CareManager Multi-Factor Authentication

Rollout & Training Guide

Prepared by

Nicki Grose

Netsmart

www.ntst.com

4950 College Boulevard
Overland Park, KS 66211
800.842.1973

Table of Contents

Overview

In order to improve security and ensure that users have proper access to CareManager, Netsmart is implementing Multi-factor authentication (MFA). Multi-factor authentication is an authentication method in which a computer user's identity is confirmed by successfully presenting two or more pieces of evidence (or factors) to an authentication protocol before access is granted access.

CareManager's offering for Multi-factor authentication will use **Okta**, a third-party authentication application, to manage user's identities and perform the two factor authentication process. The authentication process at login will also require users to have a the **Okta Verify** app downloaded their smartphone. This document will outline the Netsmart's roll-out plan and required steps to make this roll-out a success. It will also include a user training guide.

As part of Netsmart's MFA solution, Netsmart will be merging user accounts for those users who work for multiple NY Health Homes. This will allow staff working for multiple health homes to have a single login that will be used across all tenants (health homes). Users will be prompted to select the applicable tenant during the login process. This will make the login process easier for end users as they will only need to have one Username and Password for CareManager.

The implementation of the multi-tenant login and MFA solution will require coordination with Netsmart and your organization. The MFA solution will be turned on for all NY Health Homes on **April 20, 2020**. To ensure your end users are not impacted by this roll-out, your organization will need to adhere to deadlines outlined in the roll-out plan.

MFA Roll-out Plan

Below is the timeline for the release and roll-out of the login changes and MFA enhancements. There is required preparation on behalf of your organization to make this roll-out successful. ***Missing the dates for the "Client" deliverables may impact your organization's ability to test the changes in UAT and go live without user impact on April 20th.***

Due Date	Task Description	Responsibility
March 9	Communicate roll-out plan and user accounts to clients.	Netsmart
March 16	Confirm domain list.	**Client**
March 20	Deadline for clients to respond with confirmed user accounts.	**Client**
March 25	Complete review of user accounts and deliver lists to engineering.	Netsmart
March 25	Send Netsmart a list of users from your Health Home and each CMA that will be testing the changes in UAT.	**Client**

Due Date	Task Description	Responsibility
March 27	Create scripts to merge user accounts.	Netsmart
March 30	Release CareManager enhancements to UAT, run user account merge scripts, and send email to provision user accounts identified for UAT testing.	Netsmart
April 4	Organizations must conduct their accounting provisioning and MFA testing in UAT starting **March 31st** and have it completed by **April 4th**.	Netsmart
April 6	Release CareManager enhancements to PROD, run user account merge scripts, and provision all users. ***NOTE: At this point, the multi-tenant login enhancements will take effect. All users will also need a valid email address to log into their account and to receive user account provision email.***	Netsmart
April 6	Emails will be sent to all user accounts to prompt users to provision their accounts for authentication.	Netsmart
April 19	Users must complete the account provision process, which will provision users to Netsmart's centralized authentication platform.	Client
April 20	Turn on MFA for NY Health Homes. ***Note: All users will use the new accounts created. Old passwords will not work any longer.***	Netsmart

User Account Verification

For the multi-tenant login enhancement, all users must have a valid and accessible email address that will used across all configured organizations. In the past, if a user had access to multiple organizations, the first configured organization would have a real, valid email address, and any other organizations would use "fake" email address. Before Netsmart releases these updates, NY Health Homes will need review all user accounts across all CMA's to provide the valid, accessible email address for each user. Netsmart will be merging the duplicative user accounts into one account that will use the valid email address.

Netsmart will provide your organization with a list of all ACTIVE user accounts currently associated with your Health Home. Your organization will need to verify the following for each account in the list:

- The user is still active. With the implementation of MFA, all active users will receive an email for the provisioning process. Netsmart needs to ensure that only TRUE active users are sent this email.
- the email address for every active account across all your Health Home and CMAs is a valid, accessible email

The list will contain the staff name and email address being used for your tenant. If the user also works for another Health Home agency and has an active CareManager account, you will need to pay close attention to the email address listed. It will be your responsibility to confirm the correct email address that should be used across all accounts. Your organization's spreadsheet will contain two tabs. One is for Health Home only users that are not associated with a CMA and the others will be users that are associated to a CMA. Below is the approach to take for this verification process.

1. Health Users tab
    a. Review every user account in this tab and verify the user is still active.
        i. Enter 'Y' or 'N' in the Deactivate Account column for each user. Netsmart will automatically deactivate each account set to 'Y' in the spreadsheet.
    b. Review ever user account's email in this tab and enter the valid email address in the 'Valid Email Address for User' column, if the username listed in the spreadsheet is not correct/valid email.

