Origin Security Designate Guide

Global Identity Services

Contents

1. Introduction

1.1 What is Origin

Welcome! Experian Information Technology division has implemented the Experian Origin application for delegated administration of Users.

Origin Administrator guide provides detailed instructions for Experian Administrators to create and maintain client users and their access to Experian business applications.

1.2 Forward

The Security Designate role in this process is extremely critical, as you are the first point of contact and validation outside of Experian. New and/or existing customers like you; hereafter referred to as a Security Designate; will be validated and approved by Experian. You will be able to logon to the Experian Origin to create and maintain your organization's users.

Experian recognizes that the Internet is at the core of our business model. As a public network, the Internet provides a virtually limitless platform for any organization conducting business in a global marketplace. Using such open, public network does expose Experian to risks, which must be mitigated through secure processes and procedures. In conjunction, with secure process and procedures, applications such as the one being implemented by Experian helps to build an environment of trust between the end user and Experian

1.3 Definitions

This document contains references to the terms that are explained below.

Term	Meaning
Access Control	What users can access (resources) on a Web Server or application
Authentication	A process to prove a user's identity
Authorization	Which functions can a user perform within an application
Delegated Administration	Which administrators can implement policy beyond the central administration group
Federation	Federation allows different IdP systems to exchange Identities
Intrusion Detection and Response	Used to define an attack and what policies can be implemented to respond to the intrusion
oAuth	oAuth is a framework for providing authorization services for remote resources.
OpenId	OpenId is a modern and light weight delegated authentication framework for web connected applications and APIs

Origin	An Experian cloud application for managing and administrating users and access to business applications for client users.
SAML	Security Assertion Markup Language is a standard for providing authentication for web applications.
Single Sign-On (SSO)	Seamless access to application and resources across Web servers, having one User ID that grants access to multiple web-enabled applications
Team(s)	A group of users who are logically organized within the organization
User(s)	A user who will be accessing Experian application

1.4 Overview

This document covers the following Administrator functionality and screens-shots.

- Registration and Login
- Dashboard - Searching for users and Teams
- Adding subcodes
- Creating and managing Teams
- Create and manage end Users
- Assigning applications to Users and Teams
- Lock/Unlock users
- Forgot Password

2. Registration and Login

Experian Administrators creates Security Designate for a company when the company is setup. This account could be used to login to Origin and then use to create End users.

2.1 Origin Instance

Experian has an instance of Origin for each Business Region. An instance of Origin has a unique URL. To access the Origin instance the Security Designate needs an Id and password and optionally an MFA* token.

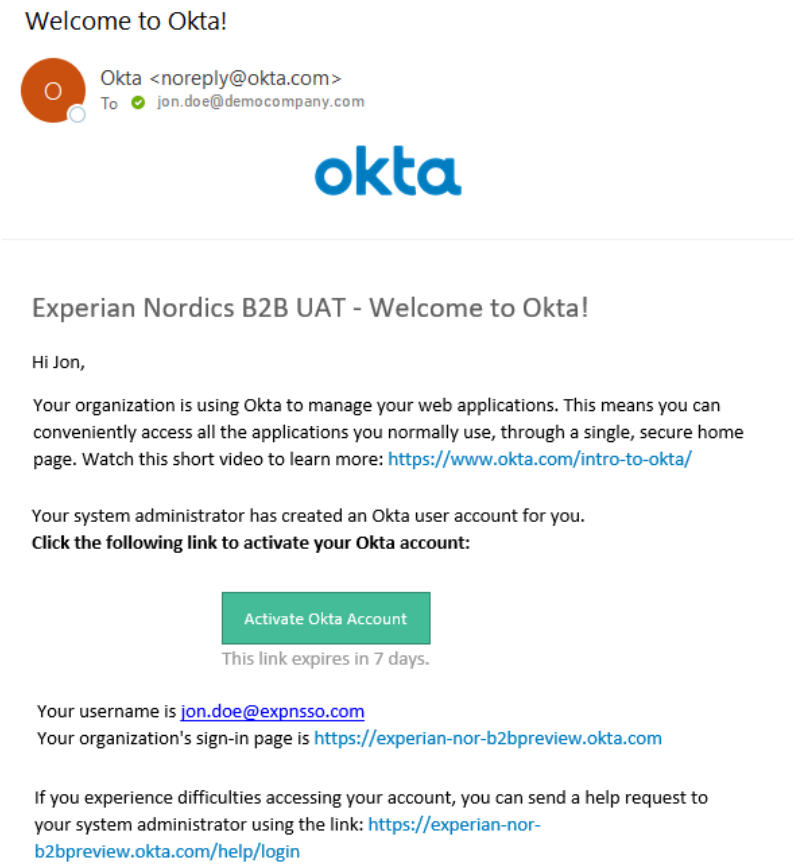
* MFA options will be displayed to user during the account registration process.

2.2 Account Registration

Once an Experian Administrator has given access to Origin, the Security Designate will receive an email to activate the account. by clicking on the link provided on the registration email. The first-time logon refers to the first logon to the system. During this first logon, you will be asked to set your password and also update the MFA for secure login. NOTE: The email address is critical to the operation and security of our system. All communications of user credentials are sent to this email address. Note: Use of a personal email address is not acceptable.

2.2.1 Registration email

Check your email for the activation email. This email has a 7-day expiration. Check your spam folder if email is not received. The activation link is accessible only once. For any reason if the activation steps are not completed you will need to request a new activation email through Experian Administrators or helpdesk.



Welcome to Okta!

Okta <noreply@okta.com>
To jon.doe@democompany.com

okta

Experian Nordics B2B UAT - Welcome to Okta!

Hi Jon,

Your organization is using Okta to manage your web applications. This means you can conveniently access all the applications you normally use, through a single, secure home page. Watch this short video to learn more: https://www.okta.com/intro-to-okta/

Your system administrator has created an Okta user account for you.
Click the following link to activate your Okta account:

Activate Okta Account

This link expires in 7 days.

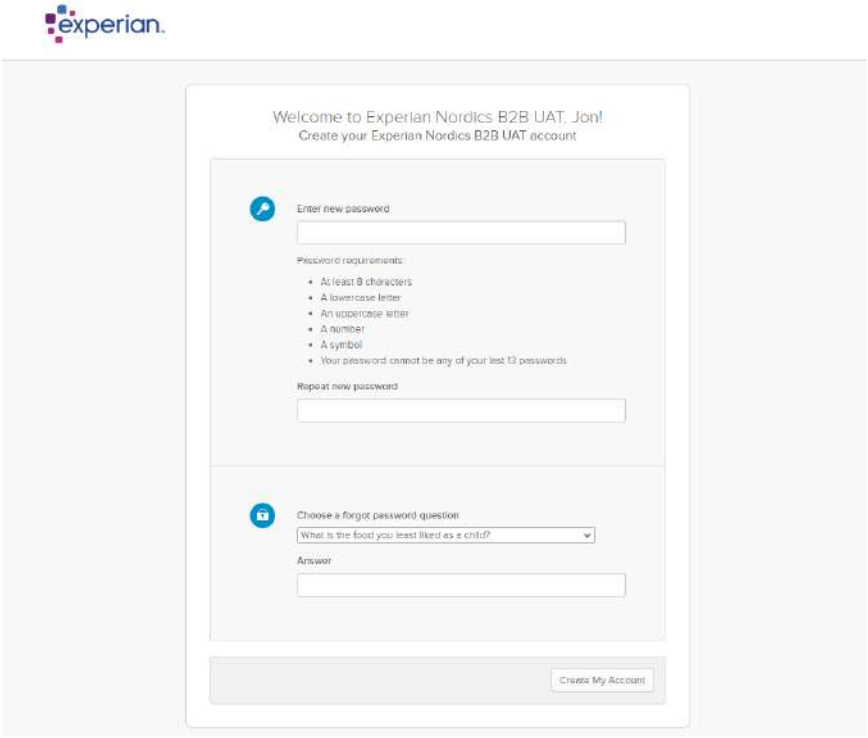
Your username is jon.doe@expnsso.com
Your organization's sign-in page is https://experian-nor-b2bpreview.okta.com

If you experience difficulties accessing your account, you can send a help request to your system administrator using the link: https://experian-nor-b2bpreview.okta.com/help/login

Note: You may ignore the domain while entering the user id to login.

2.2.2 Set password and forgot password answers

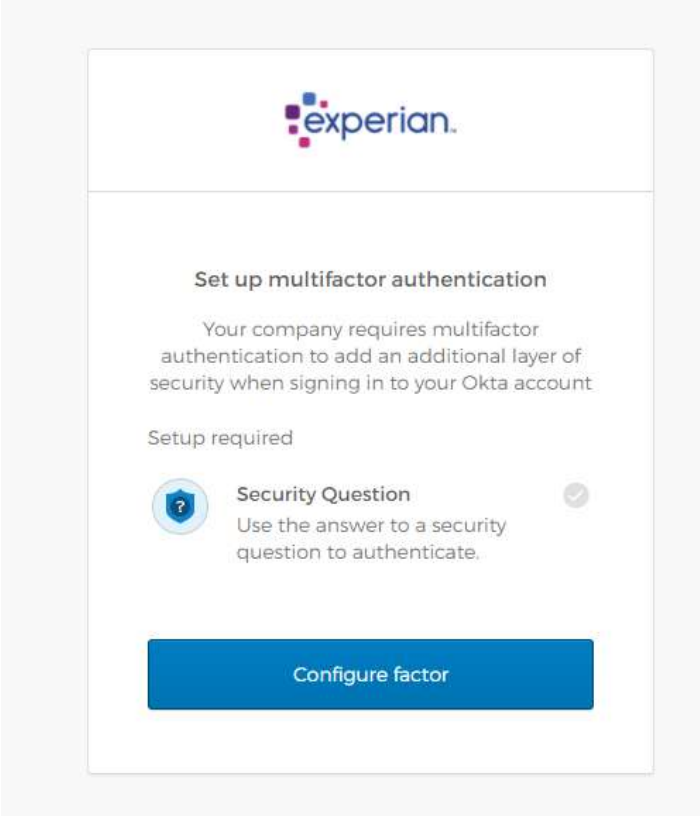
When clicked on "Activate Okta Account" button in the email, user will be directed to Okta to set the password and forgot password answer.



