PepsiCo Email MFA Associate SSO service (Okta) Implementation Phase I

Training Document

Helpdesk Administration Guide

Last Updated: 1/7/2020

Version 1.3

Contents

1 Requesting the Helpdesk Admin Role 4

2 Associate SSO service (Okta) Helpdesk Workflows 6

2.1 Helpdesk Admin UI Overview 7

2.2 View User Profile 8

2.3 Manage Users 10

Reset Multifactor 10

Clear User Sessions 11

Reset Behavior Profile 11

2.4 Authentication Troubleshooting 12

3 User Self Service 14

3.1 MFA Reset or Setup 14

3.2 Password Resets 16

About this Document

Purpose

This document describes the capabilities of an Associate SSO service (Okta) helpdesk Admin and common actions they may need to perform when assisting end users.

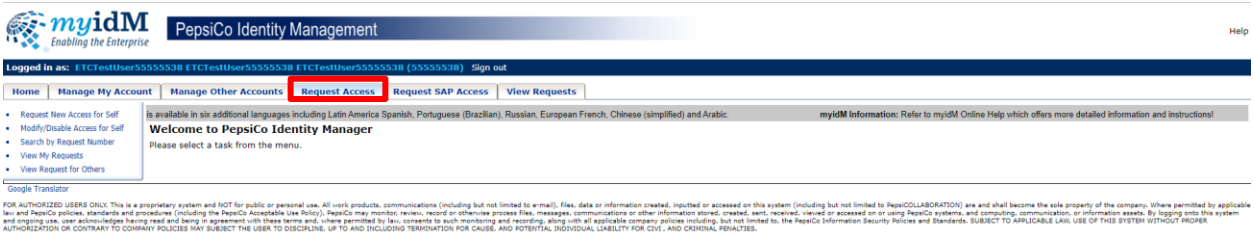
Intended Audience

- Helpdesk Admins

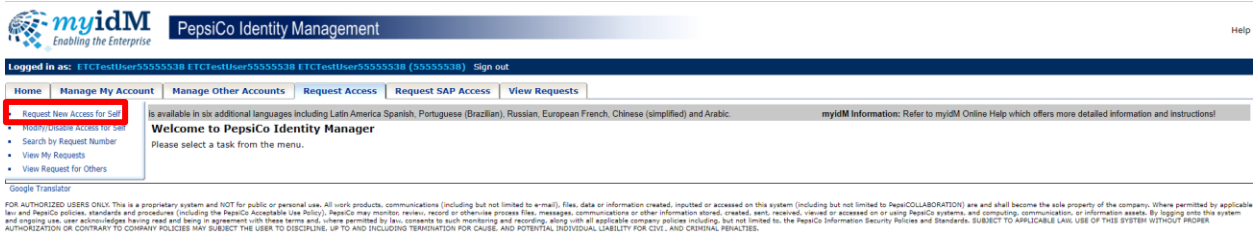
1 Requesting the Helpdesk Admin Role

Helpdesk admins will need to request the helpdesk role in order to be able to access the helpdesk admin dashboard. To do this:

1. Navigate to myidm.mypepsico.com and login
2. Click the “Request Access” tab

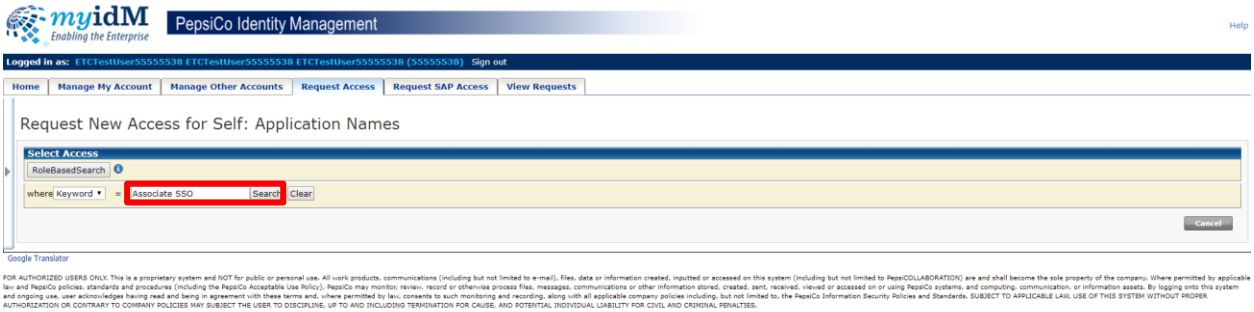


3. Click “Request New Access for Self”



4. Scroll to the bottom and click “Request New Access”

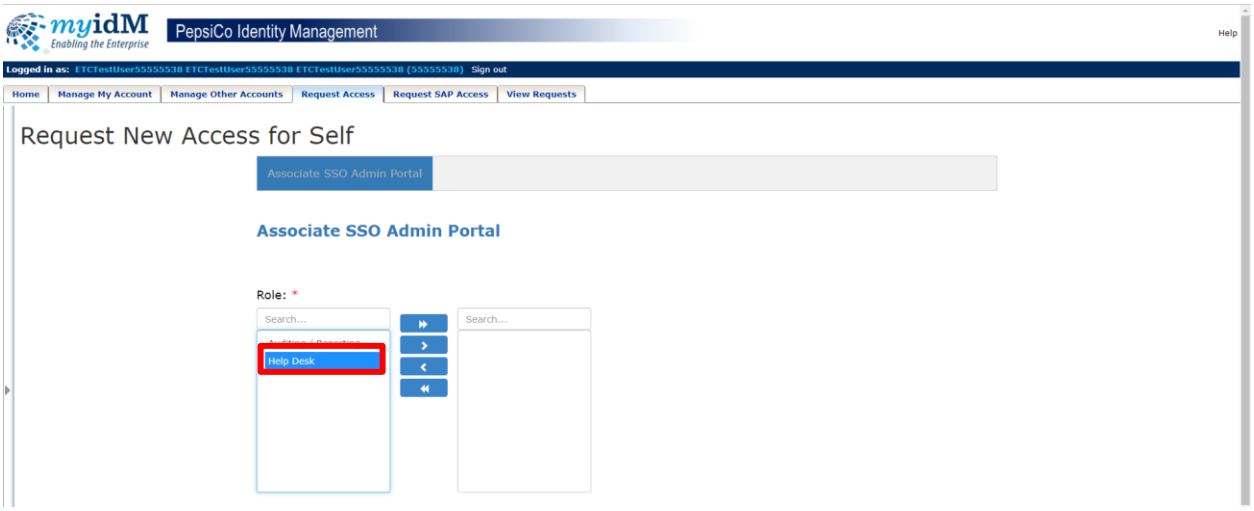
5. Search for “Associate SSO”



