

**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



The screenshot shows the myidM login page. The navigation bar includes 'Home', 'Manage My Account', 'Manage Other Accounts', 'Request Access' (highlighted with a red box), 'Request SAP Access', and 'View Requests'. Below the navigation bar, there is a 'Welcome to PepsiCo Identity Manager' message and a list of links: 'Request New Access for Self', 'Modify/Disable Access for Self', 'Search by Request Number', 'View My Requests', and 'View Request for Others'. A 'Request Access' link is also visible in the navigation bar.

3. Click “Request New Access for Self”



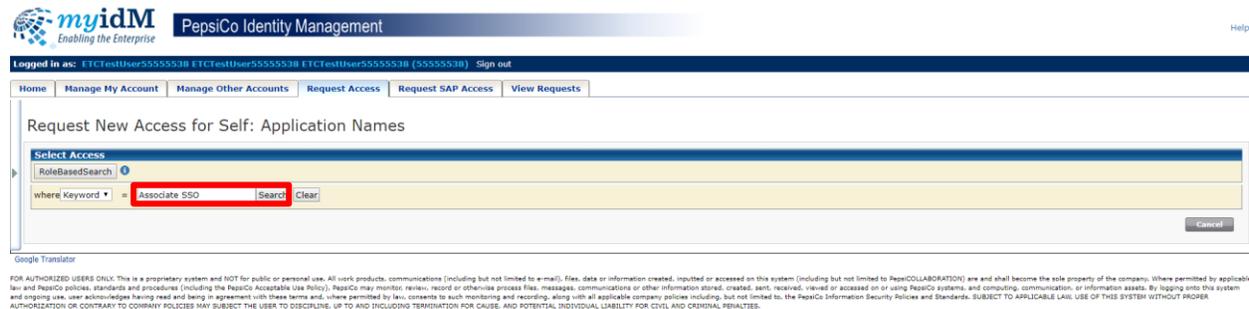
The screenshot shows the 'Request New Access for Self' page. The navigation bar includes 'Home', 'Manage My Account', 'Manage Other Accounts', 'Request Access' (highlighted with a red box), 'Request SAP Access', and 'View Requests'. Below the navigation bar, there is a 'Request New Access for Self' link (highlighted with a red box) and a list of links: 'Modify/Disable Access for Self', 'Search by Request Number', 'View My Requests', and 'View Request for Others'. A 'Request Access' link is also visible in the navigation bar.

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



The screenshot shows the 'Request New Access for Self: Application Names' page. The navigation bar includes 'Home', 'Manage My Account', 'Manage Other Accounts', 'Request Access' (highlighted with a red box), 'Request SAP Access', and 'View Requests'. Below the navigation bar, there is a table with columns 'Application Name', 'Description', and 'Request Status'. The table contains one row: 'AD Group Membership' with the description 'Add and remove non-privileged Active Directory groups.' Below the table, there is a 'Request New Access' link (highlighted with a red box) and 'Next' and 'Cancel' buttons.

5. Search for “Associate SSO”



The screenshot shows the search interface for 'Request New Access for Self: Application Names'. The navigation bar includes 'Home', 'Manage My Account', 'Manage Other Accounts', 'Request Access' (highlighted with a red box), 'Request SAP Access', and 'View Requests'. Below the navigation bar, there is a search box with the text 'Associate SSO' (highlighted with a red box) and a 'Search' button (highlighted with a red box). There is also a 'Clear' button and a 'Cancel' button.

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

myidM PepsiCo Identity Management

Logged in as: ETCTestUser5555538 ETCTestUser5555538 ETCTestUser5555538 (5555538) Sign out

Home Manage My Account Manage Other Accounts Request Access Request SAP Access View Requests

### Request New Access for Self: Application Names

Select Access

RoleBasedSearch

where Keyword = Search Clear

Select	Application Name	Description	Self Subscribing
<input checked="" type="checkbox"/>	Associate SSO Admin Portal	Access request for admin and help desk associates to gain access to Okta Admin Portal.	<input checked="" type="checkbox"/>

1-1 of 1

1-1 of 1

Select Cancel

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

myidM PepsiCo Identity Management

Logged in as: ETCTestUser5555538 ETCTestUser5555538 ETCTestUser5555538 (5555538) Sign out

Home Manage My Account Manage Other Accounts Request Access Request SAP Access View Requests

### Request New Access for Self: Application Names

Application Name	Description	Request Status
Associate SSO Admin Portal	Access request for admin and help desk associates to gain access to Okta Admin Portal.	

Basic Access - Computer Logon basic Access - Computer Logon provisions PepsiCo network access, email accounts, and PerSend access. For non-employees in CORP/VI (US and Canada), this is also for optional wireless access.

