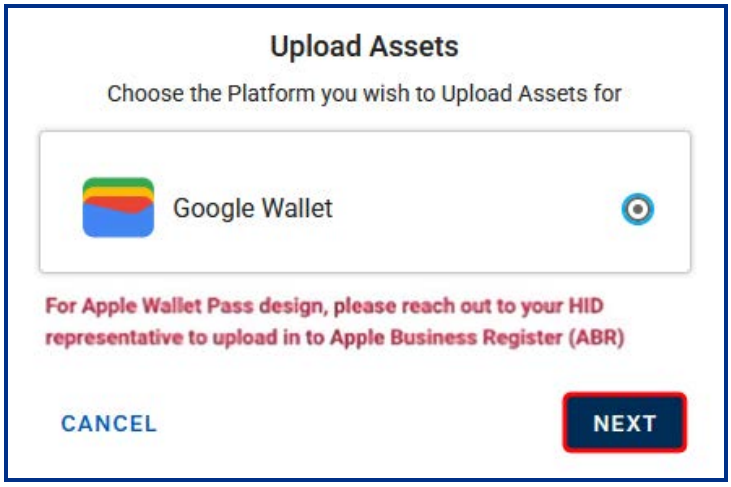
Pass Designs are used when creating a new Pass Template (see the **Create a new Pass Template** section).

1. To create a new Pass Design, on the **Credentials** screen, click **Pass Design**.
2. Firstly, upload platform assets (background and logo images) to be used when creating a new Pass Design. In the **My Assets** section, click **UPLOAD ASSETS**.



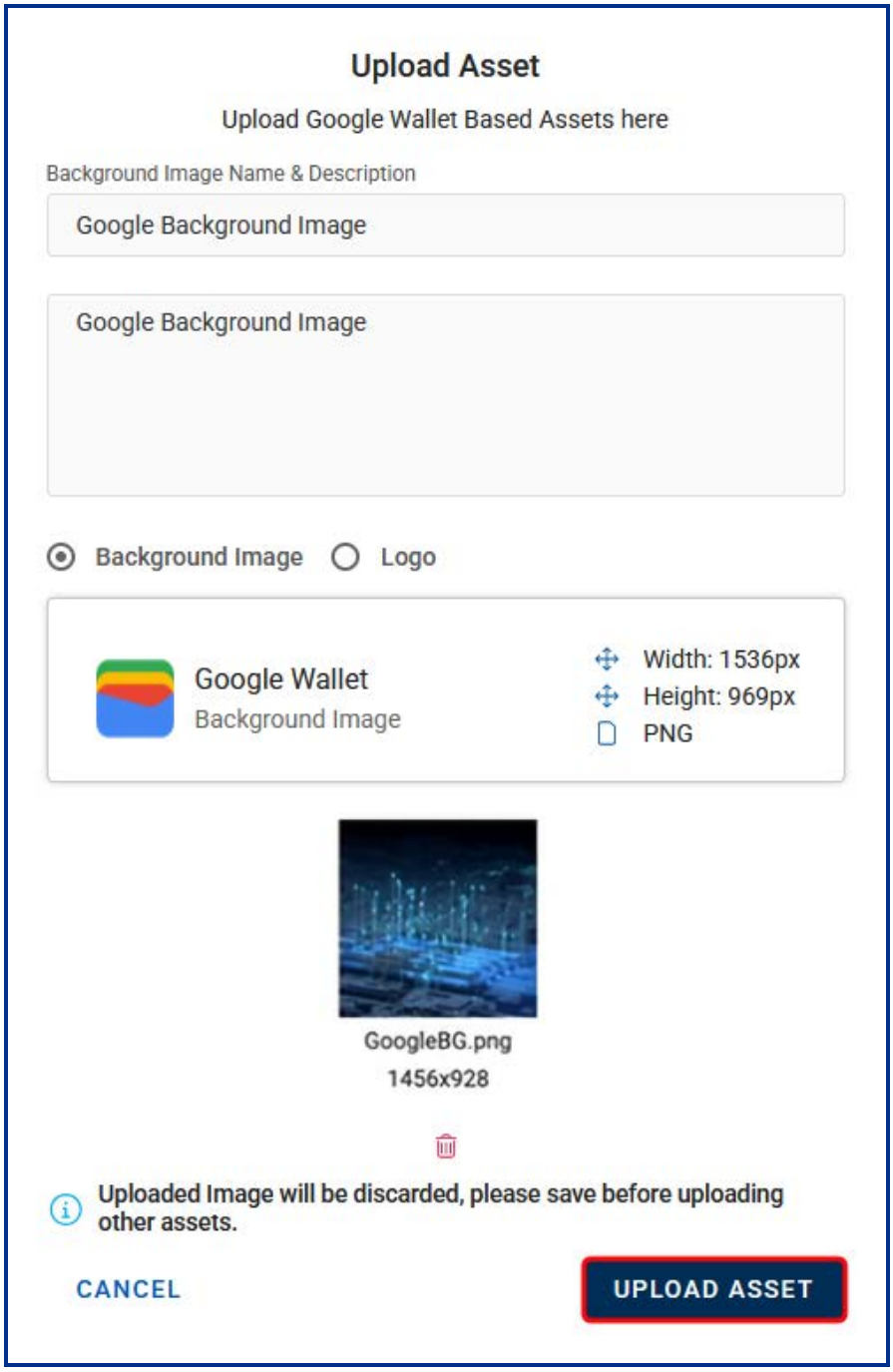
3. Select the platform and click **NEXT**.

> **Note:** For an Organization administrator only Google Wallet Assets can be uploaded. For an Apple Wallet Pass Design contact your HID Representative.

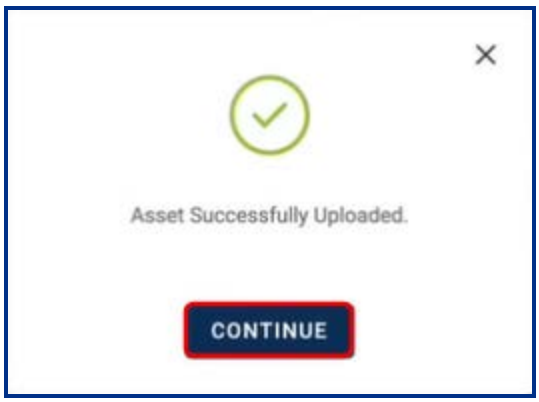


4. In the **Upload Asset** dialog, select the **Background Image** option and enter a **Background Image Name & Description** for the background image.
5. Click **UPLOAD BACKGROUND IMAGE**. Navigate to and select the required image to upload.

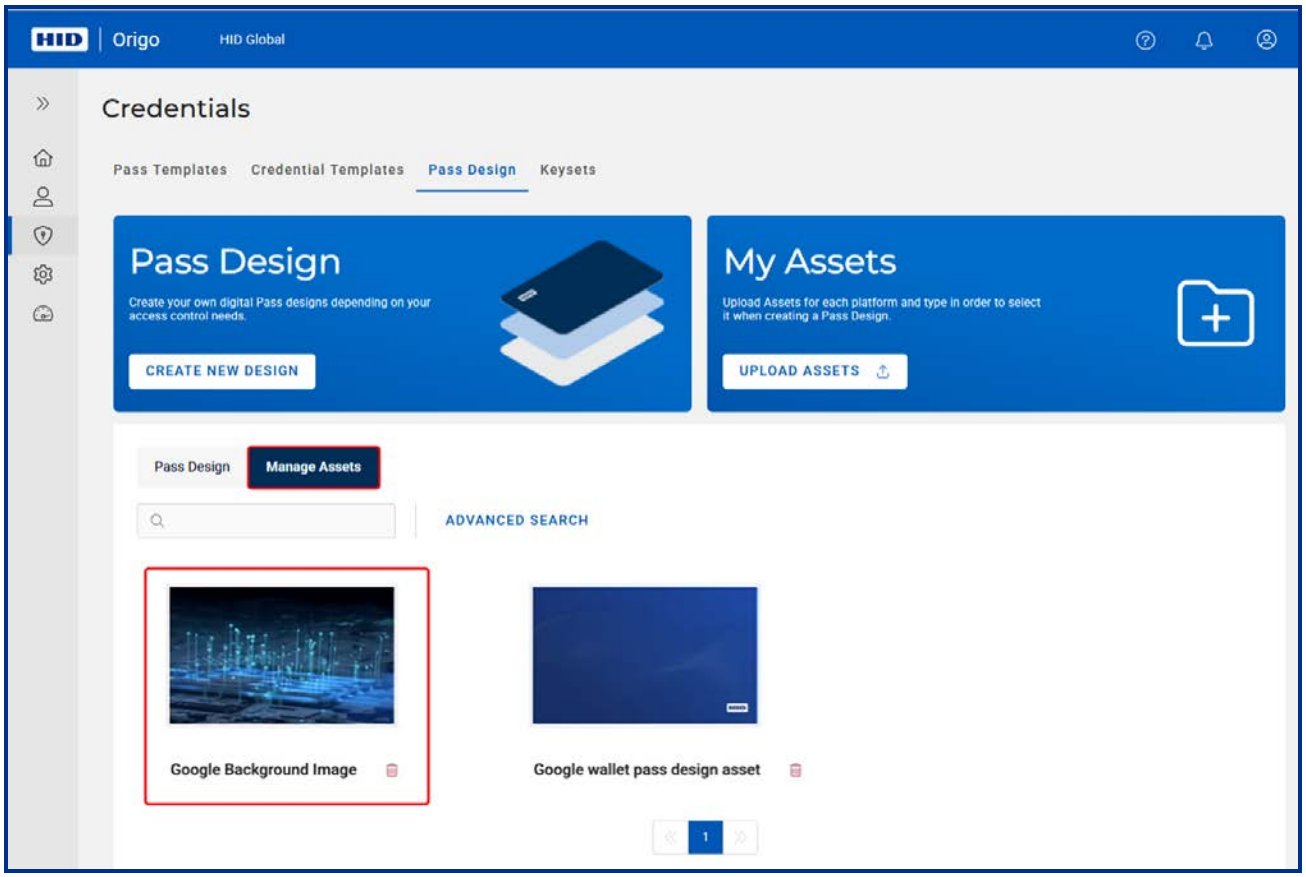
   Note: Make sure that the selected image conforms to the displayed image size, format type, and maximum file size, otherwise the image will not be uploaded.
6. When the selected image is displayed in the **Upload Asset** dialog, click **UPLOAD ASSET**.



7. In the displayed success message dialog, click **CONTINUE**.



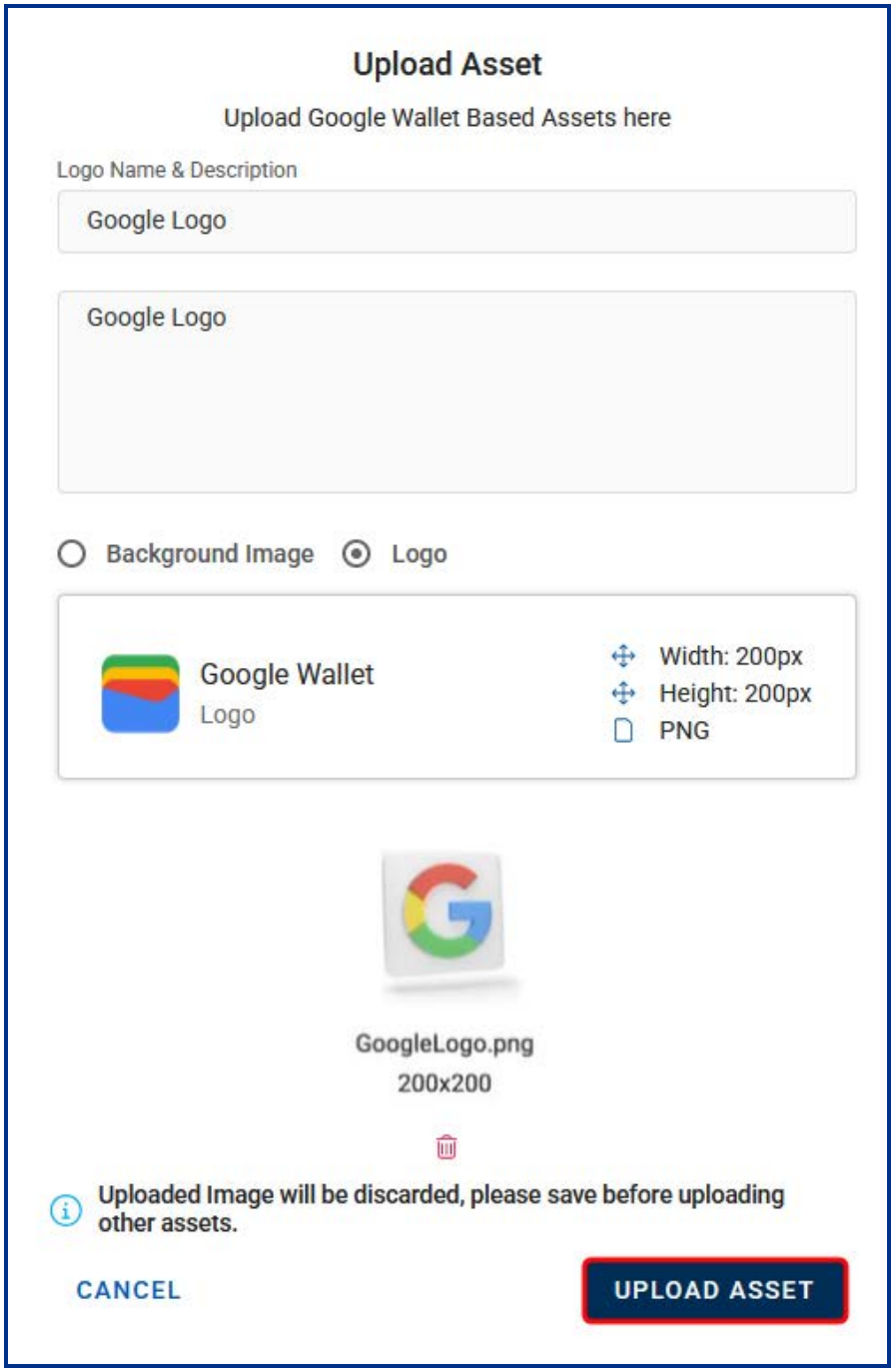
The uploaded background image is displayed under the **Manage Assets** option on the **Pass Design** page.



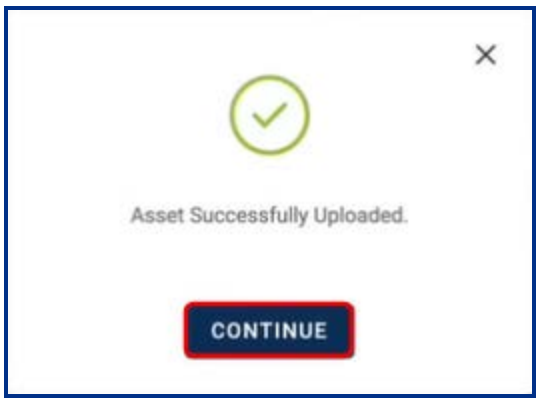
8. Click the **UPLOAD ASSETS** option again, select the platform and click **NEXT**.
9. In the **Upload Asset** dialog, select the **Logo** option and enter a **Logo Name & Description** for the logo image.
10. Click **UPLOAD LOGO**. Navigate to and select the required image to upload.

> **Note:** Make sure that the selected image conforms to the displayed image size, format type, and maximum file size, otherwise the image will not be uploaded.

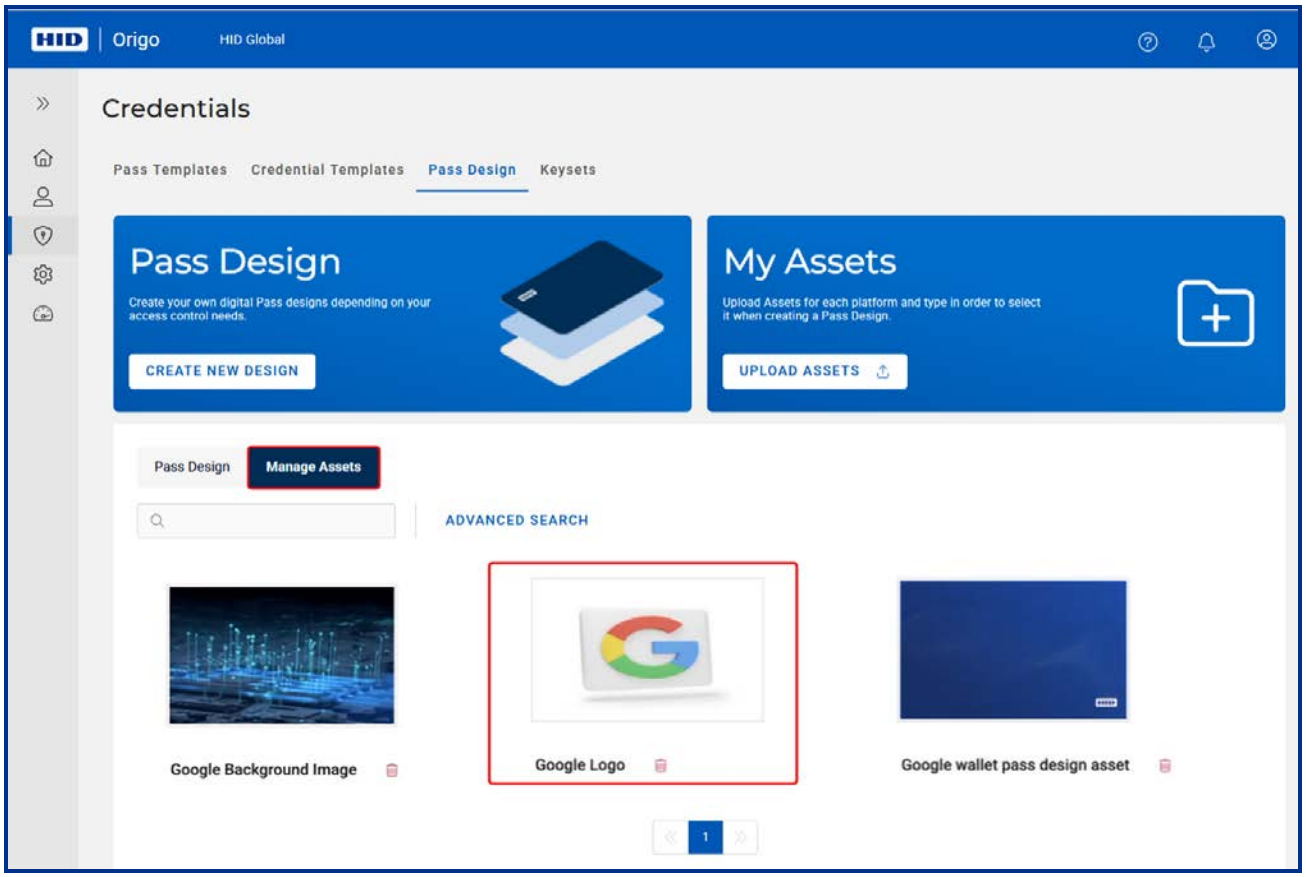
11. When the selected image is displayed in the **Upload Asset** dialog, click **UPLOAD ASSET**.



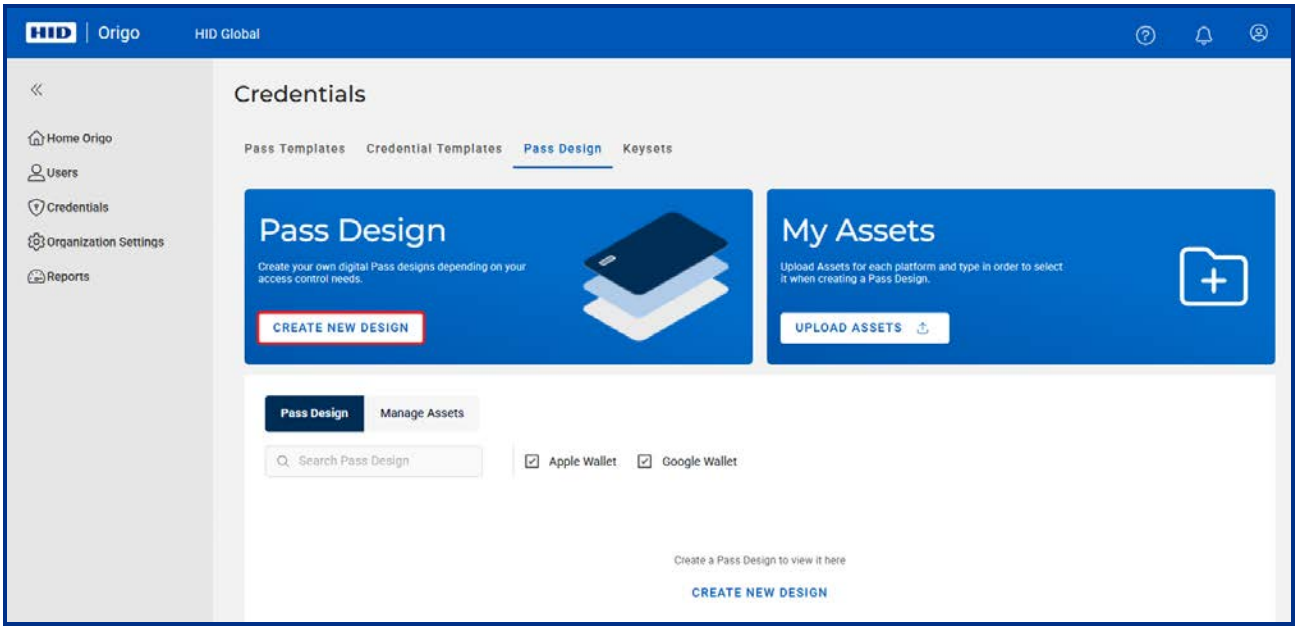
12. In the displayed success message dialog, click **CONTINUE**.



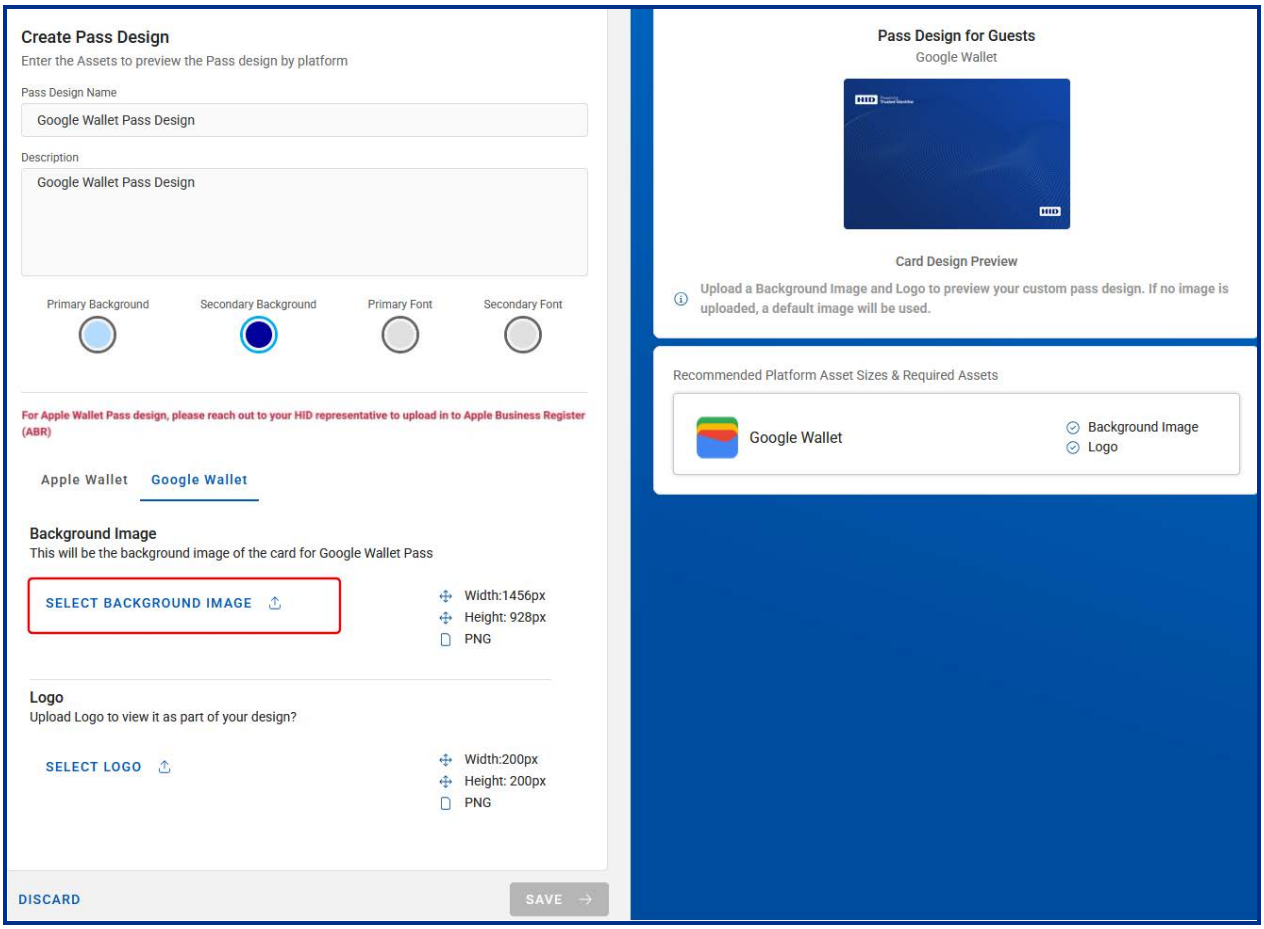
The uploaded logo image is displayed under the **Manage Assets** option on the **Pass Design** page.



