**How to configure SCIM for CloudGate**

**Contents:**

* Supported Features
* Requirements
* Configuration Steps

**Supported Features:**

* Create Users
* Update User Attributes
* Deactivate Users
* Push Groups

**Requirements:**

To configure SCIM for CloudGate, you need to have admin access to your client’s CloudGate web portal. You may also contact CloudGate support for any assistance with the configurations.

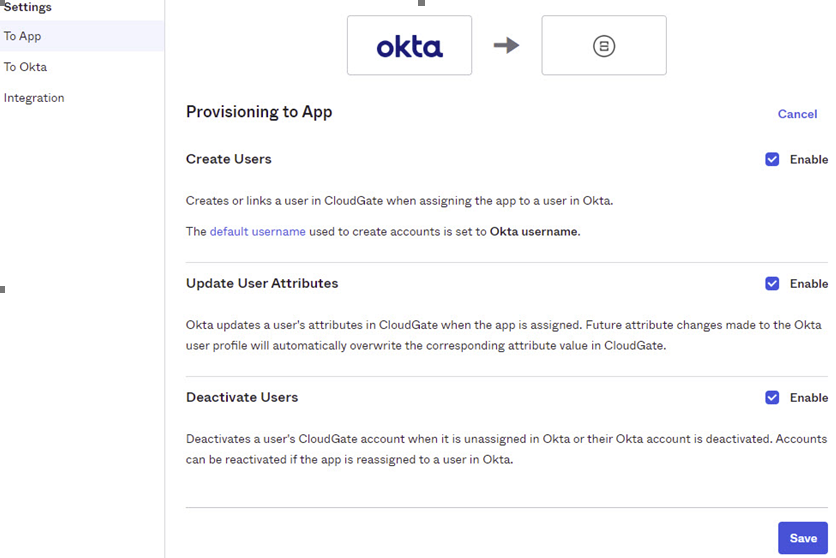
**Configuration Steps**

# Step 1: Provisioning

# 

# Log into Okta. Go to Admin > Applications and select the CloudGate application. Click on Provisioning.

# 

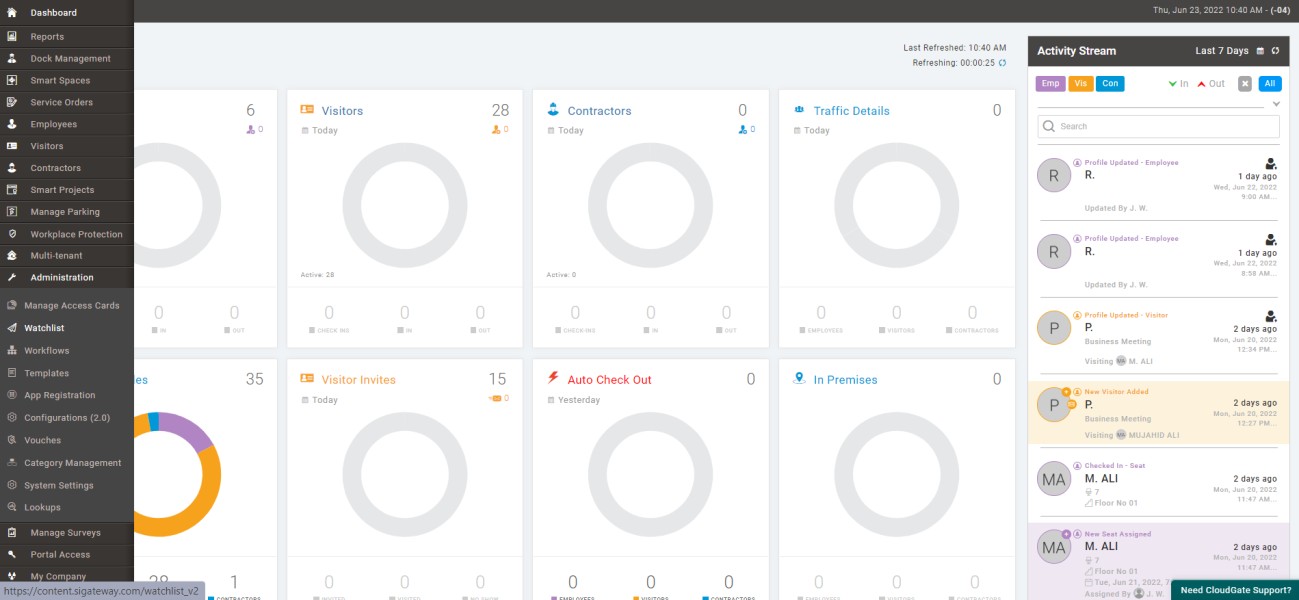
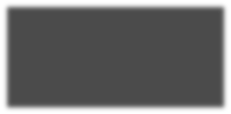


For required fields of **SCIM connection** admin will be required to log into CloudGate web portal.