Request New Access

Next Cancel

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

myidM PepsiCo Identity Management

Logged in as: ETCTestUser5555538 ETCTestUser5555538 ETCTestUser5555538 (5555538) Sign out

Home Manage My Account Manage Other Accounts Request Access Request SAP Access View Requests

### Request New Access for Self

Associate SSO Admin Portal

#### Associate SSO Admin Portal

Role: \*

Search... Search...

Help Desk

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

**Associate SSO Admin Portal**

Role: \*

Search... Auditing / Reporting

Search... Help Desk

**Business Justification:**

Need access to perform helpdesk duties

Submit

Prev Cancel

Google Translate

FOR AUTHORIZED USERS ONLY. This is a proprietary system and NOT for public or personal use. All work products, communications (including but not limited to e-mail), files, data or information created, inputted or accessed on this system (including but not limited to PepsiCOLLABORATION) are and shall become the sole property of the company. Where permitted by applicable law and PepsiCo policies, standards and procedures (including the PepsiCo Acceptable Use Policy), PepsiCo may monitor, review, record or otherwise process files, messages, communications or other information stored, created, sent, received, viewed or accessed on or using PepsiCo systems, and computing, communication, or information assets. By logging onto this system and ongoing use, user acknowledges having read and being in agreement with these terms and, where permitted by law, consents to such monitoring and recording, along with all applicable company policies including, but not limited to, the PepsiCo Information Security Policies and Standards. SUBJECT TO APPLICABLE LAW, USE OF THIS SYSTEM WITHOUT PROPER AUTHORIZATION OR CONTRARY TO COMPANY POLICIES MAY SUBJECT THE USER TO DISCIPLINE, UP TO AND INCLUDING TERMINATION FOR CAUSE, AND POTENTIAL INDIVIDUAL LIABILITY FOR CIVIL AND CRIMINAL PENALTIES.

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.

**myidM** PepsiCo Identity Management

Help

Logged in as: ETCTestUser5555538 ETCTestUser5555538 ETCTestUser5555538 (5555538) Sign out

Home Manage My Account Manage Other Accounts Request Access Request SAP Access View Requests

Request New Access for Self  
Modify/Disable Access for Self  
Search by Request Number  
View My Requests  
View Request for Others

**Access Request Confirmation**

Your access request was successfully submitted.

The ticket number assigned to this request is **2852639**, please save this number to reference the request in the future.

Google Translate

FOR AUTHORIZED USERS ONLY. This is a proprietary system and NOT for public or personal use. All work products, communications (including but not limited to e-mail), files, data or information created, inputted or accessed on this system (including but not limited to PepsiCOLLABORATION) are and shall become the sole property of the company. Where permitted by applicable law and PepsiCo policies, standards and procedures (including the PepsiCo Acceptable Use Policy), PepsiCo may monitor, review, record or otherwise process files, messages, communications or other information stored, created, sent, received, viewed or accessed on or using PepsiCo systems, and computing, communication, or information assets. By logging onto this system and ongoing use, user acknowledges having read and being in agreement with these terms and, where permitted by law, consents to such monitoring and recording, along with all applicable company policies including, but not limited to, the PepsiCo Information Security Policies and Standards. SUBJECT TO APPLICABLE LAW, USE OF THIS SYSTEM WITHOUT PROPER AUTHORIZATION OR CONTRARY TO COMPANY POLICIES MAY SUBJECT THE USER TO DISCIPLINE, UP TO AND INCLUDING TERMINATION FOR CAUSE, AND POTENTIAL INDIVIDUAL LIABILITY FOR CIVIL AND CRIMINAL PENALTIES.

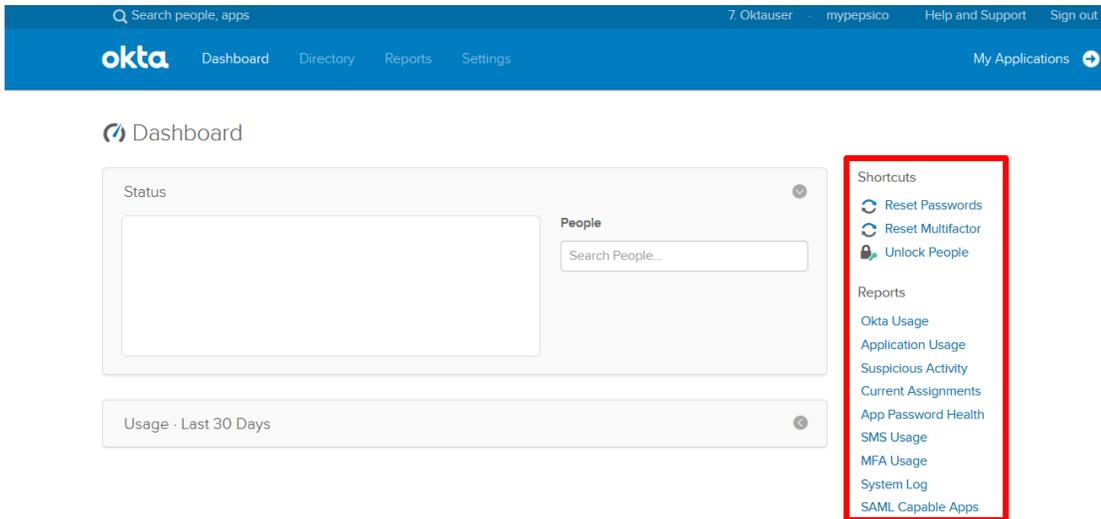
## 2 Associate SSO service (Okta) Helpdesk Workflows