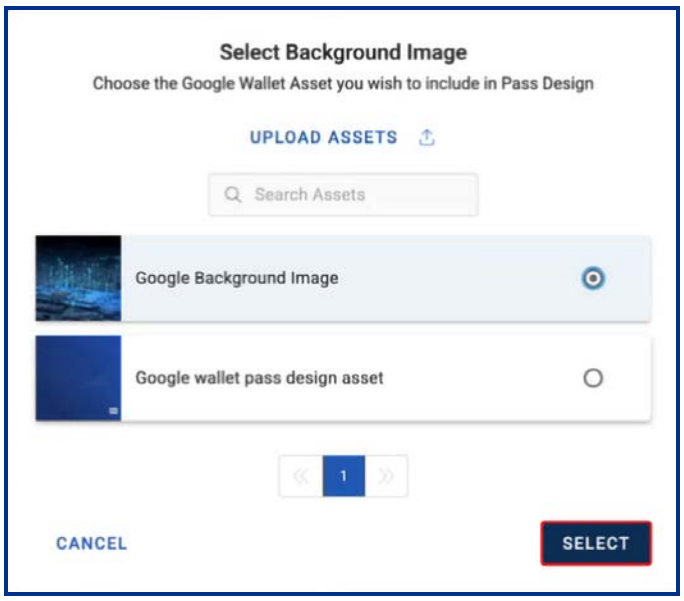
13. To create a new Pass Design, in the **Pass Design** section, click **CREATE NEW DESIGN**.



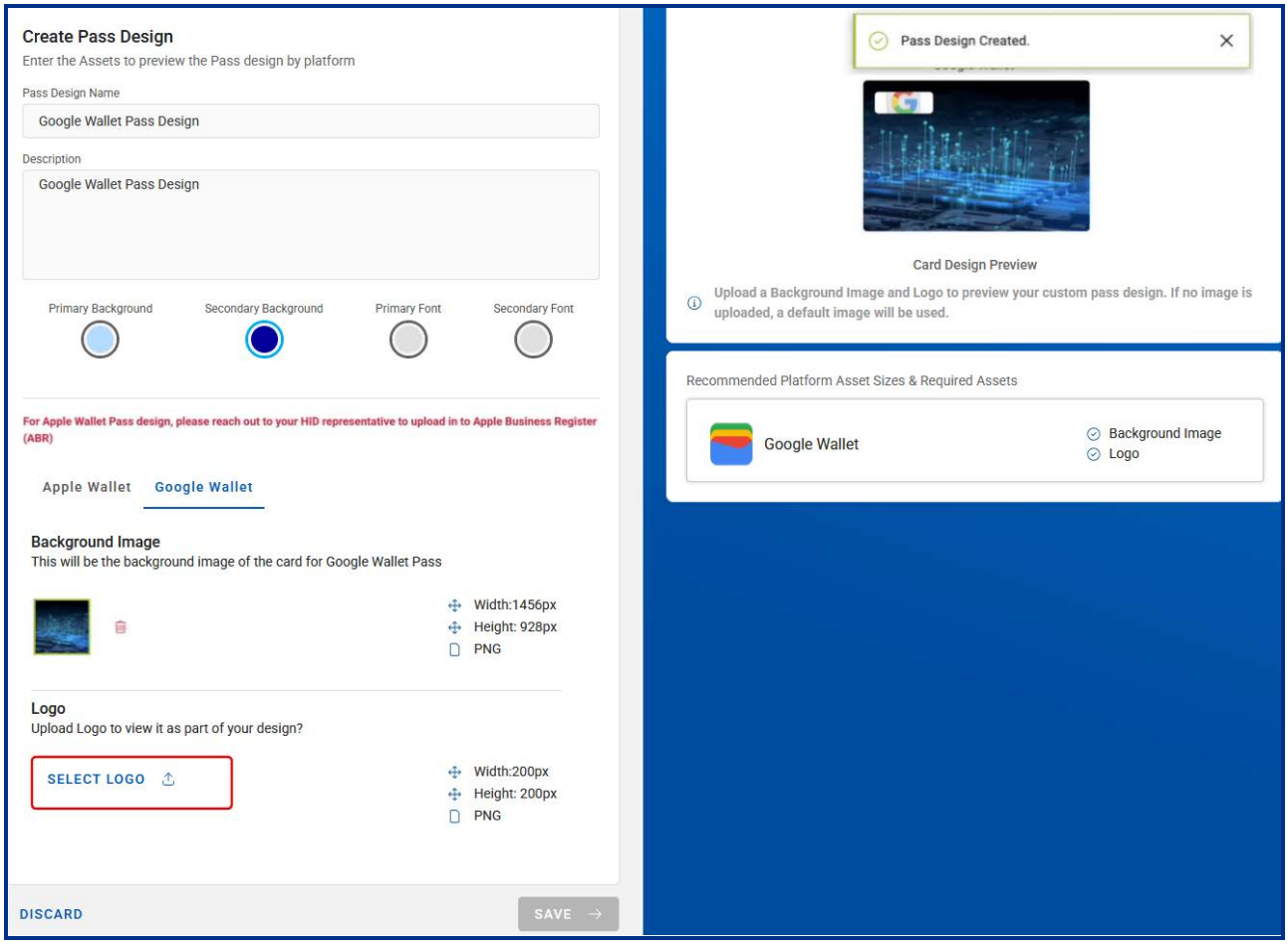
14. In the **Create Pass Design** dialog, enter a **Pass Design Name** and **Description** and click **SELECT BACKGROUND IMAGE**.



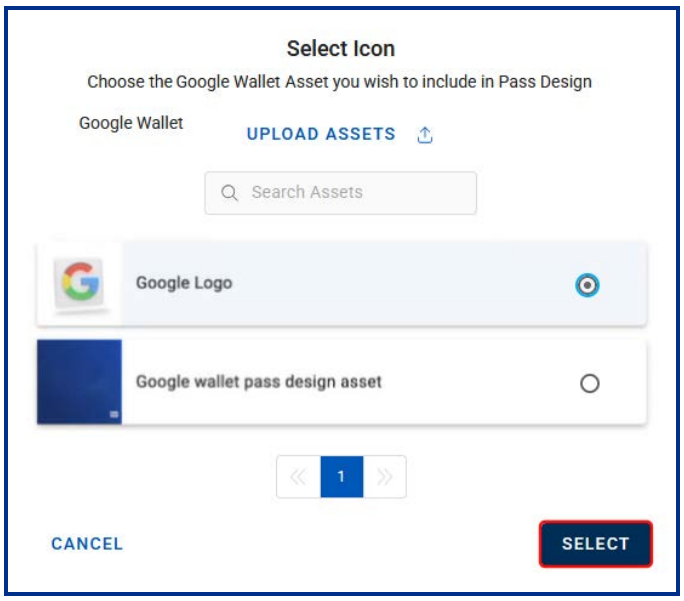
15. Choose the required background image and click **SELECT**.



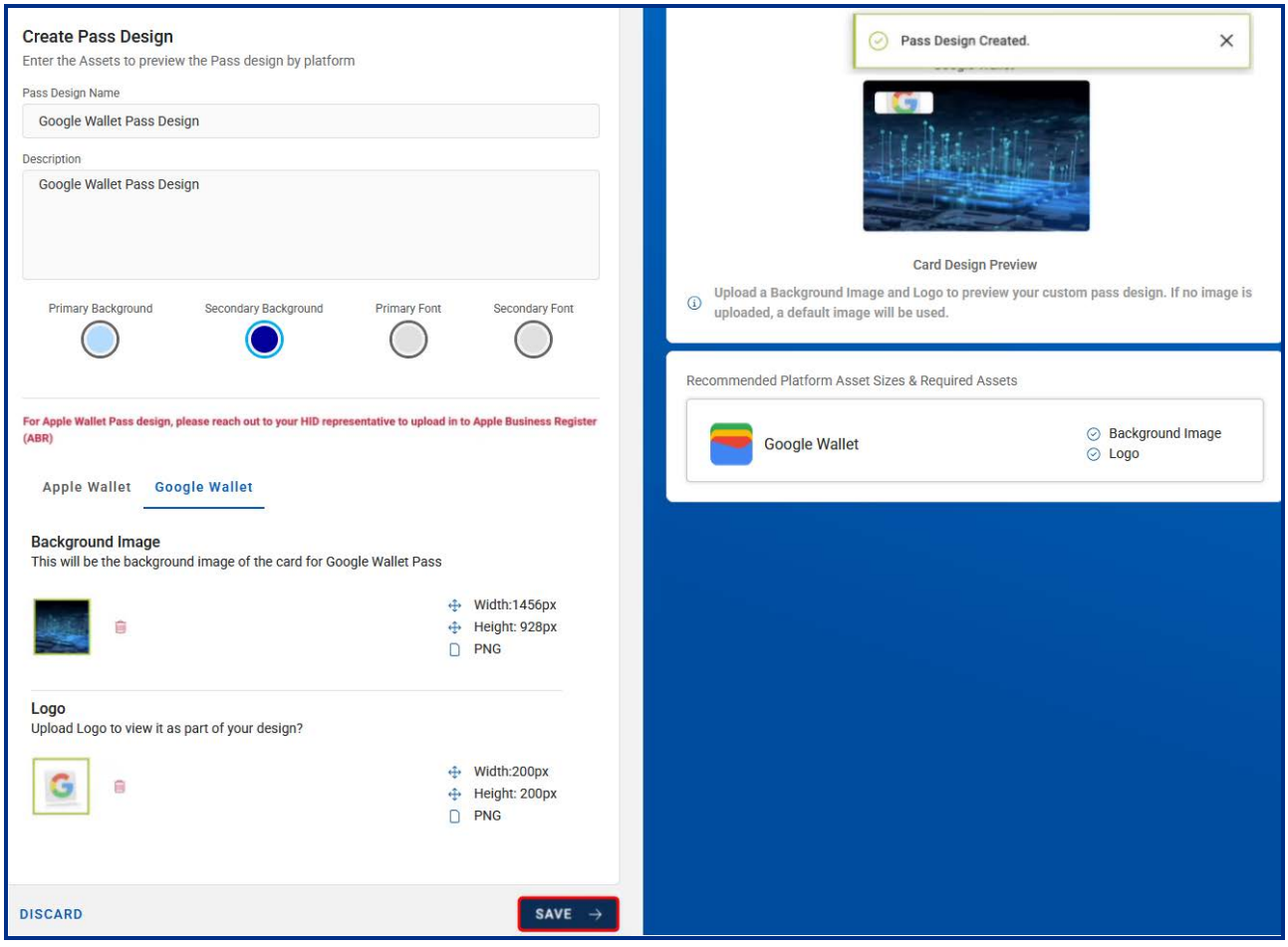
16. Back in the **Create Pass Design** dialog click **SELECT LOGO**.



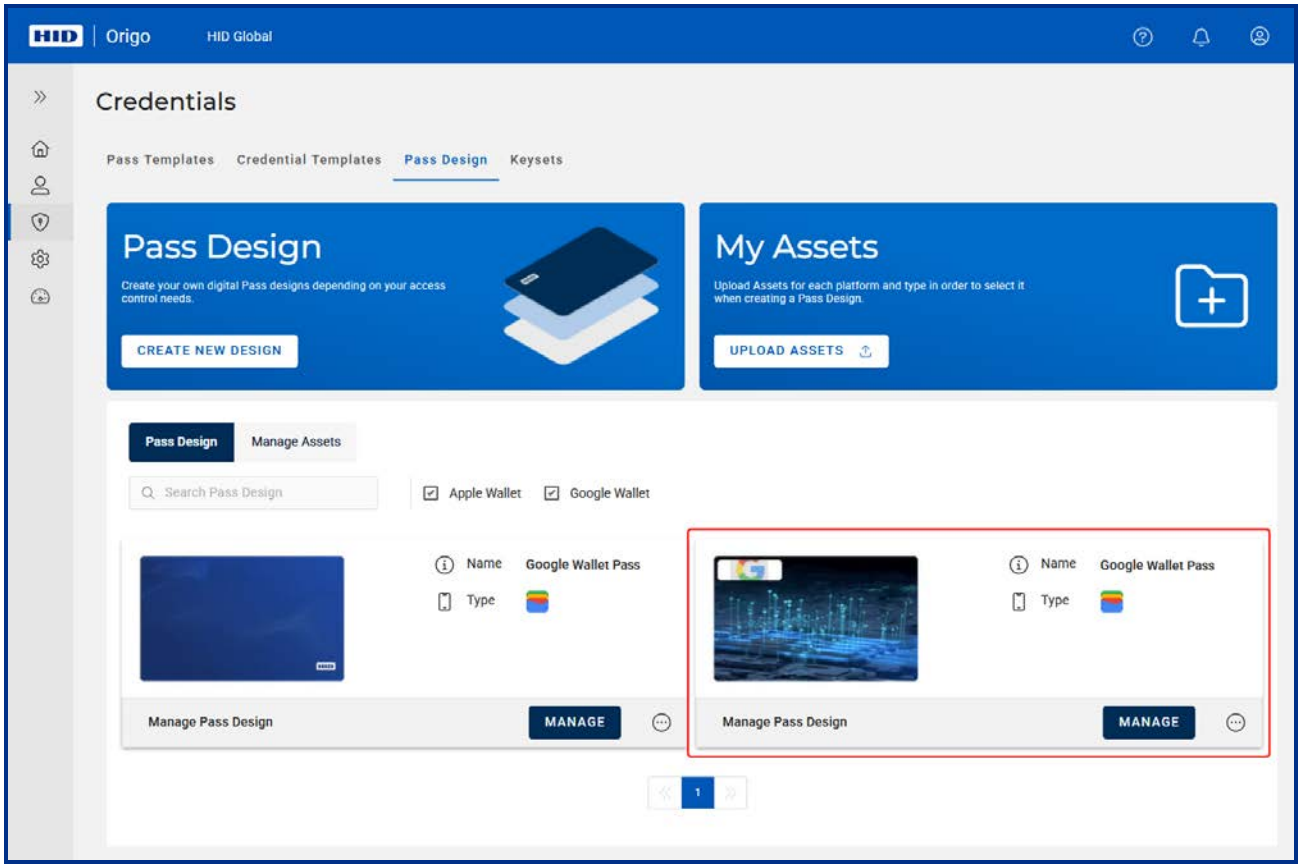
17. Choose the required logo image and click **SELECT**.



18. Click **SAVE**.



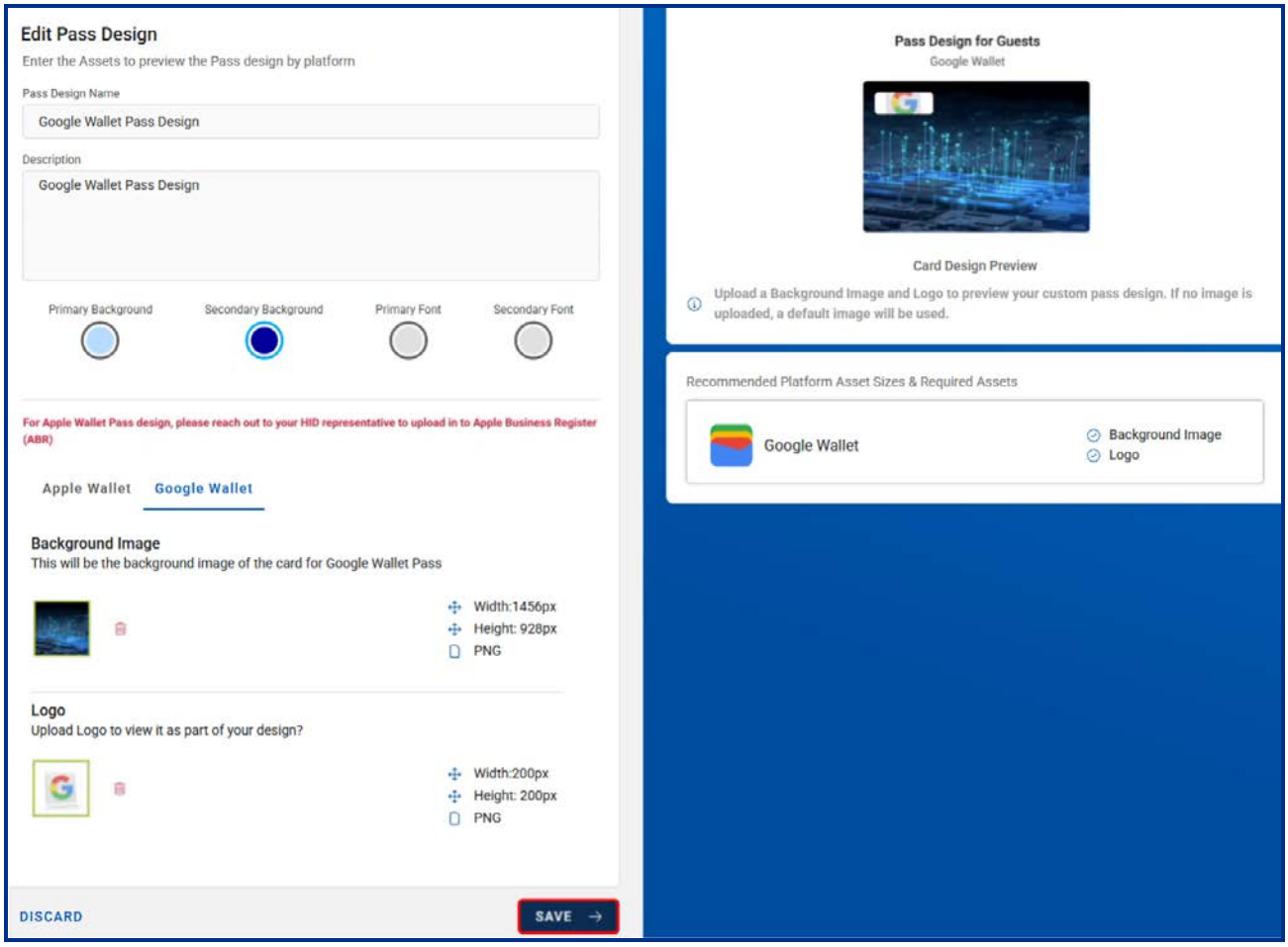
19. The new Pass Design is displayed on the **Pass Design** screen. Pass Templates can now be created based on the new Pass Design, see the **Create a new Pass Template** section.



5.2.1 Manage Pass Designs

1. On the **Pass Design** screen select the **Pass Design** option to view existing Pass Designs.
2. Enter the name of a Pass Design in the search field to display a specific Pass Design.

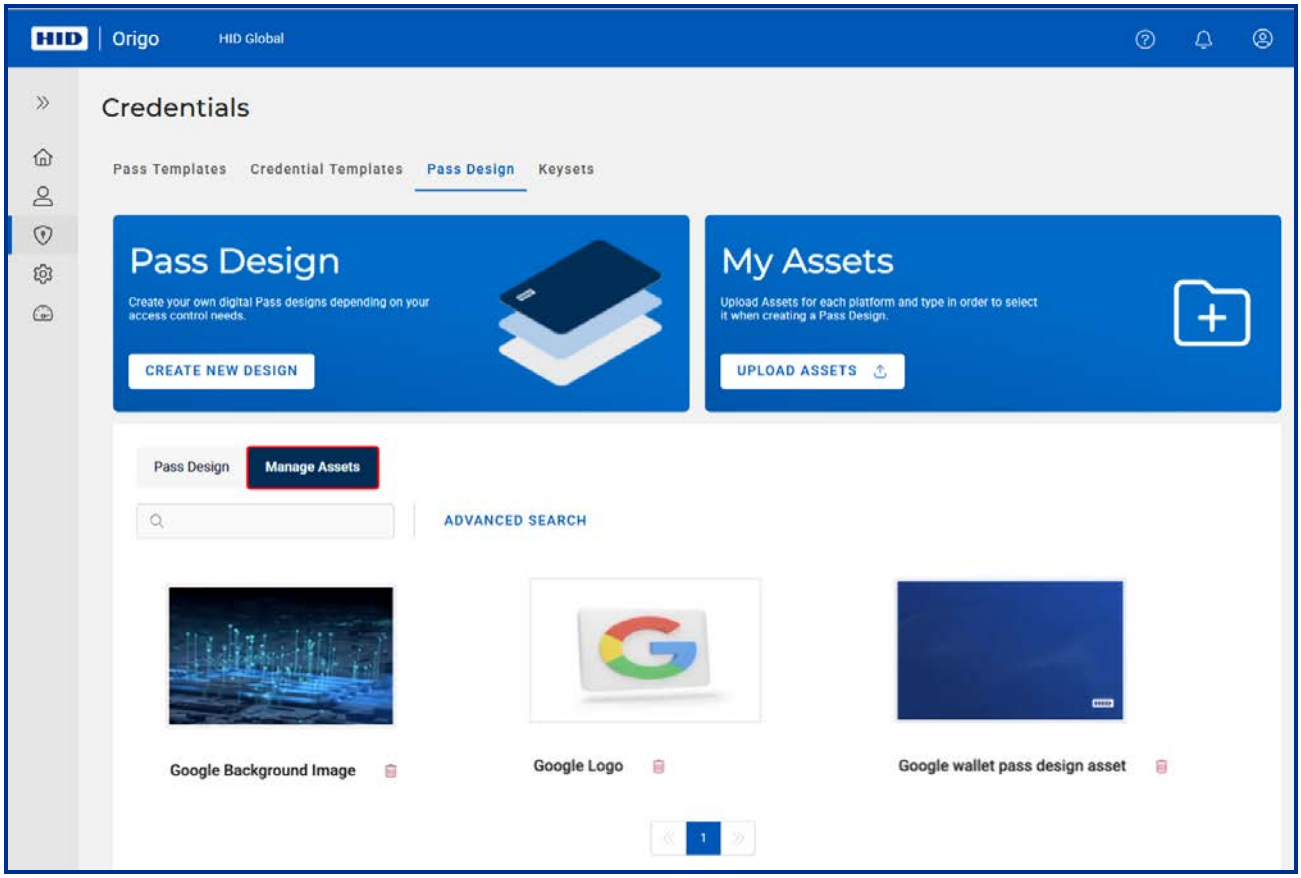
   Note: Select a Platform to limit the search to that particular Platform.
3. For a displayed Pass Design, click **MANAGE** to edit the Pass Design.
4. Edit the Pass Design as required and click **SAVE**.



5. To duplicate or delete a Pass Design, click the ellipses icon [⋯] associated with a displayed Pass Design and select the required option.

5.2.2 Manage Assets

1. On the **Pass Design** screen select the **Manage Assets** option to view uploaded Assets.
2. Enter the name of an Asset in the search field to display a specific Asset or select **ADVANCED SEARCH** to search for an Asset by **Type** or **Platform**.
3. To delete an Asset, click the delete icon [🗑] associated with a displayed Asset.