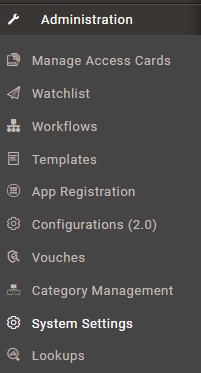
# CloudGate SSO Configuration

Admin can access the **SCIM Connector Base URL** by following steps below.

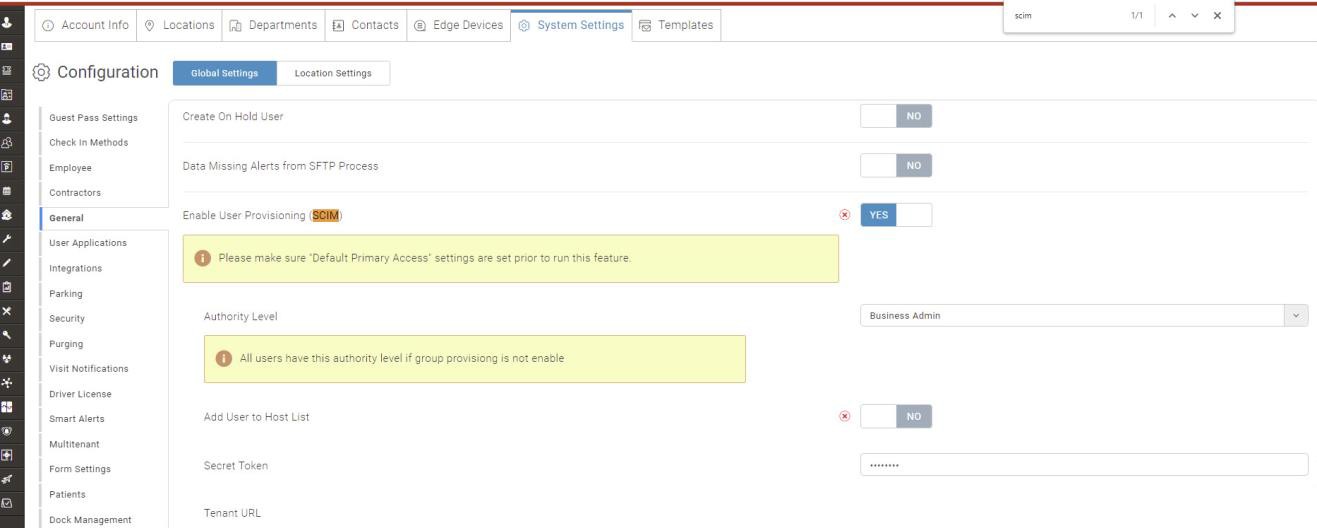
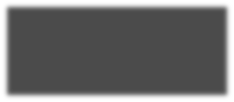
* **Login** into CloudGate web portal.



* In the left side menu of the dashboard, Click **Administration** then click **System Settings** in its Sub-menu.



* Go to **System Settings** > **General** > **Global Settings**.



1. Here admin will toggle On **Enable Users Provisioning**.



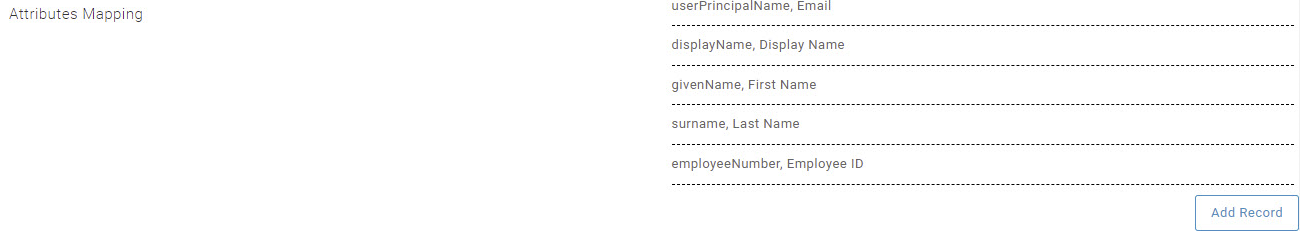
1. **Tenants URL** corresponds to **SCIM connector base URL**. Copy the URL from here to paste it into Okta **SCIM Connections.**