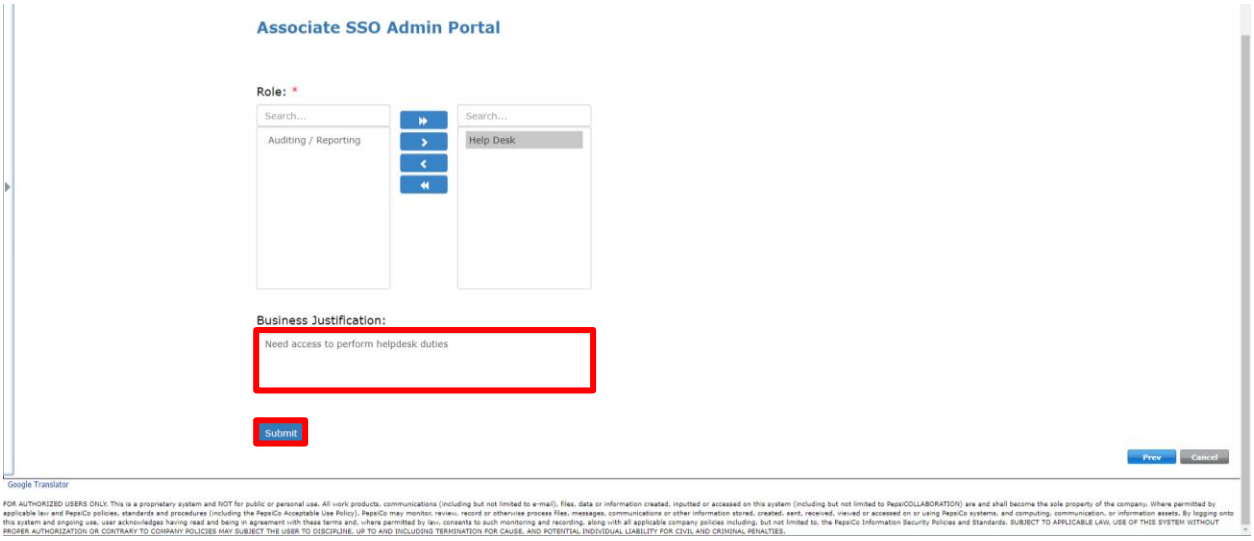
6. Check the box for “Associate SSO Admin Portal” and click “Select”

7. Ensure that “Associate SSO Admin Portal” is present and click “Next”

8. Double click “Help Desk” to select the role and move it to the right column.



9. Enter “Need access to perform helpdesk duties” for business justification and click “Submit”



10. The request will have been submitted and awaiting approval. The ticket number on the confirmation page can be used to track the status of the request.

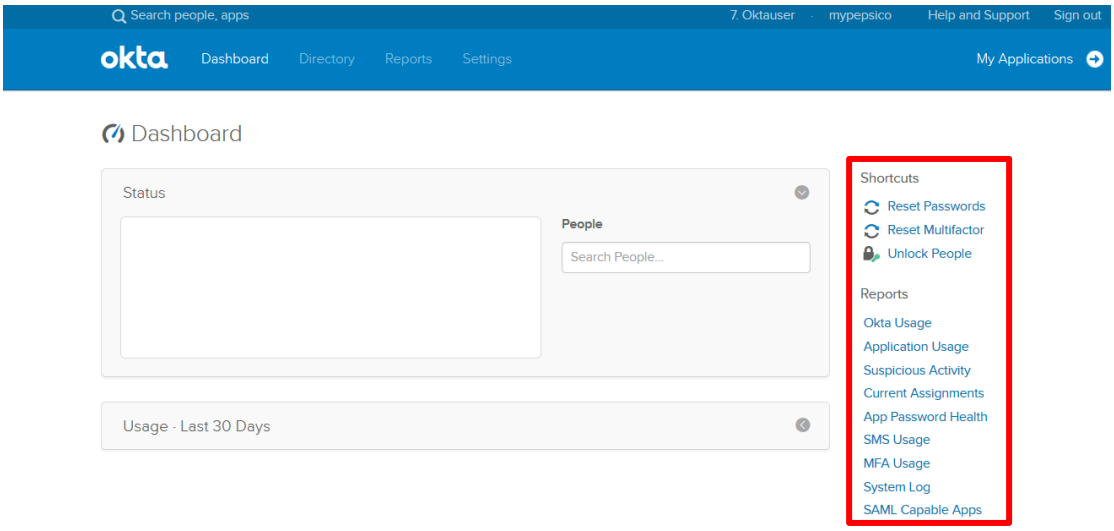
2 Associate SSO service (Okta) Helpdesk Workflows

There are various workflows that define helpdesk admin activities around:

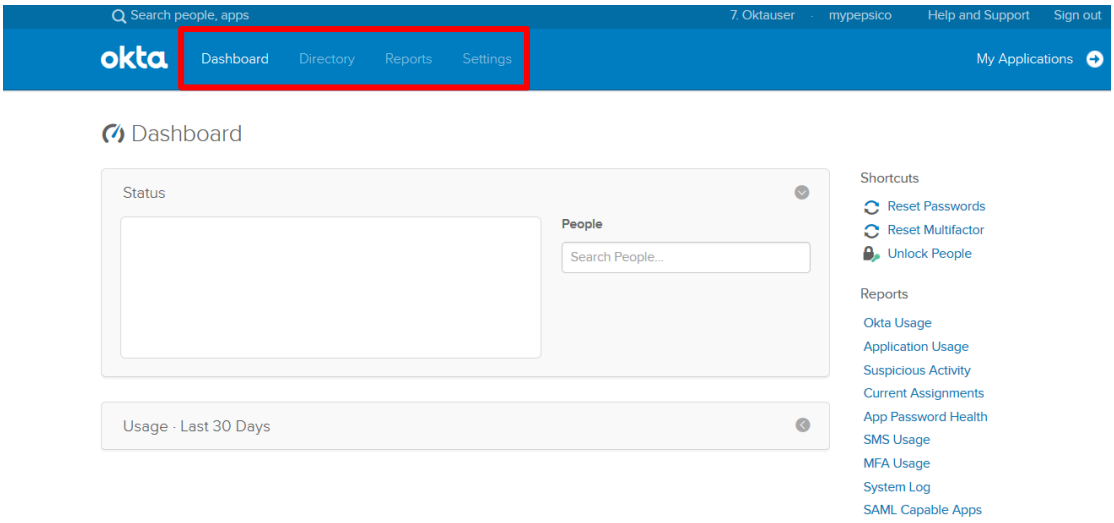
- Viewing user profiles – e.g. when users are unable to login because their account is locked or inactive
- Managing users – e.g. when users are unable to access their account and need to reset MFA
- Authentication troubleshooting – e.g. when users face issues logging in either on the username/password screen or MFA screen

2.1 Helpdesk Admin UI Overview

On the admin dashboard, helpdesk admins can see several shortcuts for common actions such as user administration and reports.

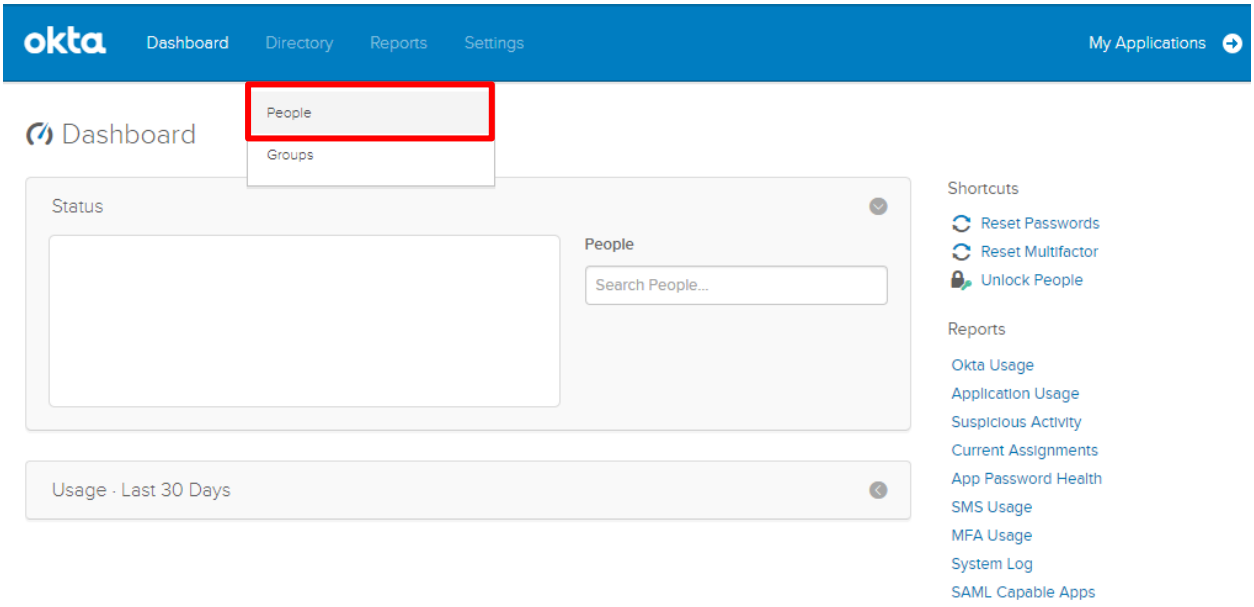


For other admin tasks, the ribbon at the top of the dashboard will be used.