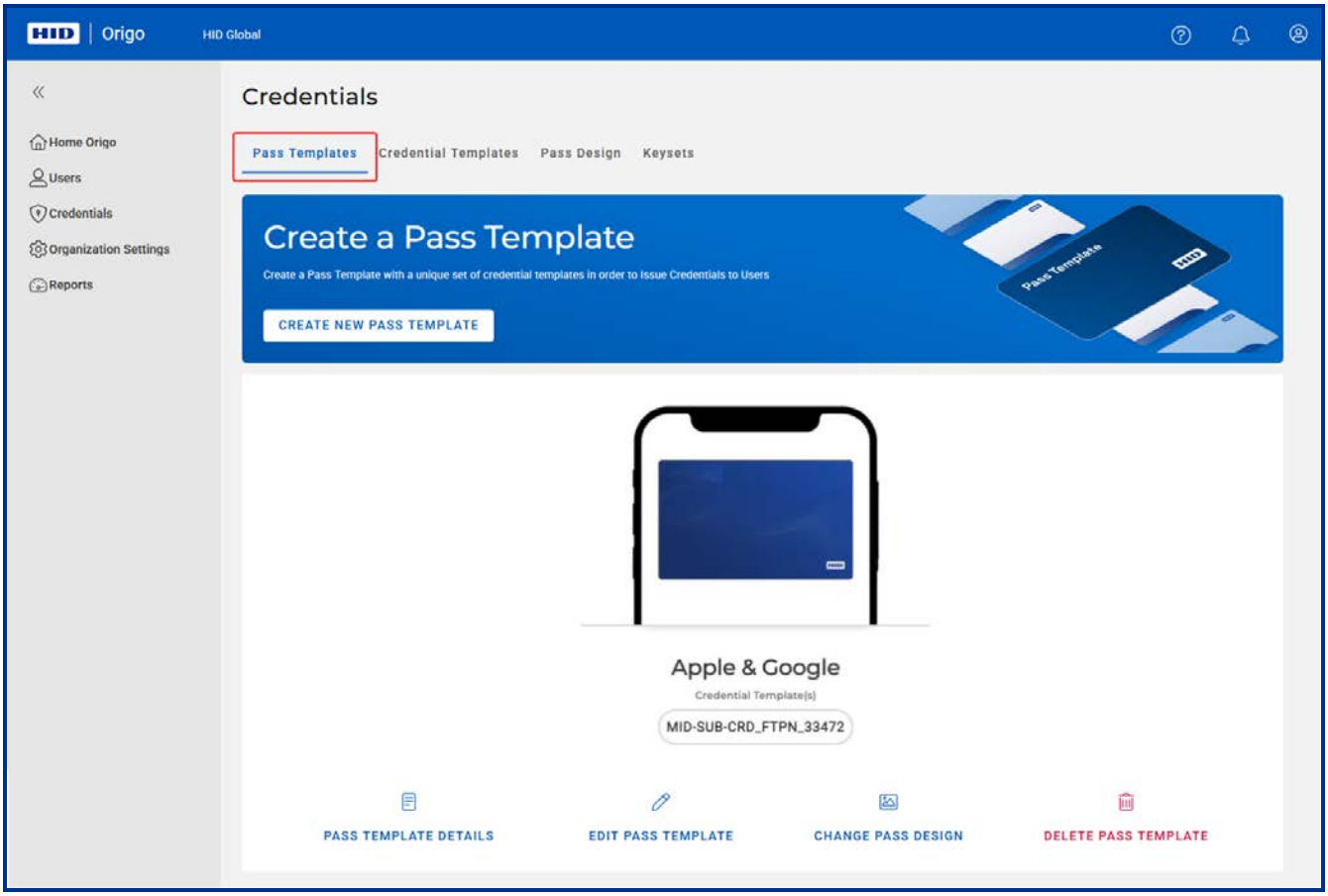


5.3 Create and manage Pass Templates

On the **Credentials** screen, and with the **Pass Templates** option selected, an administrator has the ability to create a new Pass Template, see **Create a new Pass Template** section.

Options are also available for the following:

- View details of a displayed Pass Template, see the **View Pass Template details** section.
- Edit a displayed Pass Template, see the **Edit Pass Template** section.
- Change a Pass Design, see the **Change Pass Design** section.
- Delete a Pass Template, see the **Delete Pass Template** section.



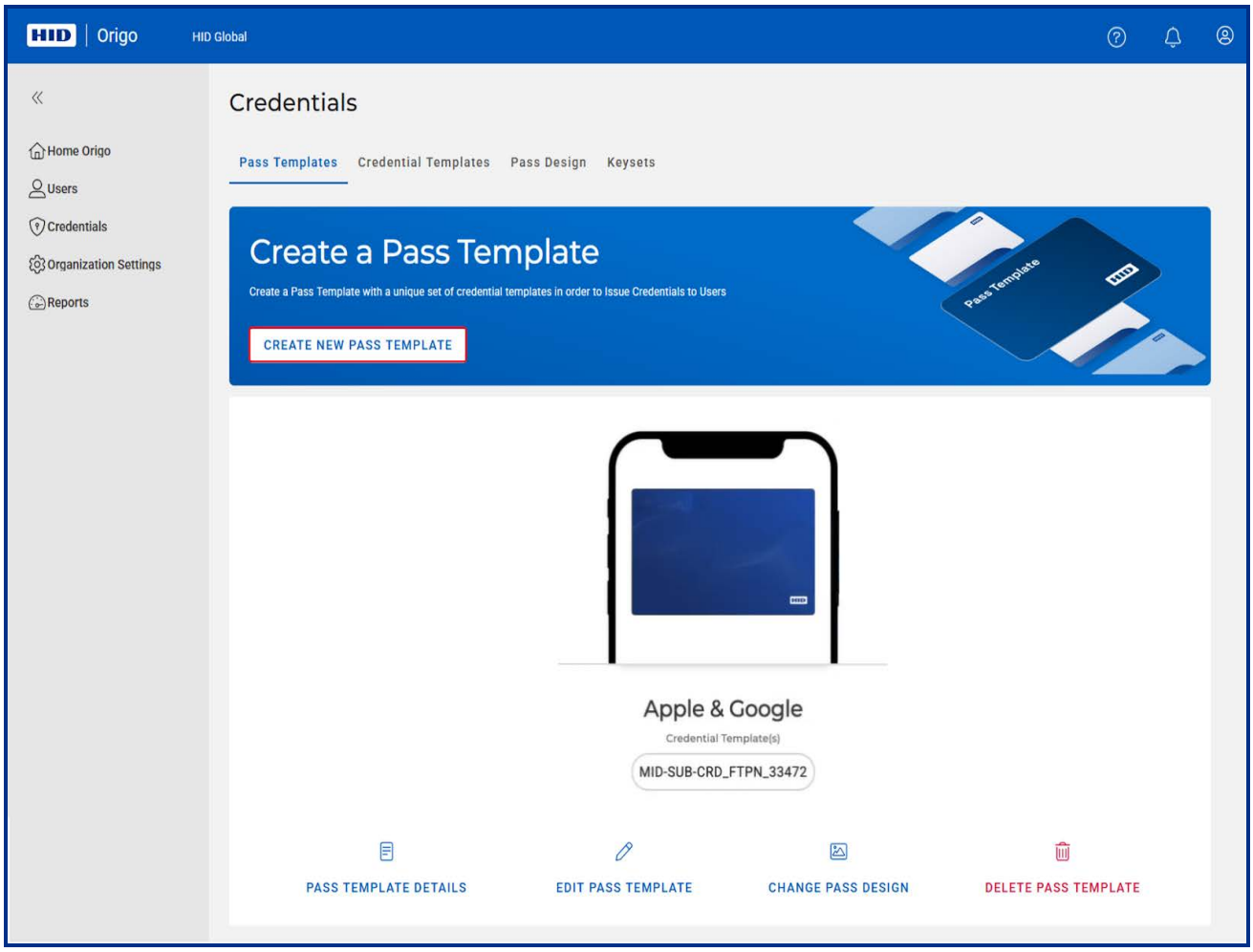
5.3.1 Create a new Pass Template

Note:
Before creating a new Pass Template:

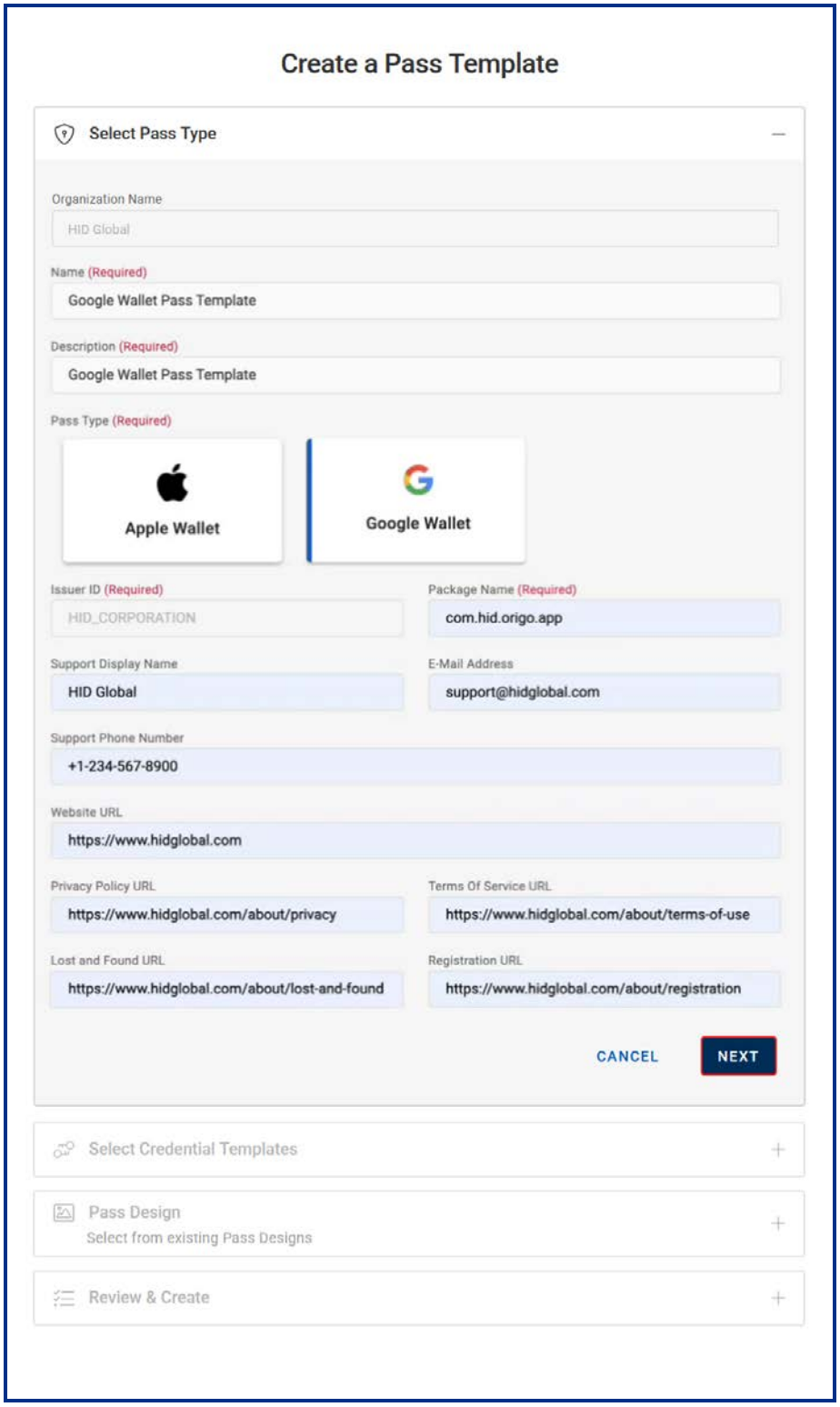
- Make sure the Organization has valid contracts, see the **License Usage & Reports** section.
- Make sure there are existing Credential Templates (see **View Credential Templates**) and Keysets (see **View Keysets**).
- Organization Pass Designs can be created for use in Pass Templates, see the **Create a Pass Design** section. If no Organization Pass Designs are available, the default blue background Pass Deign can be used.

To create a new Pass Template:

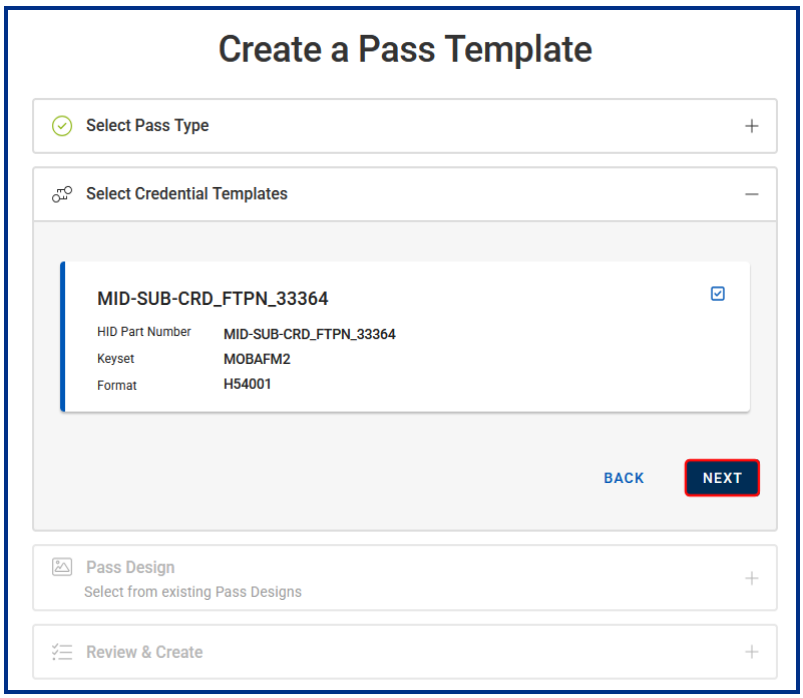
1. On the **Pass Templates** screen, click **CREATE NEW PASS TEMPLATE**.



2. In the **Select Pass Type** section, click the plus icon [+] to expand the section.
3. Enter the Pass information in the required fields and click **NEXT**.

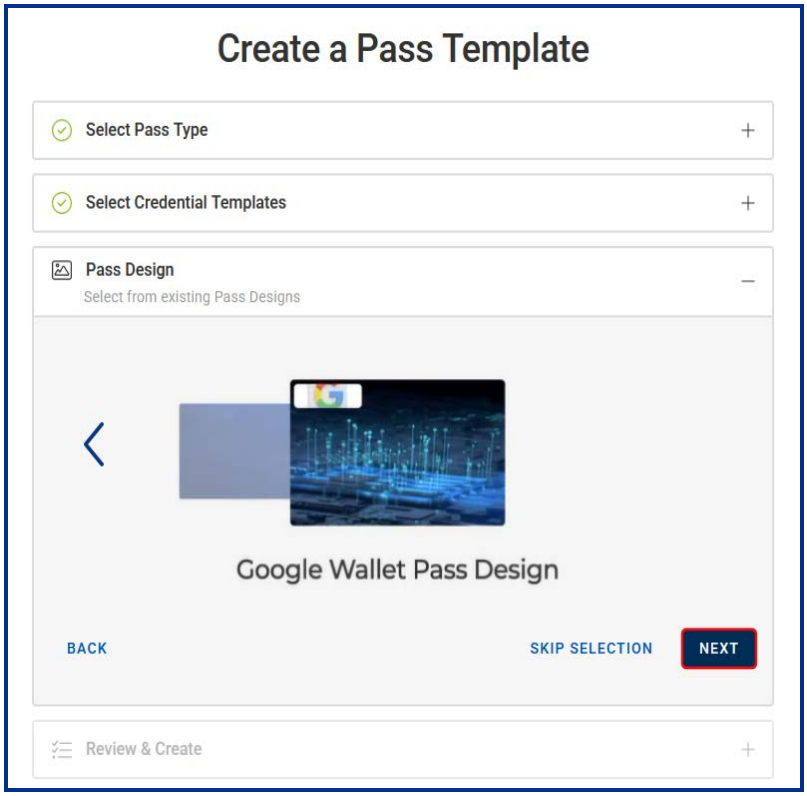


4. In the **Select Credential Templates** section, select the required Credential Template and click **NEXT**.



5. On the **Pass Design** screen use the arrow icons to scroll through and display existing Pass Designs. When the desired Pass design is displayed click **NEXT**.

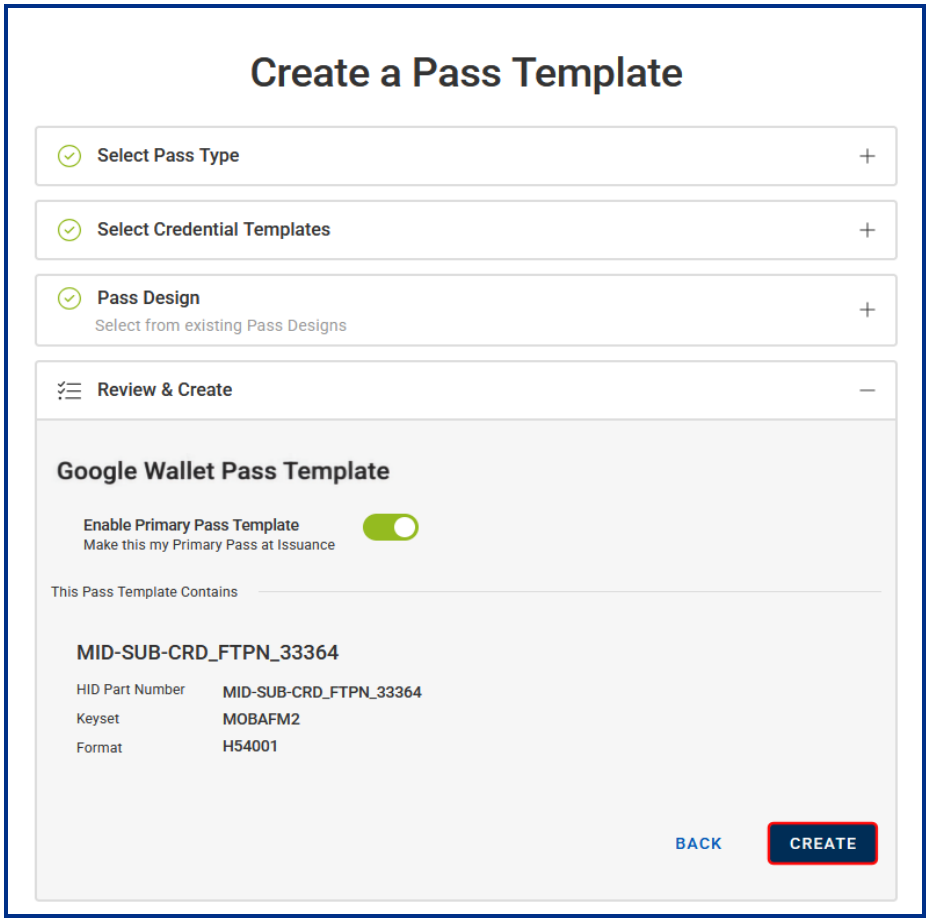
> **Note:** If no Organization Pass Designs are available, or the **SKIP SELECTION** option is selected, then the default blue background Pass Design is used.



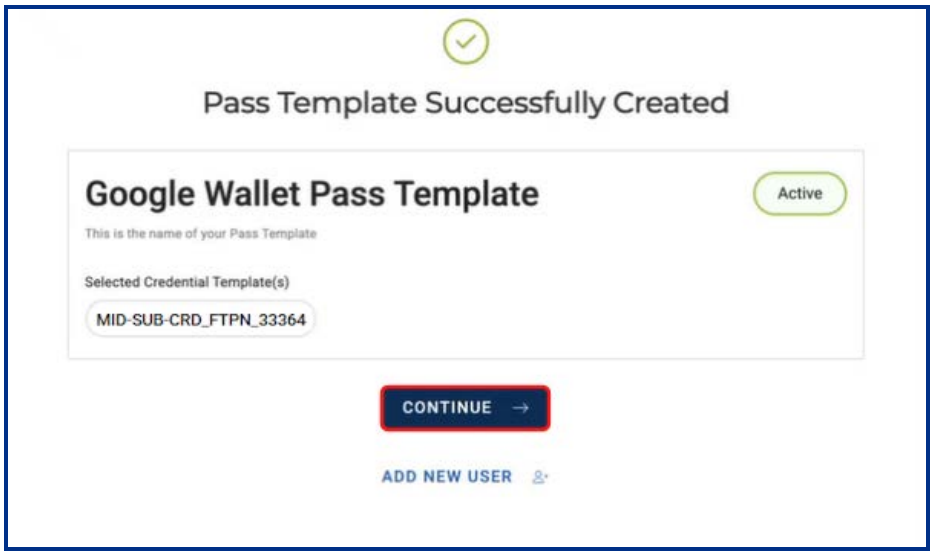
6. On the **Review & Create** screen review the Pass Template Name and included Credentials.

   Note: To make this Pass the primary Pass at issuance enable the **Enable Primary Pass Template** option.

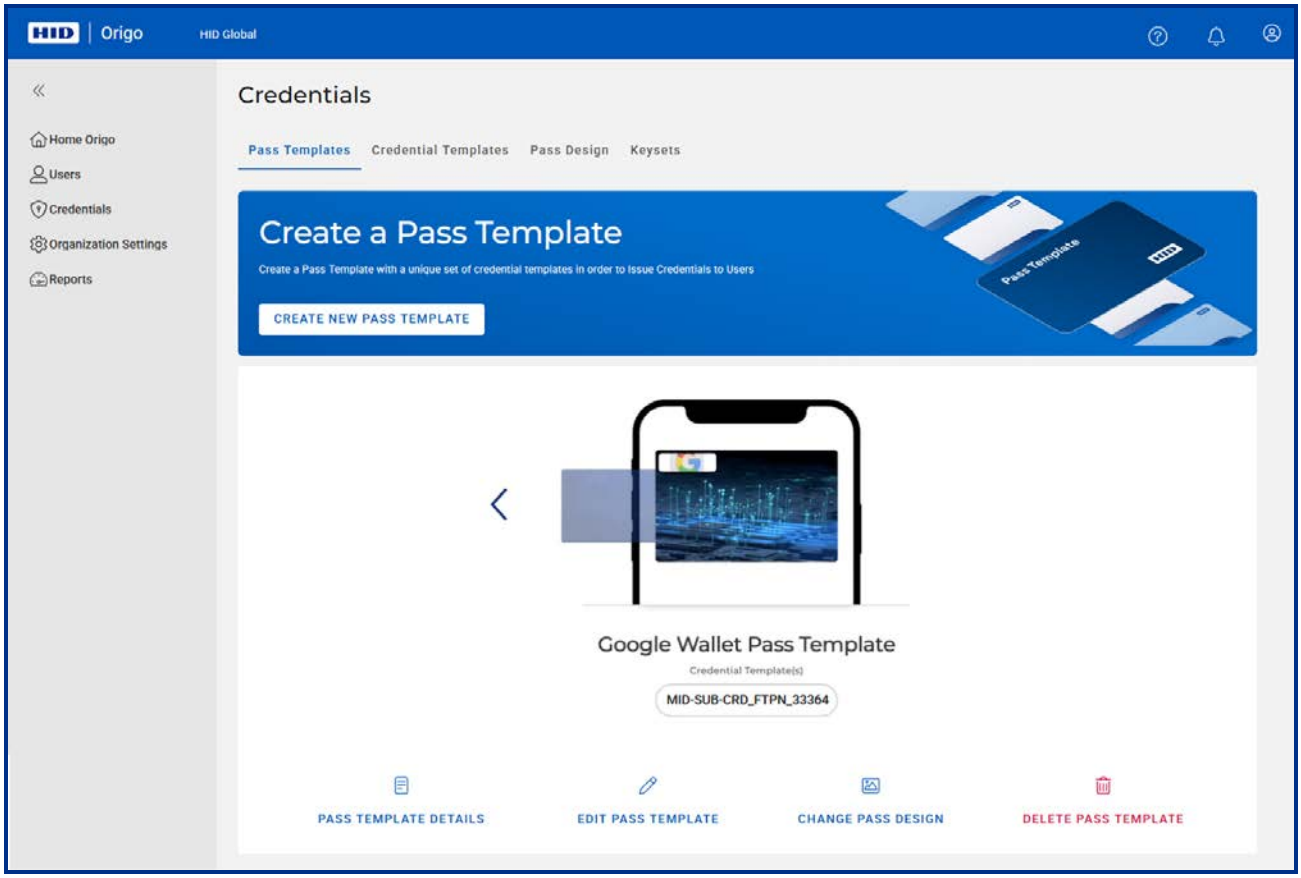
7. Click **CREATE** to save the Pass Template.



8. When the Pass Template is successfully created, click **CONTINUE**.

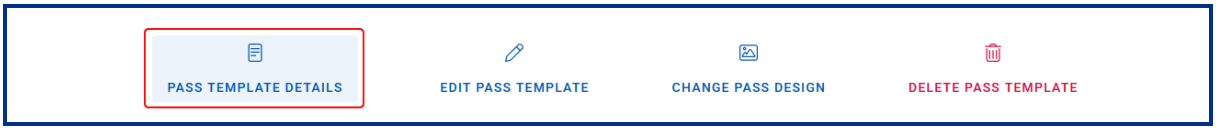


9. The Portal re-directs to the main **Pass Templates** screen where the newly created Pass Template is displayed. A Pass based on the newly created Pass Template can be issued to a user, see the **Issue Pass to Google Wallet** section.