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

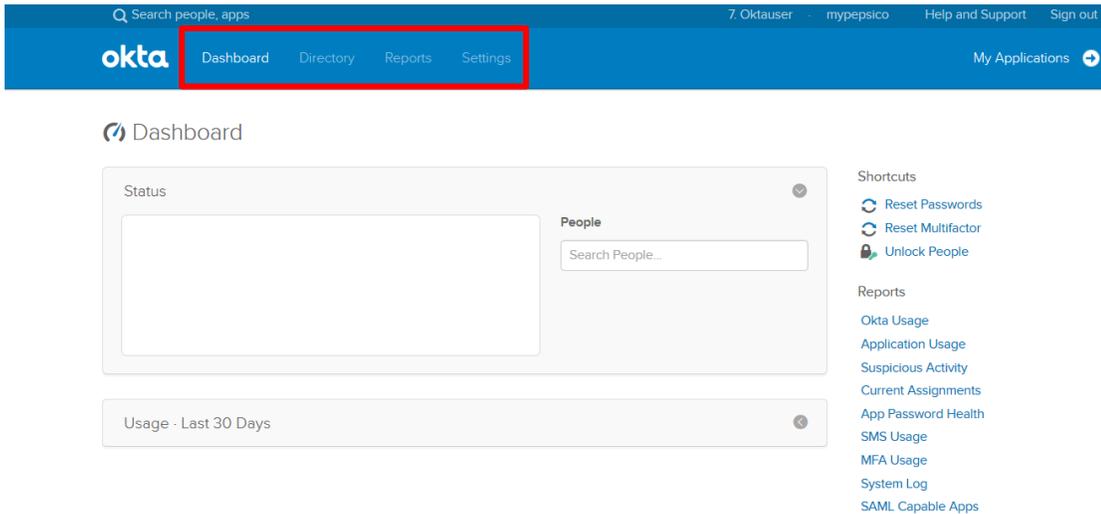
## 2.1 Helpdesk Admin UI Overview

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



The screenshot shows the Okta Admin Dashboard interface. At the top, there is a search bar for people and apps, and user information for '7. Oktauser' and 'mypepsico'. The main navigation ribbon includes 'Dashboard', 'Directory', 'Reports', and 'Settings'. The 'Dashboard' section is active, displaying a 'Status' card with a search box and a 'People' card with a 'Search People...' input. A 'Usage - Last 30 Days' card is also visible. On the right side, a 'Shortcuts' menu is highlighted with a red box, listing actions like 'Reset Passwords', 'Reset Multifactor', and 'Unlock People', as well as various reports such as 'Okta Usage', 'Application Usage', and 'Suspicious Activity'.

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



This screenshot is identical to the one above, but with a red box highlighting the navigation ribbon at the top of the dashboard. The ribbon contains the 'Okta' logo and the menu items 'Dashboard', 'Directory', 'Reports', and 'Settings'. The 'Dashboard' item is currently selected.

## 2.2 View User Profile

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

The screenshot shows the Okta dashboard with the navigation menu at the top. The 'People' option is highlighted with a red box. Below the navigation menu, there is a 'Status' section with a search bar labeled 'Search People...'. To the right, there are 'Shortcuts' and 'Reports' sections. The 'Shortcuts' section includes 'Reset Passwords', 'Reset Multifactor', and 'Unlock People'. The 'Reports' section includes 'Okta Usage', 'Application Usage', 'Suspicious Activity', 'Current Assignments', 'App Password Health', 'SMS Usage', 'MFA Usage', 'System Log', and 'SAML Capable Apps'.

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

The screenshot shows the 'People' page with a search bar containing 'okta7120001'. Below the search bar, there are buttons for 'Reset Passwords', 'Reset Multifactor', and 'More Actions'. The search results are displayed in a table with columns for 'Person & Username', 'Primary Email', and 'Status'. The first row shows a user with ID 71200001, username 'Oktauser', email 'okta71200001@preview.com', and status 'Active'. The second row shows a user with ID 71200002, username 'Oktauser', email 'okta71200002@preview.com', and status 'Locked out'.

Person & Username	Primary Email	Status
71200001 Oktauser okta71200001@pepsicorptst.com	okta71200001@preview.com	Active
71200002 Oktauser okta71200002@pepsicorptst.com	okta71200002@preview.com	Locked out

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.