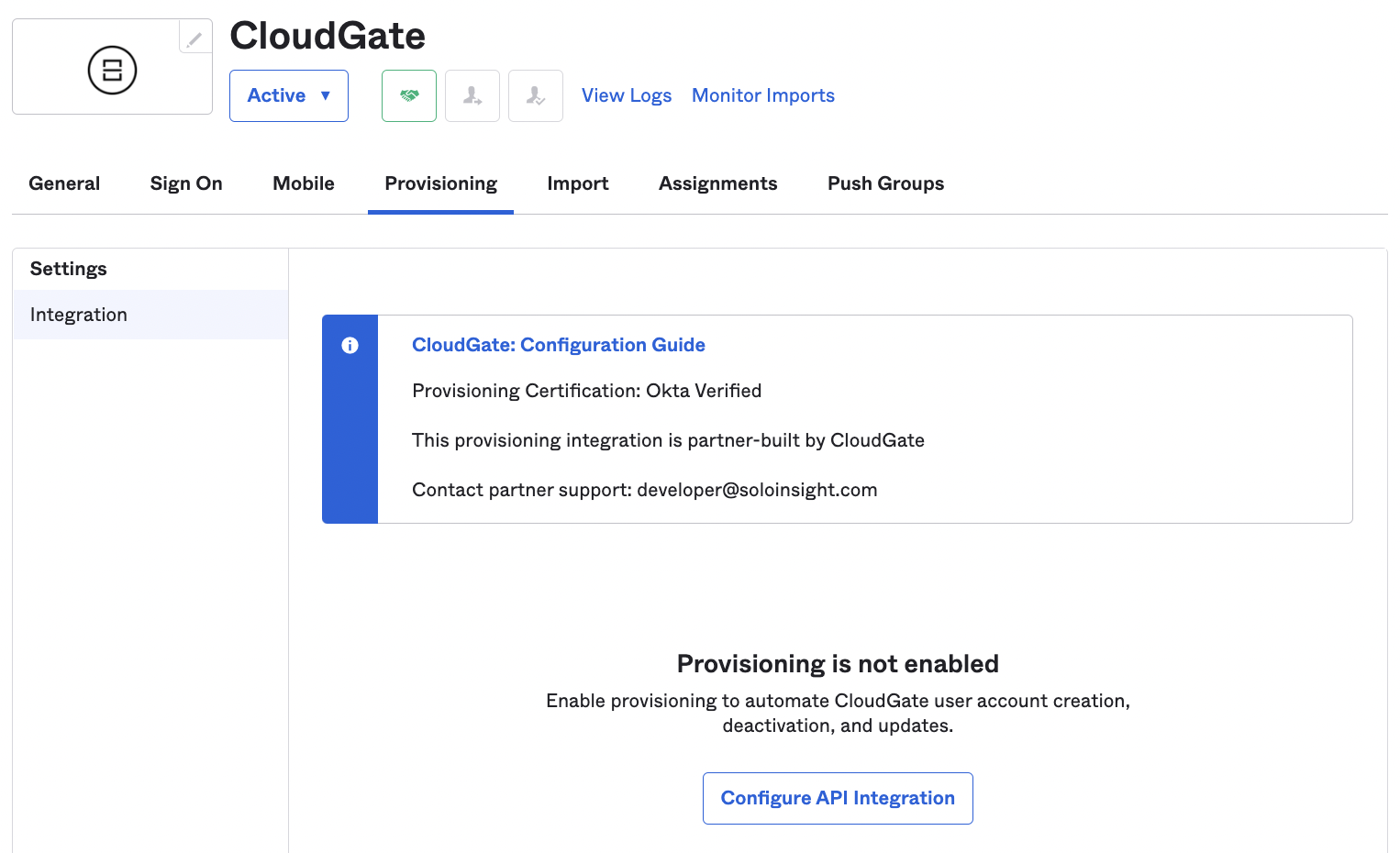
1. **Secret Token** corresponds to the **Authorization** field that will be visible in Okta when **Authentication Mode** is set to **HTTP Header.**



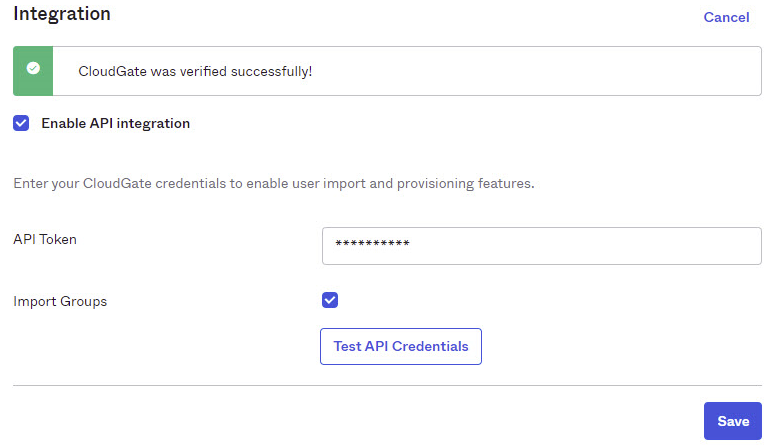
1. **Attribute Mapping** Here user will map attributes as same as its seen below.