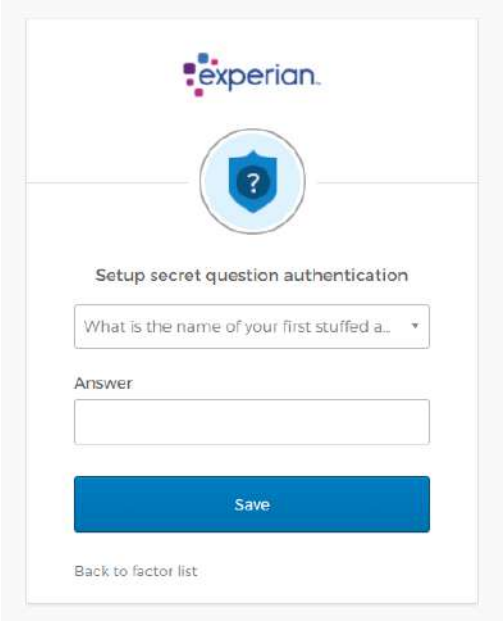
Once the values are entered, click on "Create My Account" button.

2.2.3 Set MFA

The following dialog will be presented.



Click on "Configure factor"

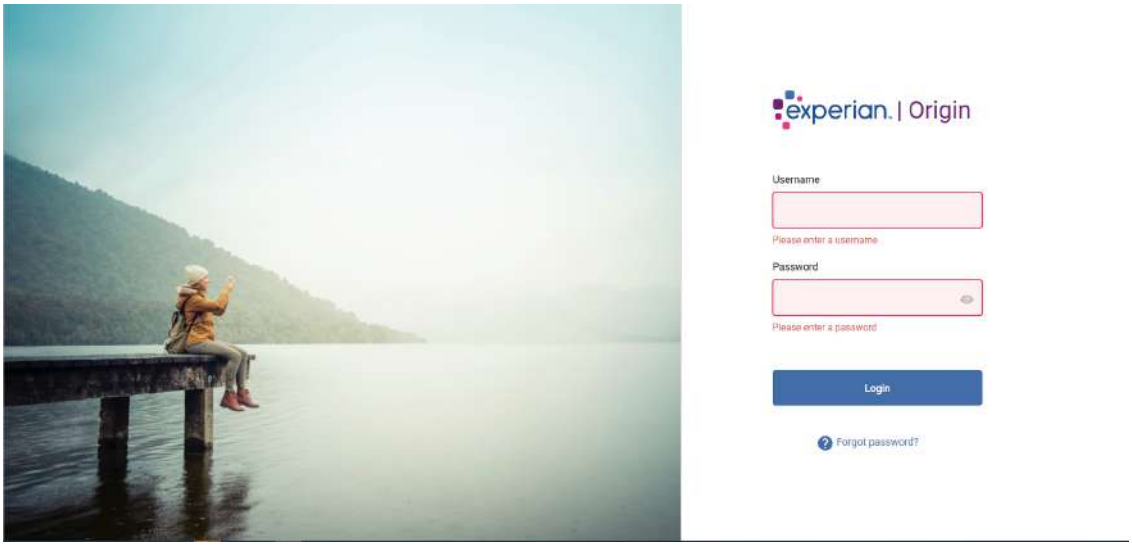


Select a secret question and provide an answer you can remember. Answer must be at least 4 characters. And hit Save. This will complete the Registration process. Once this step is completed user will be taken to the Okta dashboard. You may close the Okta dashboard. Your account is now eligible to login to Origin.

2.3 Login to Origin

Once the registration is successfully completed, an Administrator can login to Origin. The following information is needed to access Origin.

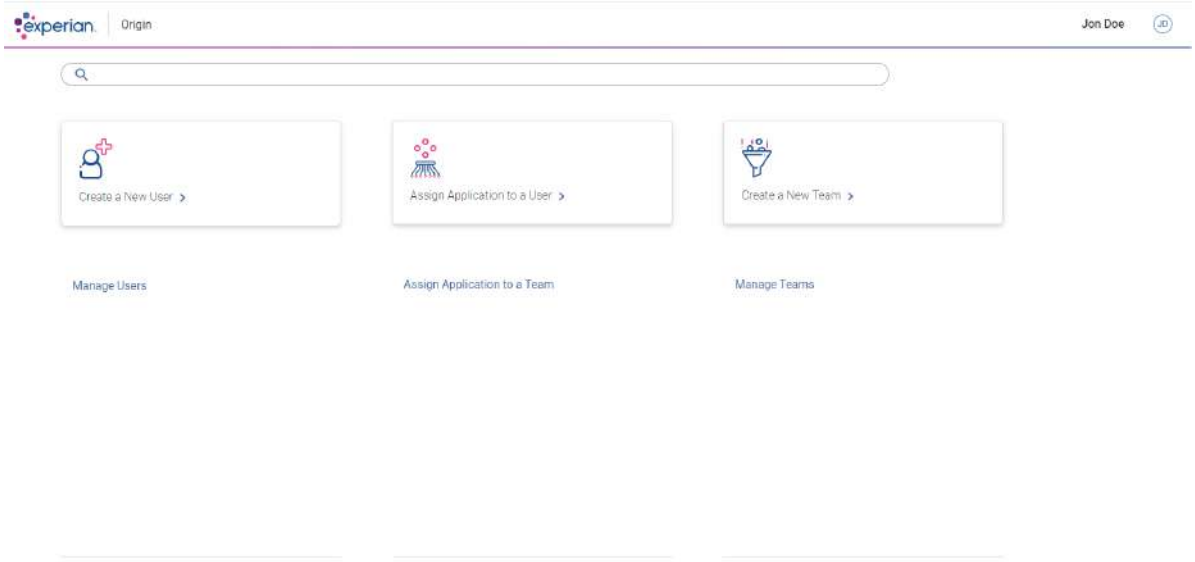
1. URL of Origin instance
2. A valid user Id
3. Password
4. MFA response. A security Question/Answer is supported in the current release.



When authentication is successful, security designate user will be landed in the dashboard.

3. Security Designate Dashboard

Upon successful login, a Security Designate is presented with the Dashboard screen. The Dashboard contains quick links to commonly used functions such as Creating/Editing Users, Creating Teams, and Assign application to users and Teams etc.



Dashboard allows to access the following functionality,

1. Search for users, Teams
2. Manage users, Edit users, Create new users
3. Manage Teams, Edit Team, Create new Team
4. Assign application to Users, Teams, etc.
    a. Note: You may see an application assigned to employees titled “MyExperian Portal (Experian Customer Community)”. This is Experian’s self-service option for clients and there is no fee or access to contracted products associated with this application.
5. Lock or Unlock users

4. Team Management

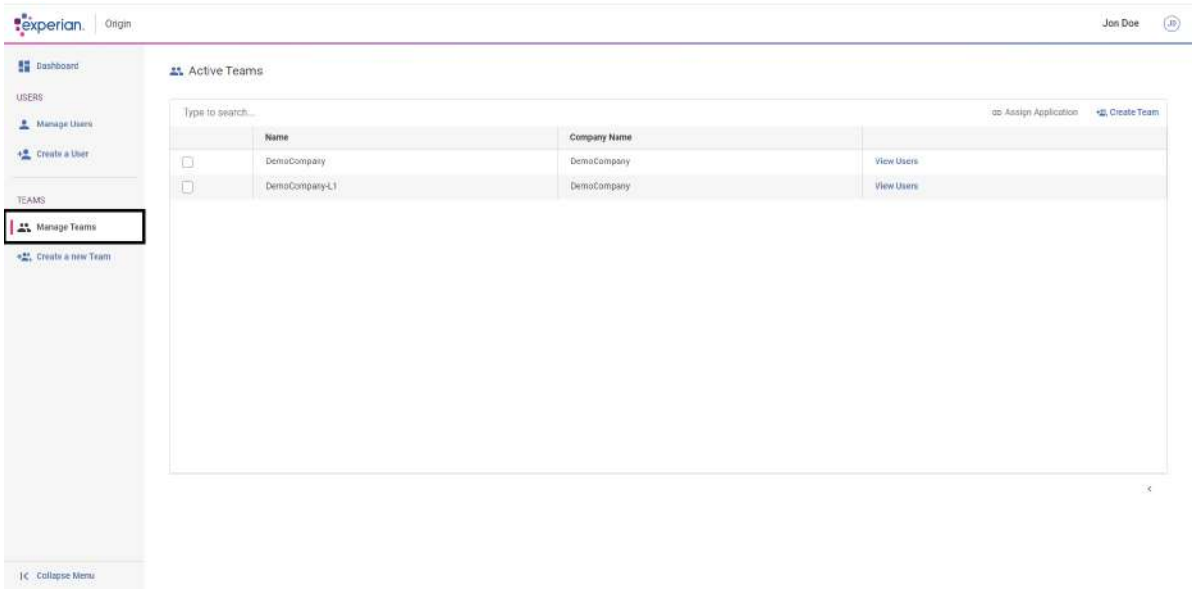
Team provides a grouping for users. A company can have teams in a hierarchical level. A company has a default team with the same name as Company. This team is referred as "Root Team". Any number of Teams can be added below the Root Team. Team may be added hierarchically. A security Designate may be added to each of the Team nodes. A Security Designate at a Team node is allowed to view and manage users at their level or below the hierarchy.

This section covers the following,

1. Manage Teams - view the list of teams belonging to the Security Designate.
2. Search for team- Search and find teams by name search.
3. View team details
4. Edit a team
5. Create a team
6. Add/Remove IP restrictions to a team
7. View users of a team

4.1 Manage Teams

Manage team menu on the left navbar displays the all the team belongs to the Security Designate logged in.



This page displays the Team name, Company name values in a table. Page allows the following functionality.

- A text search ability.
- View users of the team
- Assign application and attributes

A security designate role user is allowed to view teams' data belonging to his level and below.

4.2 Search for Team

A designate can search for a team by Team name. Both full name and partial name are supported. When user types characters in the search area, the matching teams are displayed in the table below.