The screenshot shows the 'People' page with a search bar containing 'okta7120001'. Below the search bar, there are buttons for 'Reset Passwords', 'Reset Multifactor', and 'More Actions'. The search results are displayed in a table with columns for 'Person & Username', 'Primary Email', and 'Status'. The first row shows a user with ID 71200001, username 'Oktauser', email 'okta71200001@preview.com', and status 'Active'. The second row shows a user with ID 71200002, username 'Oktauser', email 'okta71200002@preview.com', and status 'Locked out'. The 'Status' column is highlighted with a red box.

Person & Username	Primary Email	Status
71200001 Oktauser okta71200001@pepsicorptst.com	okta71200001@preview.com	Active
71200002 Oktauser okta71200002@pepsicorptst.com	okta71200002@preview.com	Locked out

**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.

People Help

Reset Passwords Reset Multifactor More Actions

Everyone	251742	Person & Username	Primary Email	Status
		71200001 Oktauser	okta71200001@preview.com	Active
ONBOARDING		okta71200001@pepsicorptst.com		
Staged	3	71200002 Oktauser	okta71200002@preview.com	Locked out
		okta71200002@pepsicorptst.com		

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

71400001 Oktauser  
okta71400001@preview.com

Active Profile mastered by Active Directory View Logs

Reset Multifactor More Actions

Groups Profile

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.

71400001 Oktauser  
okta71400001@preview.com

Active Profile mastered by Active Directory View Logs

Reset Multifactor More Actions

Groups Profile

**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.

08Tst 08BaLine  
Tst.BaLine@preview.com

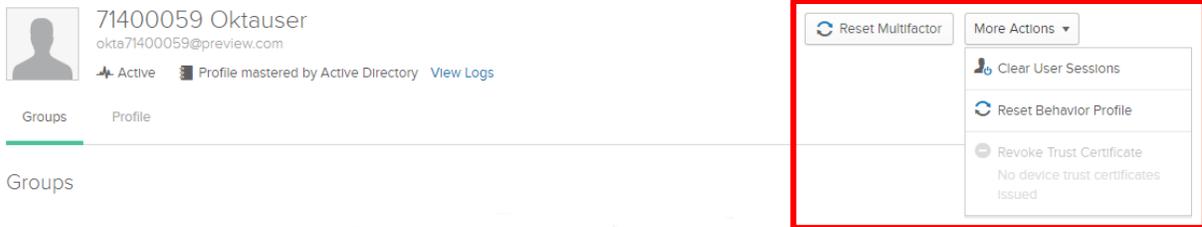
Password expired. User is now In one-time password mode. View Logs

Resend Password Email Reset Multifactor

Groups Profile

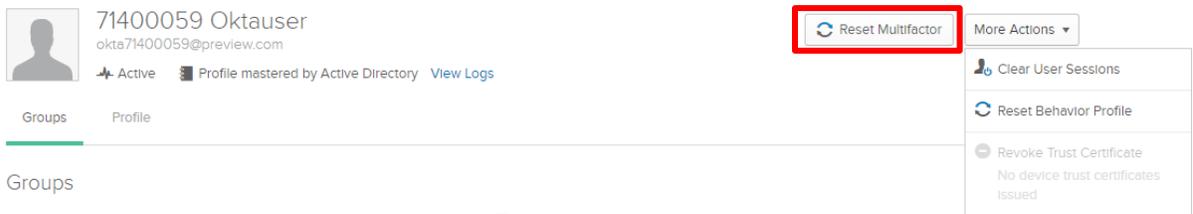
## 2.3 Manage Users

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.

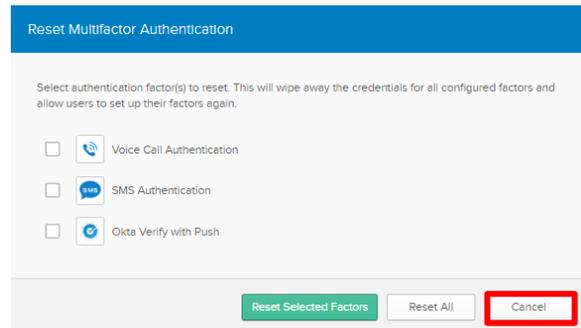


### Reset Multifactor

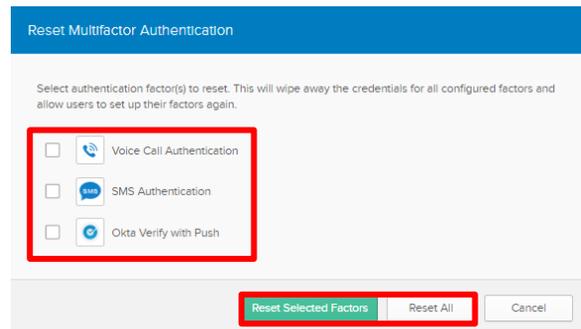
- a. Before resetting a user's MFA configuration, validate the user using the existing Identity Verification method.
- b. Click "Reset Multifactor" to open a pop-up containing a user's registered MFA choices (Voice call, SMS, and/or Okta Verify).