**Provisioning to App**



* Here admin will click **Edit** which will open a new window seen below.



* Here admin will Check **Enable API integration.**



* Here in **API Token** admin will add **Secret Token** copied from CloudGate dashboard settings.

****

* Here admin will check **Import Groups.**

****

* Now to test API credentials admin will **click** on **Test API Credentials**.

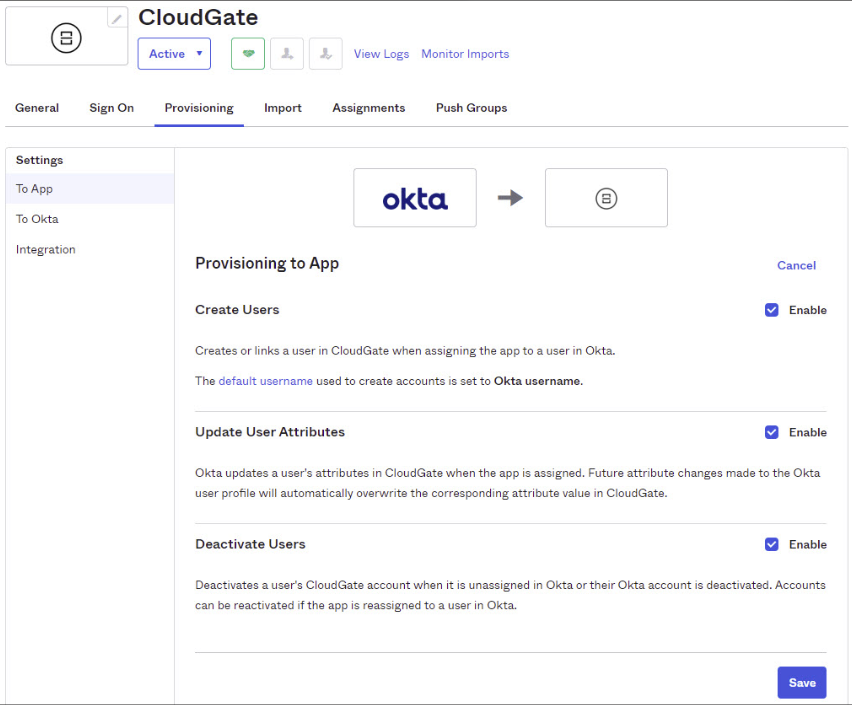


* Admin will see popup once API credentials get successfully verified.