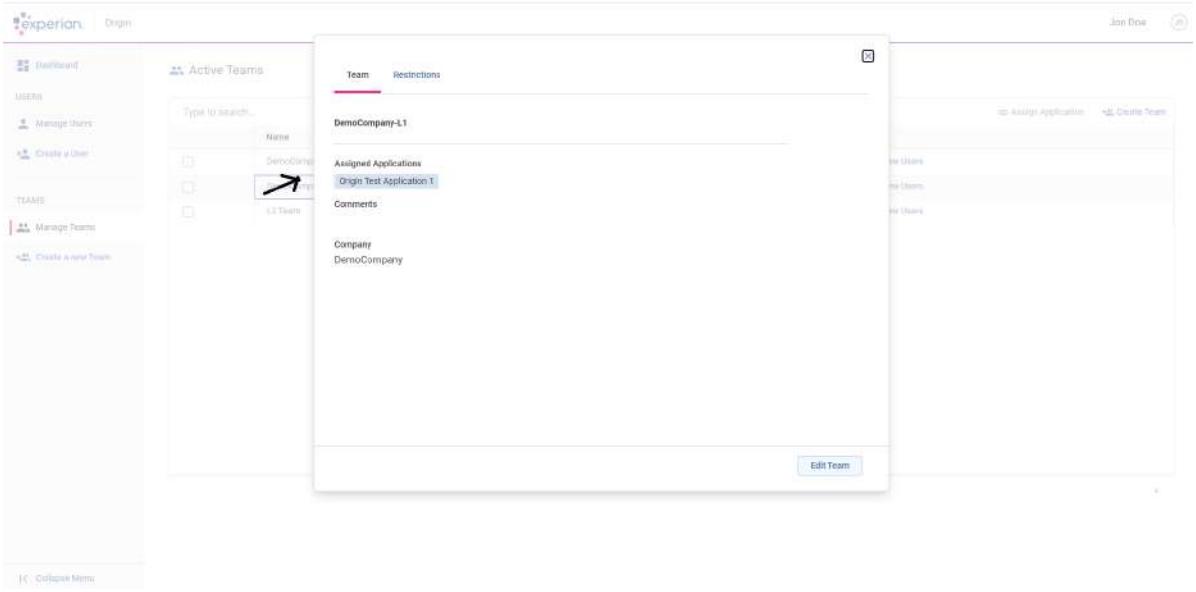
4.3 View Team details

Clicking a row from the table shows a popup with the Team details. This page is read only by default. This page has 2 tabs

- Team details
- IP Restriction

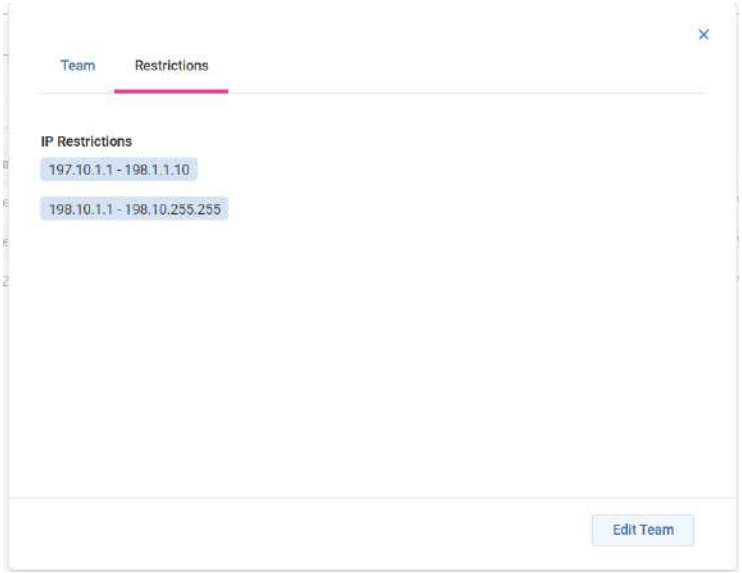
4.3.1 Team details

This tab displays Team name, Assigned applications, Company and the comments.



4.3.2 View IP restriction

IP Restriction tab displays the IP restrictions assigned to the team.



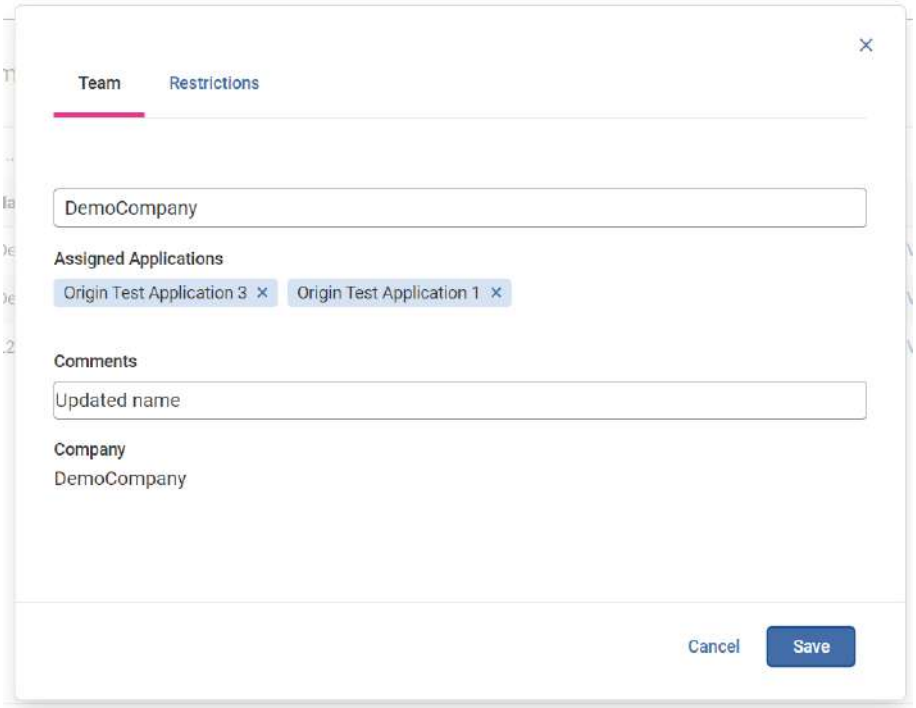
IP Restrictions are displayed as a range value in IPV4 formats.

4.4 Edit a Team

Edit Team allows the team details to be updated. In this page a Security Designate can,

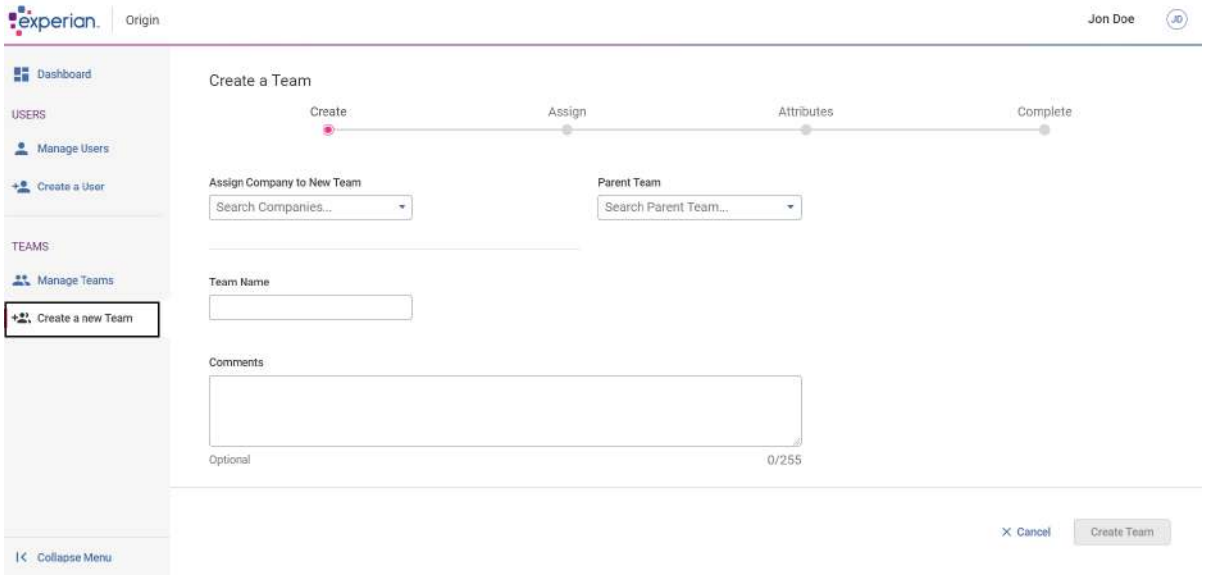
i. Edit the name of Team.
ii. Add or modify the comments
iii. Remove one or more of Assigned applications

Updated data will be saved when "Save" button is clicked.



4.5 Create a team

Click on the "Create a team" link from dashboard or the menu link on the left nav bar to open the create team page.



Create team page is organized to a 3 step process as follows,

a) Create a team
b) Assign application(s)
c) Assign attribute(s)

4.5.1 Create a team

Select the company from the drop down. Also select a team *. Enter the Team name. Optionally add a comments. And click on "Save Team".
At this point the team will be created and user will be directed to Assign Application tab.

4.5.2 Assign applications to a team

At this page, an application can be selected from the list and click on "Assign Application" button. One or more application can be assigned to the team. Once the application is added, click on "Attributes" button to move to the next step.

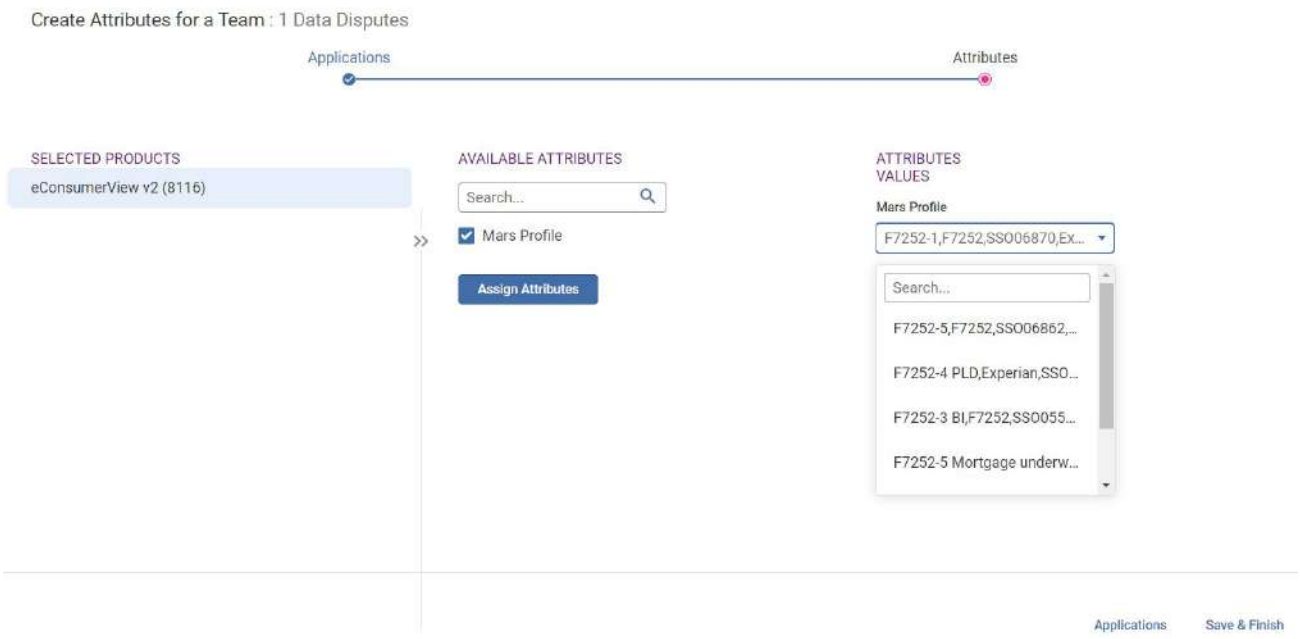
4.5.3 Assign attributes to an application assigned to the team.