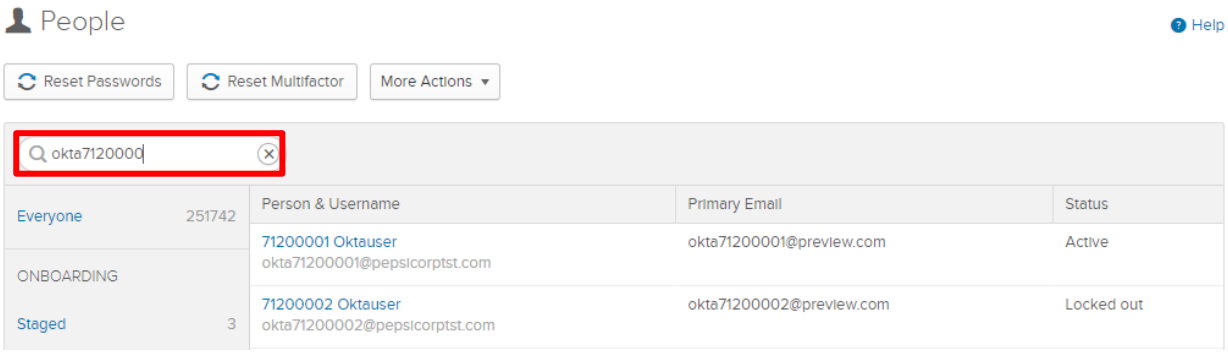


2.2 View User Profile

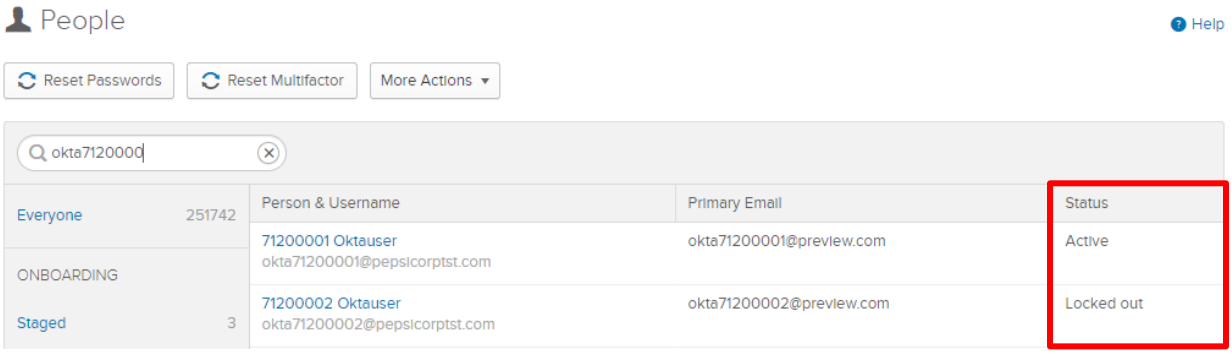
1. Helpdesk Admins can lookup a user's status by navigating to Directory > People



2. Search for the user's details (username, email, etc.)

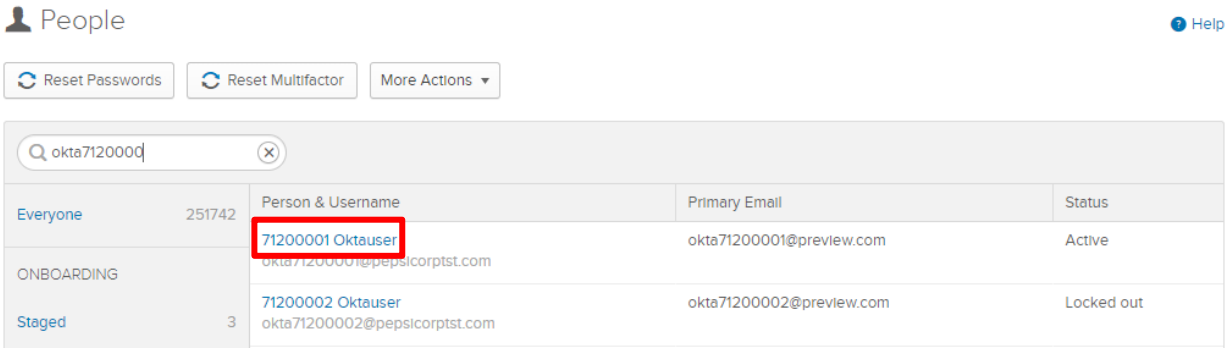


3. The status of the user is shown in the search results. The most common user statuses will be Active, Deactivated, Locked Out, or Password Expired.

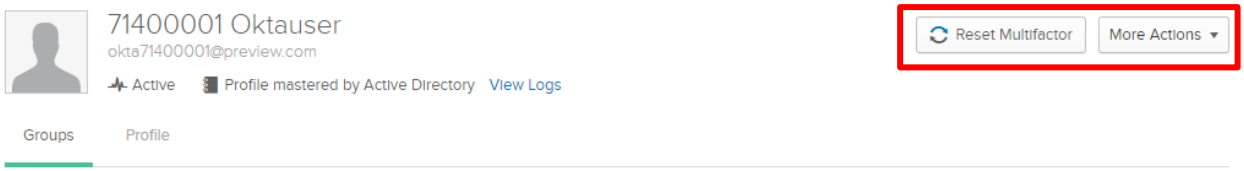


Note: IMPORTANT! Do NOT manage user lockouts through Associate SSO service (Okta). Lockouts will automatically timeout in 16 min.

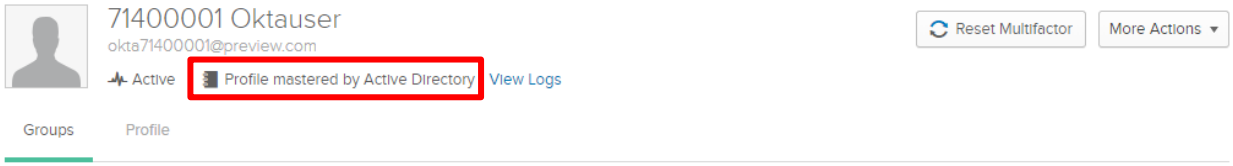
4. For further details about the user navigate to the user's account page by clicking on the user.



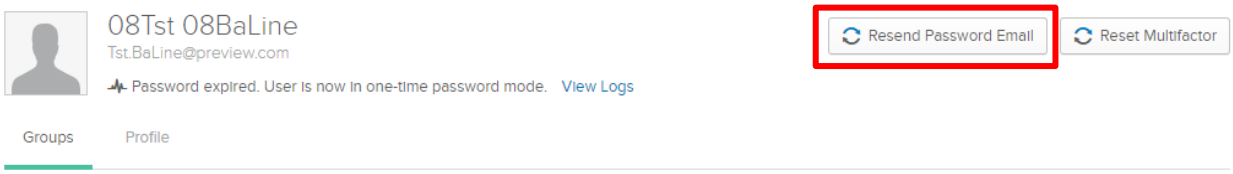
5. The available actions that can be taken on the user's account are shown on the top left.