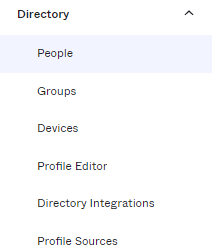
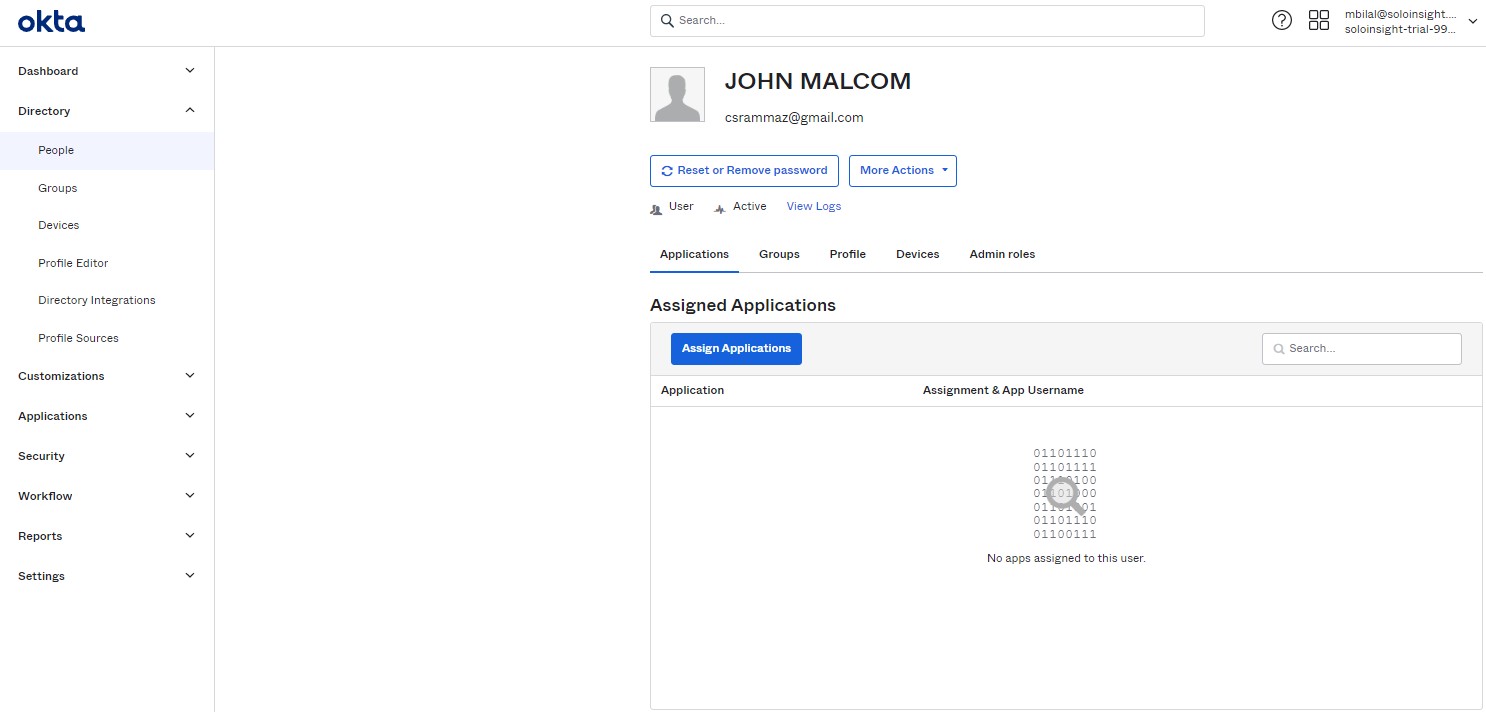
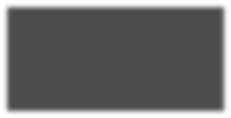


* Click **Save**.