In this page, all assigned application list is shown and selecting an application on left shows all the attributes. Selecting the checkbox on the attribute shows the value field. Value are of the following type,

a) Text value - enter a value.
b) Boolean (Check or uncheck)
c) Arrays - enter a list of values
d) Composite attributes

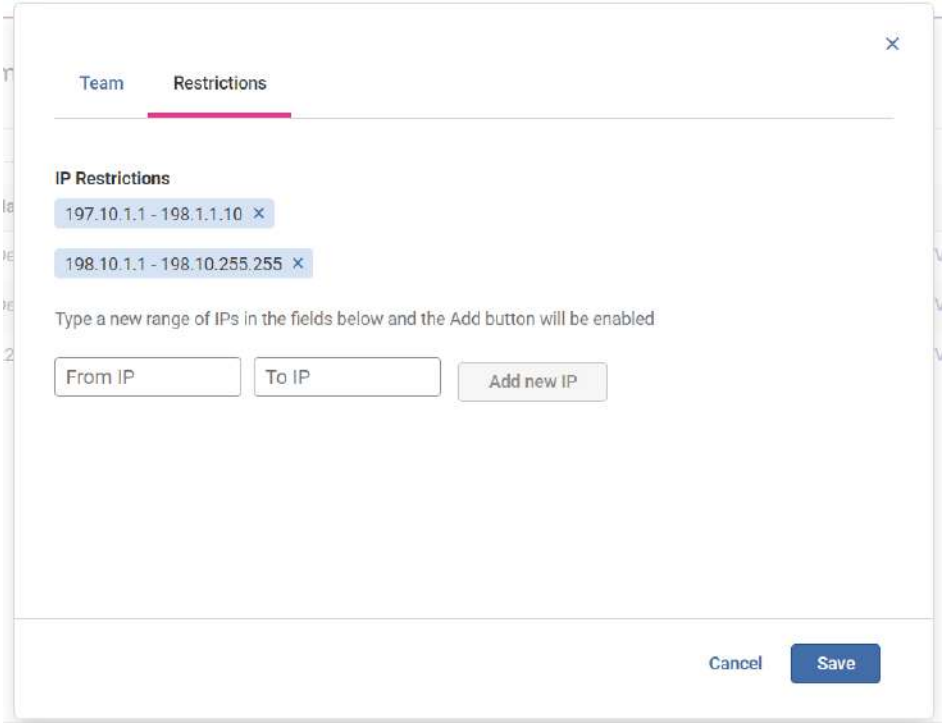
4.5.4 Assign composite attributes to a team

If the company is assigned with a composite attribute profile (ex:” Mars Profile”), a Security Designate will be able to assign one or more of the composite attributes the company level to a team the SD has access to. SD will be able to assign one or more Mars profile attribute to a child team.



4.6 Add/Remove IP Restrictions

In this tab, existing IP restrictions can be removed or new IP restrictions can be added.



Data will be saved when "Save" button is clicked. Edit mode can be exited by clicking on "Cancel" button.

4.7 View users of a team

Clicking on "View Users' link from the Manage Teams page, displays the users of the selected Team. The view will be switched to Manage users page with a filter applied on the Team.

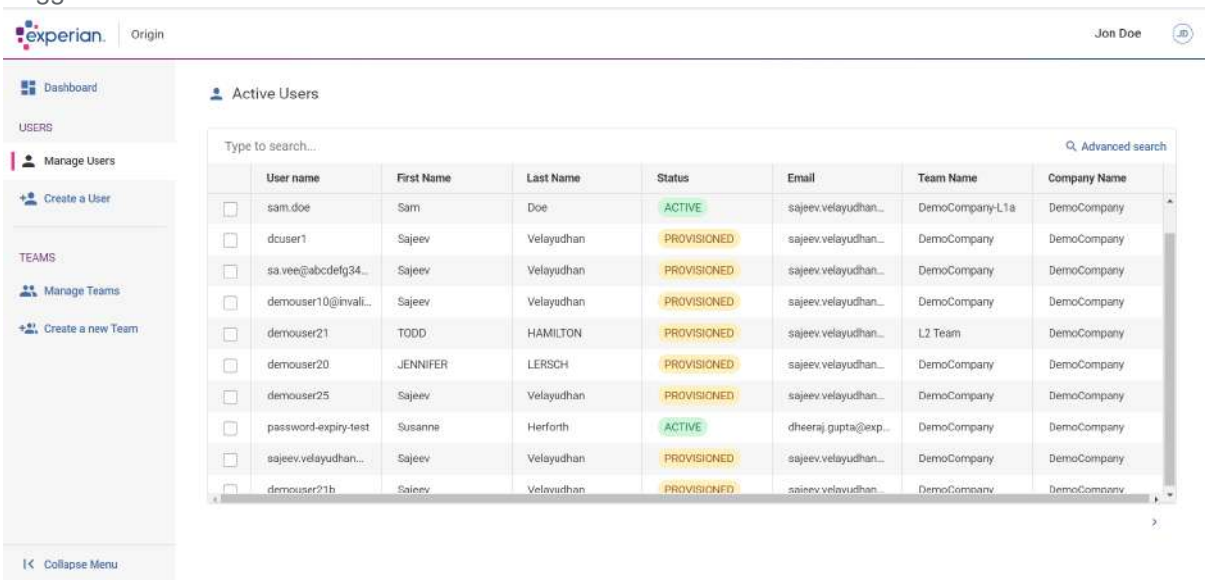
5. User Management

A Security Designate can manage users in his/her team or users in any child teams. This section covers the following,

1) Manage Users - view the list of users belonging to the Security Designate.
2) Search for users - Search and find users by name search.
3) View user details
4) Edit a user
5) Create a user

5.1 Manage Users

Manage user menu on the left navbar displays the all the users belongs to the Security Designate logged in.



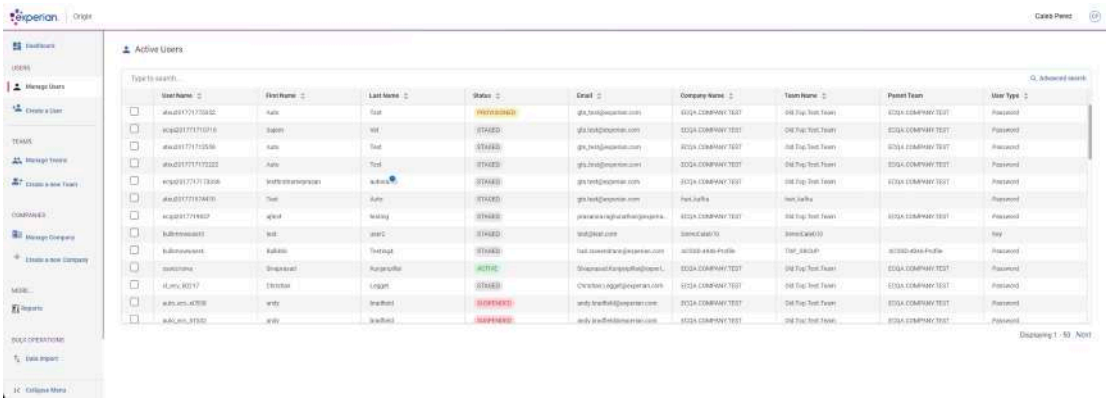
This page displays the user name, First name, Last name, Status, Email, Team name and Company name values in a table. Page allows the following functionality.

- A text search ability.
- Assign application and attributes to the user
- View user

A security designate role user is allowed to view users belonging to his team and team below.

5.2 Search for users

A designate can search for a user by username, first name, last name, and email. Both full name and partial name are supported. When user types characters in the search area, the matching users are displayed in the table below.



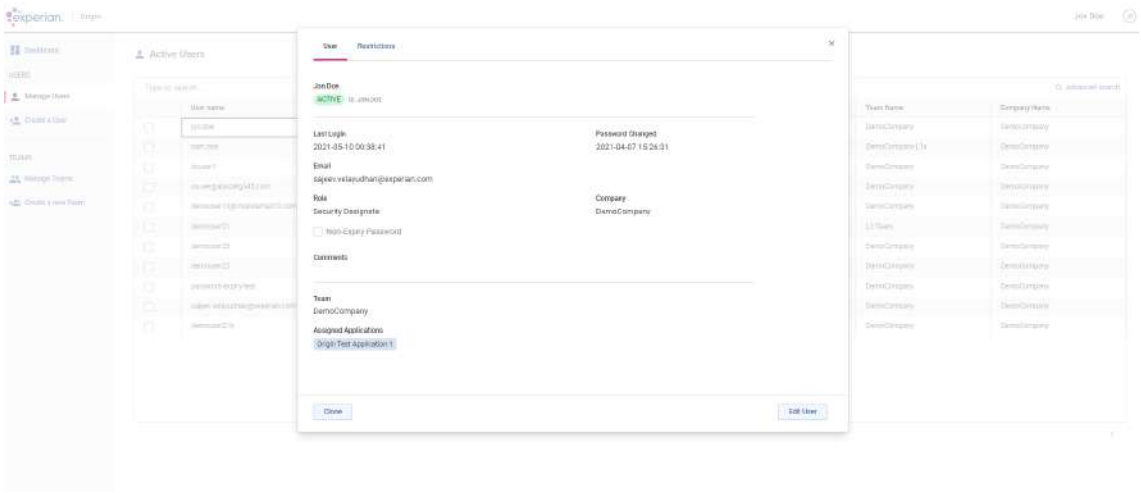
5.3 user details

Clicking a row from the table shows a popup with the user details. This page is read only by default and provides the following functionality.