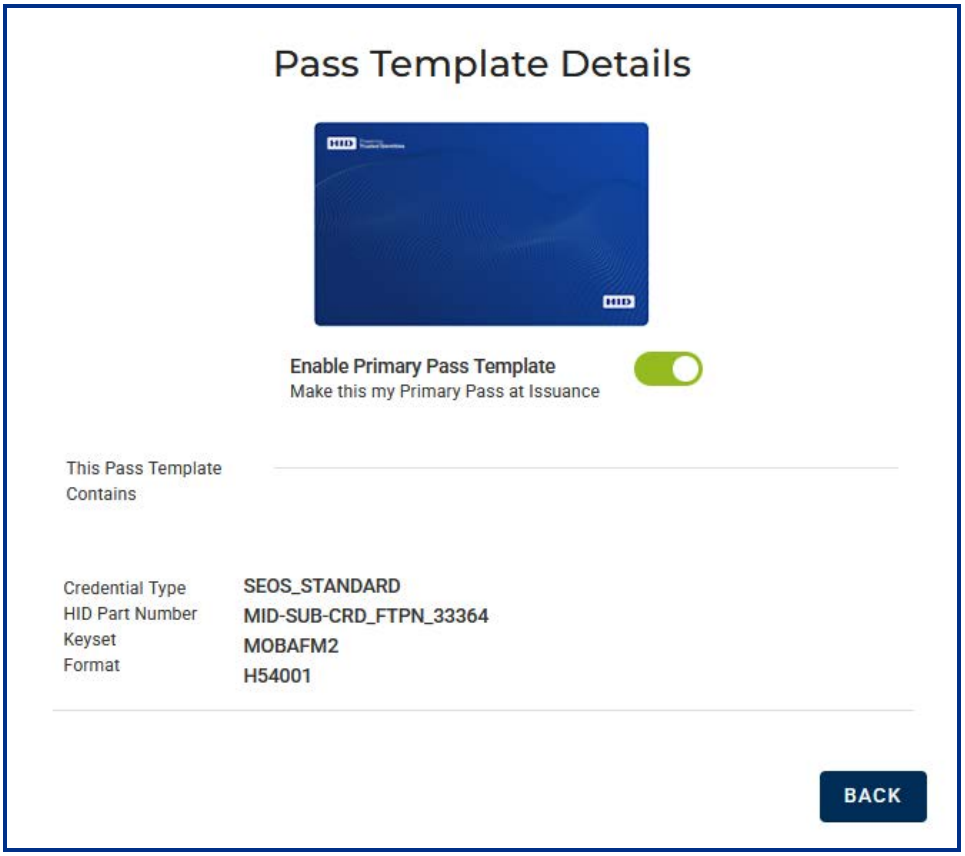
5.3.2 View Pass Template details

On the **Pass Templates** screen, for a displayed Pass, select the **PASS TEMPLATE DETAILS** option.



On the **Pass Template Details** screen you can view the credentials contained within the Pass.

> **Note:** To make this Pass the primary Pass at issuance, enable the **Enable Primary Pass Template** option.

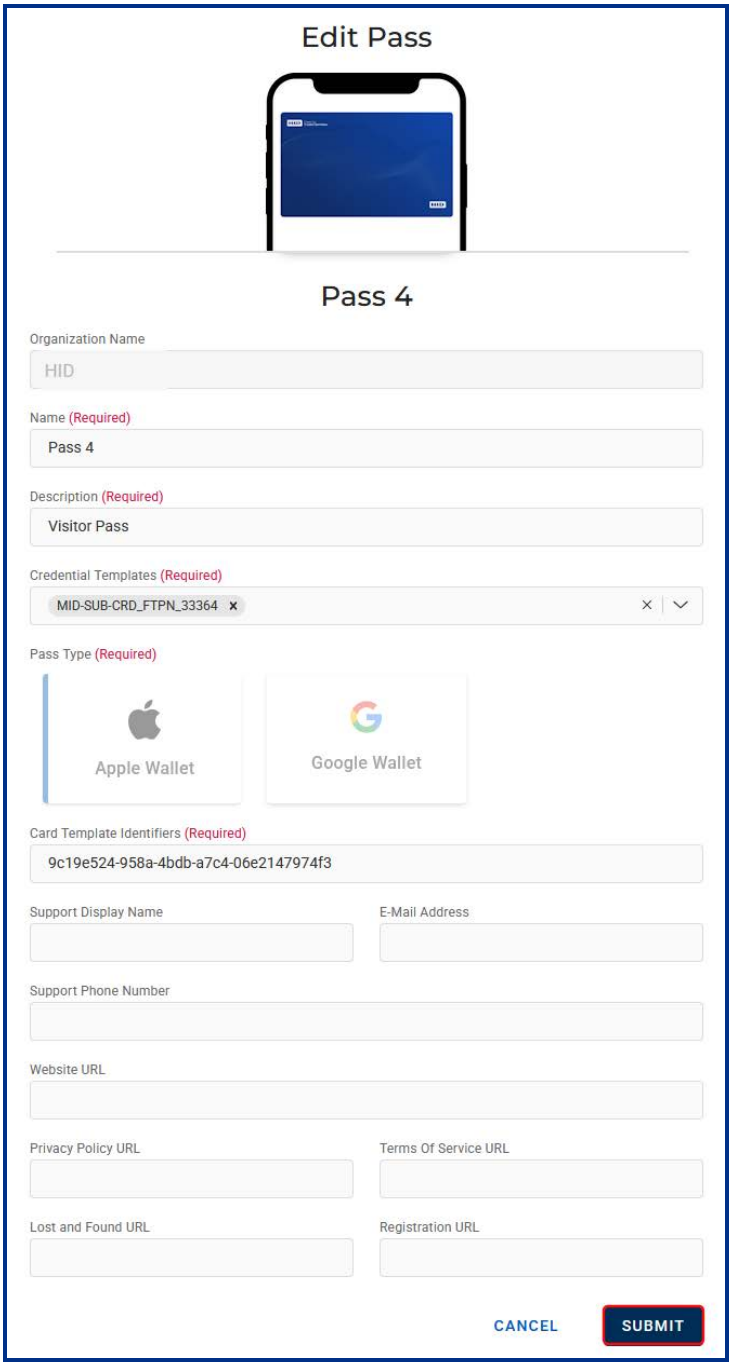


5.3.3 Edit Pass Template

On the **Pass Templates** screen, for a displayed Pass, select the **EDIT PASS TEMPLATE** option.



On the **Edit Pass** screen, update the required fields and click **SUBMIT**.

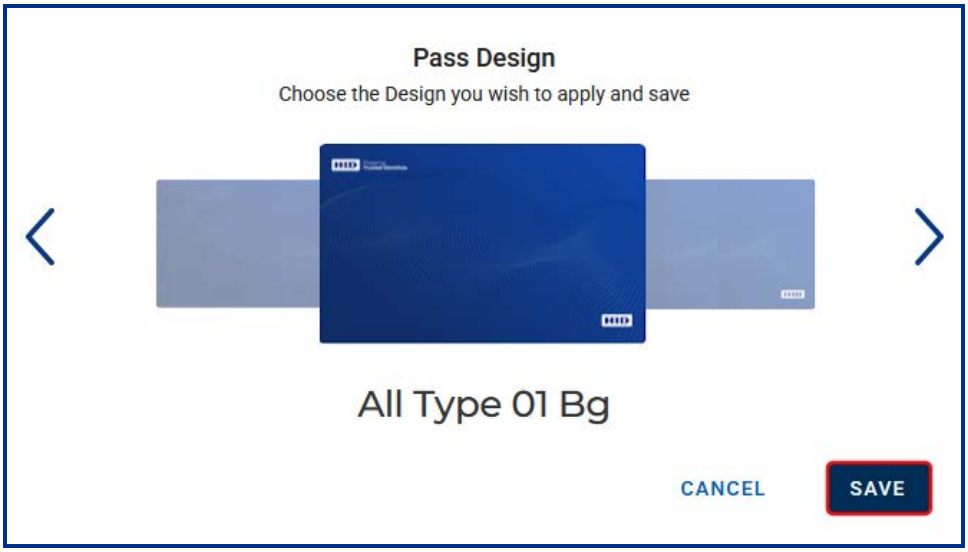


5.3.4 Change Pass Design

On the **Pass Templates** screen, for a displayed Pass, select the **CHANGE PASS DESIGN** option.



On the **Pass Design** screen, use the arrow icons to scroll through existing Pass designs. When the desired Pass design is displayed click **SAVE**.



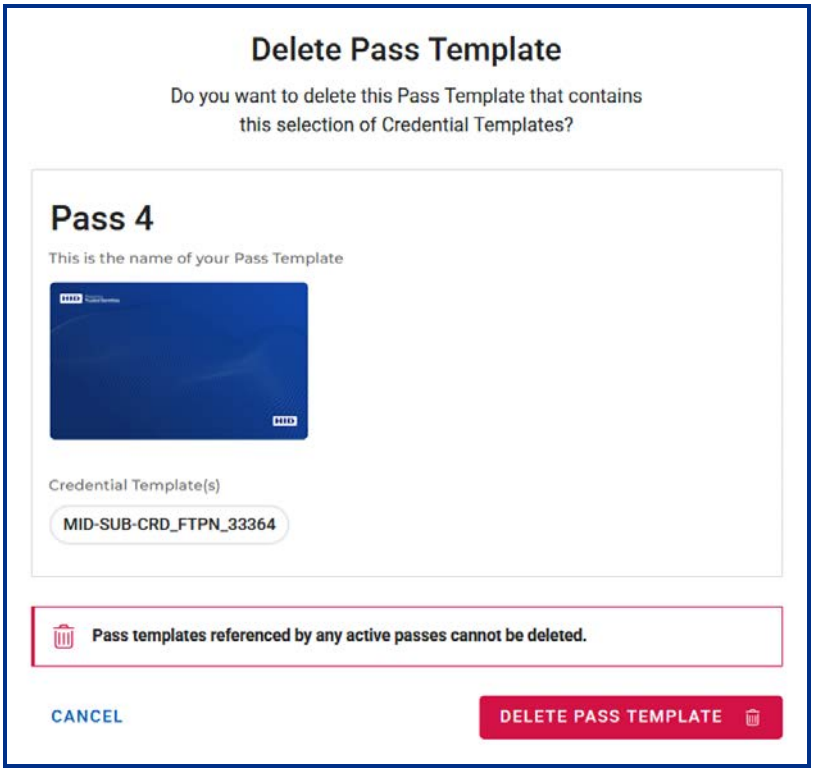
5.3.5 Delete Pass Template

On the **Pass Templates** screen, for a displayed Pass, select the **DELETE PASS TEMPLATE** option.



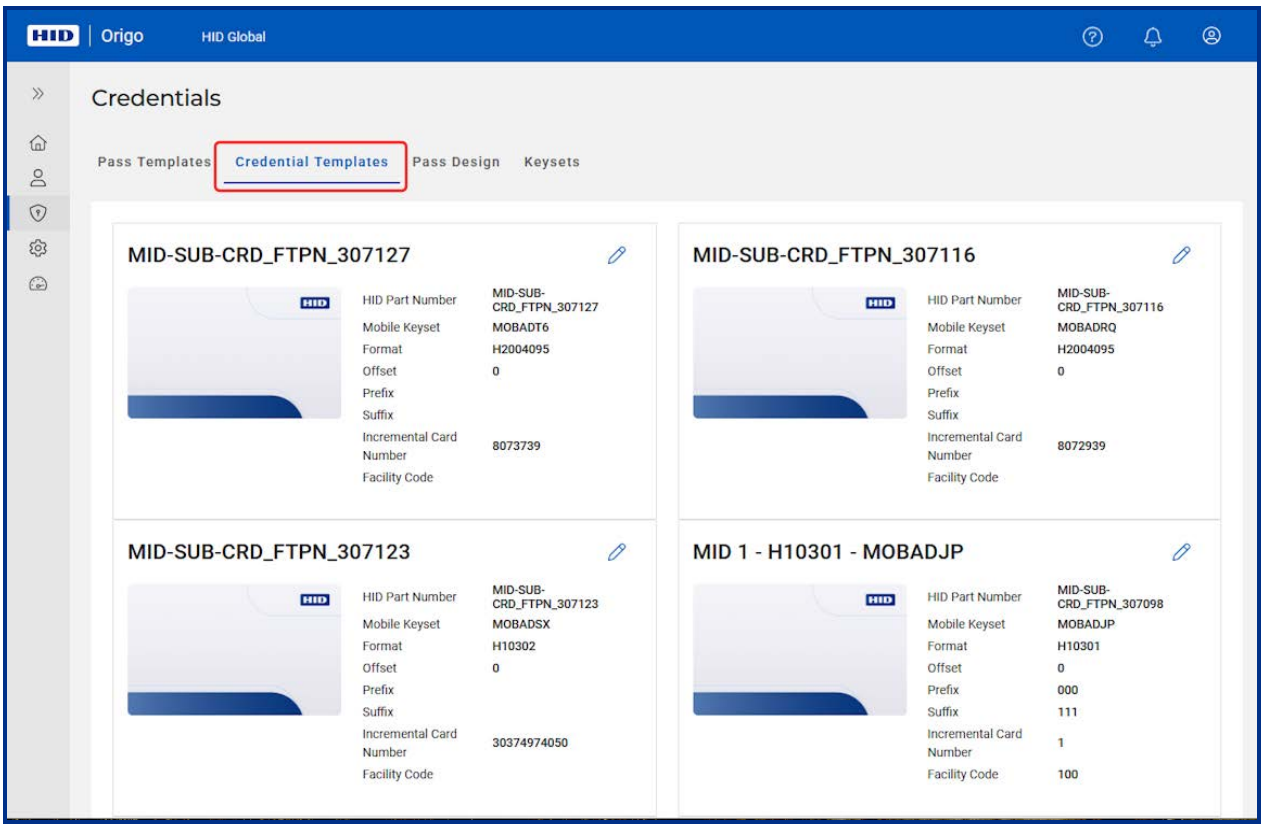
Click **DELETE PASS TEMPLATE** to remove the Pass Template.

Note:
- This action only deletes the Pass. The Credentials are not deleted.
- A Pass Template cannot be deleted if it is referenced by any Active passes.

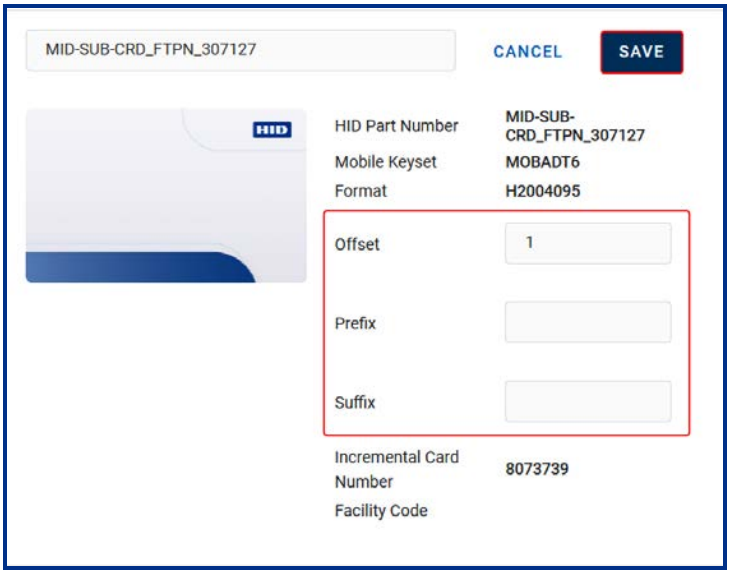


5.4 View Credential Templates

On the **Credentials** screen, click **Credential Templates**. The Credentials associated with your Organization are displayed.

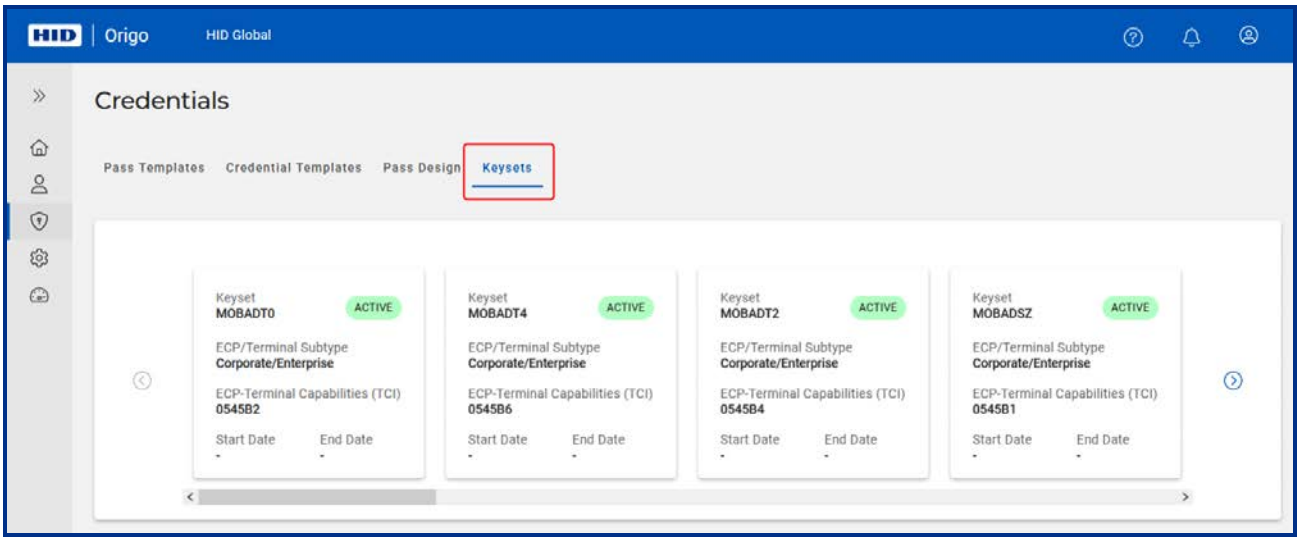


An Administrator has the ability to set the **Offset** value and enter a **Prefix** and **Suffix**. Click the edit icon [✎] associated with a displayed Credential. Set the **Offset** value and enter a **Prefix** and **Suffix** as required and click **SAVE**.



5.5 View Keysets

On the **Credentials** screen, click **Keysets**. The Keysets associated with your Organization are displayed.



Section 06

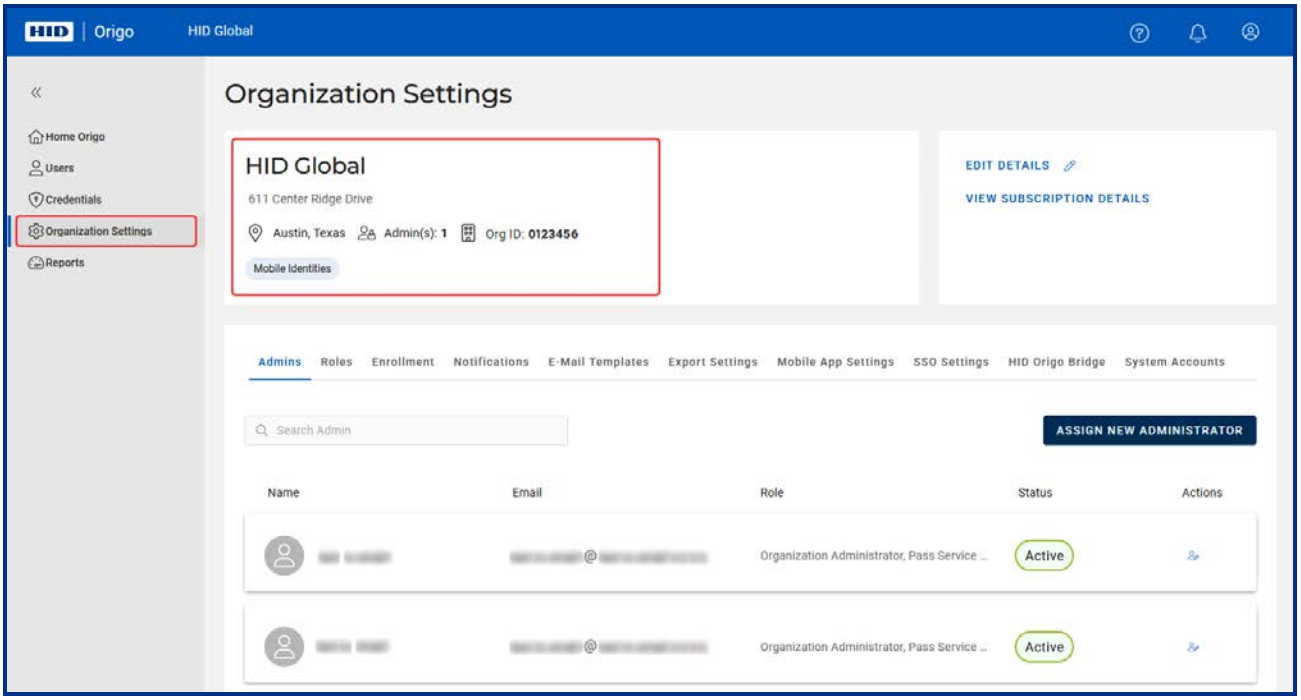
Organization Management

6.1 Organization management overview

From the left navigation menu, select the **Organization Settings** option. On the **Organization Settings** screen, the top left section displays a widget containing Organization specific details including, Organization name, Organization ID, Address, Admin(s), and the services your Organization has enrolled in.

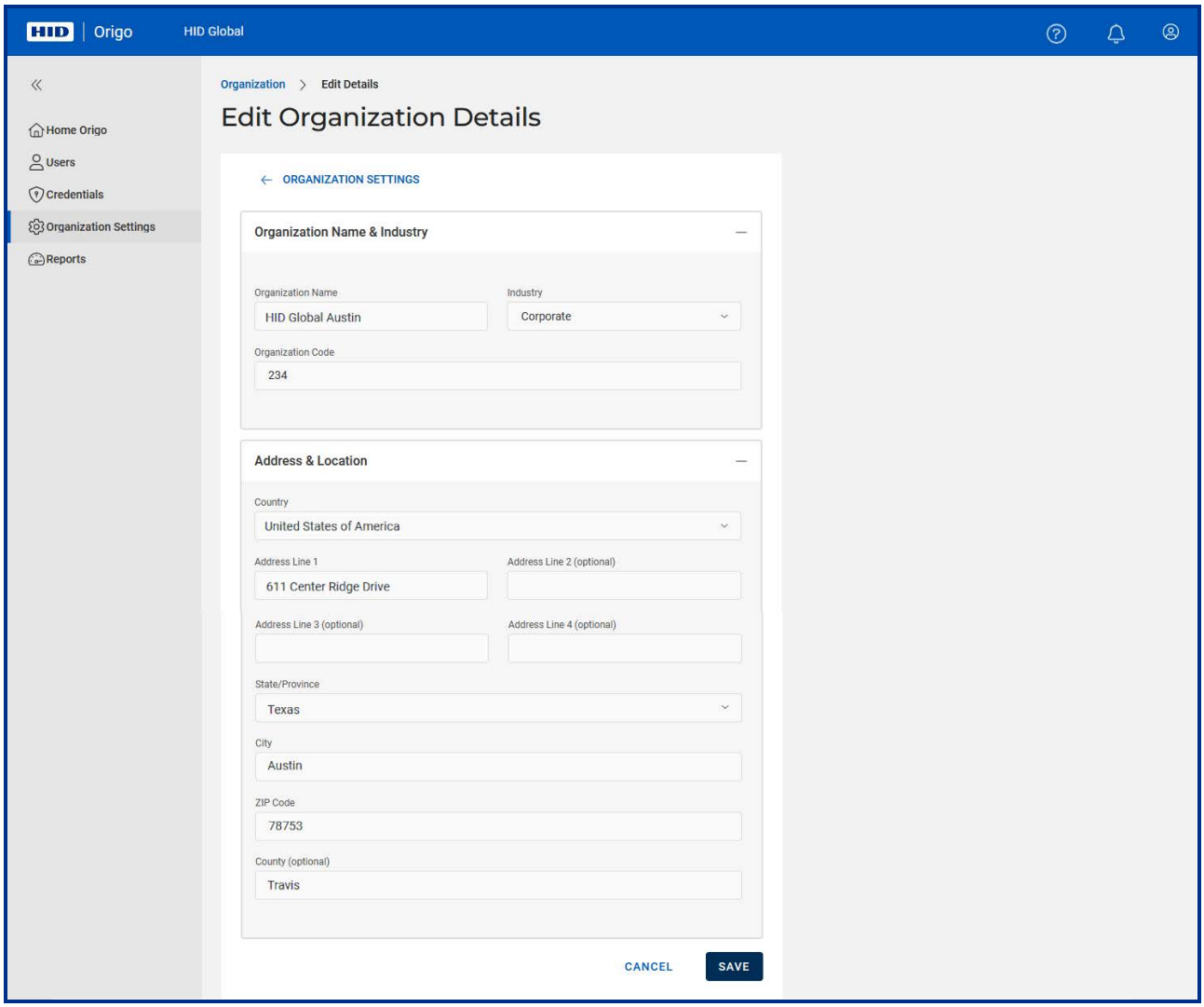
The **Organization Settings** screen also provides administrators with options to:

- Edit the details of an Organization. See the **Edit Organization details** section.
- View Subscription plan and License information. See the **View Subscription details** section.
- Assign new Administrators and manage existing Administrators. See the **Manage Administrators** section.
- View Administrator roles and associated permissions. See the **View Roles and Permissions** section.
- Select the data fields that are displayed for user enrollment. See the **Configure enrollment details** section.
- Configure notifications. See the **Configure notifications** section.
- Customize or edit E-Mail Templates. See the **Customize or edit E-Mail templates** section.
- Select the items to be included when the user records are exported. See the **Export settings** section.
- Configure HID Mobile Access App settings. See the **Mobile App settings** section.
- Configure Single Sign On (SSO) settings. See the **Configure Single Sign On settings** section.
- Create and manage system accounts. See the **Create and manage System Accounts** section.