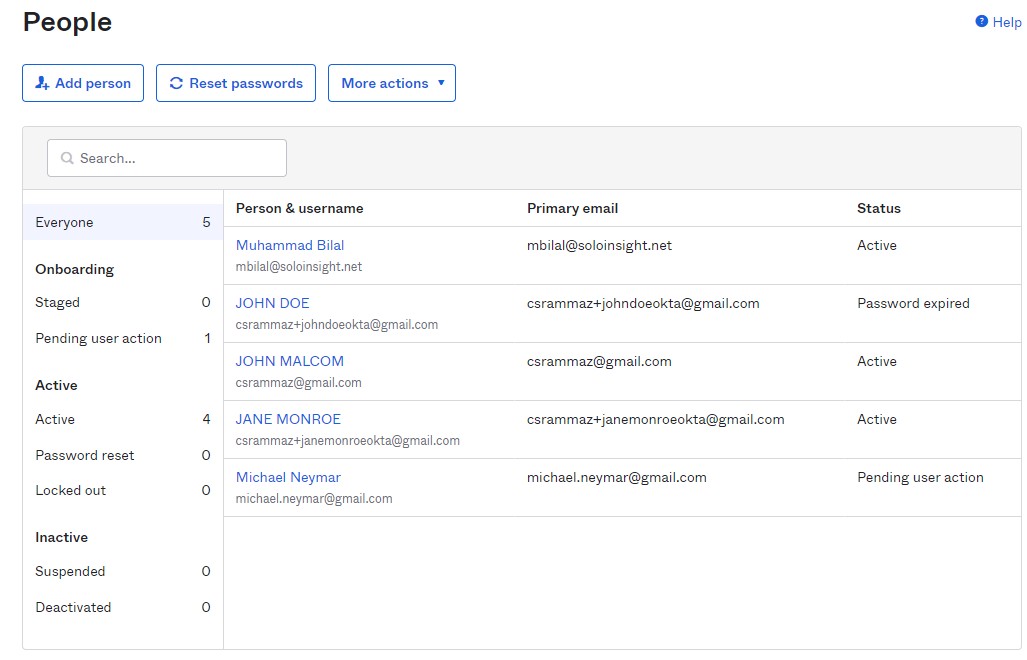
**Mapping Attributes**



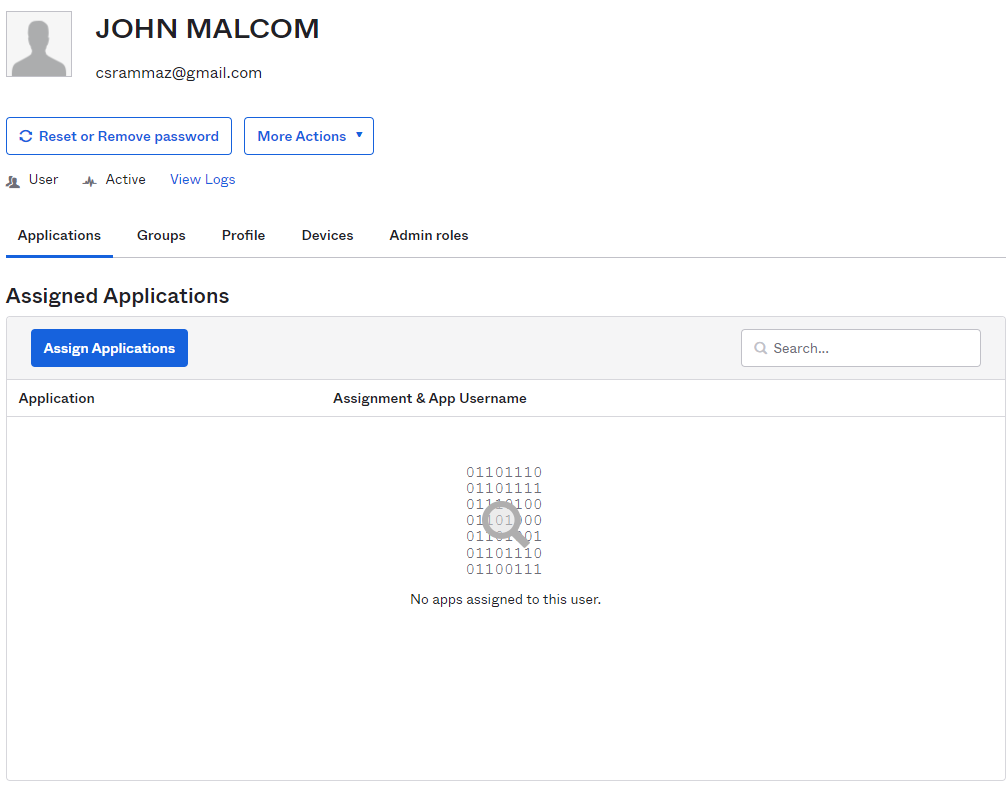
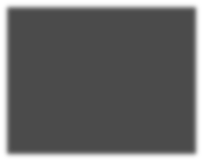
# Assigning Application to user



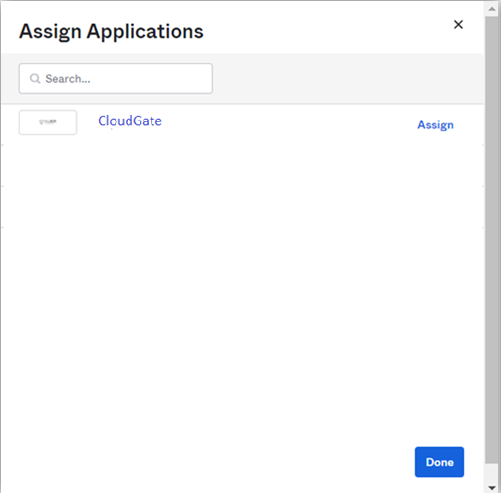
In the left side menu click **Directory,** then click **People** from sub-menu which will open a list of user in right side seem below.



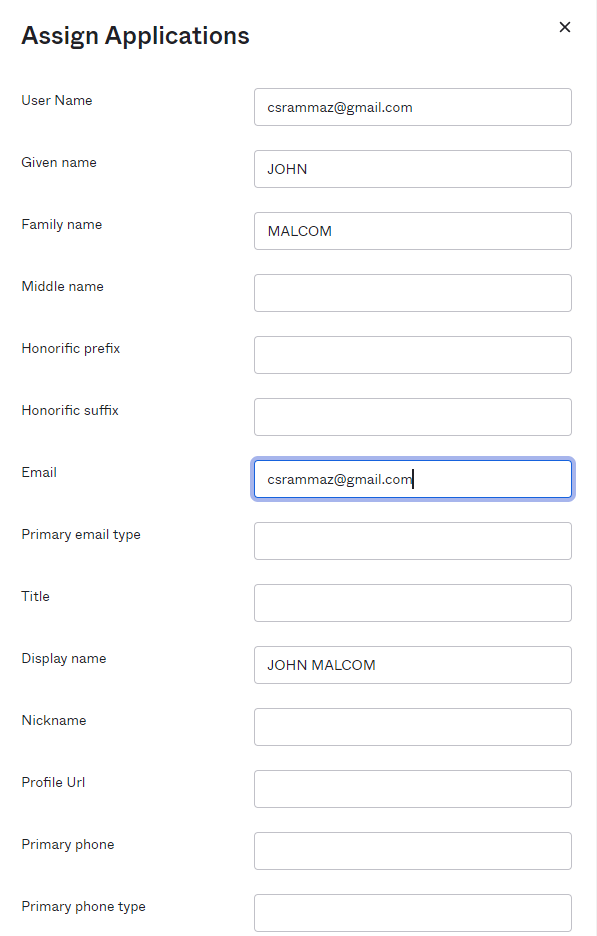
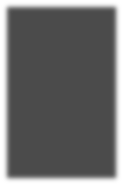
* Here admin will click on required user which will open a new page seen below.