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



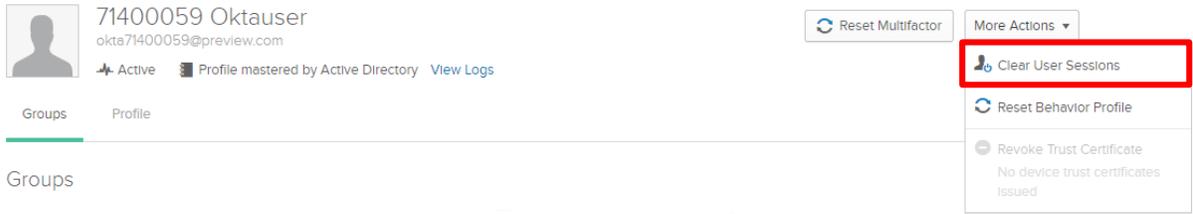
- d. Helpdesk admins can also select specific factors to reset or reset all factors, forcing the user to re-register their MFA devices.



## Clear User Sessions

- a. Clicking “Clear User Sessions” will kill the user’s active sessions and force a re-login.

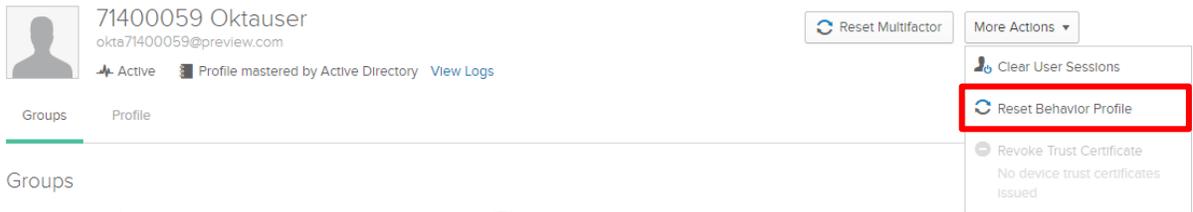
**Note:** Desktop thick clients don’t force a re-login until they are signed out.



The screenshot shows the user profile for '71400059 Oktauser' (okta71400059@preview.com). The user is 'Active' and has a 'Profile mastered by Active Directory'. A 'Reset Multifactor' button is visible. The 'More Actions' dropdown menu is open, showing options: 'Clear User Sessions' (highlighted with a red box), 'Reset Behavior Profile', and 'Revoke Trust Certificate' (with a note: 'No device trust certificates issued').

## 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.

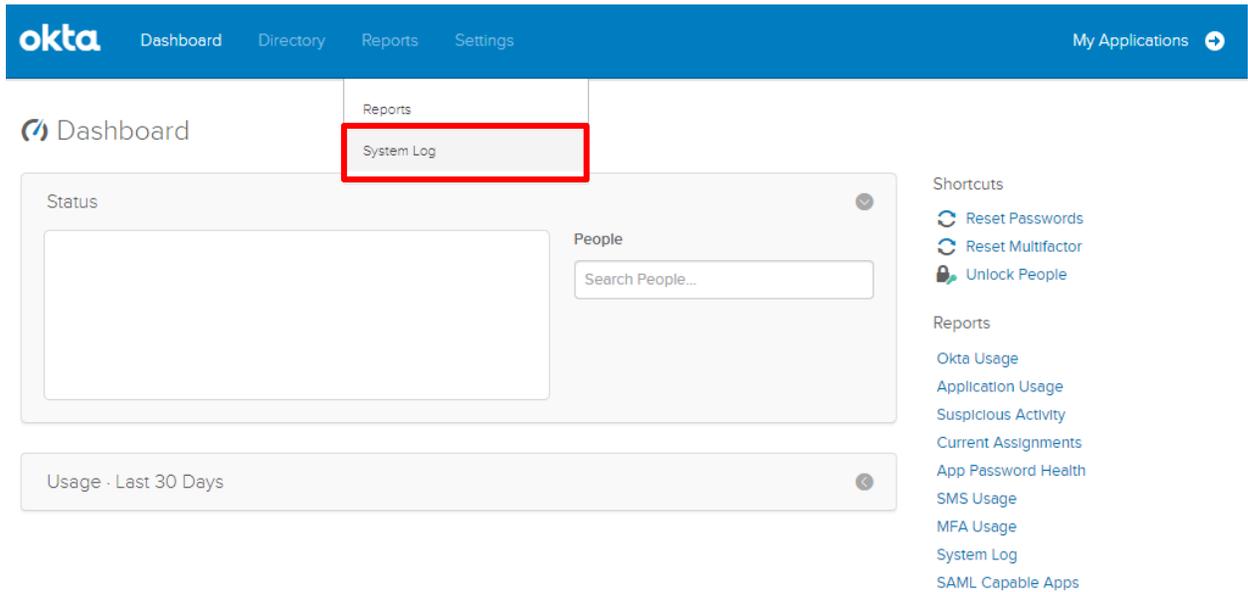


The screenshot shows the user profile for '71400059 Oktauser' (okta71400059@preview.com). The user is 'Active' and has a 'Profile mastered by Active Directory'. A 'Reset Multifactor' button is visible. The 'More Actions' dropdown menu is open, showing options: 'Clear User Sessions', 'Reset Behavior Profile' (highlighted with a red box), and 'Revoke Trust Certificate' (with a note: 'No device trust certificates issued').