6. The actions needed to be taken on the account may vary depending on how the account is mastered i.e. if user is AD or LDAP (IDX) mastered, action will need to be taken in AD or IDX and will reflect in Associate SSO service (Okta) during the next periodic import.

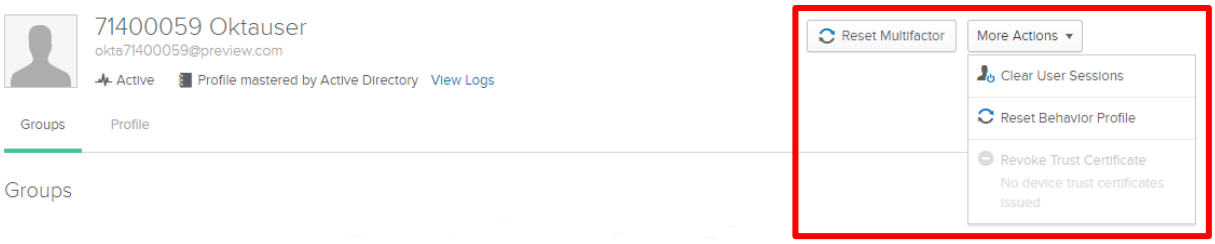


Note: Since the below user is created by Associate SSO service (Okta) and not Active Directory, "Resend Password Email" is shown. Most accounts are mastered by Active Directory and will not have this option.



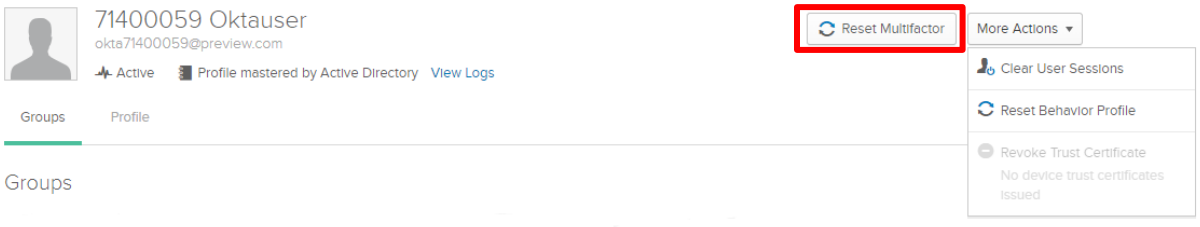
2.3 Manage Users

1. From a user's account page, admins can perform several user management tasks such as Reset Multifactor, Clear User Sessions, and Reset Behavior Profile.

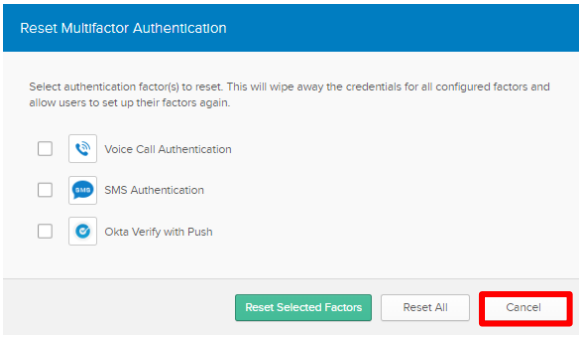


Reset Multifactor

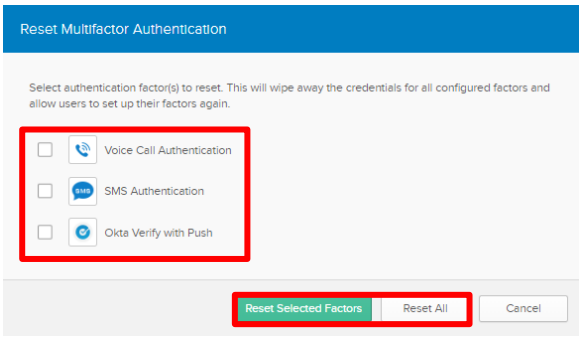
a. Before resetting a user's MFA configuration, validate the user using the existing Identity Verification method.
b. Click "Reset Multifactor" to open a pop-up containing a user's registered MFA choices (Voice call, SMS, and/or Okta Verify).



c. Helpdesk admins can click "Cancel" to leave the current MFA configurations as is.

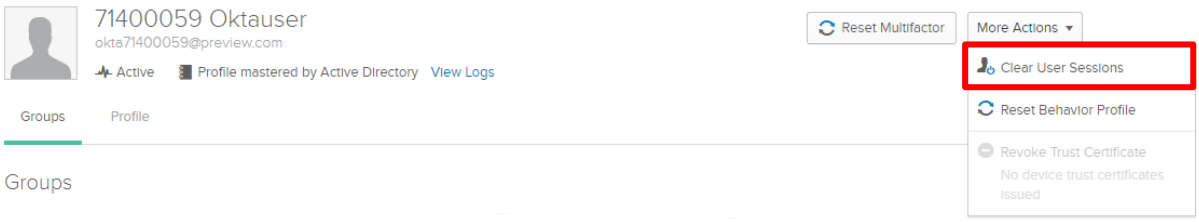


d. Helpdesk admins can also select specific factors to reset or reset all factors, forcing the user to re-register their MFA devices.



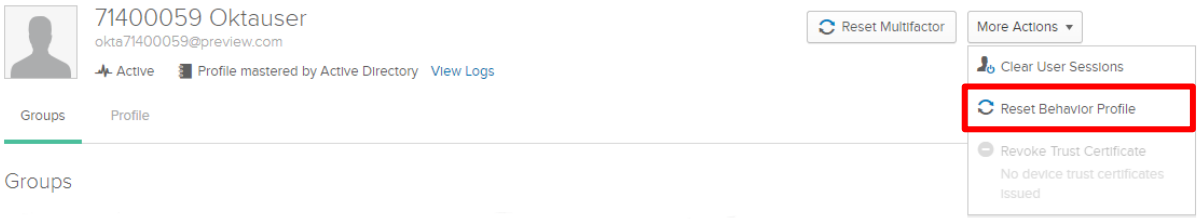
Clear User Sessions

a. Clicking “Clear User Sessions” will kill the user’s active sessions and force a re-login. **Note**: Desktop thick clients don’t force a re-login until they are signed out.