- User details
- View IP Restriction
- Clone user

5.3.1 User details

This tab displays First name, last name, User name, Status, Last Login Date, Last Password Changed Date, Email, Role, Company, Non Expiry password indicator, Comments, Team, Assigned applications.



5.3.1 View IP Restriction

IP Restriction tab displays the IP restrictions assigned to the user.

IP Restrictions are displayed as a range value in IPV4 formats.

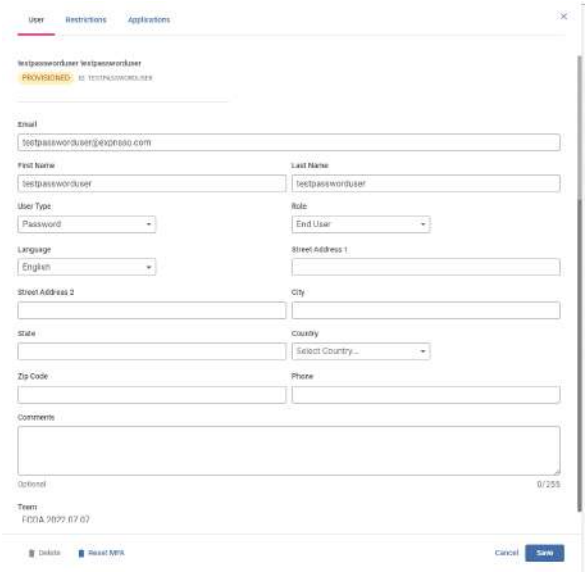
5.3.2 Clone user

Clicking on the "Clone" button on "View User" popup takes to the Create user page with the user's Company and Team selected. After entering user's profile information and saved, the user is created and all applications are assigned to the new user and the view is brought back to the "View User" popup. This step can be repeated as many times as needed.

5.4 Edit a user

Clicking on Edit User button allows the user details to be updated. In this page a Security Designate can,

i. Edit the user profile. Fields Email, First Name, Last name, Address and Comments will be editable.
ii. Fields Username, Status, Team cannot be edited.



After making changes clicking "Save" button saves the data and put the data in read only mode.
On the Restrictions tab, IP restrictions can be removed or added. See section 6.
In the "Edit mode" the following options will be available.

a) Delete user.
b) Reset MFA
c) Reset password
d) Add or remove IP restriction

5.4.1 Delete user

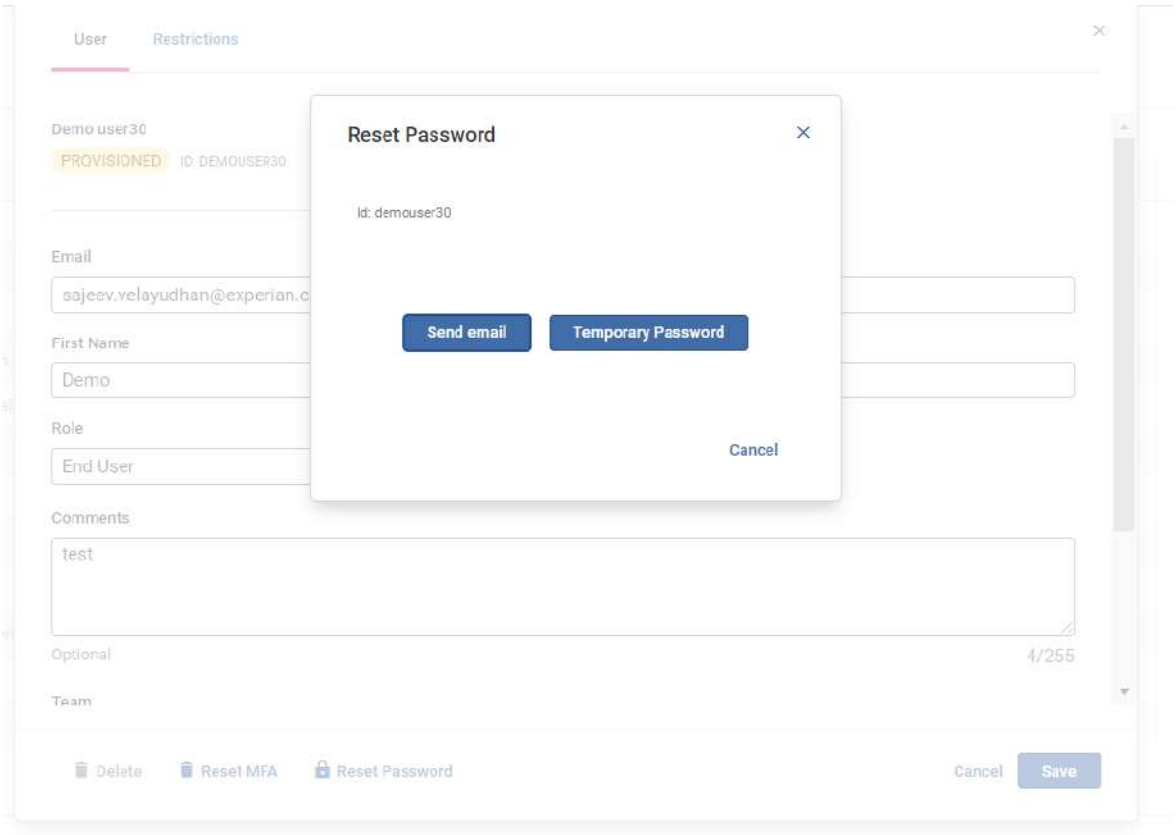
This function allows the Security Designate to delete a user from system. Delete user is a two-step function. When the security designate selects a user record in manage user screen, an option to “Deactivate” user will be displayed. Once clicked, user’s status will be changed to deactivated and user can no longer login. This is equivalent to soft delete. Security designate can select the deactivated user and option will change to “Delete”. Once clicked, user record will be permanently deleted from system and cannot be recovered (hard delete).

5.4.2 Reset MFA

This function allows the Security Designate to reset the MFA factors for the user. Clicking on "Reset MFA" button sends an email to the user with instructions to reset the MFA factors.

5.4.3 Reset password

Security designate can reset the user's password. Clicking on the "Reset Password" button displays a popup that shows 2 options.



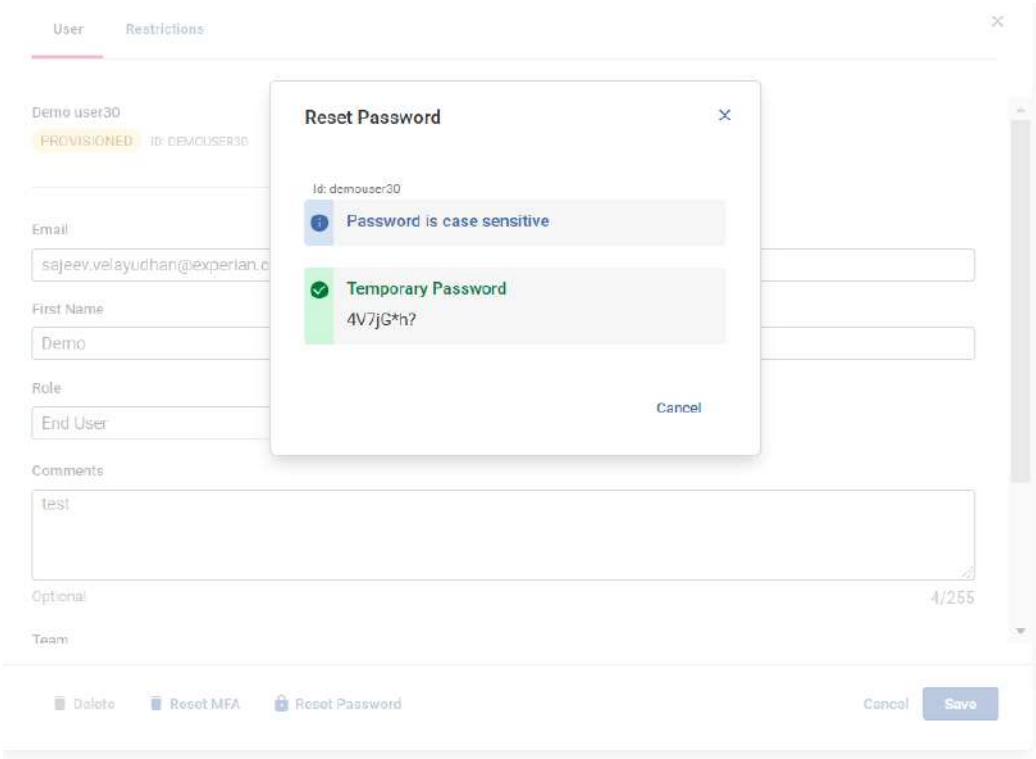
i. Send email
ii. Temporary password

5.4.3.1 Send email

Clicking on this option, send an email to the user providing option to Reset Password by the user.

5.4.3.2 Temporary password

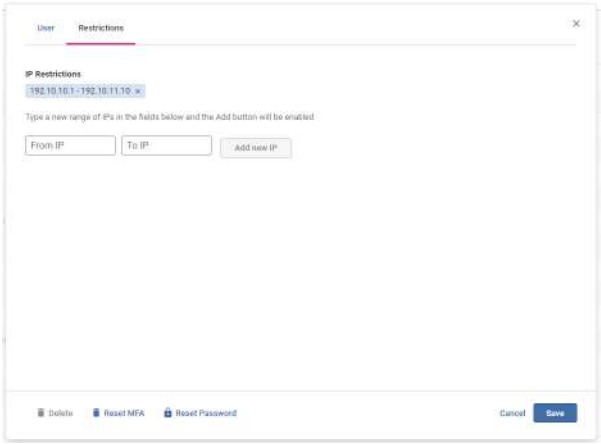
This option allows the Security Designate to read out a temporary password.