6.2 Edit Organization details

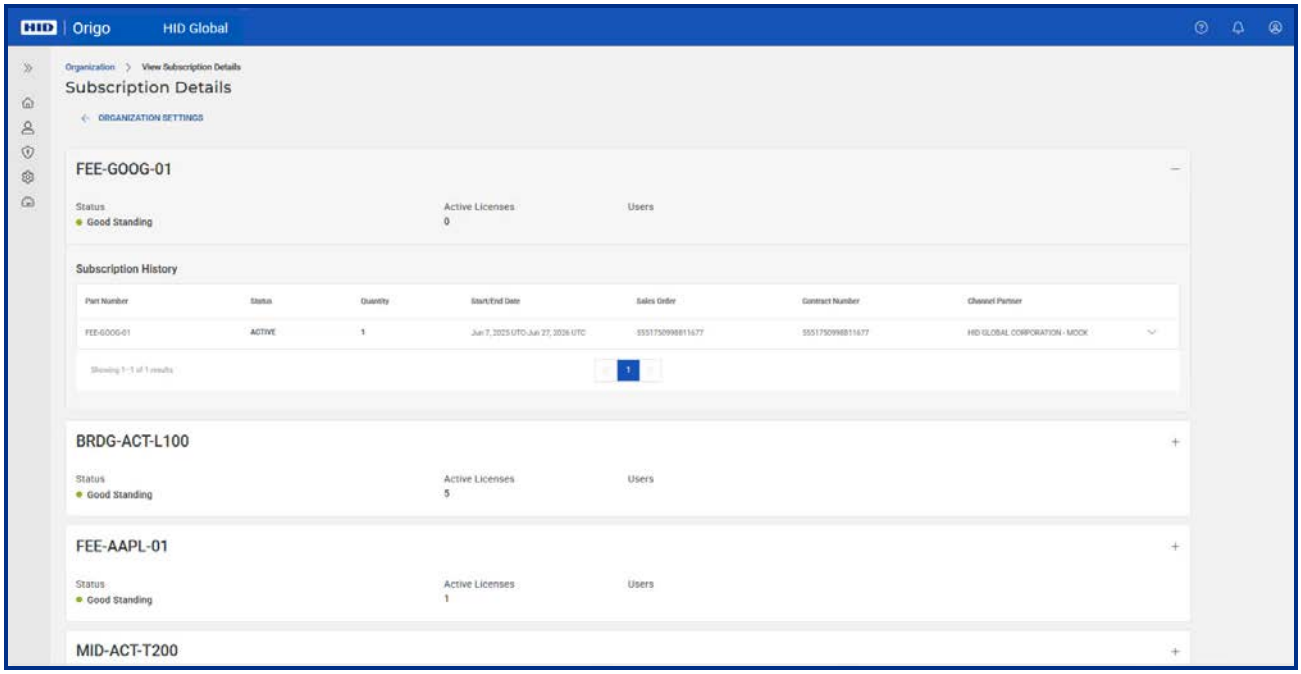
1. On the **Organization Settings** screen, click **EDIT DETAILS**.
2. On the **Edit Organization Details** screen, click the plus icon [+] to expand each section.
3. Edit the required Organization information and click **SAVE**.



6.3 View Subscription details

1. On the **Organization Settings** screen, click **VIEW SUBSCRIPTION DETAILS**.
2. Your subscription plans along with license information are displayed.

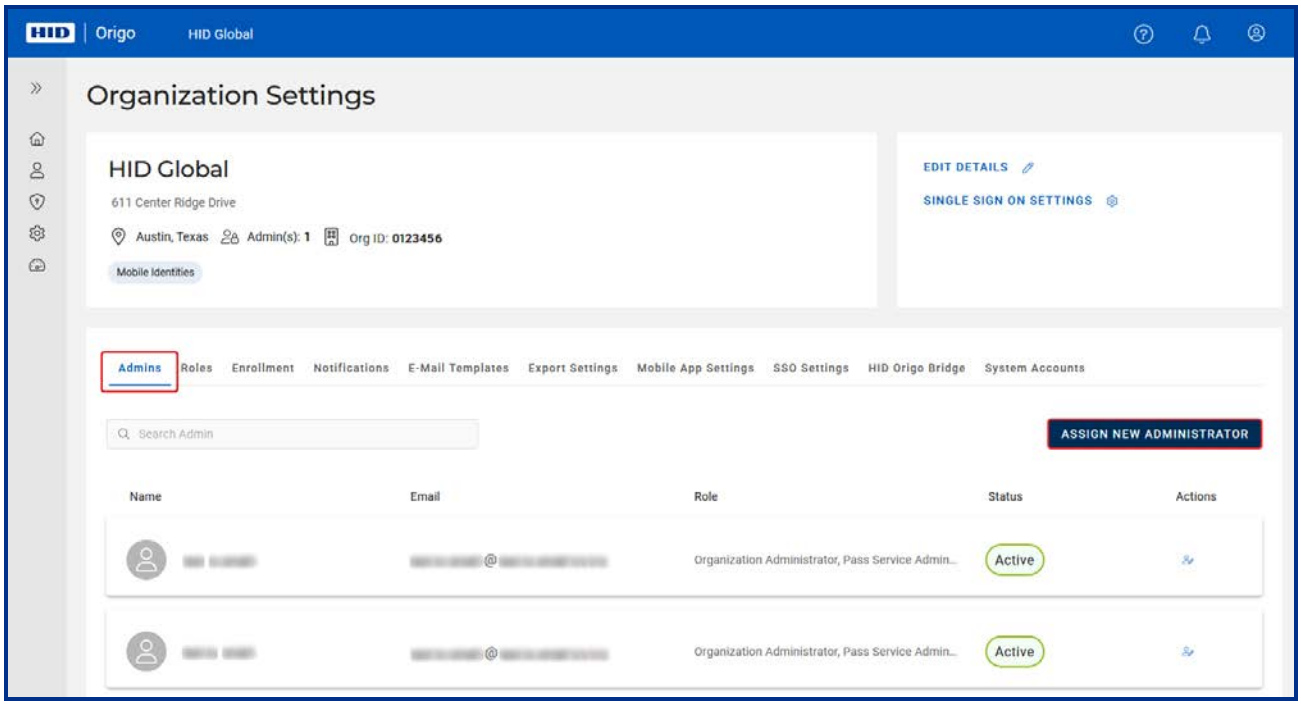
> **Note:** Click on the plus icon [+] to view additional Subscription History information.



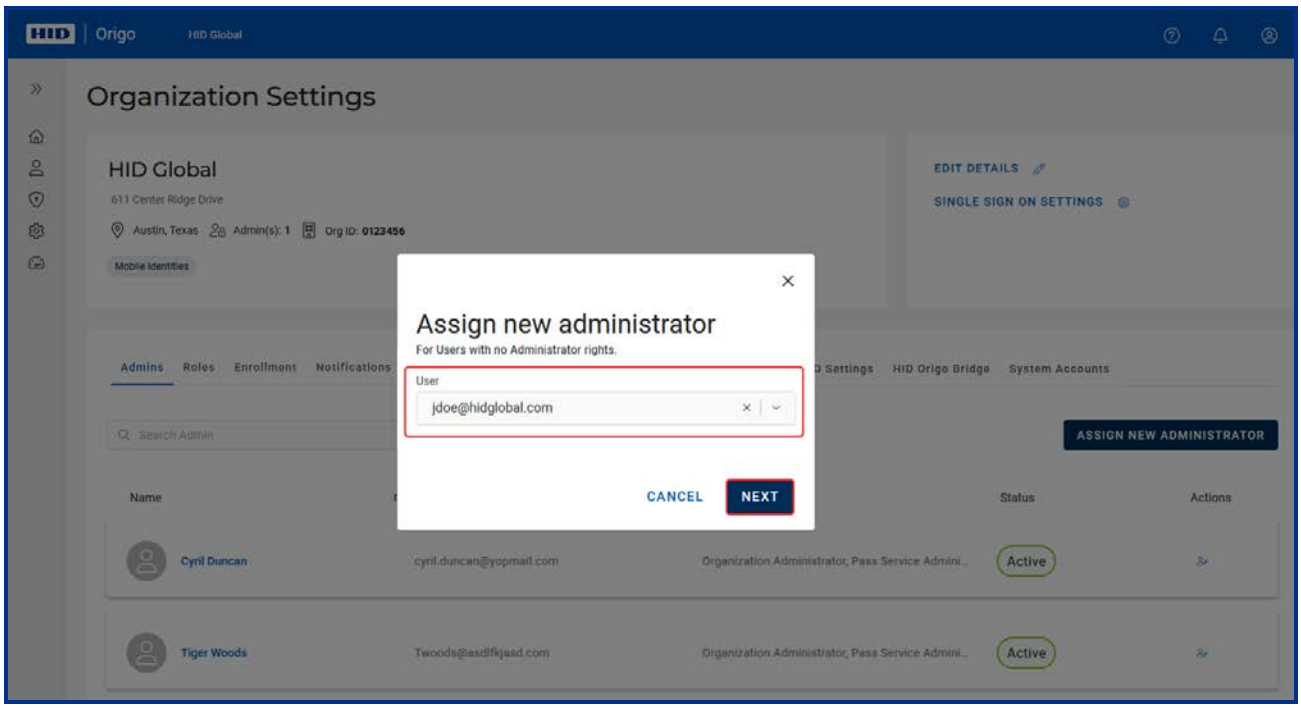
6.4 Manage Administrators

6.4.1 Assign new Administrator

1. On the **Organization Settings** screen, under **Admins**, click **ASSIGN NEW ADMINISTRATOR**.

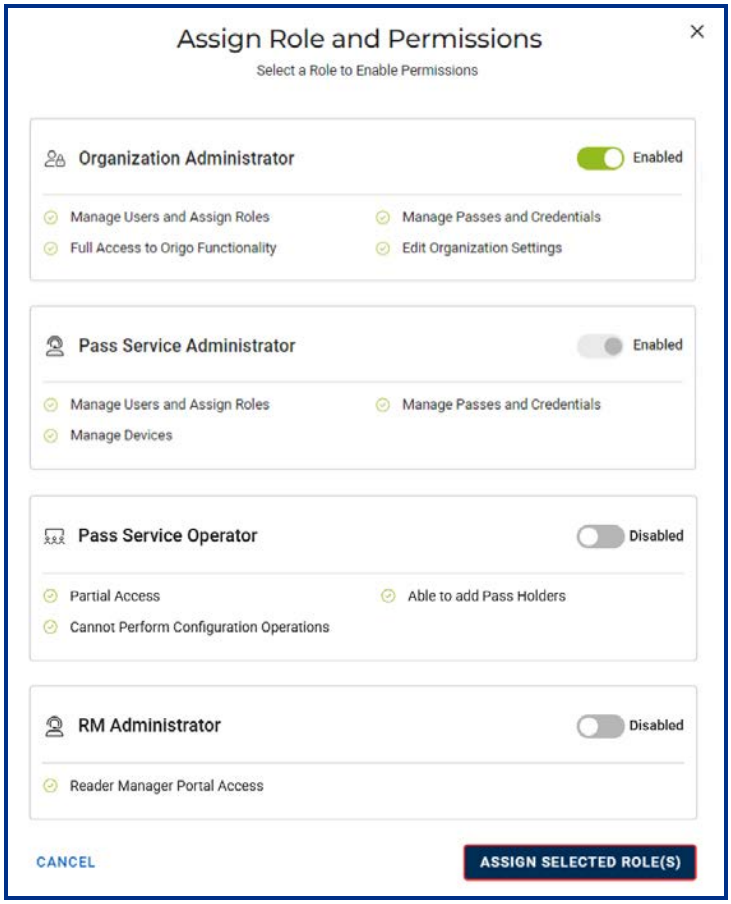


2. Select a user with no administrator rights from the drop-down list or search for an existing user by entering their E-Mail address.
3. Click **NEXT**.



4. Enable the required roles and associated permissions for the new administrator and click **ASSIGN SELECTED ROLE(S)**.

> **Note:** Enable a role to select the associated permissions.

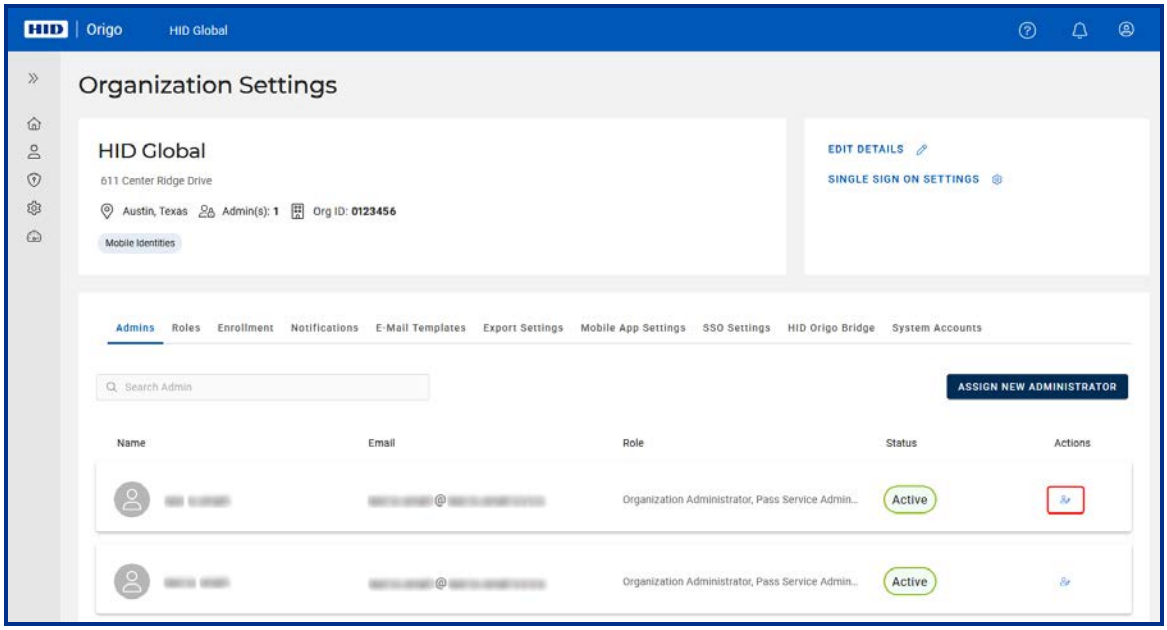


Role	Permission
Organization Admin	• Manage Users and Assign Roles • Manage Passes and Credentials • Full Access to Origo Functionality • Edit Organization Settings
Pass Service Administrator	• Manage Users and Assign Roles • Manage Passes and Credentials • Manage Devices
Pass Service Operator	• Partial Access • Able to add Users
RM Administrator	• Reader Manager Portal Access

> **Note:** Roles are hierarchical, therefore, if you enable Organization Administrator, you will also have Pass Service Administrator and Pass Service Operator enabled. If you enable Pass Service Administrator, you will also have Pass Service Operator enabled.

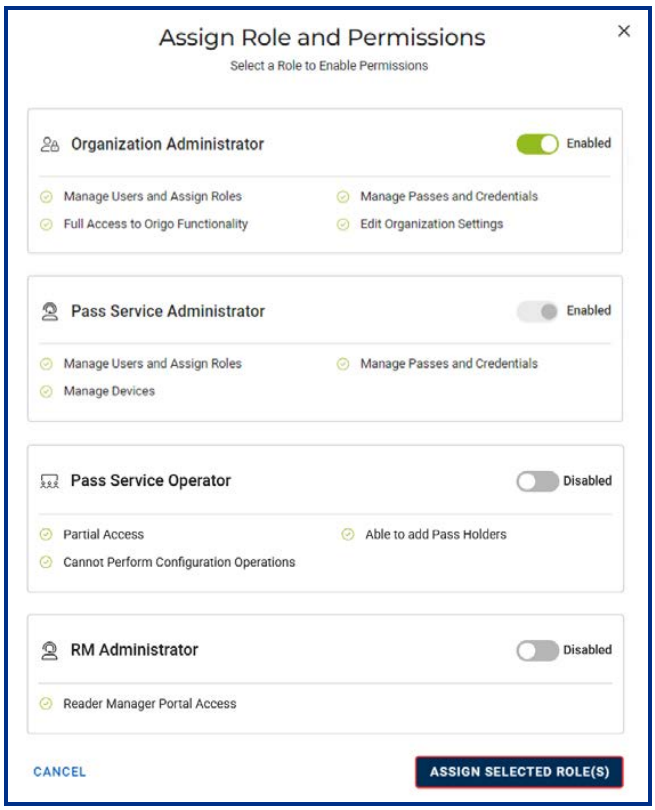
6.4.2 Manage existing Administrators

1. On the **Organization Settings** screen, under **Admins**, click the edit icon [ ] associated with a displayed administrator.



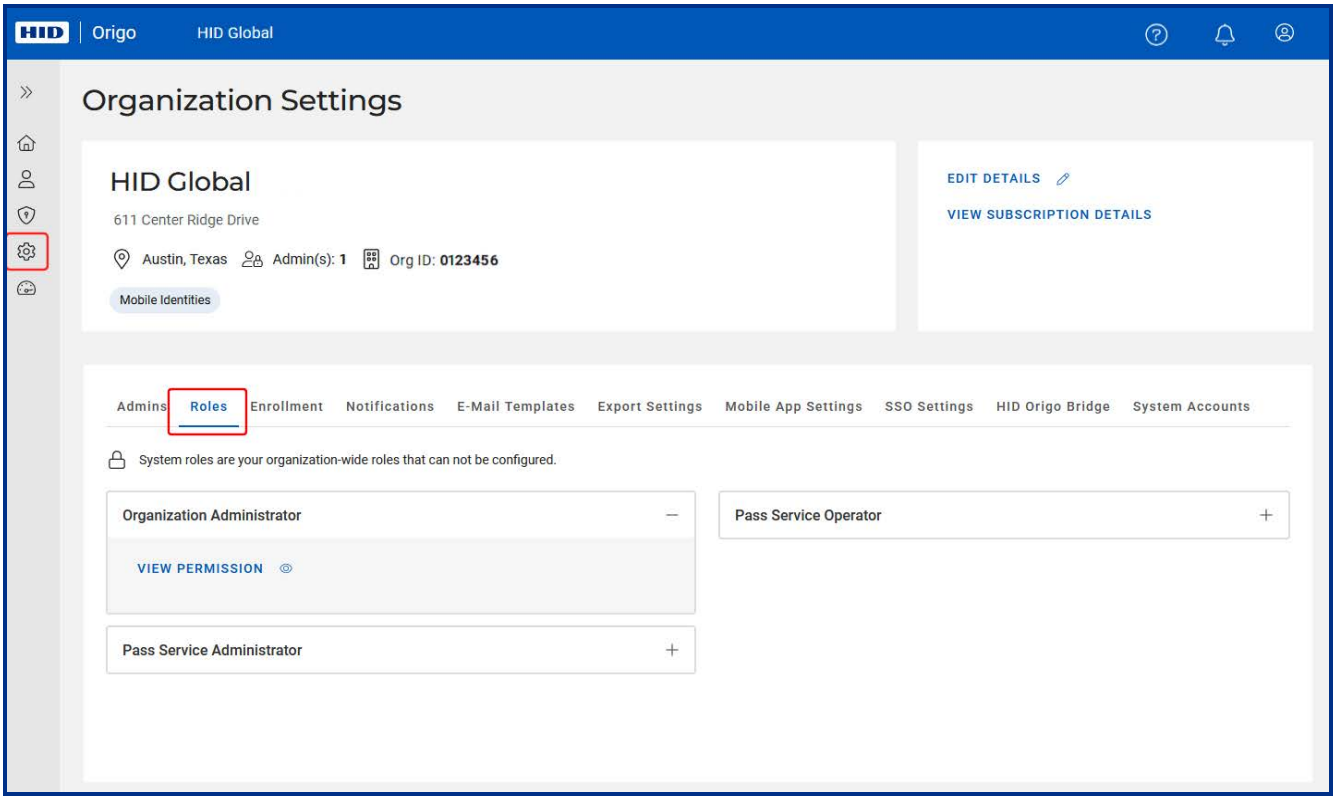
2. Enable the required roles and associated permissions for the administrator and click **ASSIGN SELECTED ROLE(S)**.

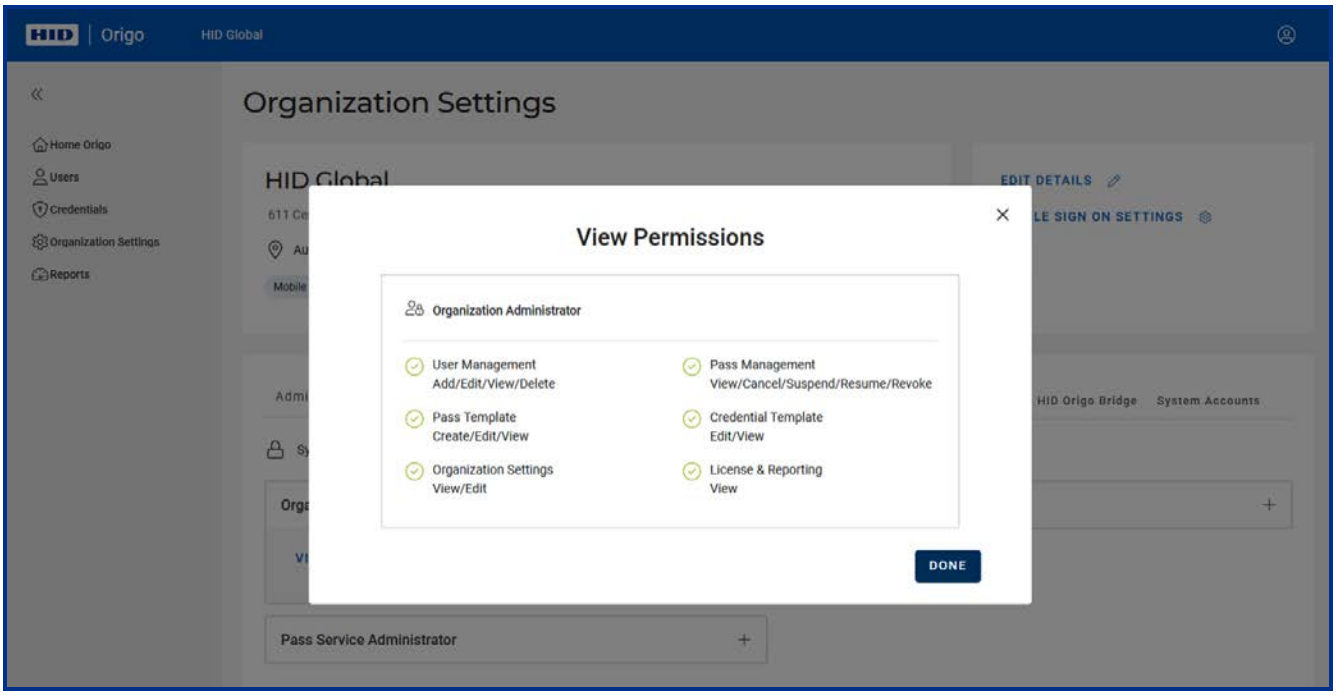
> **Note:** Enable a role to select the associated permissions.



6.5 View Roles and Permissions

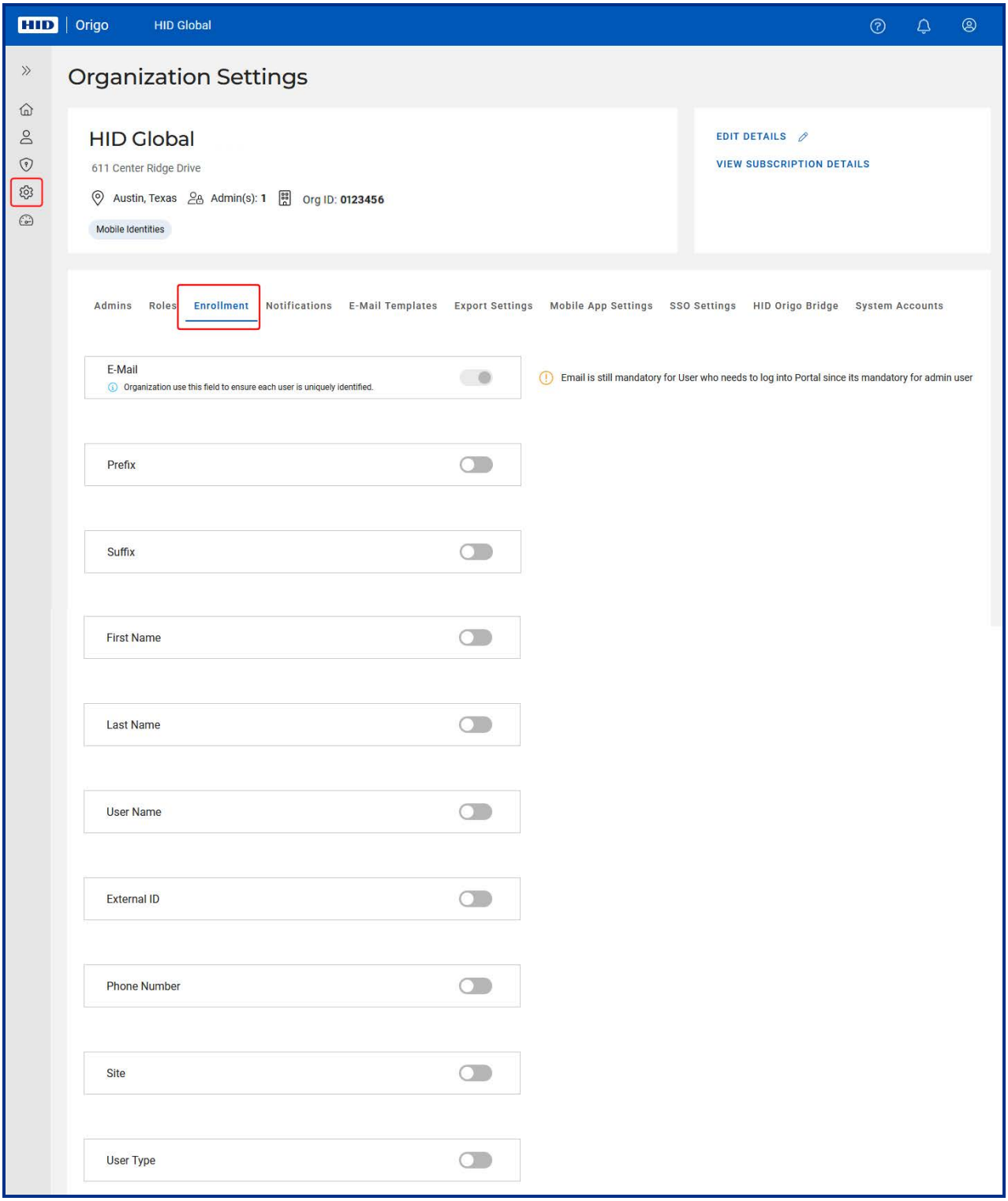
On the **Organization Settings** screen, select the **Roles** option to display the various roles that can be assigned to a user. For any displayed role, click the plus icon [+] and **VIEW PERMISSION** to display the permissions associated with that role.