Reset Behavior Profile

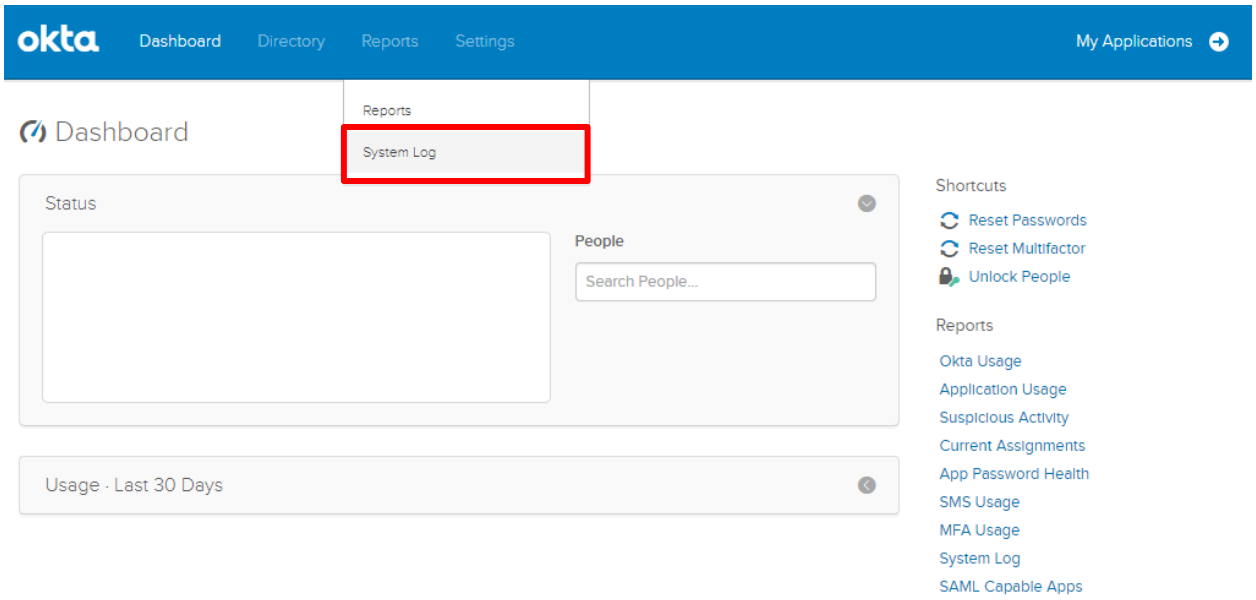
a. Clicking “Reset Behavior Profile will reset the behavior profile for a single end user and clear all tracked behavior history. However, new behavior will continue to be tracked.



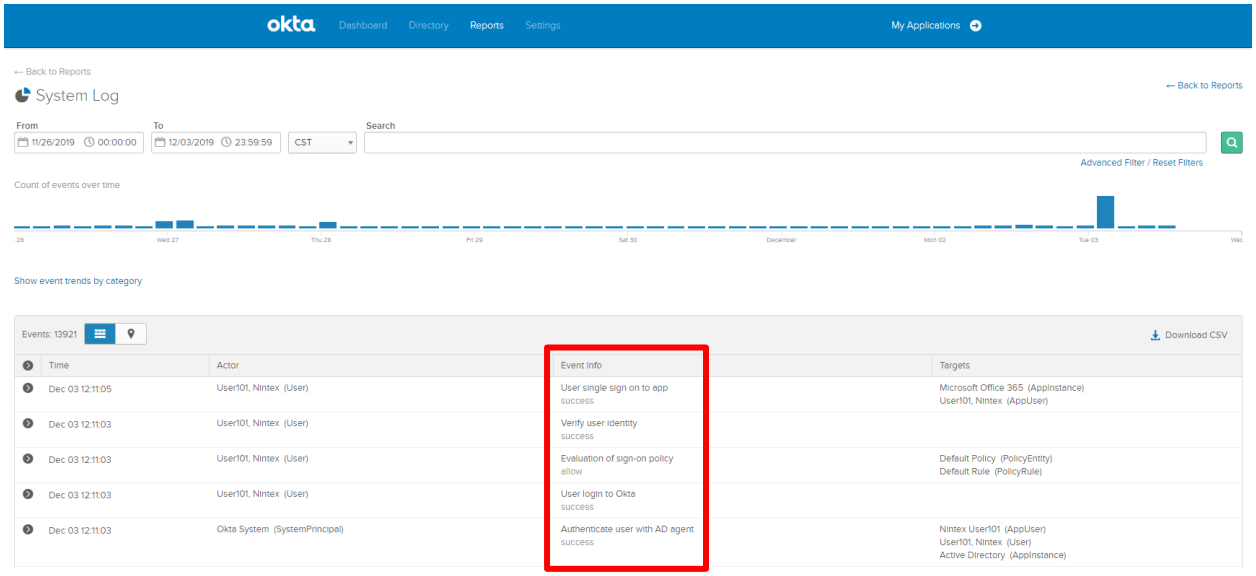
Note: It is important to note that editing profile attributes and password resets are not possible for Active Directory mastered or LDAP (IDX) mastered accounts.