       Note: When Netsmart was generating the list of active accounts, there were instances where it appeared that a staff member had two accounts and one username had an email address with a HHUNY domain name and the other had and CHHUNY domain name. In this instance, your organization needs to confirm which username/email address is the valid and should be used going forward for this staff member.

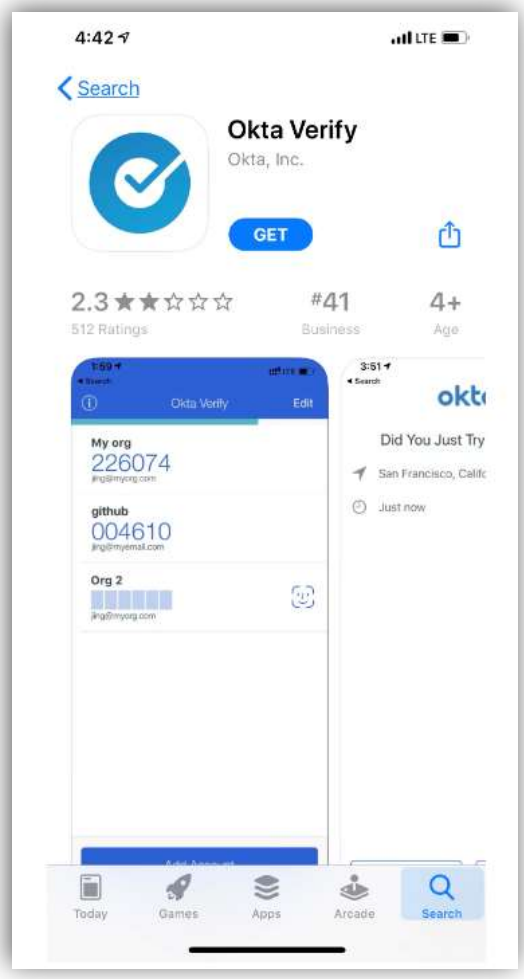
2. CMA Users tab
    a. The CMA must review every user account in this tab and verify the user is still active.
        i. Enter 'Y' or 'N' in the Deactivate Account column for each user. Netsmart will automatically deactivate each account set to 'Y' in the spreadsheet.
    b. The CMA must review ever user account's email in this tab and enter the valid email address in the 'Valid Email Address for User' column, if the username listed in the spreadsheet is not correct/valid email.

       Note: When Netsmart was generating the list of active accounts, there were instances where it appeared that a CMA staff member had multiple accounts across multiple Health Homes. For example, one username had an email address with the CMAs domain and looks correct. Others had the Health Home initials appended to the front of the email or had a Health Home domain name. In this instance, the CMA will need to confirm which username/email address is the valid and should be used going forward for this staff member.

User Guide

For the multi-factor authentication process in CareManager, users will be able to choose from using entering a code received in a text message sent to their mobile phone or a generated code in the **Okta Verify** mobile app. If users choose to use the **Okta Verify** mobile app, they will need to download the app to their smartphone from **Google Play** or the **Apple Store** prior to starting the Okta Account Setup process. Below is a screenshot of the app that needs to be downloaded.

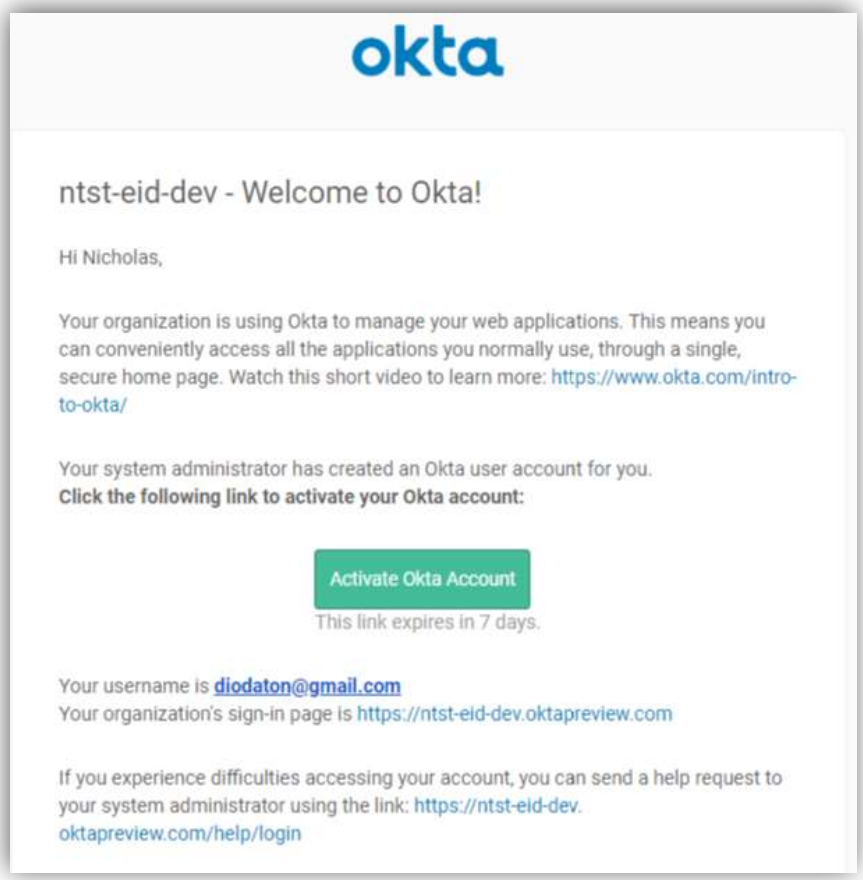
For users that may have limited mobile service, it's recommended to use the Okta Verify app. This app does not require mobile service or internet connection.