5.4.4 Add or Remove IP Restriction

When the Edit mode is on, Restrictions tab allows the following options

i. Remove an existing IP Restriction
ii. Add an IP Restriction



5.4.4.1 Remove an existing IP restriction

Existing IP restrictions can be removed by clicking on the "x" button next to it.

5.4.4.2 Add an IP Restriction

Add a from IP and To IP and click on the "Add new IP" button.

5.5 Create user

Click on the "Create a user" link from dashboard or the menu link on the left nav bar to open the create user page.

Create user page is organized to a 3 step process as follows,

- Create a user
- Assign application(s)
- Assign attribute(s)

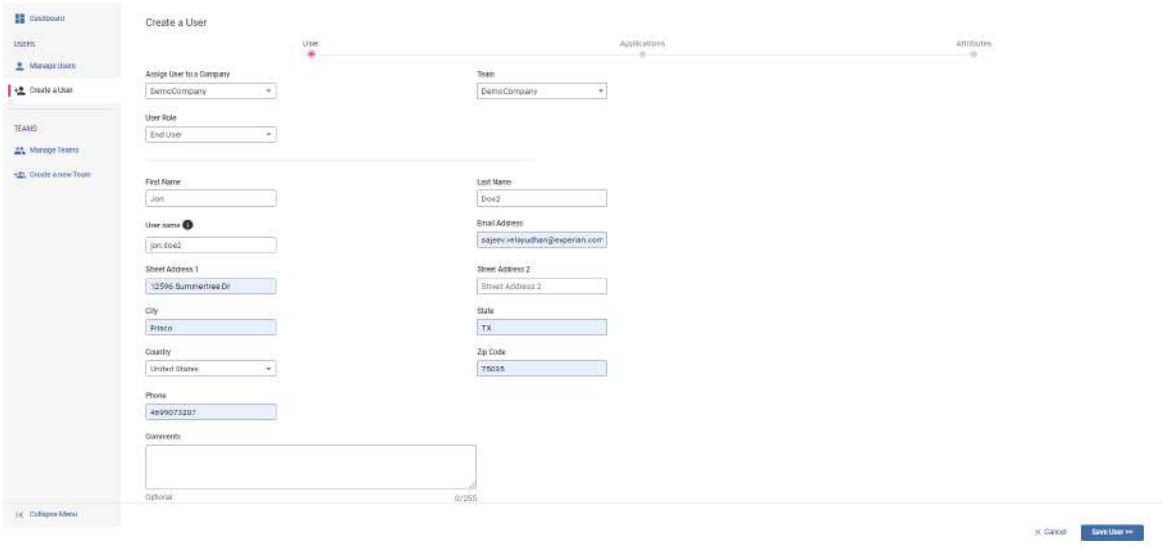
5.5.1 Create a user

Select a company and team and select a role for the user and enter all the details. Following fields are required when a user is created.

i. Company - Select a company. A security designate, will always have only one company.
ii. Team - Select a team. A Security Designate will have a one or more Teams but the teams that falls in the hierarchy below his own team.
iii. User Role - Select a Role. A Security Designate can only create a user with End User role.
iv. First Name - Enter First name.
v. Last name - Enter Last name.
vi. User name - Enter a valid User name.
vii. Email - enter a valid email.

Following values are optional

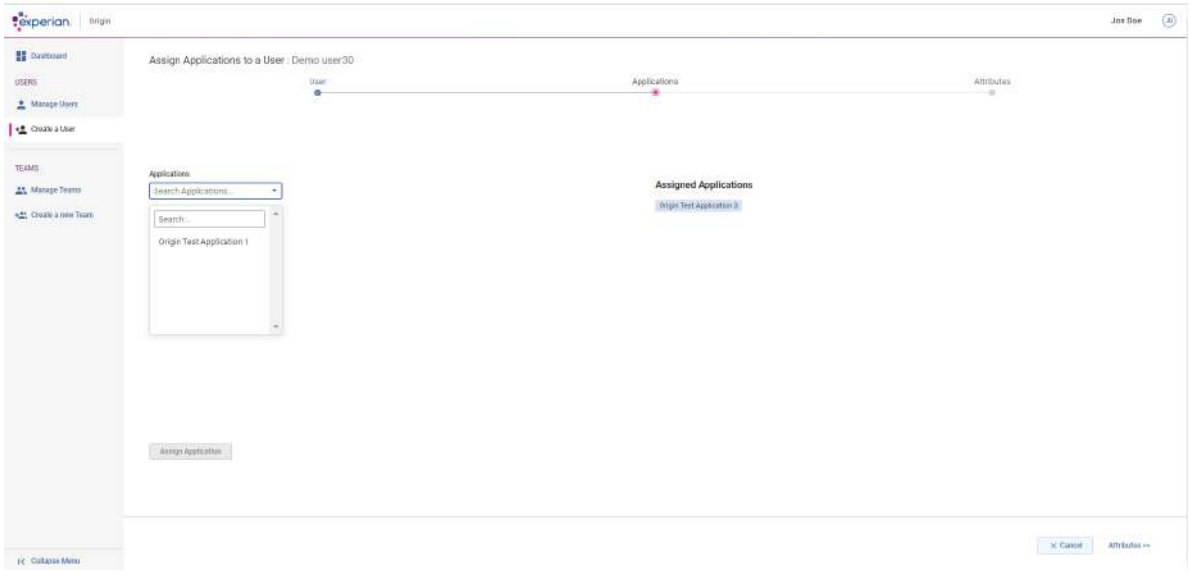
i. Street Address1
ii. Street Address2
iii. City
iv. State
v. Country
vi. Zip Code



When the required data is entered "Save User" button is enabled. Clicking on "Save User" takes the user to the "Assign Application" page.

5.5.2 Assign application(s)

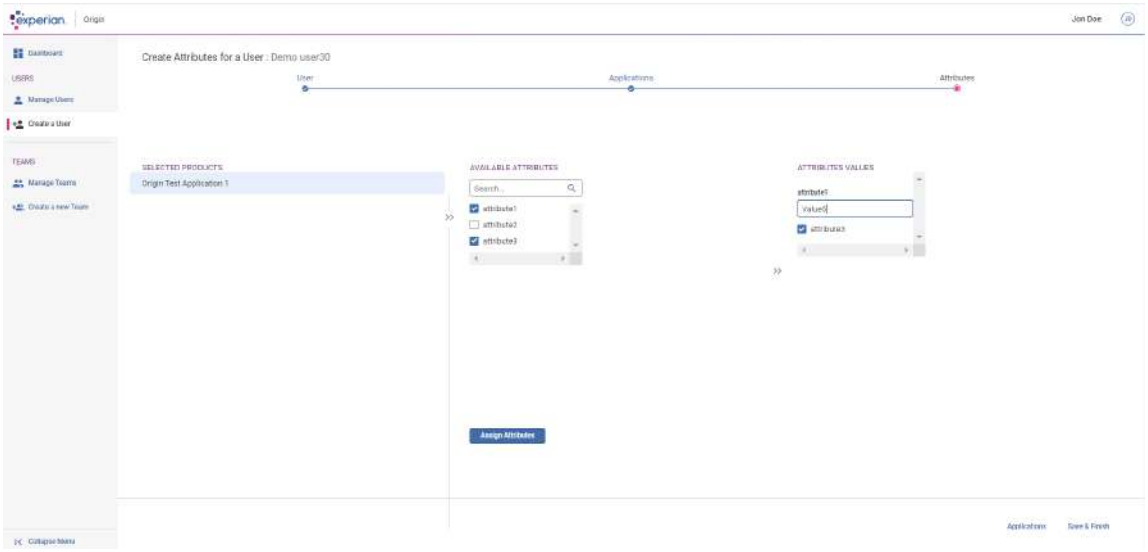
In this page, one or more application can be assigned to the user. Applications listed for assignment are coming from the user's team in the profile.



When application is selected from the drop down, "Assign Application" button is enabled. Clicking on "Assign Application" displays the application on the "Assigned Application" list. Assignment of applications can be repeated for all available applications on the "Applications" list. When one or more applications are assigned, click on "Attributes >>" button to take to "Assign Attributes" page.

5.5.3 Assign attribute(s)

In this page, one or more attributes can be selected and assigned with a value.



Selecting an application from the list, displays the available attributes. Selecting an attribute displays the attribute value section where a value can be entered.

Following types of attributes are supported,

i. Text value - value entered.

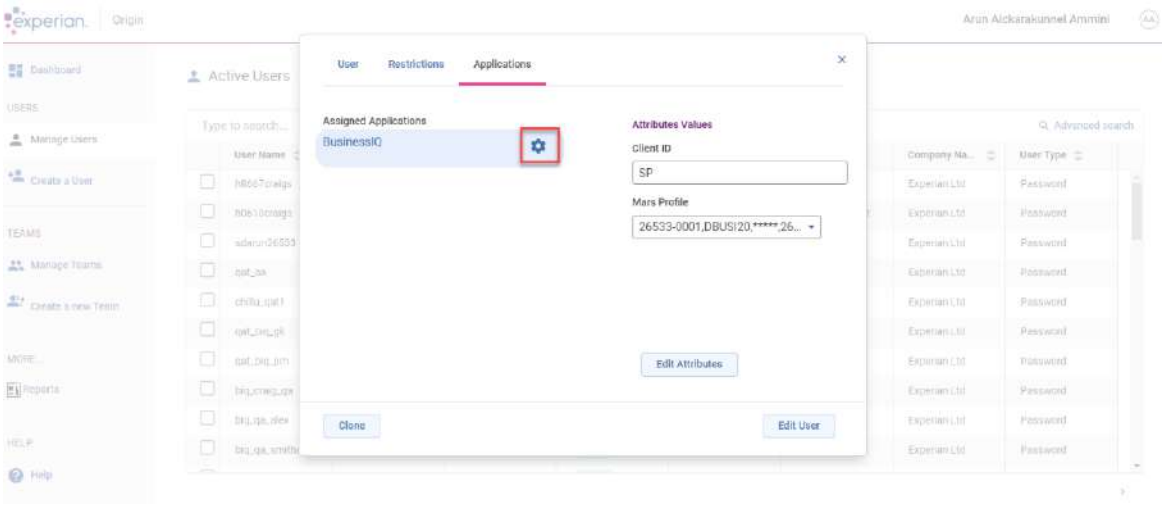
ii. boolean value - value is checked when selected.