6.6 Configure enrollment details

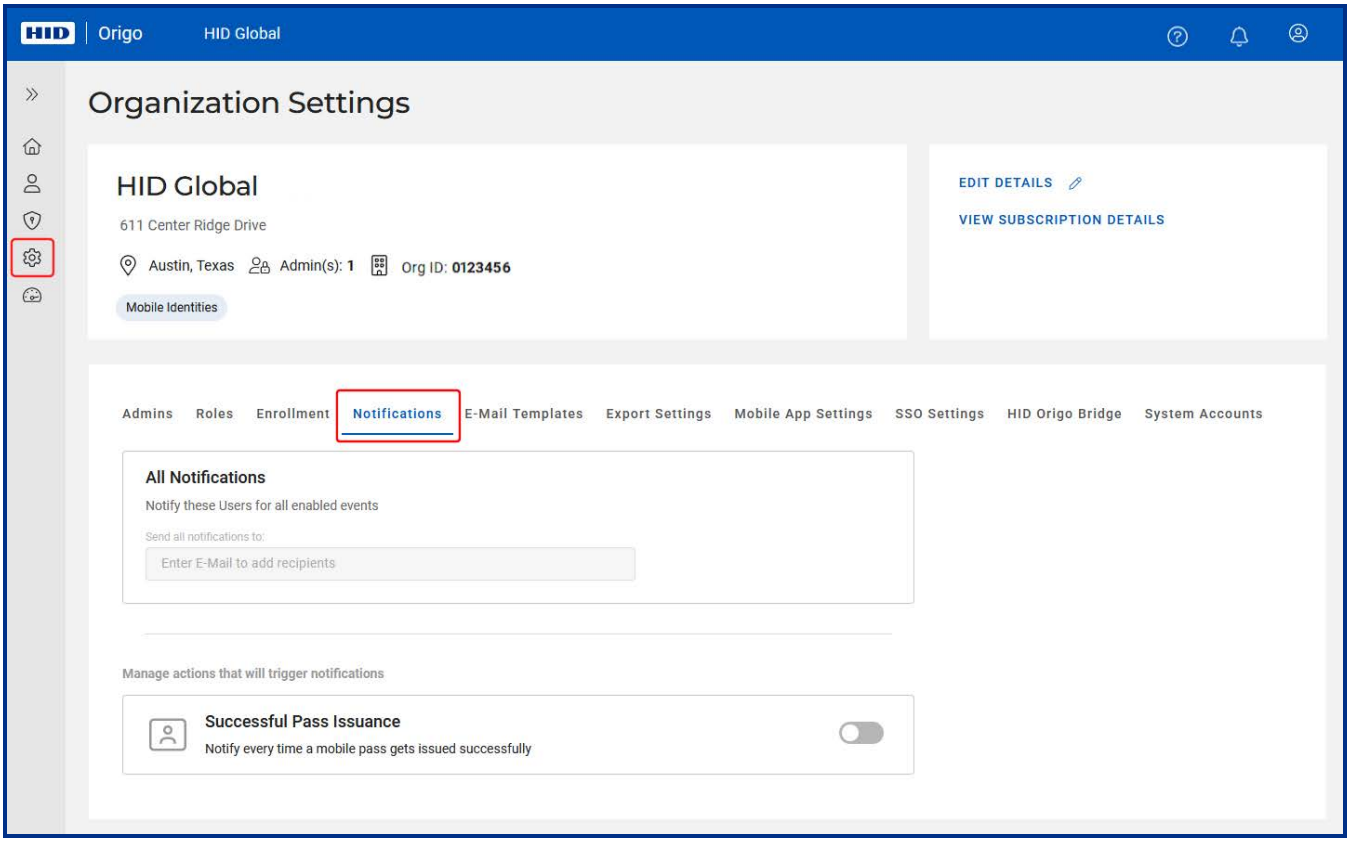
On the **Organization Settings** screen and select the **Enrollment** option. Enable the required user detail items to display when enrolling a user.



6.7 Configure notifications

On the **Organization Settings** screen, select the **Notifications** option.

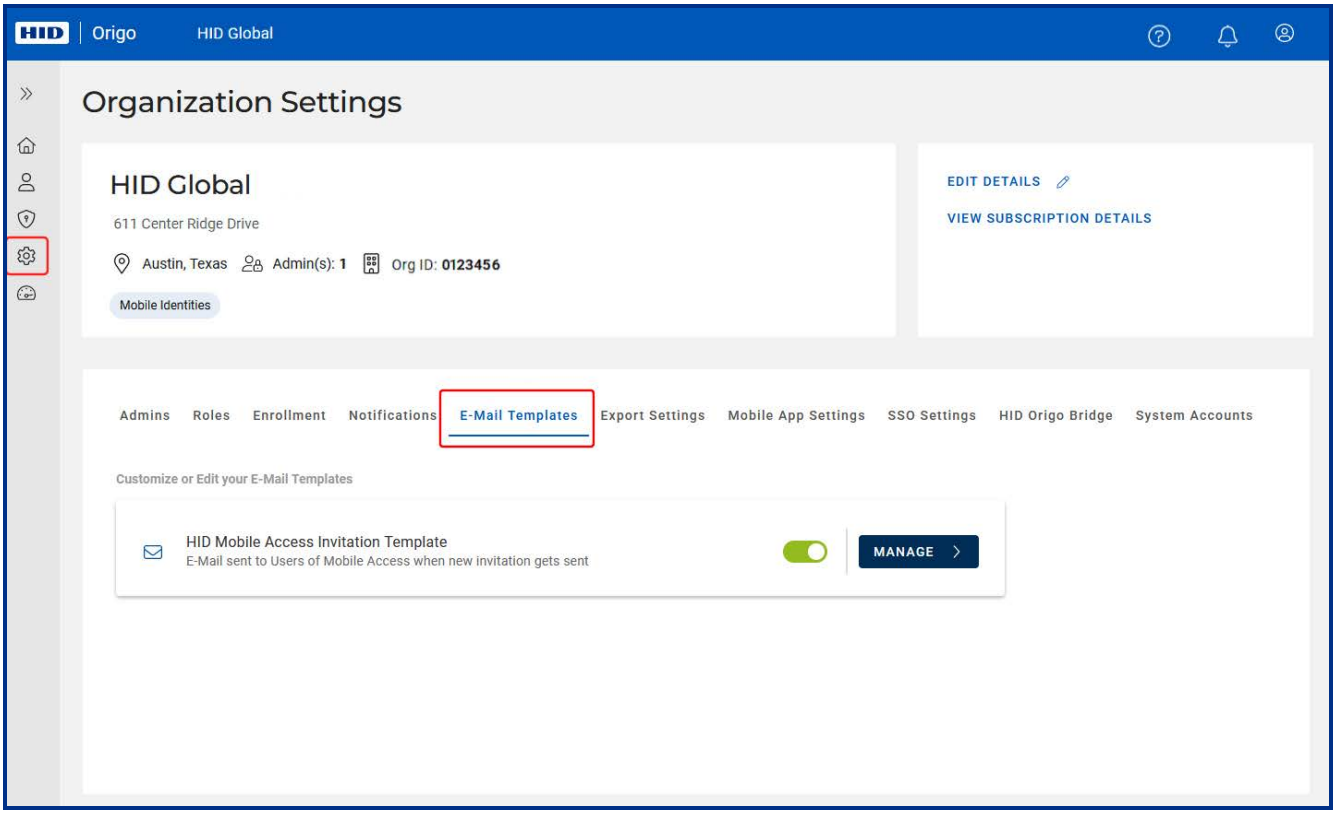
- In the **All Notifications** section you can enter user E-Mail addresses for users to receive event notifications
- Enable or disable actions that trigger notifications.



6.8 Customize or edit E-Mail templates

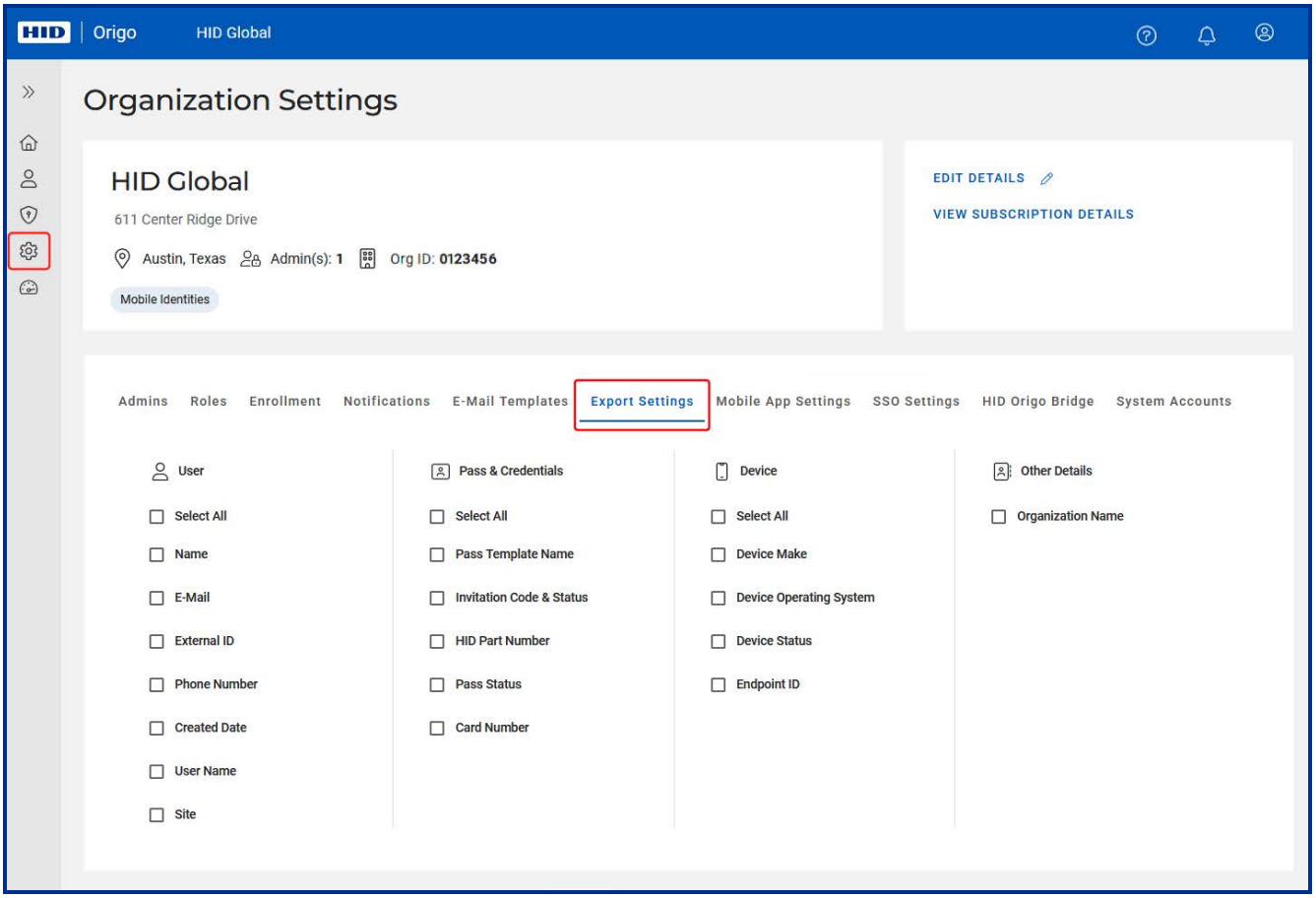
On the **Organization Settings** screen, select the **E-Mail Templates** option.

- Configure when the E-Mail is sent to users.
- Click **MANAGE** to customize and save the HID Mobile Access invitation E-Mail template or reset to the default template.



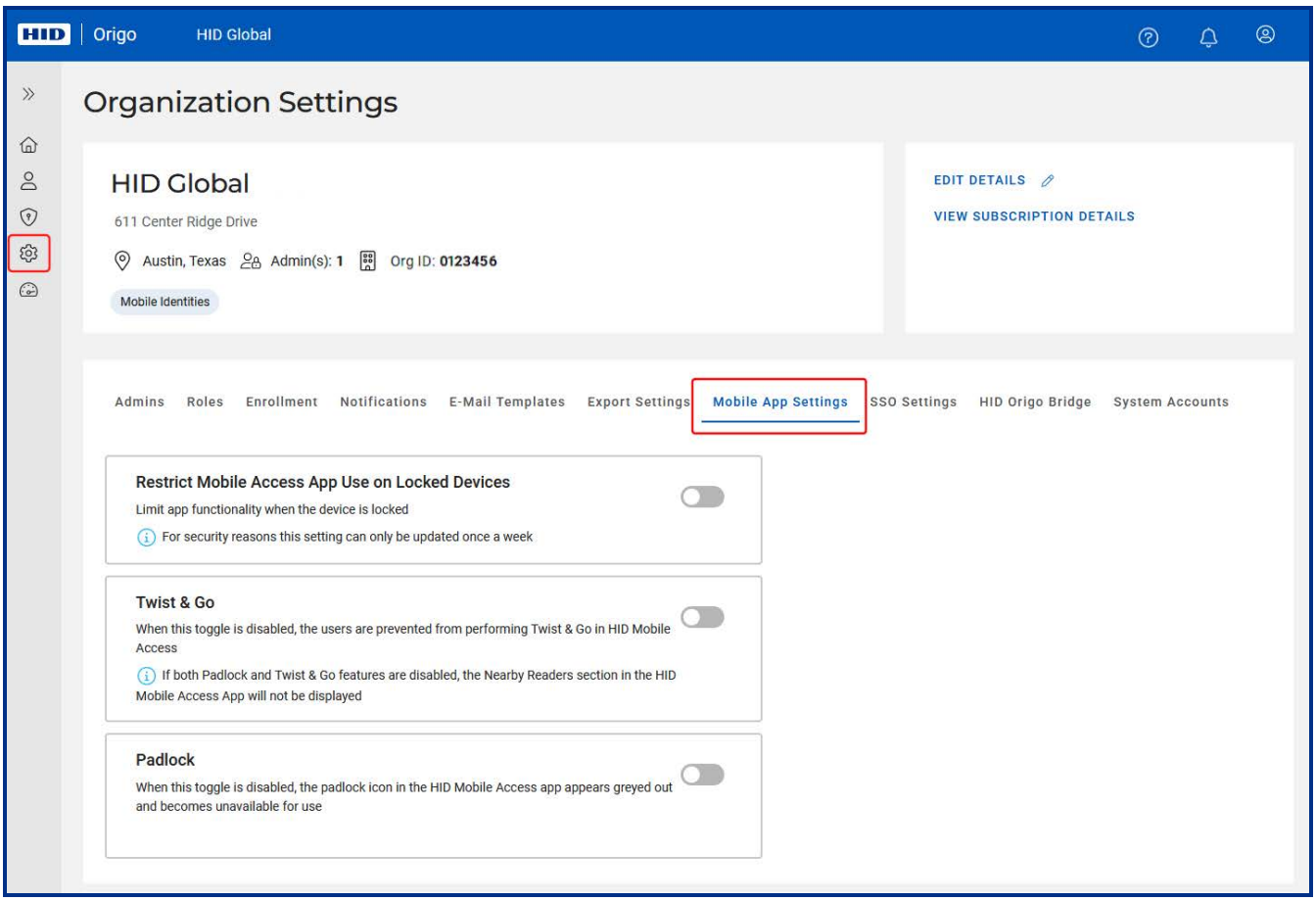
6.9 Export settings

On the **Organization Settings** screen, select the **Export Settings** option. Select the items to be included when the user records are exported.



6.10 Mobile App settings

On the **Organization Settings** screen, select the **Mobile App Settings** option and enable or disable the Organizational level settings to be applied to the HID Mobile Access App.

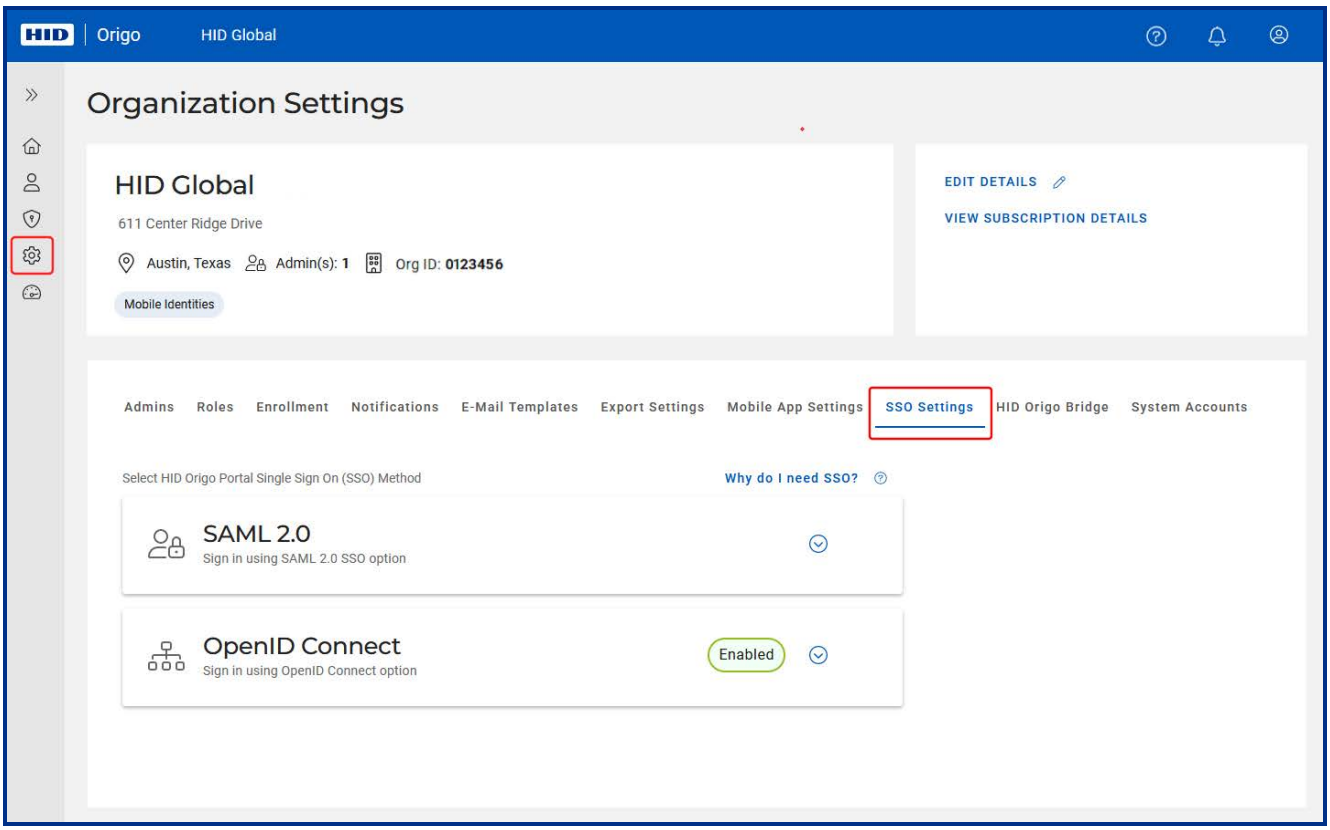


6.11 Configure Single Sign On settings

On the **Organization Settings** screen, select the **SSO Settings** option and select the Single Sign On method that will be used for all administrators signing into the Portal:

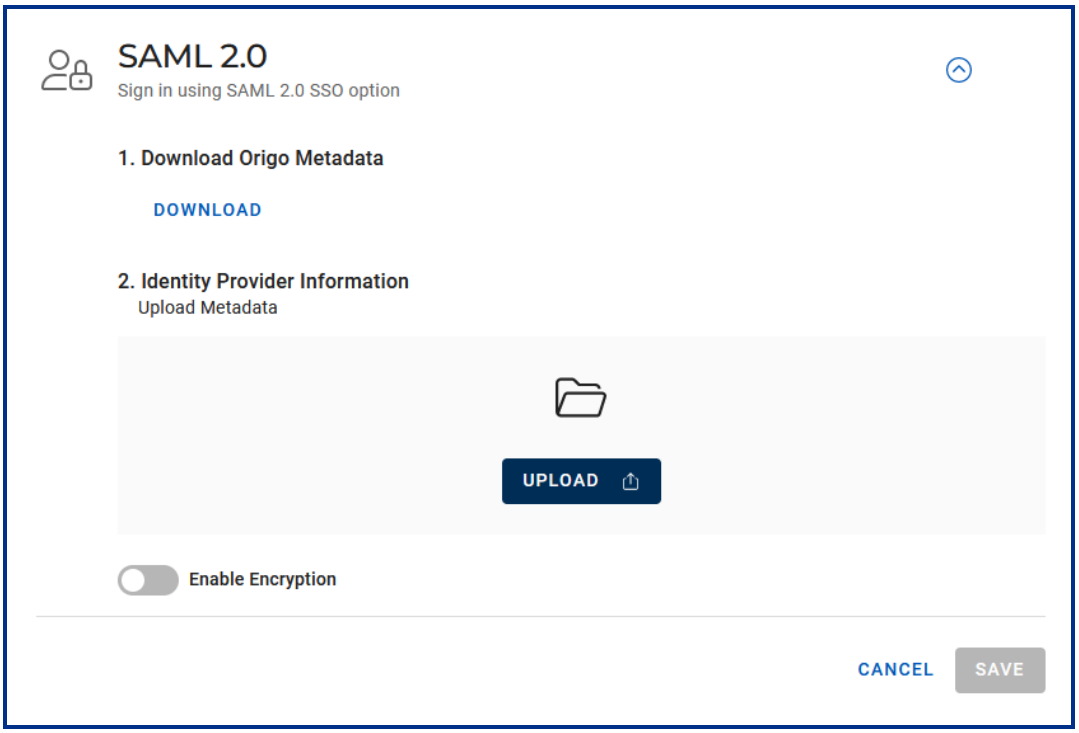
- SAML 2.0
- OpenID Connect

When the HID Origo Portal Single Sign On (SSO) method is configured the SSO Settings screen displays the **ENABLED** method.