Okta Account Setup

When Netsmart releases the MFA solution to Production on **April 6th**, all users will receive the following email to provision their account in **Okta**. Emails will be sent to the confirmed email address provided by Health Homes. Users will only have **ONE** user account across all health home organizations in which they are associated and the new login process after account setup will allow for the user to select the health home that they want to log into.

1. Users will click the '**Activate Okta Account**' button on the email to start the account setup.


okta

ntst-eid-dev - Welcome to Okta!

Hi Nicholas,

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

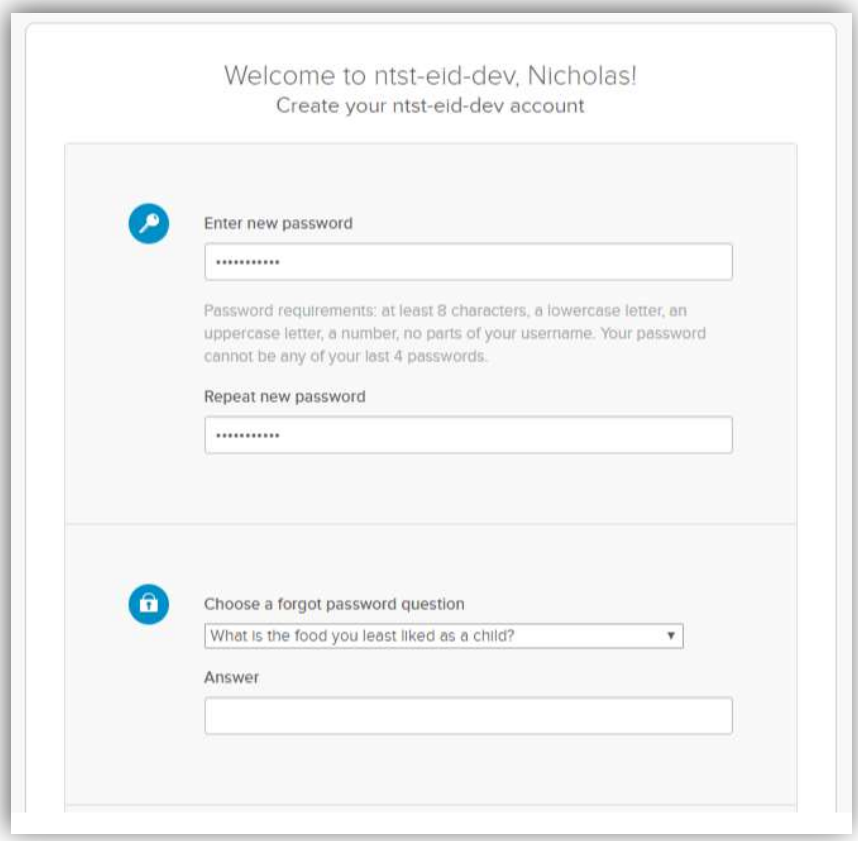
This link expires in 7 days.