**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.

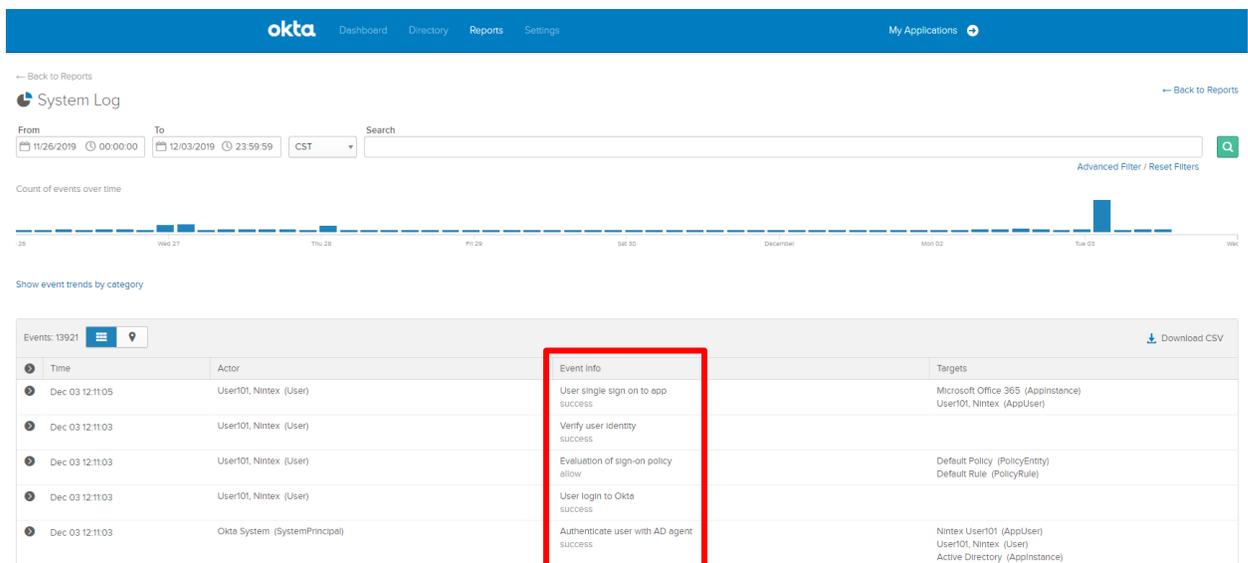
## 2.4 Authentication Troubleshooting

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.



The screenshot shows the Okta dashboard interface. At the top, there is a navigation bar with the Okta logo and links for Dashboard, Directory, Reports, and Settings. On the right side of the navigation bar, there is a 'My Applications' link with a dropdown arrow. Below the navigation bar, the main content area is titled 'Dashboard'. A dropdown menu is open under the 'Reports' link, and 'System Log' is highlighted with a red rectangular box. To the right of the main content area, there is a 'Shortcuts' section with links for 'Reset Passwords', 'Reset Multifactor', and 'Unlock People'. Below that is a 'Reports' section with links for 'Okta Usage', 'Application Usage', 'Suspicious Activity', 'Current Assignments', 'App Password Health', 'SMS Usage', 'MFA Usage', 'System Log', and 'SAML Capable Apps'. The main content area also features a 'Status' section with a search box for 'People' and a 'Usage - Last 30 Days' section.

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”



The screenshot shows the Okta System Log interface. At the top, there is a navigation bar with the Okta logo and links for Dashboard, Directory, Reports, and Settings. On the right side of the navigation bar, there is a 'My Applications' link with a dropdown arrow. Below the navigation bar, the main content area is titled 'System Log'. There is a search bar with 'From' and 'To' date pickers, a 'Search' field, and a 'Search' button. Below the search bar, there is a 'Count of events over time' chart showing a bar for Dec 03. Below the chart, there is a 'Show event trends by category' section. At the bottom, there is a table of events with 13921 events. The table has columns for Time, Actor, Event Info, and Targets. The 'Event Info' column is highlighted with a red rectangular box. The table shows several events with success messages.