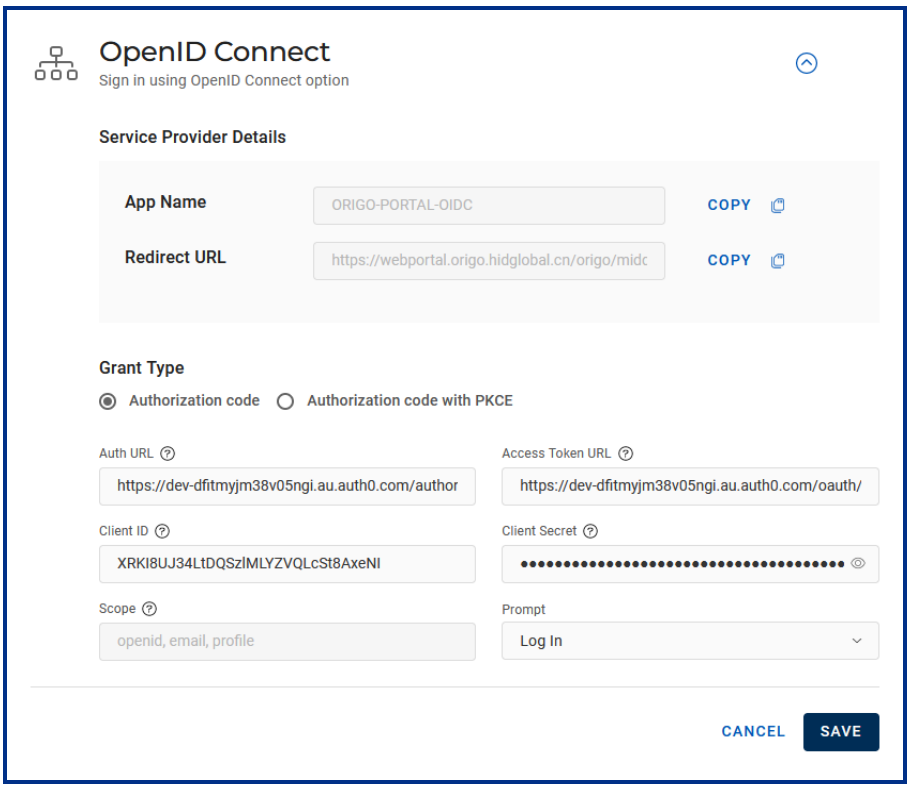
6.11.1 SAML 2.0 configuration

1. In the **SAML 2.0** section, click **DOWNLOAD** to download and save the HID Origo SAML (Security Assertion Markup Language) metadata file onto your local machine (example filename: **HID_Origo_SP_Metadata.xml**).
2. For **Identity Provider Information**, upload the Identity Provider metadata file.
3. Click **SAVE** and log out of the portal. For any subsequent log in, users will be redirected straight to the Portal Home screen without having to enter their portal password.



6.11.2 OpenID Connect configuration

In the OpenID Connect section, select the Grant Type, and enter the required data fields and click **SAVE**.

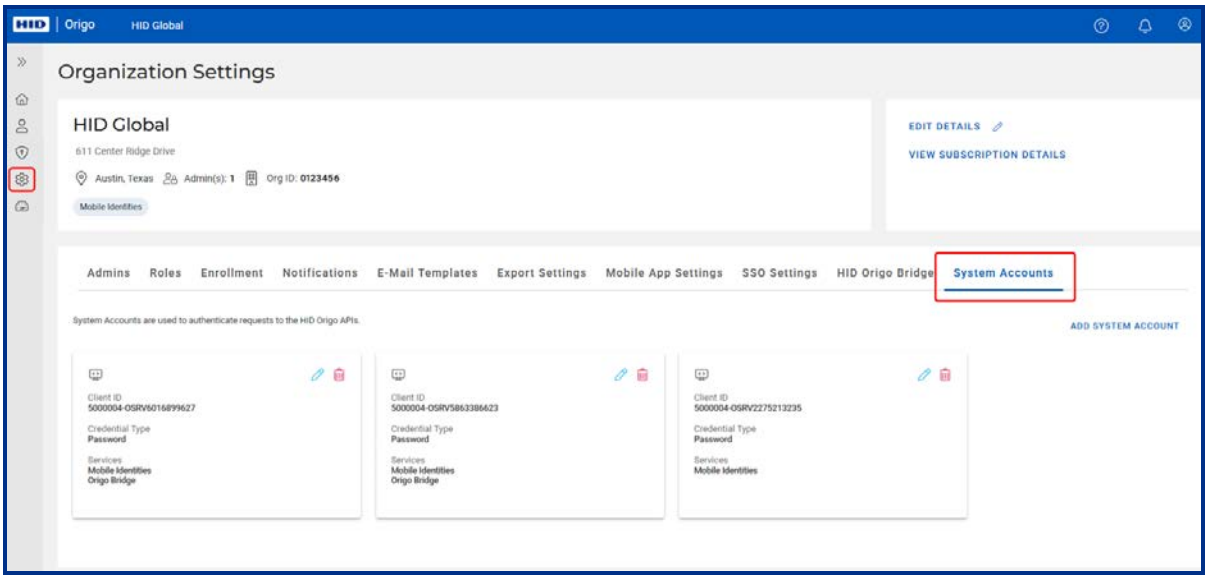


Field	Description
Auth URL[1]	Endpoint for authorization server (used to get the authorization code).
Access Token URL[1]	Endpoint for authorization server (used to exchange the authorization code for an access token).
Client ID	The Client Identifier issued to the Client during the Application registration process.
Client Secret (Auth code only)	The Client Secret issued to the Client during the Application registration process.
Code Challenge Method (Auth code with PKCE only)	The algorithm used to generate the code challenge internally by the Origo application.
Code Verifier (Auth code with PKCE only)	A random, 43 to 128 character string used to connect the authorization request to the token request. Uses the following characters: [A-Z]/[a-z]/[0-9]/"-"/"."/"-"/"~".
Scope	The scope of the access request. This can have multiple, space-delimited, values.
Prompt[2]	• None: ensures the user is not presented with any interactive prompt. If the request cannot be completed, silently via Single Sign On, the identity platform will return an error. • Login: forces the user to enter their credentials on request, negating Single Sign On. • Consent: triggers the consent dialog after the user signs in, asking to grant permissions to the app. • Select Account: sends the user to an account picker where all of the accounts remembered in the session will appear.

1. The Auth URL and Access Token URL must be provided by the customer from the IDP for authorizing and validating the user.
2. The listed Prompt options are only available if the IDP provider supports them. Therefore, some options may not be available for some IDPs.

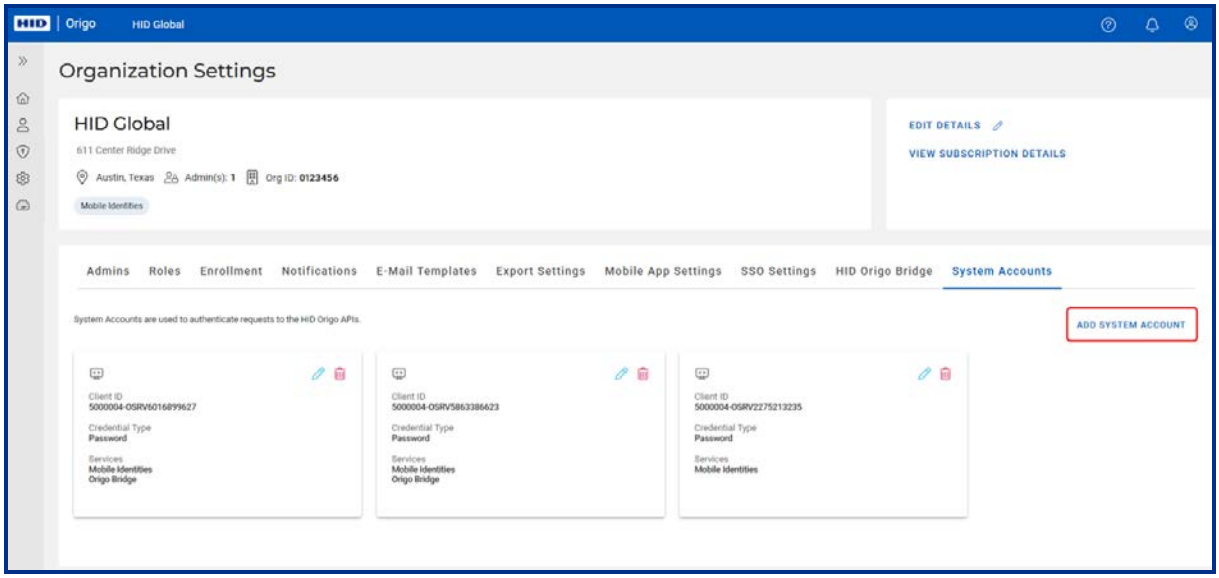
6.12 Create and manage System Accounts

On the **Organization Settings** screen, select the **System Accounts** option.



6.12.1 Add a system account

1. Under **System Accounts**, click **ADD SYSTEM ACCOUNT**.

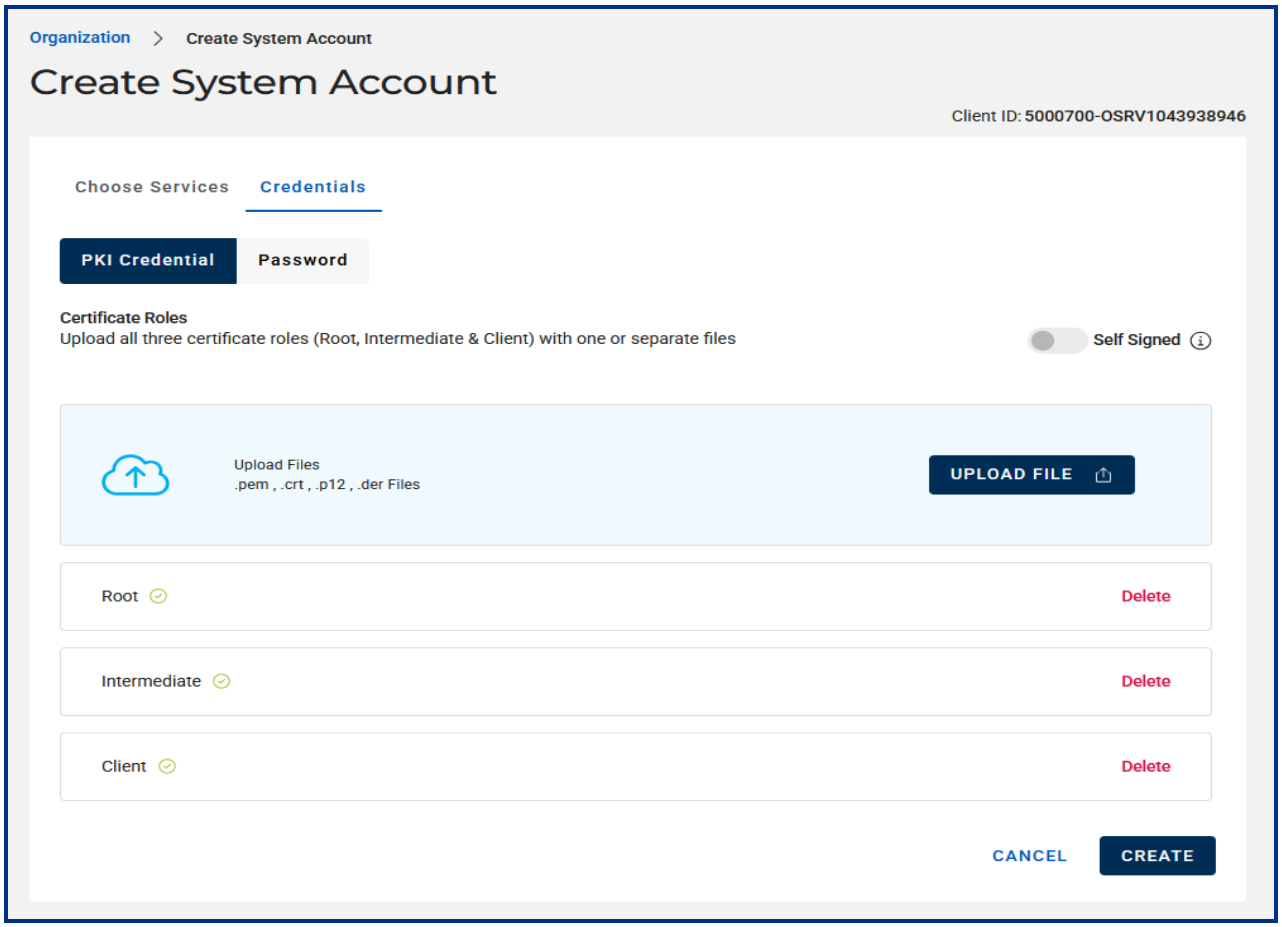


2. On the **Choose Services** tab, select the required Services to create a system account for and click **NEXT**.

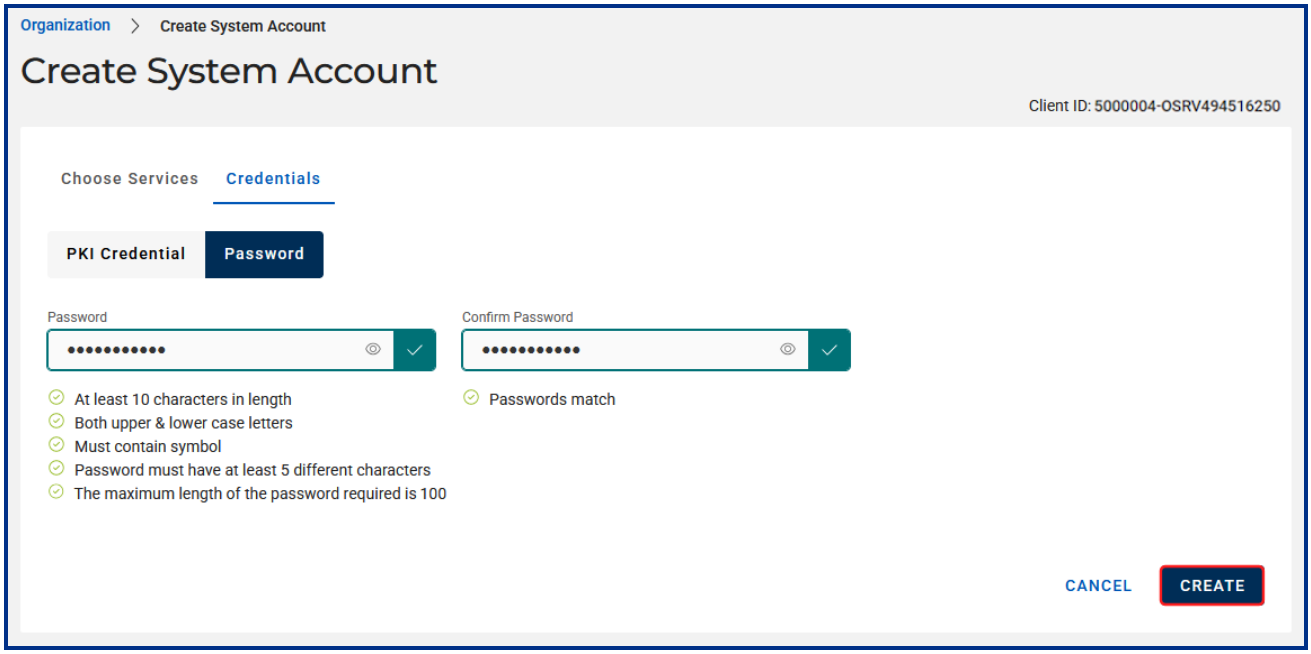


3. On the **Credentials** tab, select either **PKI Credential** or **Password**.
   - **PKI Credential**: Click **UPLOAD FILE** and upload one file combining the required certificate roles (**Root**, **Intermediate**, and **Client**) or three separate files for each certificate role. When the files are confirmed as uploaded, click **CREATE**.

     Note: If the **Self Signed** option is enabled, only the certificate file for the **Client** role is required.

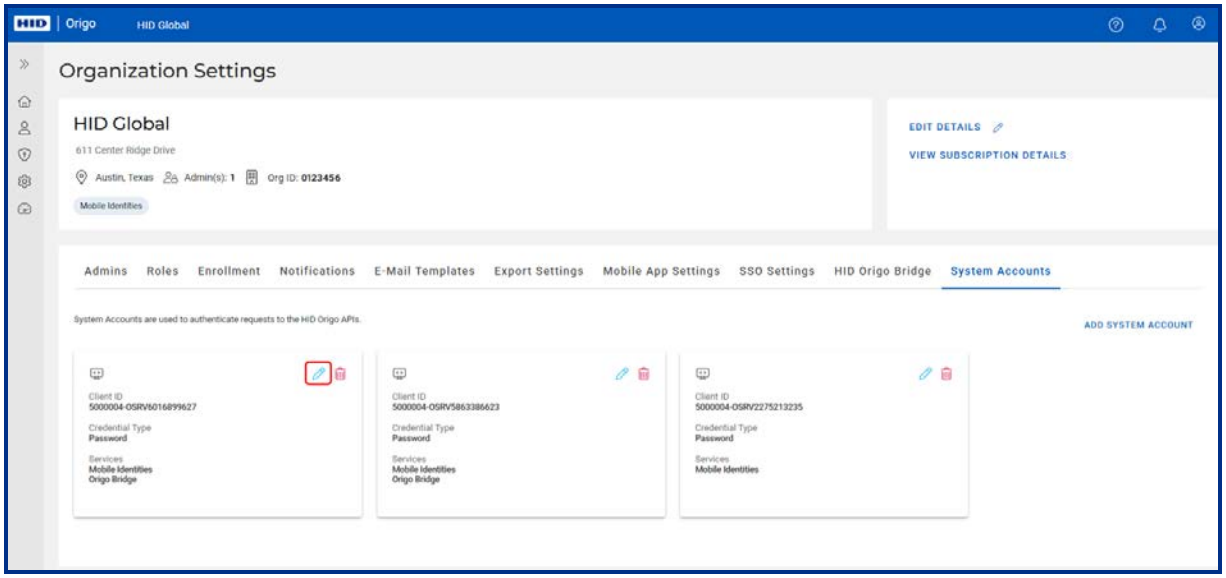


- **Password**: Enter a password, re-enter to confirm, and click **CREATE**.

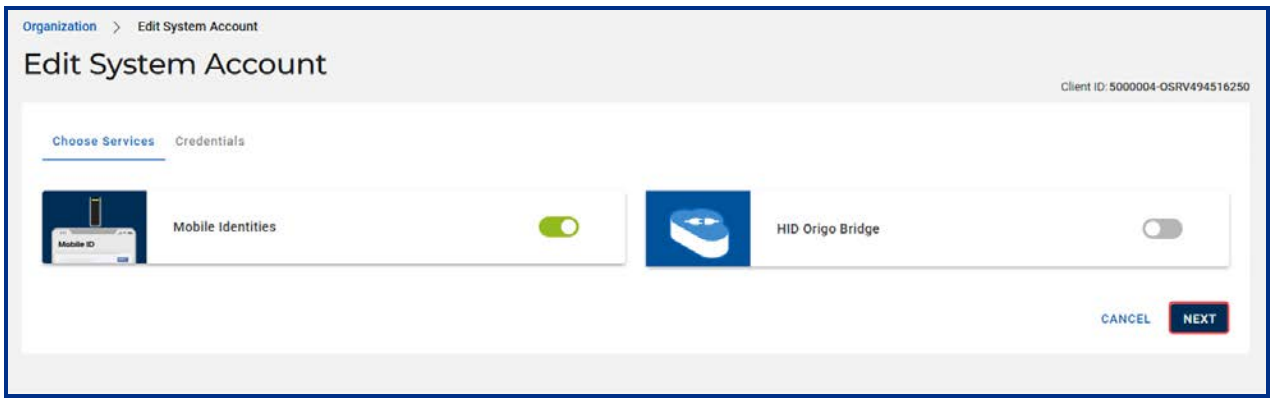


6.12.2 Edit a system account

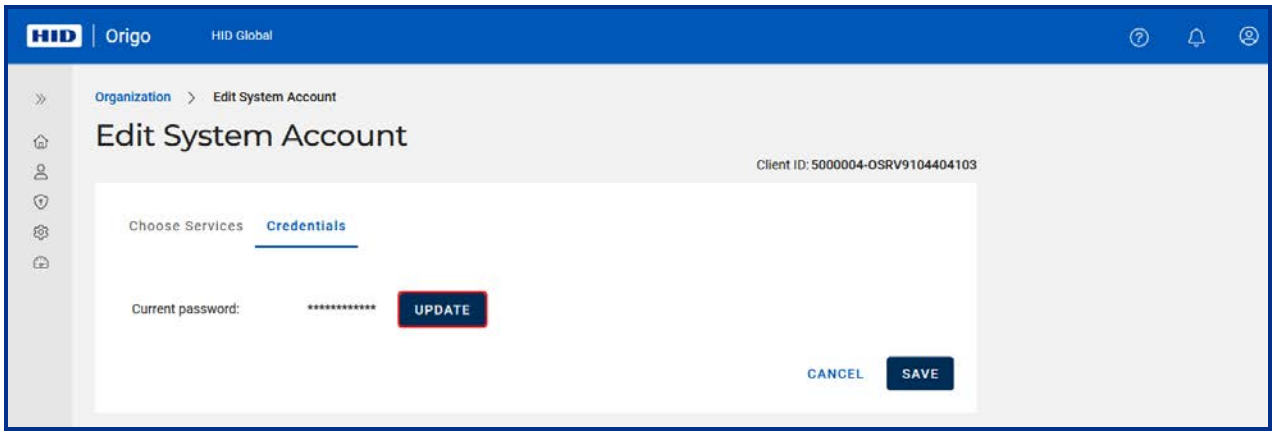
1. Under **System Accounts**, click the edit icon [✎] associated with a system account.



2. On the **Choose Services** tab, select the required Services to edit a system account for and click **NEXT**.



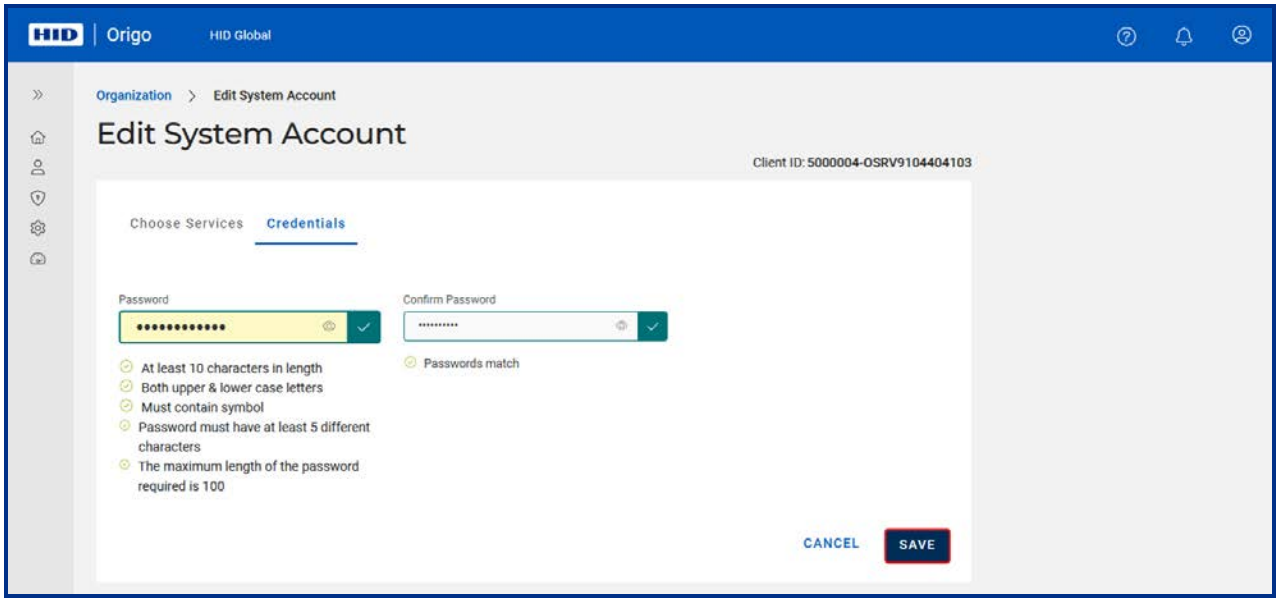
3. Click **UPDATE**.



4. Enter a password and re-enter to confirm.

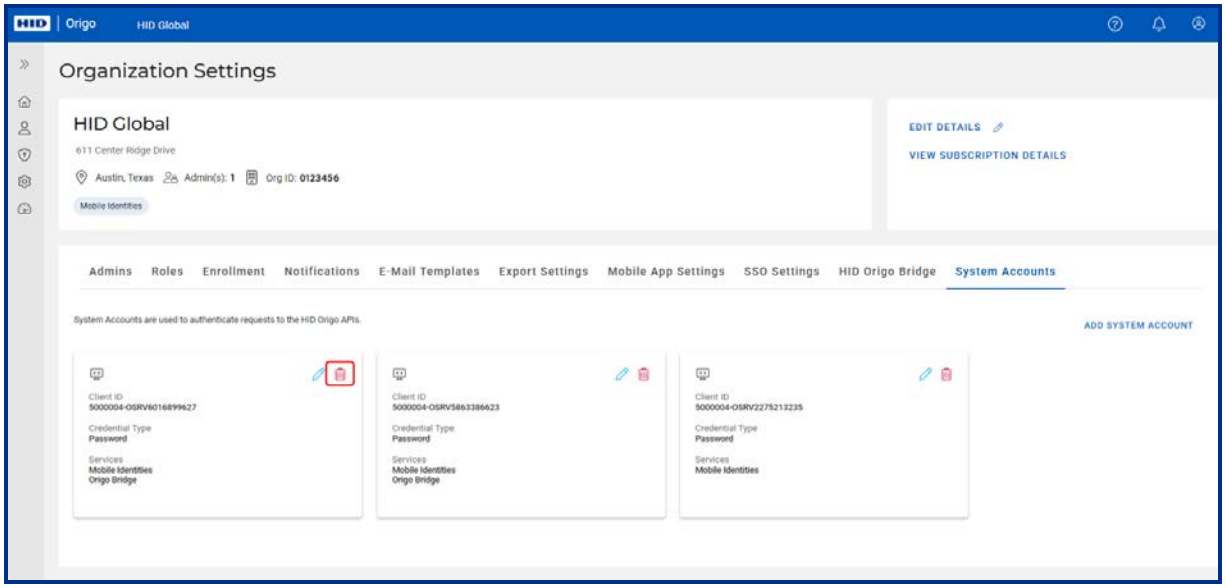
> **Note:** When entering a password observe the required password conditions.