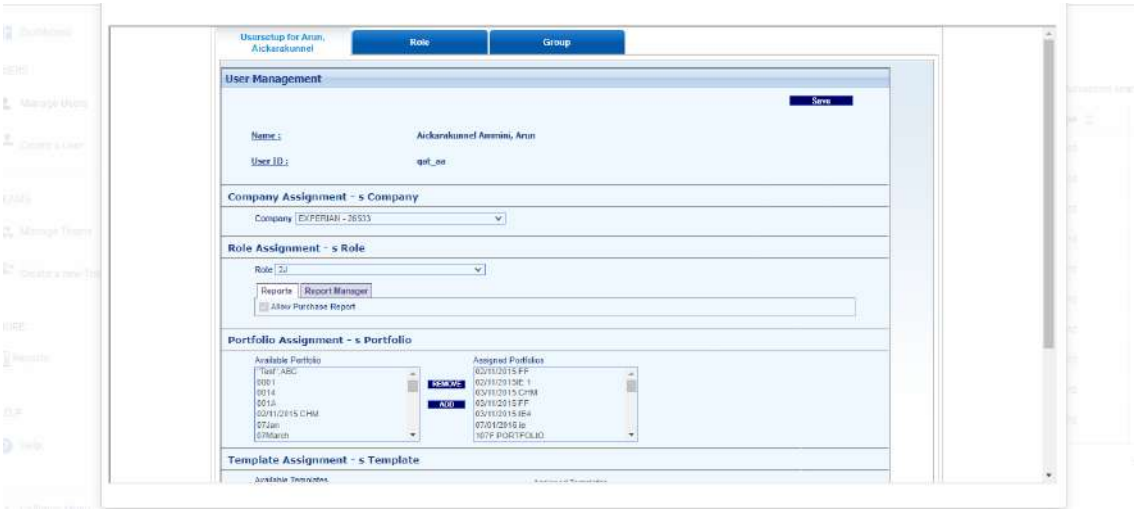
When one or more attributes are assigned, click on "Save & Finish" button which will complete the process.

Note: Attribute assignment are an optional step. It can be completed at a later point if desired.

5.6 BusinessIQ Provisioning

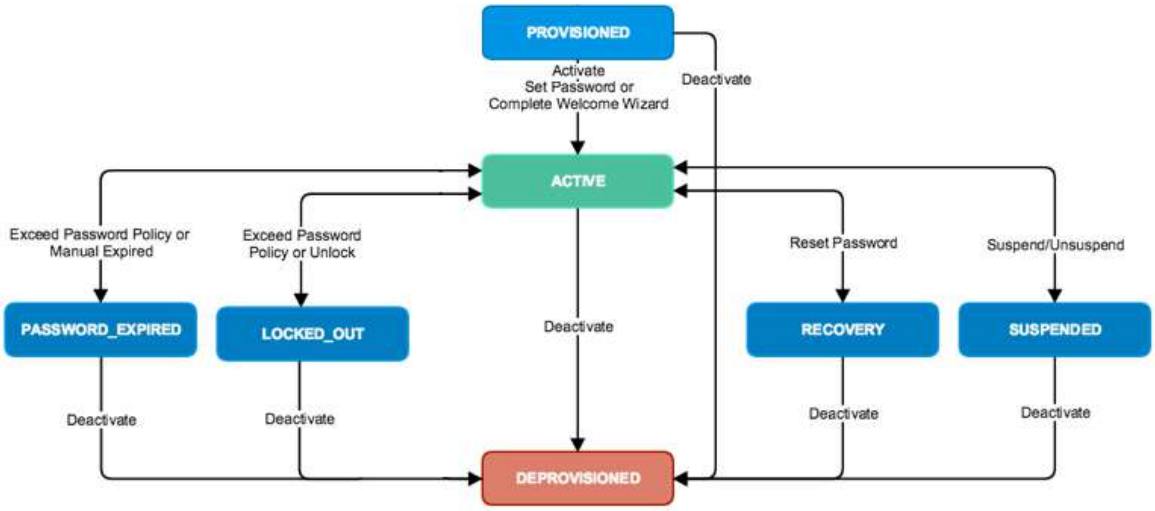
To complete the user provisioning for BusinessIQ application, when the BusinessIQ application and attributes are assigned to user, Origin system will open the BusinessIQ provisioning screen for the Security Designate to complete provisioning. In case to make updates to existing users, BusinessIQ provisioning screen can also be opened by clicking on gear icon next to the application name in view users screen as shown below.





6. Origin User States

An Origin Security Designate can perform various life cycle operations to move user from one state to another as depicted in the diagram below.



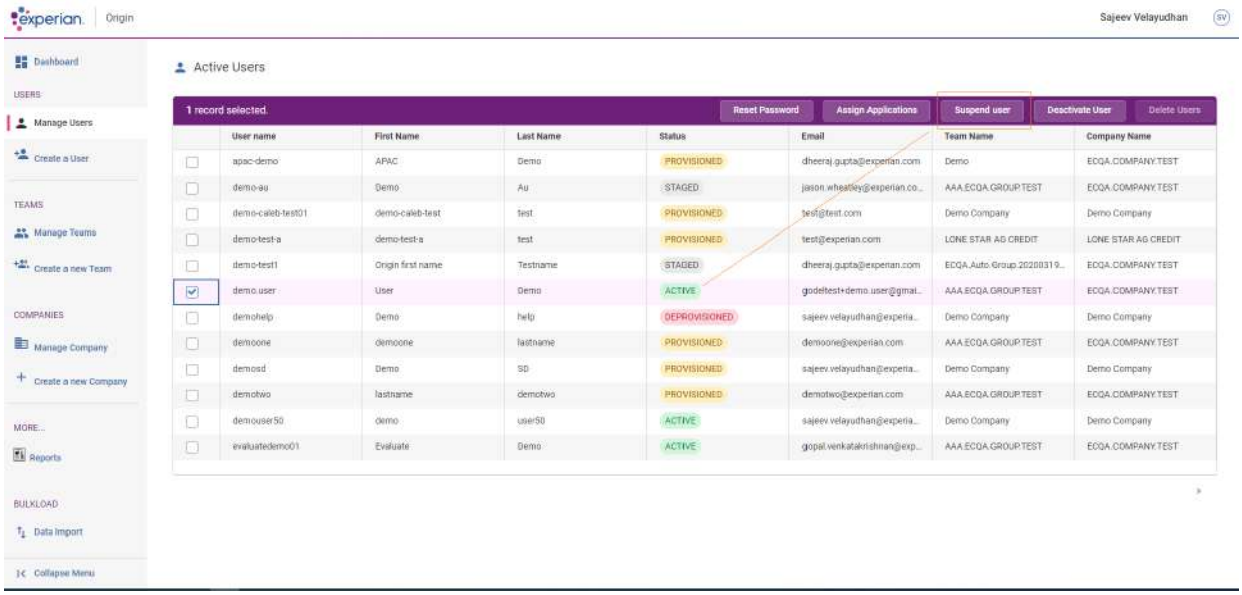
Status	Description	Permitted Actions
PROVISIONED	New users created in Origin	Activate (self service), Deactivate (Security Designate)
ACTIVE	User is activated and credentials are set	Reset password(self service, (Security Designate)), Suspend((Security Designate)), Locked(system), password expiry(system), Deactivate(Security Designate)
DEPROVISIONED	Deactivated from Origin	Delete(Security Designate)
PASSWORD_EXPIRED	User's password expired through password policy	Deactivate(Security Designate)
SUSPENDED	User can't login. Applications will be kept assigned. User cant be unsuspended	Unsuspend(Security Designate)
DEPROVISIONED	User can't login. User can only be deleted.	Delete(Security Designate)
LOCKED_OUT	User is locked out by password policy	Unlock(self service), Deactivate(Security Designate)

7. User Lifecycle Management

A Security Designate can manage a user's life cycle. The following operations can be performed based on the user status.

User status	Action	Target status	Comments
PROVISIONED	Deactivate	DEPROVISIONED	
ACTIVE	Suspend	SUSPENDED	
	Deactivate	DEPROVISIONED	
	Reset Password	PASSWORD_RESET	
DEPROVISIONED	Delete	--	User will be hard deleted
SUSPENDED	Unsuspend	ACTIVE	
	Deactivate	DEPROVISIONED	
PASSWORD_RESET	Deactivate	DEPROVISIONED	

One or more users can be selected from the manage user's page and select an available operation.