Time	Actor	Event Info	Targets
Dec 03 12:11:05	User101, Nintex (User)	User single sign on to app success	Microsoft Office 365 (AppInstance) User101, Nintex (AppUser)
Dec 03 12:11:03	User101, Nintex (User)	Verify user identity success	
Dec 03 12:11:03	User101, Nintex (User)	Evaluation of sign-on policy allow	Default Policy (PolicyEntry) Default Rule (PolicyRule)
Dec 03 12:11:03	User101, Nintex (User)	User login to Okta success	
Dec 03 12:11:03	Okta System (SystemPrincipal)	Authenticate user with AD agent success	Nintex User101 (AppUser) User101, Nintex (User) Active Directory (AppInstance)

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

Events: 13924 Download CSV

Time	Actor	Event Info	Targets
Dec 03 12:24:53	71200035 Oktauser (User)	User login to Okta failure: INVALID_CREDENTIALS	

Events: 13924 Download CSV

▶ Actor: 71200035 Oktauser (id: 00u0edfcf770nZo0h7)  
 ▶ Client: CHROME on Windows 10 Computer from 195.201.43.85  
 ▶ Event: failed user.session.start (id: XeeodWnpkuGvvoAhrbrugAACZQ)  
 ▶ Request  
 ▶ Target

[Expand All](#)

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

Events: 13924 Download CSV

Time	Actor	Event Info	Targets
Dec 03 12:24:53	71200035 Oktauser (User)	User login to Okta failure: INVALID_CREDENTIALS	

▶ Actor: okta71200035@pepsicorpst.com  
 ▶ DetailEntry  
 ▶ DisplayName: 71200035 Oktauser  
 ▶ ID: 00u0edfcf770nZo0h7  
 ▶ Type: User  
 ▶ Client: Computer  
 ▶ Device: Computer  
 ▶ GeographicalContext: Dallas, United States  
 ▶ Geolocation: 32.8242, -96.7507, 75214, Texas  
 ▶ IPAddress: 195.201.43.85  
 ▶ UserAgent: CHROME, Windows 10  
 ▶ RawUserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3904.108 Safari/537.36  
 ▶ Event: AuthenticationContext, AuthenticationProvider, AuthenticationStep: 0, CredentialProvider, CredentialType, ExternalSessionId: unknown, Interface, Issuer, DisplayMessage: User login to Okta  
 ▶ Outcome: Reason: INVALID\_CREDENTIALS, Result: FAILURE  
 ▶ Published: 2019-12-03 12:24:53  
 ▶ SecurityContext

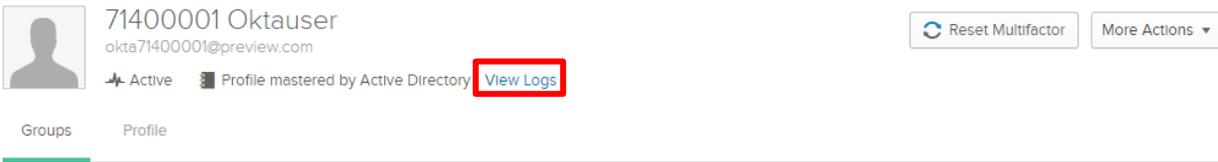
- MFA events are also logged into System Logs. Helpdesk admins can search user UPNs and see high level information on MFA verification attempts. The Success or Failure messages will be shown in the Event Info.

Events: 13924 Download CSV

Time	Actor	Event Info	Targets
Dec 03 13:31:26	71200035 Oktauser (User)	User rejected Okta push verify failure: User rejected Okta push verify	

▶ Actor: okta71200035@pepsicorpst.com  
 ▶ DetailEntry  
 ▶ DisplayName: 71200035 Oktauser  
 ▶ ID: 00u0edfcf770nZo0h7  
 ▶ Type: User  
 ▶ Client: Mobile  
 ▶ Device: Mobile  
 ▶ GeographicalContext: Dallas, United States  
 ▶ Geolocation: 32.972, -96.7994, 75248, Texas  
 ▶ IPAddress: 174.206.2145  
 ▶ UserAgent: UNKNOWN, iOS  
 ▶ RawUserAgent: Okta Verify/4.4.0 (iPhone; iOS 12.31; Scale/2.00)  
 ▶ Event: AuthenticationContext, AuthenticationProvider: FACTOR\_PROVIDER, AuthenticationStep: 0, CredentialProvider: OKTA\_CREDENTIAL\_PROVIDER, CredentialType, ExternalSessionId: trspzggq5c1p0r\_vCmpeMKg, Interface, Issuer, DisplayMessage: User rejected Okta push verify  
 ▶ Outcome: Reason: User rejected Okta push verify, Result: FAILURE  
 ▶ Published: 2019-12-03 13:31:26  
 ▶ SecurityContext