5. Click **SAVE**.

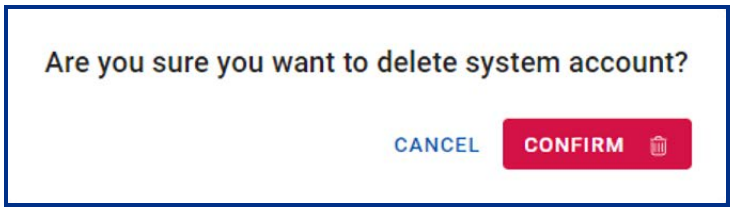


6.12.3 Delete a system account

1. Under **System Accounts**, click the delete icon [🗑] associated with a system account.



2. Click **CONFIRM** to delete the system account.

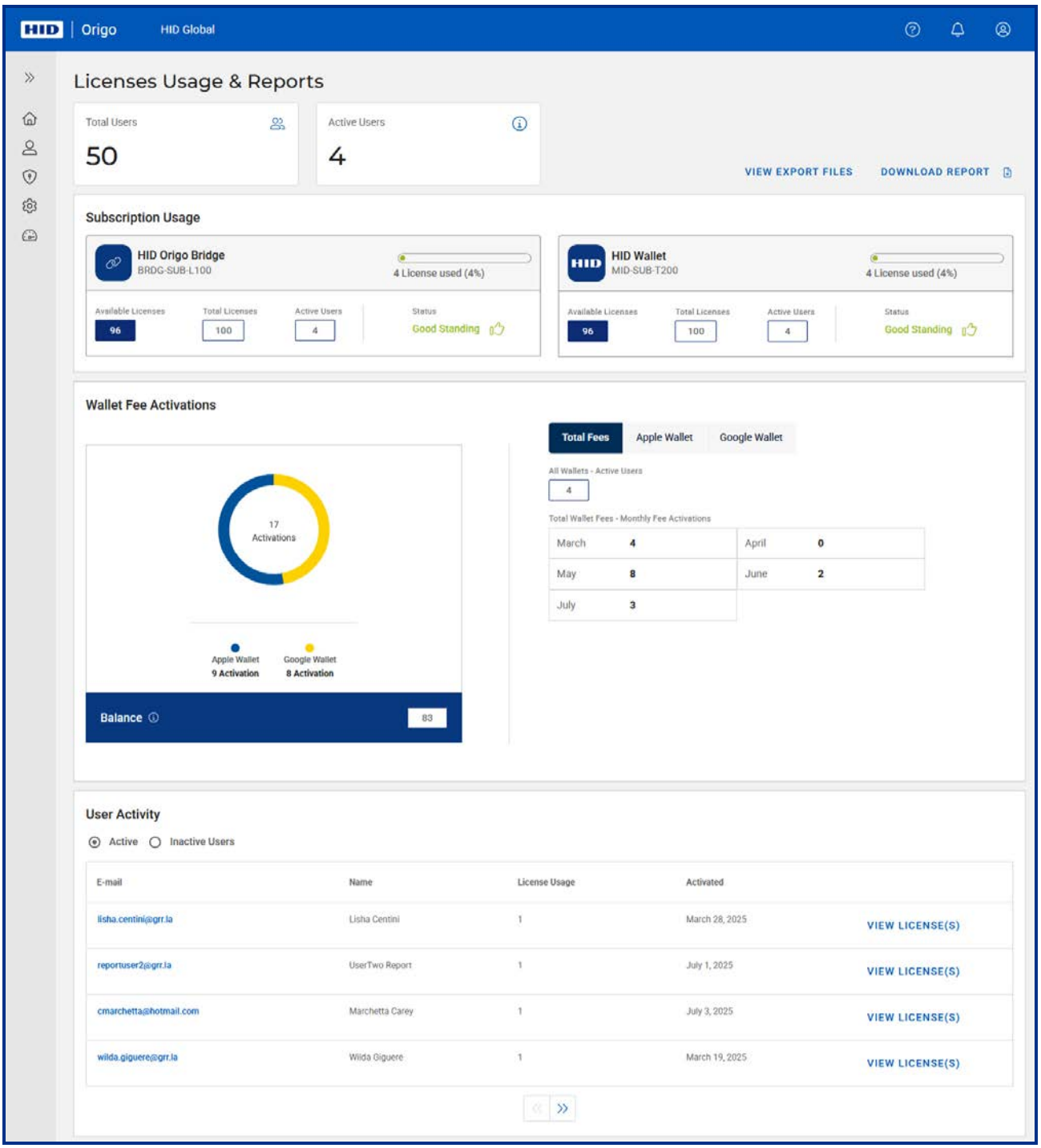


Section 07

Report Management

7.1 License Usage & Reports

Log into the HID Origo Management Portal as Organization Administrator and from the left navigation menu, select the **Reports** option. On the **License Usage & Reports** screen you can view a breakdown of Users and User Activity, Subscription Usage, and Wallet Fee Activations.



7.1.1 License Usage & Reports page widgets

The top of the **License Usage & Reports** page contains several widgets that display information relating to Users.



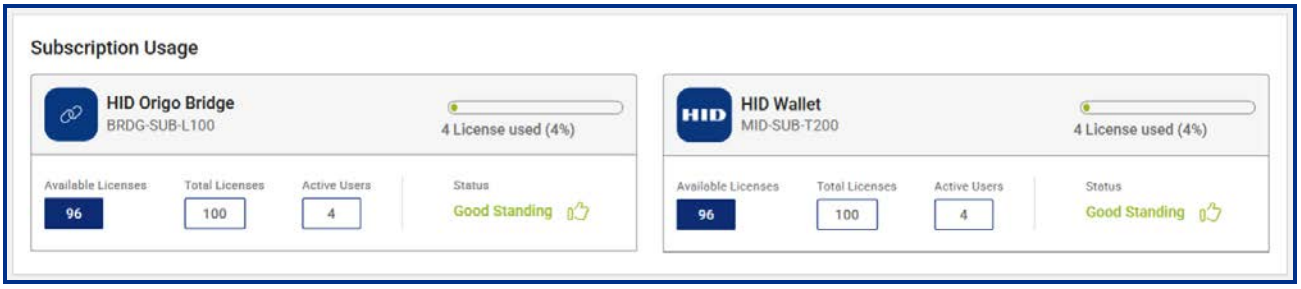
- **Total Users**: This widget displays the total number of users associated with the Organization. Click the total users icon [👥] to display the total number of users associated with the organization.
- **Active Users**: This widget displays the number of Users that hold an active Pass. Click the users icon [ⓘ] to display the number of users that are currently using at least one service.

7.1.2 Subscription Usage

Prepaid Subscription Usage

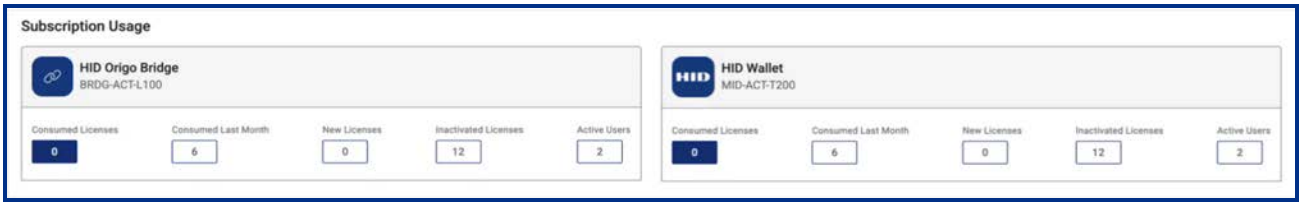
For Prepaid Subscription the **Subscription Usage** section displays license information (total and available licenses) and the number of active users. There is also a color-coded **Licenses used** progress bar and displayed status information:

- Up to 80%: The **Licenses used** progress bar displays Green with a status of **Good Standing**.
- Above 80%: The **Licenses used** progress bar displays Amber with a status of **Need Attention**.
- 100%: The **Licenses used** progress bar displays Red with a status of **Full Usage**.



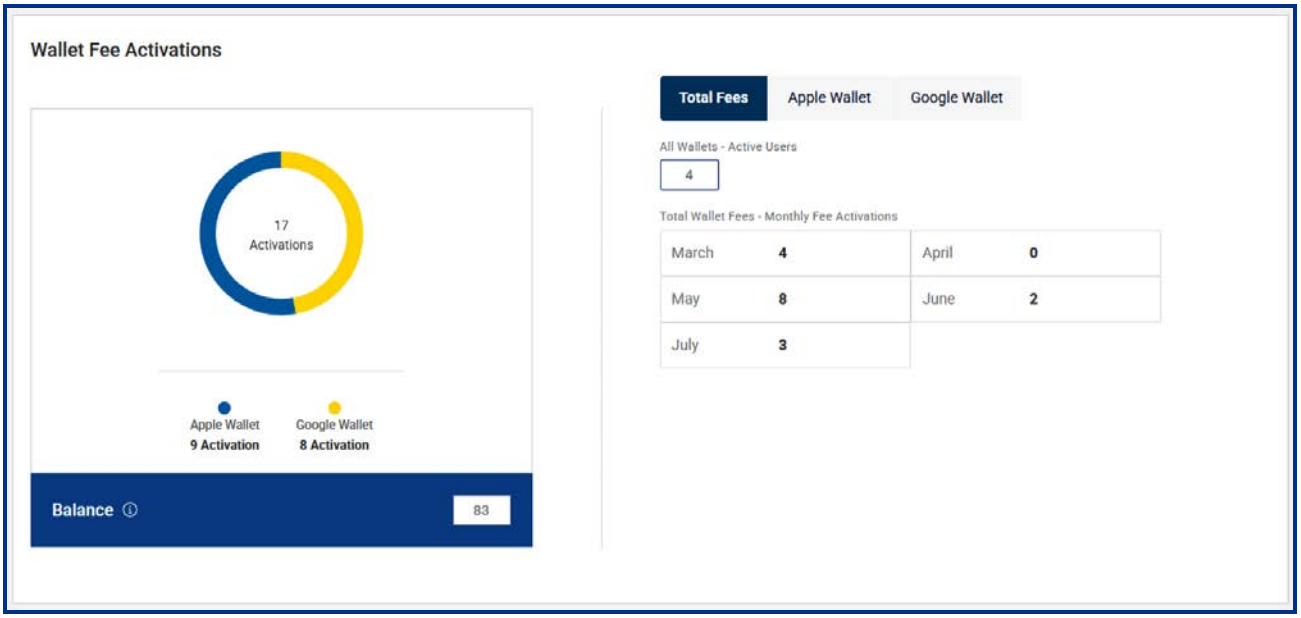
Pay-as-you-go (Activation-based) Subscription Usage

For Pay-as-you-go (ABB) Subscription the **Subscription Usage** section displays license information (consumed, new, and inactive licenses) and the number of active users.



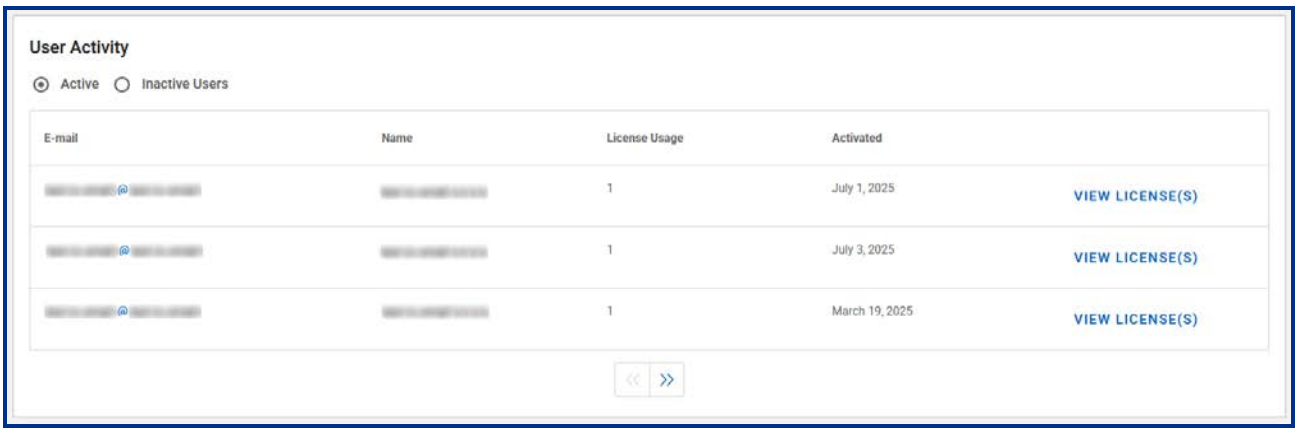
7.1.3 Tech Giant Wallet Fee Activations

The left side of the **Wallet Fee Activations** section graphically displays the specific number of Apple Wallet and Google Wallet Activations, plus the total used and remaining Activations. The right side of this section displays information relating to the total active users for all Wallets, plus a history of monthly Fee Activations. The same information can also be displayed specifically for Apple Wallet or Google Wallet.

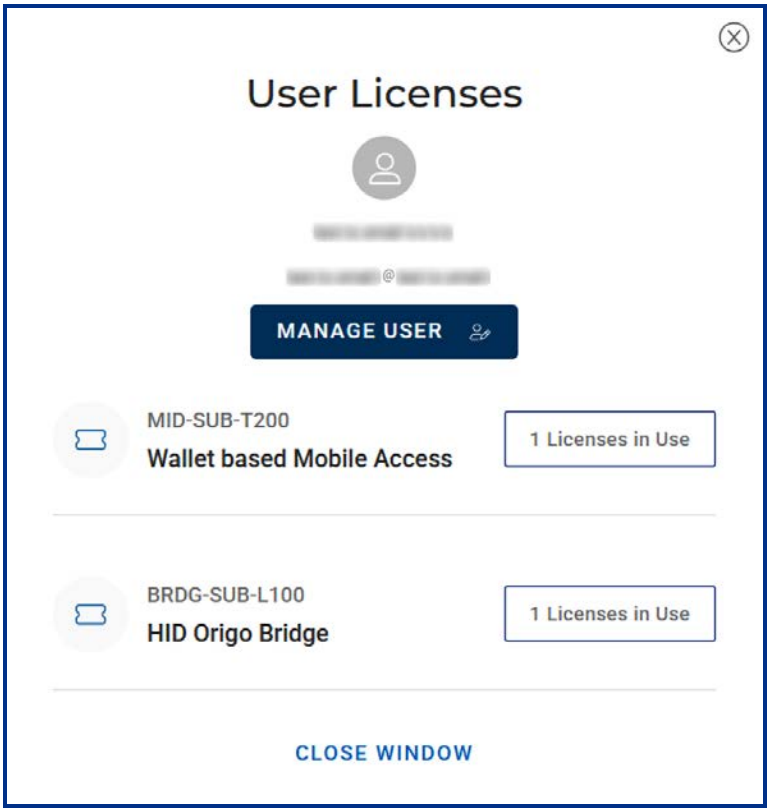


7.1.4 User Activity

In the **User Activity** section, you can display the Active User or the Inactive Users, click within a displayed license widget to view specific user activity information.

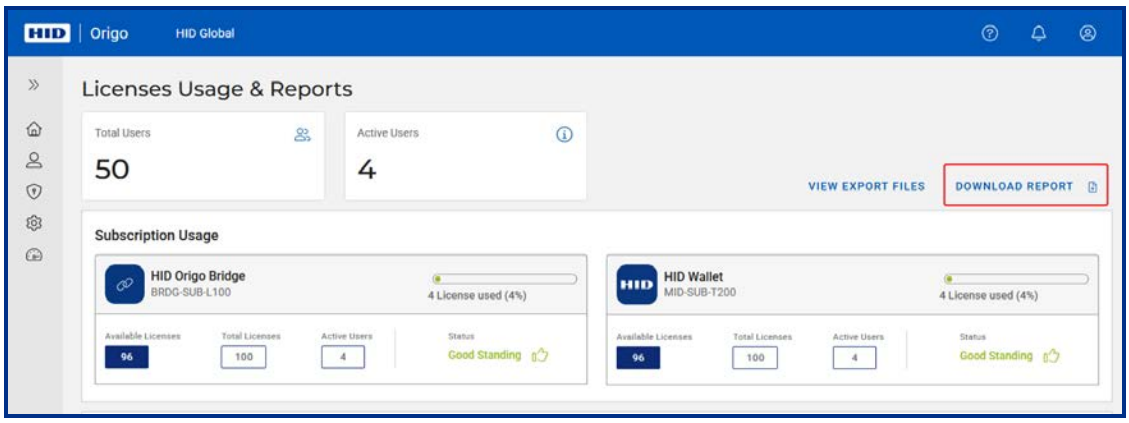


Click the **VIEW LICENSE(S)** link for a user to view the licenses associated with that user.

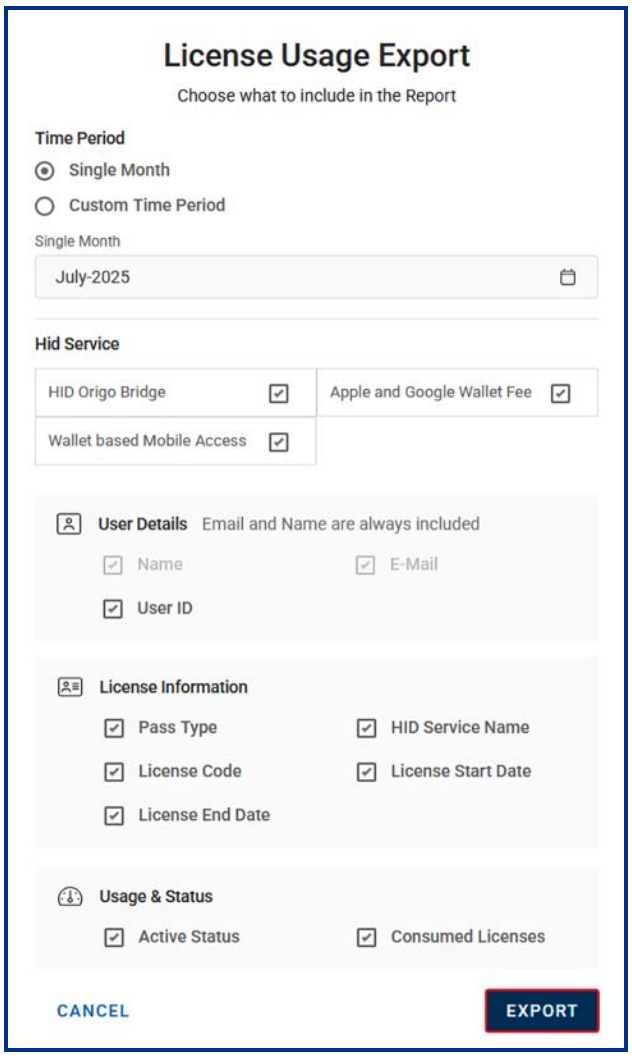


7.2 Export License Usage data

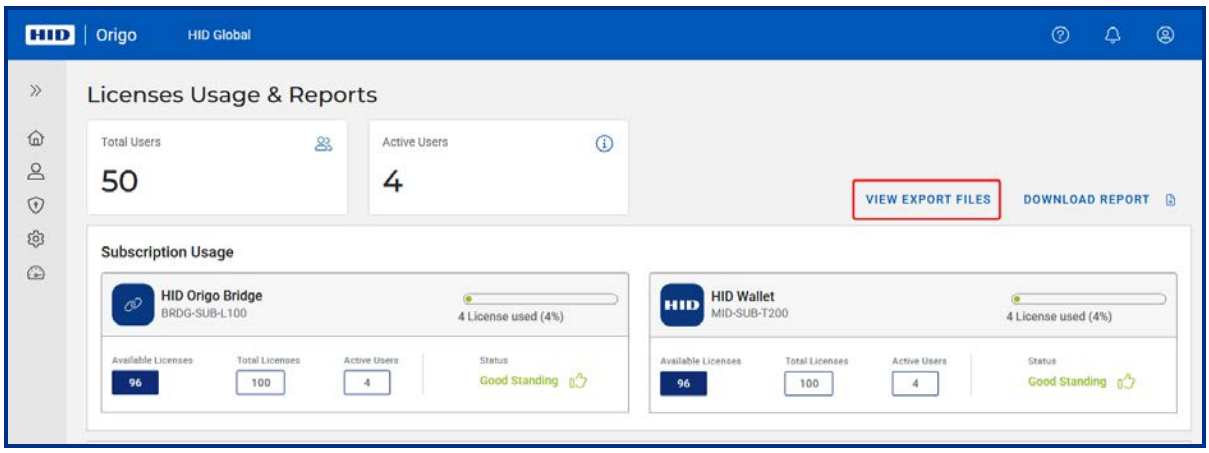
1. To collect user activity report information, on the **Licenses Usage & Reports** page, click **DOWNLOAD REPORT**.



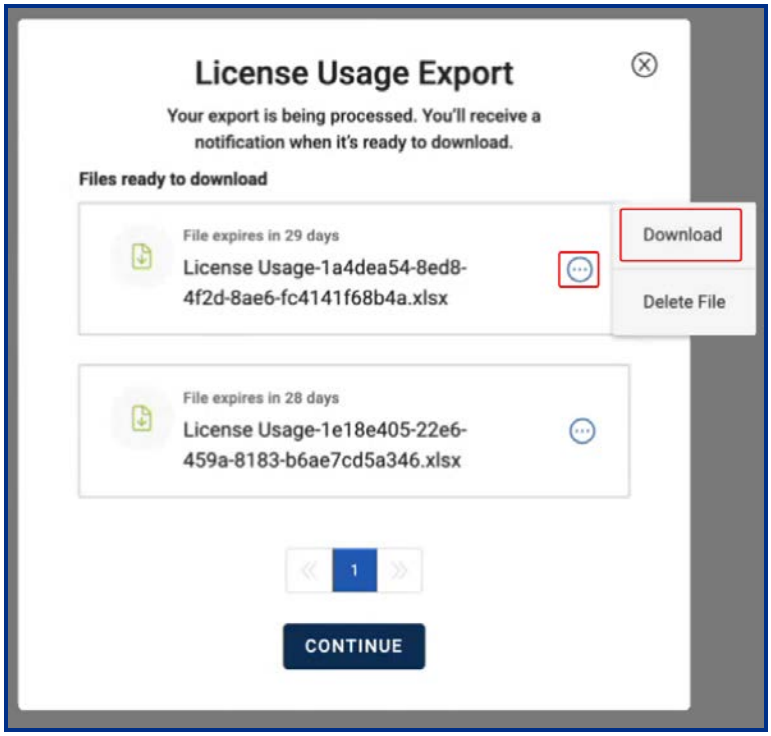
2. From the **License Usage Export** dialog, select a time period for the report (single month or custom time period) and choose the items to include in the report.
3. Click **EXPORT**.



4. On the **Licenses Usage & Reports** page, click **VIEW EXPORT FILES**.



5. The files ready to download are displayed in the **License Usage Export** dialog with a notification of the file expiry date. Click the ellipses menu icon [⋯] associated with a displayed file and select **Download**.



6. In the **Save As** dialog, enter a name for the report and select where to download the file to.
7. Click **Save**. The report is saved as an **.xls** file.

Revision history

Date	Description	Revision
January 2026	• Section 2.1. Updated section for completing account registration. • Section 2.4. Updated section for the Portal Help Center feature. • Section 3.4. New section added for user search and filtering functionality. • Section 3.6. Updated content for issuing a Pass to Wallet. • Section 3.9. Updated section for export users file. • Section 4 Credential Management. Updated section for Pass Design functionality. • Section 5.12 Create and manage System Accounts. Updated section for Public Key Infrastructure (PKI) based authentication for System Accounts. • Section 6 Report Management. Updated the section for new report information layout and for pre-paid subscription reports for Wallet and Bridge.	A.2
August 2025	• Section 2.4. New section added for the Portal Help Center feature. • Section 3.4. Added content for issuing a Pass to Wallet.. • Section 04 Credential Management. Updated section for Pass Design functionality. • Section 5.6 Create and manage System Accounts. Updated section for Public Key Infrastructure (PKI) based authentication for System Accounts. • Section 6 Report Management. Updated the section for new report information layout and for pre-paid subscription reports for Wallet and Bridge.	A.1
September 2024	Initial release.	A.0

hidglobal.com

For technical support, please visit: https://support.hidglobal.com

© 2026 HID Global Corporation/ASSA ABLOY AB.
All rights reserved.
PLT-07733, Rev. A.2

Part of ASSA ABLOY