2.4 Authentication Troubleshooting

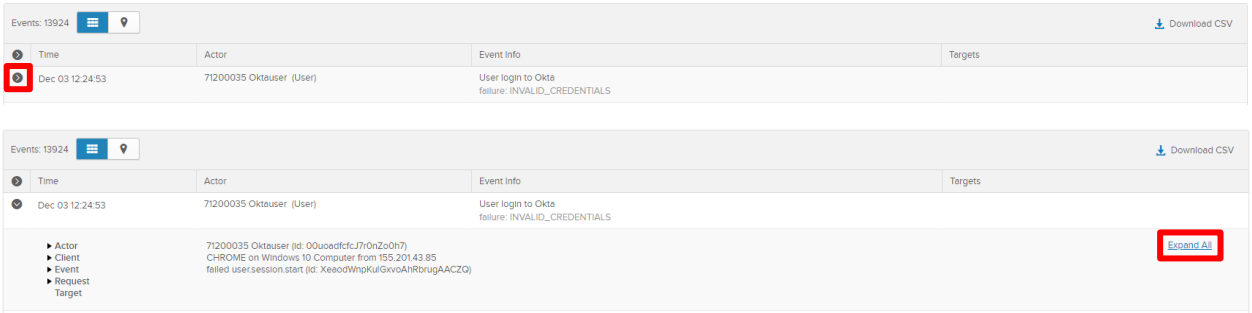
1. As an initial step for troubleshooting, have users try to login directly to secure.pepsico.com if they are having issues logging in to office.com. If users are able to access secure.pepsico.com but not office.com, this would indicate that Office 365 is experiencing issues.
2. All user related events are logged into System Logs. These can be viewed by navigating to Reports > System Log.



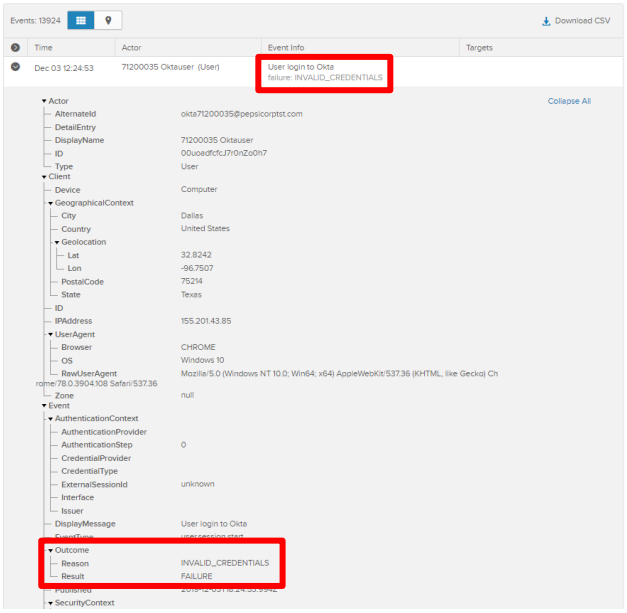
3. Here, Helpdesk admins can search user UPNs and see high level information about authentication failures. The Success, Failure, or Locked Out messages will be shown in the "Event Info"



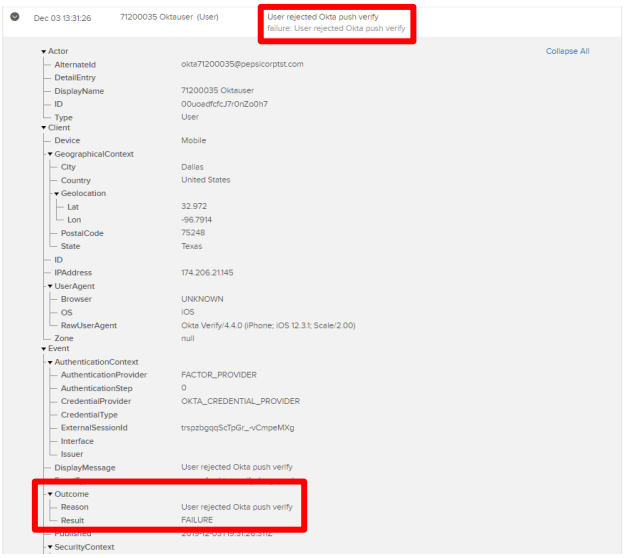
4. The “Expand all” link on the right side of each result can be used to see detailed information on the event.



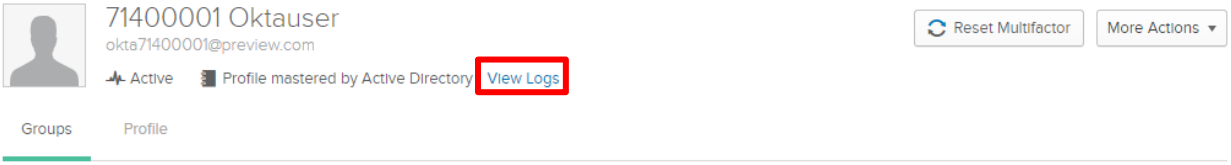
5. Invalid Credentials and Lockout are some of the most common scenarios for failed authentication.



6. MFA events are also logged into System Logs. Helpdesk admins can search user UPNs and see high level information on MFA verification attempts. The Success or Failure messages will be shown in the Event Info.



7. Logs for a specific user can also be accessed by clicking on “View Logs” from the user’s profile page.



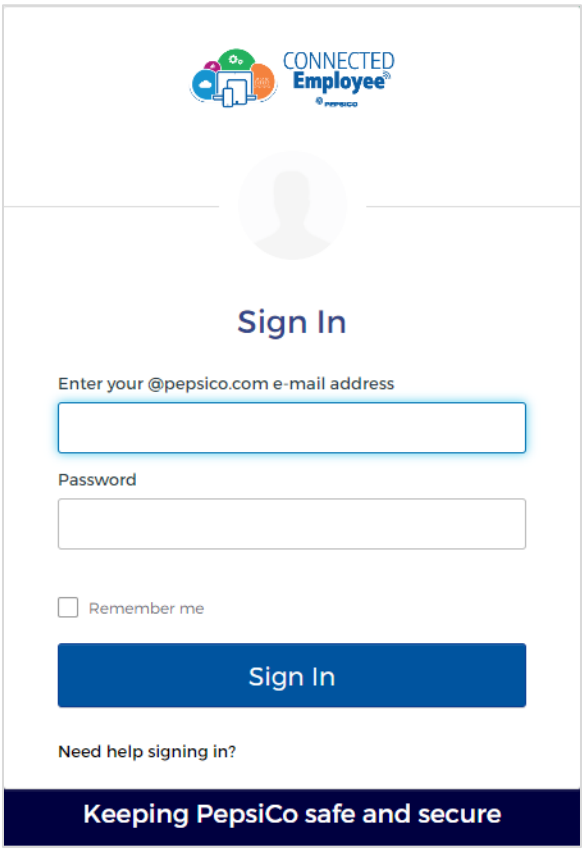
3 User Self Service

Occasionally users may require assistance with managing their accounts. Some of these activities include:

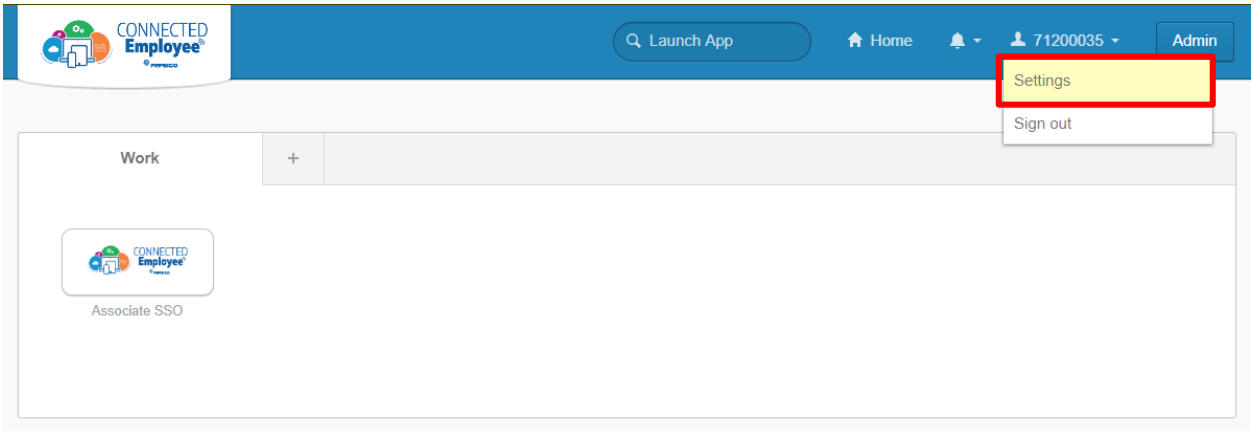
- Resetting or setting up new MFA devices on their account if they need add or remove devices from their current MFA configuration
- Resetting their password if they have forgotten it and are unable to login

3.1 MFA Reset or Setup

1. Login to secure.pepsico.com

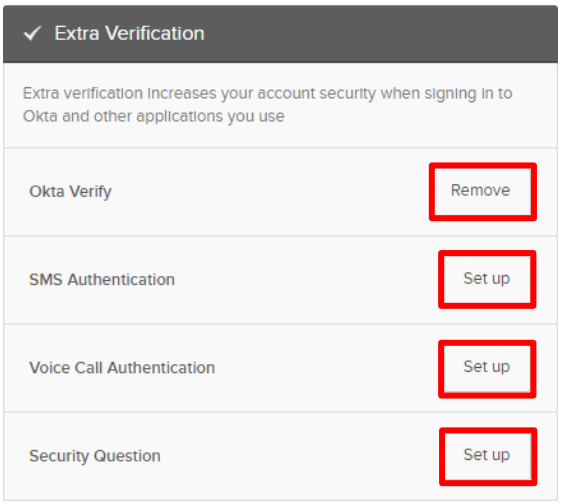


2. On the right side, navigate to [First Name/Last Name] > Settings



Note: The screenshot is showing a GPID because this is a test account. End users will see a first name/last name.

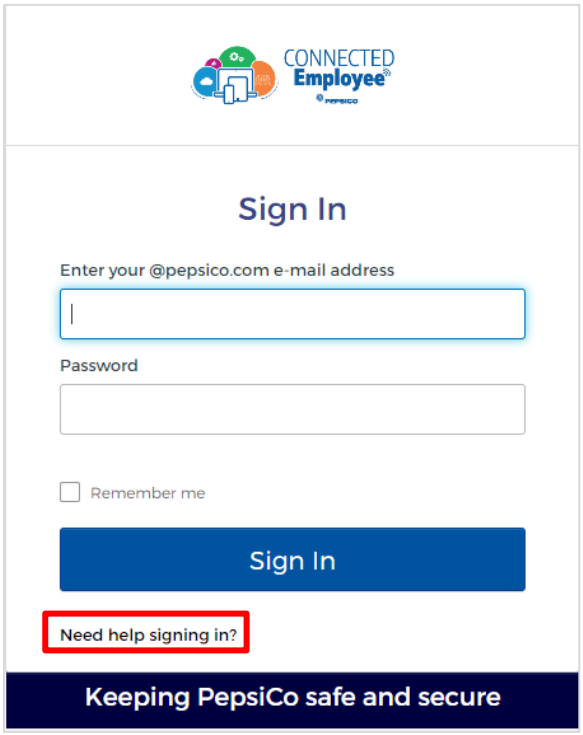
3. Scroll down to the "Extra Verification" section
4. Under "Extra Verification", users can remove and set up new MFA devices.



3.2 Password Resets

User password resets are not managed in Associate SSO service (Okta). If a user needs to reset their password, please direct them to myidM. This can be reached by

1. Clicking the “Need help signing in?” on the login screen at secure.pepsico.com.



2. Clicking “Forgot your password?”. This will redirect the user to myidM’s password reset page.