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



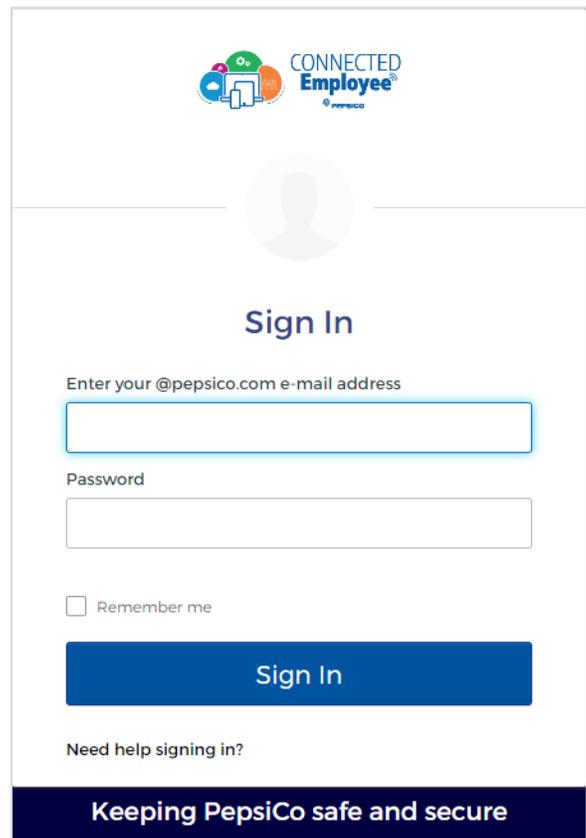
### 3 User Self Service

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

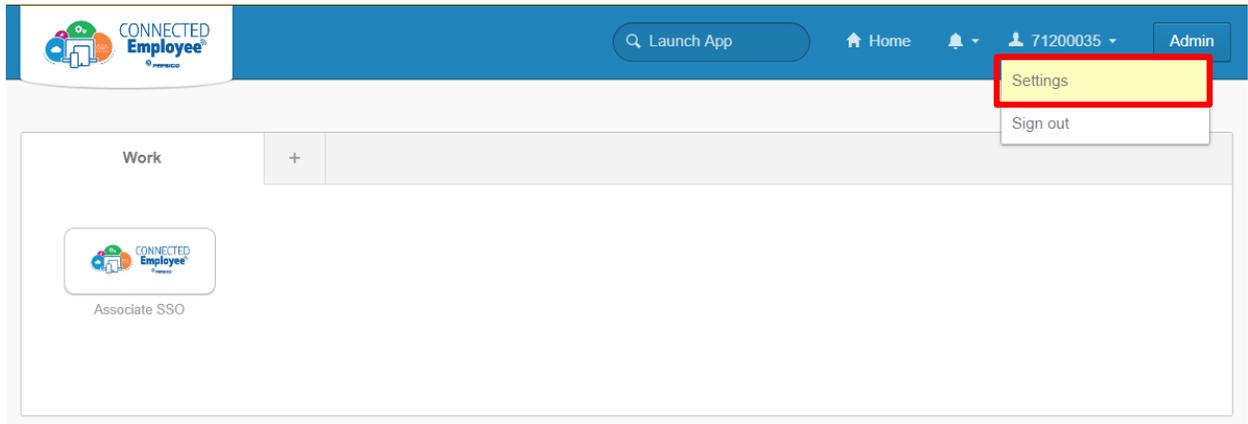
- Resetting or setting up new MFA devices on their account if they need add or remove devices from their current MFA configuration
- Resetting their password if they have forgotten it and are unable to login

#### 3.1 MFA Reset or Setup

1. Login to secure.pepsico.com

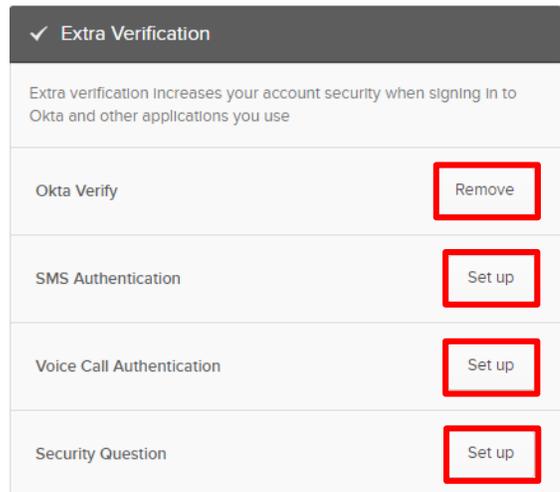


2. On the right side, navigate to [First Name/Last Name] > Settings



**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.

CONNECTED Employee  
pepsico

## Sign In

Enter your @pepsico.com e-mail address

Password

Remember me

Sign In

Need help signing in?

Keeping PepsiCo safe and secure

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

CONNECTED Employee  
pepsico

## Sign In

Enter your @pepsico.com e-mail address

Password

Remember me

Sign In

Need help signing in?

Forgot your password? First time user? | Login Help

Keeping PepsiCo safe and secure