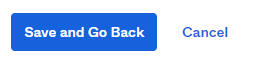
* Click **Assign Applications**. Which will open a pop-up displaying all available applications for user seen below.



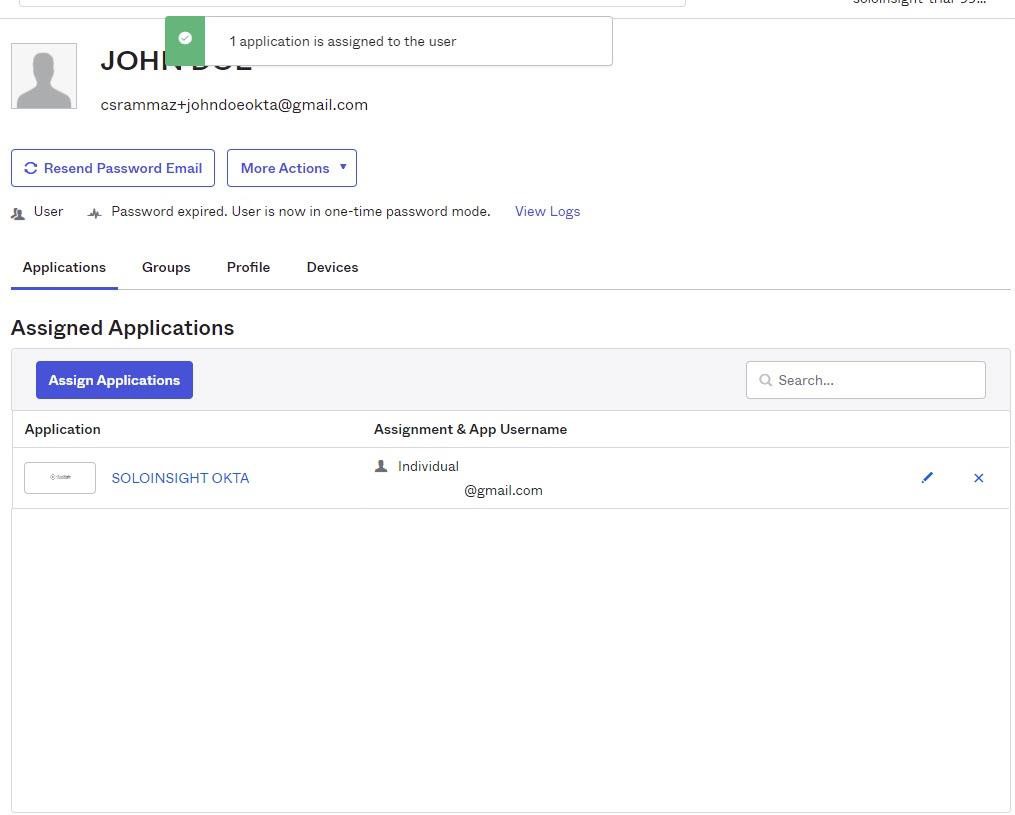
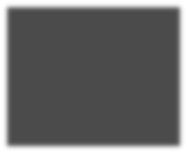
* Here admin will assign required application to user by a single click on **Assign** Button next to any app in the list. Clicking on assign will open a pop-up where admin will add information for the user seen below.



* Once admin has done verifying all required fields, Click **Save & Go Back**.