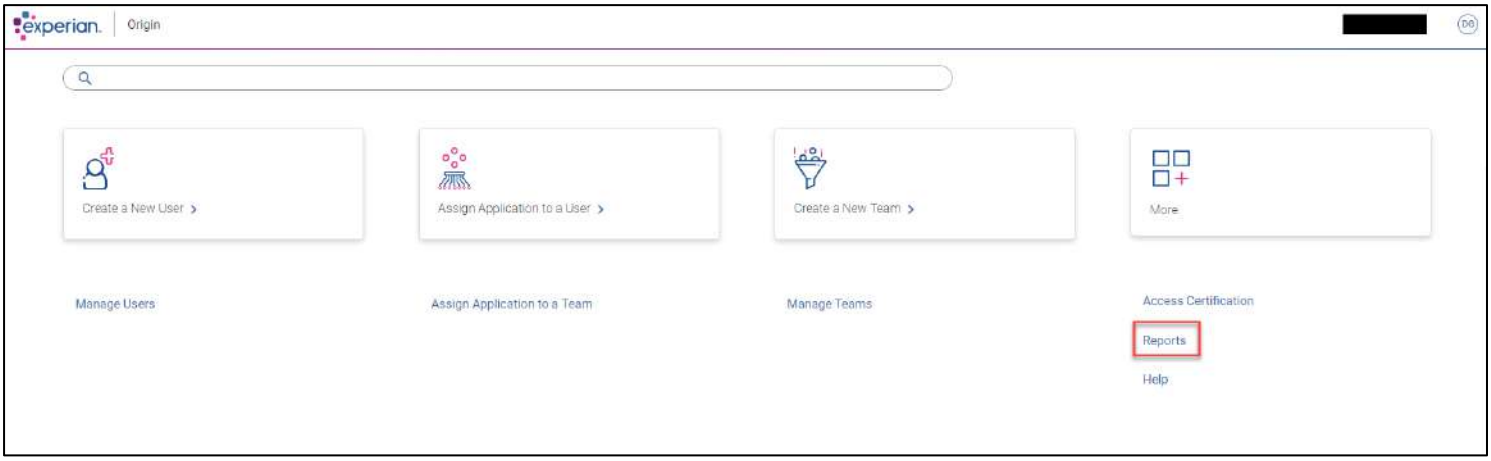


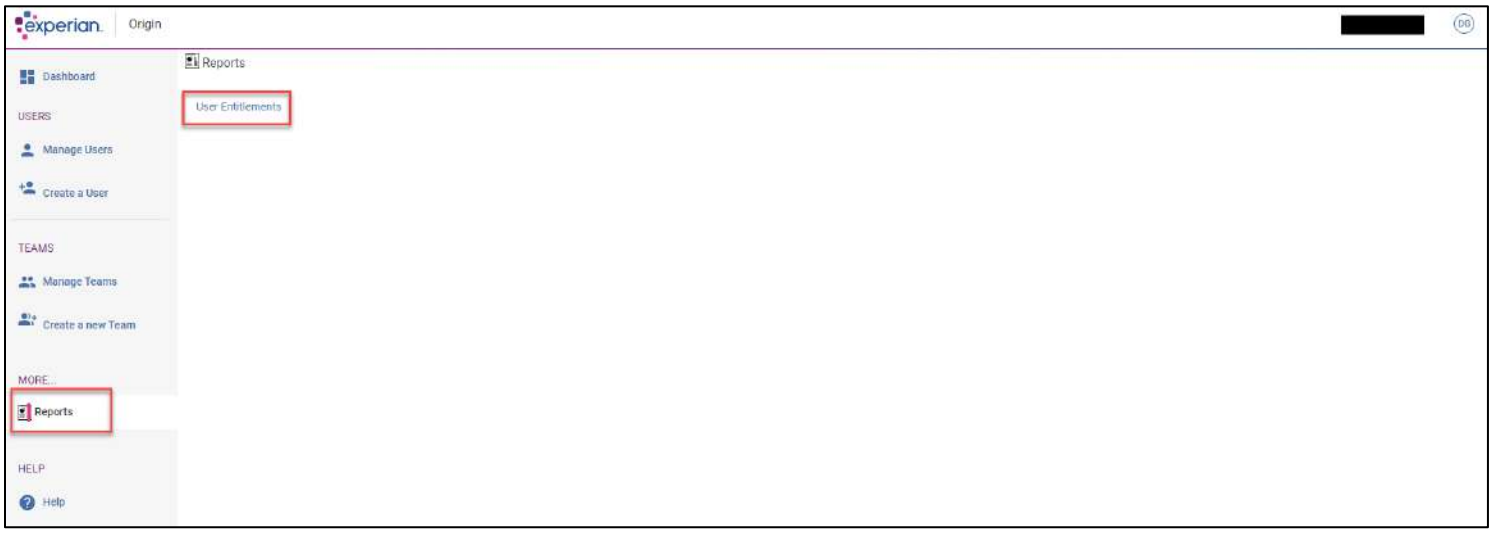
Please note, a user must remain in an ‘active’ status to prevent their account from being suspended. To remain in this status the user must login at least once per 90 days. If a user remains inactive for 90 days, their account will be suspended and if they are not active for 180 days their account will be hard deleted. If the user’s account is suspended, they must reach out to their Security Designate or Experian’s Technical Support (1-800-854-7201 Option 3) to unlock their account and proceed to login to regain active status.

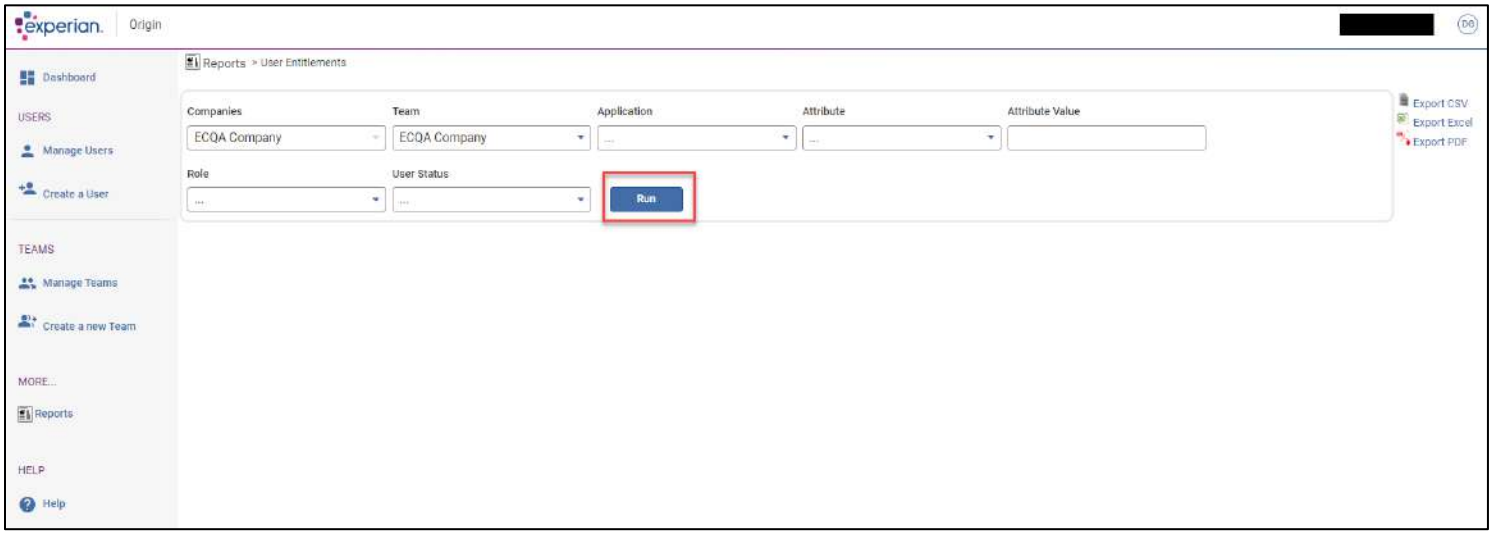
8. Reports

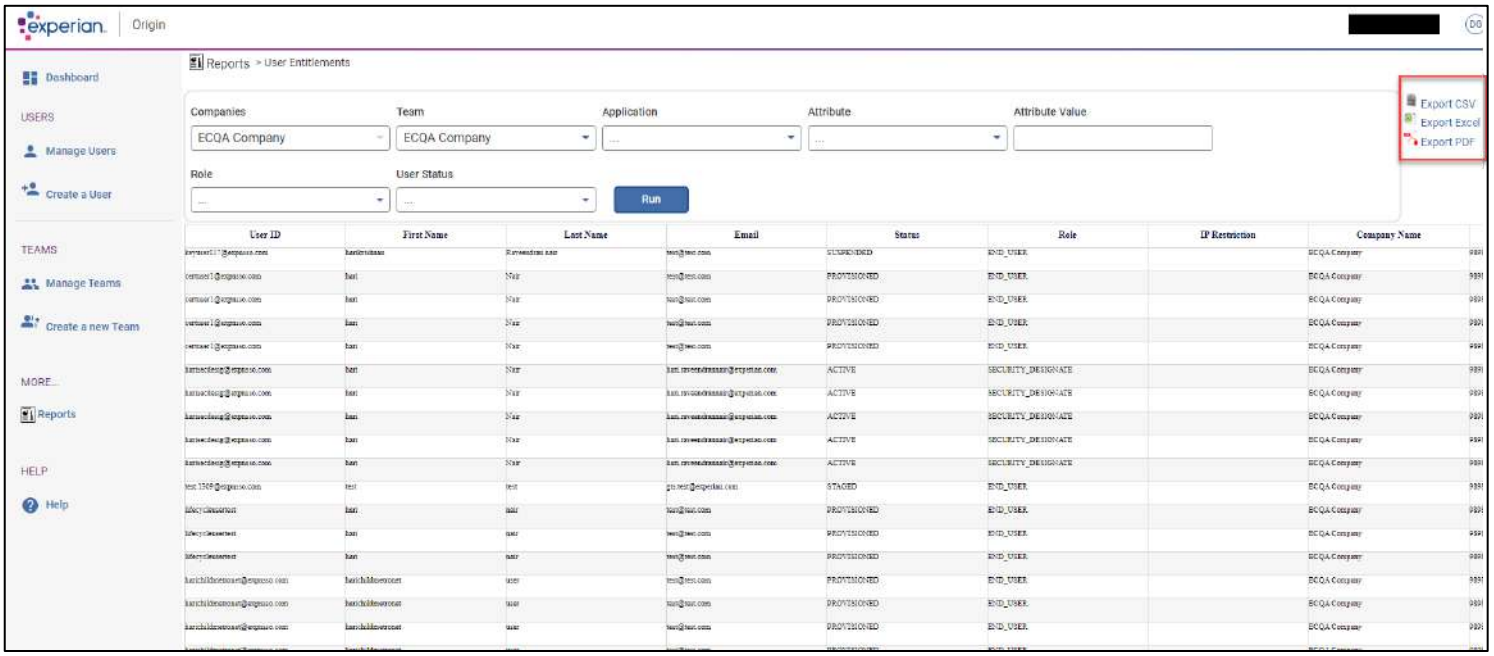
A security designate can generate the entitlement reports from Origin which will list down all users having application entitlements. The report will list all user details and the entitlements they have. Report can be extracted in pdf/excel/csv format.

To access user entitlement report, click on the “Reports” link in dashboard and then click on “User Entitlement Report”. Please refer the screenshots below.






experian.
Origin
Dashboard
USERS
Manage Users
Create a User
TEAMS
Manage Teams
Create a new Team
MORE...
Reports
HELP
Help
Reports > User Entitlements
Companies
ECQA Company
Team
ECQA Company
Application
Attribute
Attribute Value
Role
User Status
Run
Export CSV
Export Excel
Export PDF


experian.
Origin
Dashboard
USERS
Manage Users
Create a User
TEAMS
Manage Teams
Create a new Team
MORE...
Reports
HELP
Help
Reports > User Entitlements
Companies
ECQA Company
Team
ECQA Company
Application
Attribute
Attribute Value
Role
User Status
Run
Export CSV
Export Excel
Export PDF
User ID
First Name
Last Name
Email
Status
Role
IP Restriction
Company Name