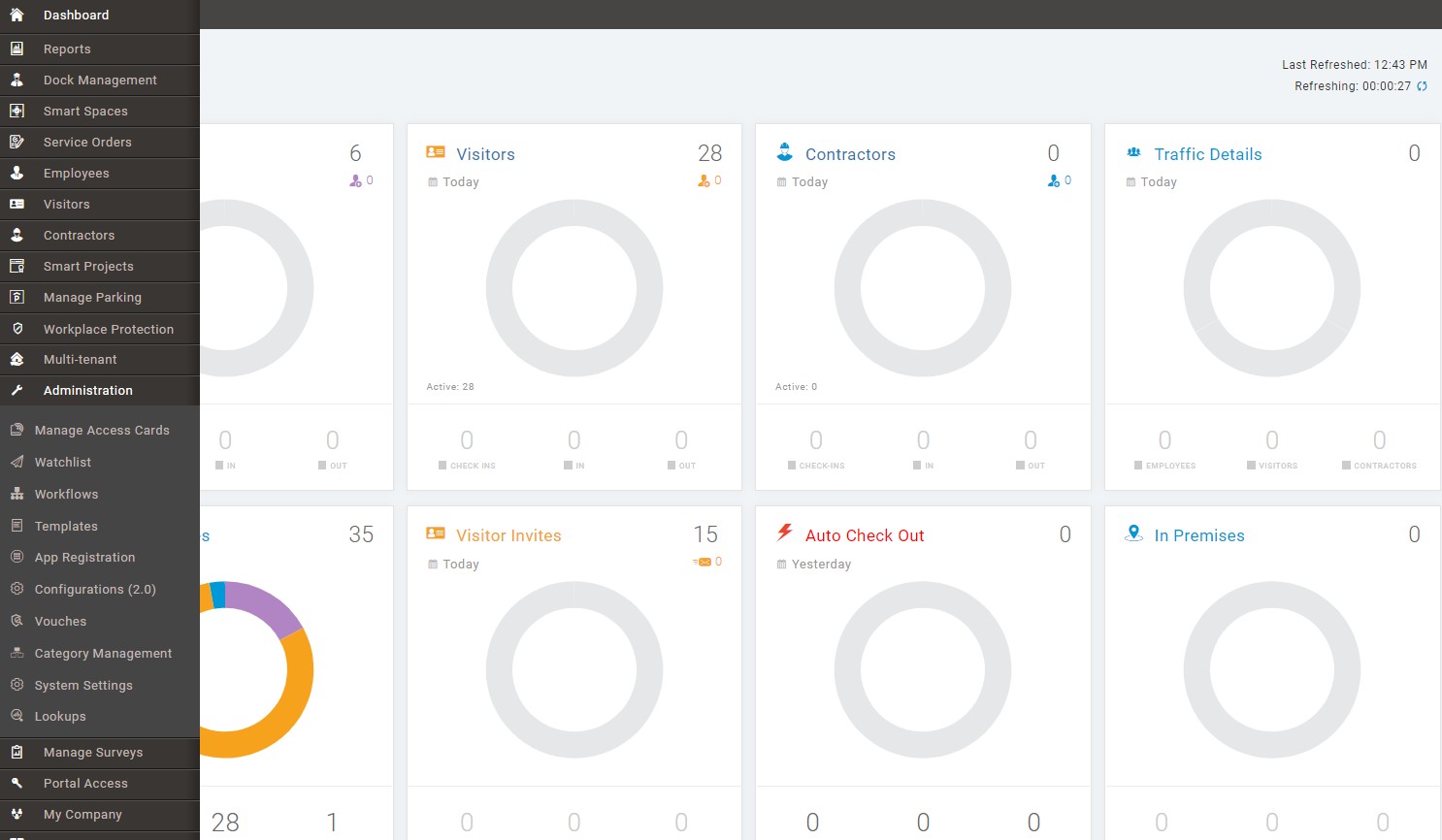
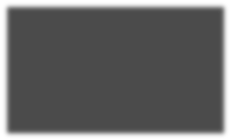


* Clicking on Save & Go Back will redirect admin to previous page displaying **1 application assigned to the user** as seen below.



# Provisioned user in CloudGate from OKTA

* First login into CloudGate Dashboard.



* In left side menu, Click **Employees** which will open a new page seen below.

Graphical user interface

Description automatically generated with medium confidence

* Here in employees list user can be verified by the same username and registered email.

# Known Issues/Troubleshooting

# N/A

# Note: In current version of application we are not targeting imports so [https://okta.cloudgate.ws/scim/v2/sync2/Users?startIndex=1&count=2](https://urldefense.com/v3/__https:/okta.cloudgate.ws/scim/v2/sync2/Users?startIndex=1&count=2__;!!PwKahg!9tGbxZiDXXOp3qh8NvsjjpYkneYXot6uODMbiyIBQZH18BMG2zPOnpdsTWOBp0yz-aeyzqzmpdN-FVSta0yhojW6Ww$) is not yet implemented.