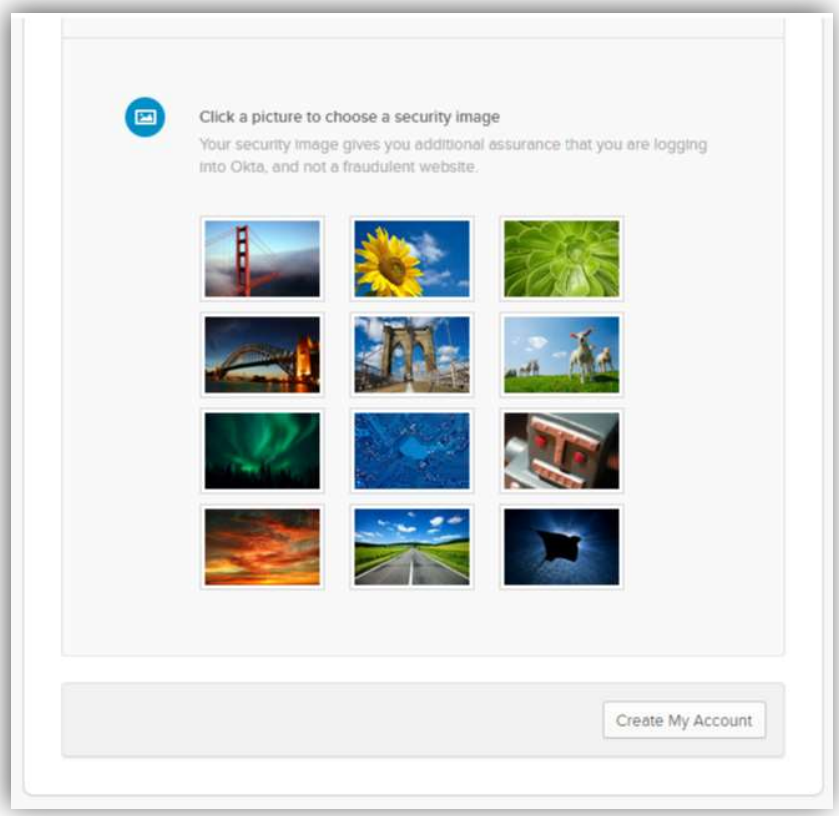
Your username is diodaton@gmail.com
Your organization's sign-in page is https://ntst-eid-dev.oktapreview.com

If you experience difficulties accessing your account, you can send a help request to your system administrator using the link: https://ntst-eid-dev.oktapreview.com/help/login

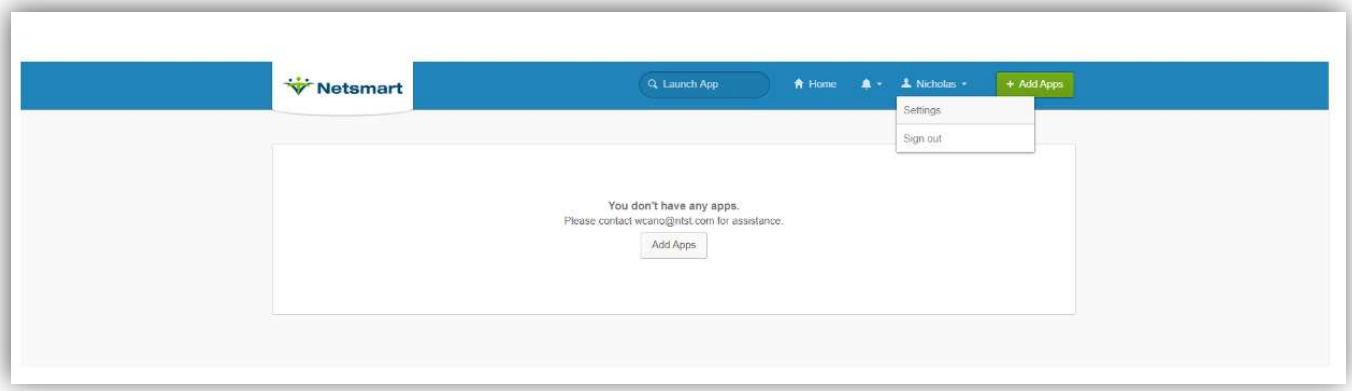
Users will be prompted to enter a new password at this time. They will also need to set up a security question and answer that can be used when resetting their password. They will then select a picture to choose as a security image. This will be displayed on the login screen after the initial setup the first time the user logs into CareManager.

2. Users will click on the **'Create My Account'** button at the bottom of the page to complete the account setup.


Welcome to ntst-eid-dev, Nicholas!
Create your ntst-eid-dev account
Enter new password
Password requirements: at least 8 characters, a lowercase letter, an uppercase letter, a number, no parts of your username. Your password cannot be any of your last 4 passwords.
Repeat new password
Choose a forgot password question
What is the food you least liked as a child?
Answer


Click a picture to choose a security image
Your security image gives you additional assurance that you are logging into Okta, and not a fraudulent website.
Create My Account

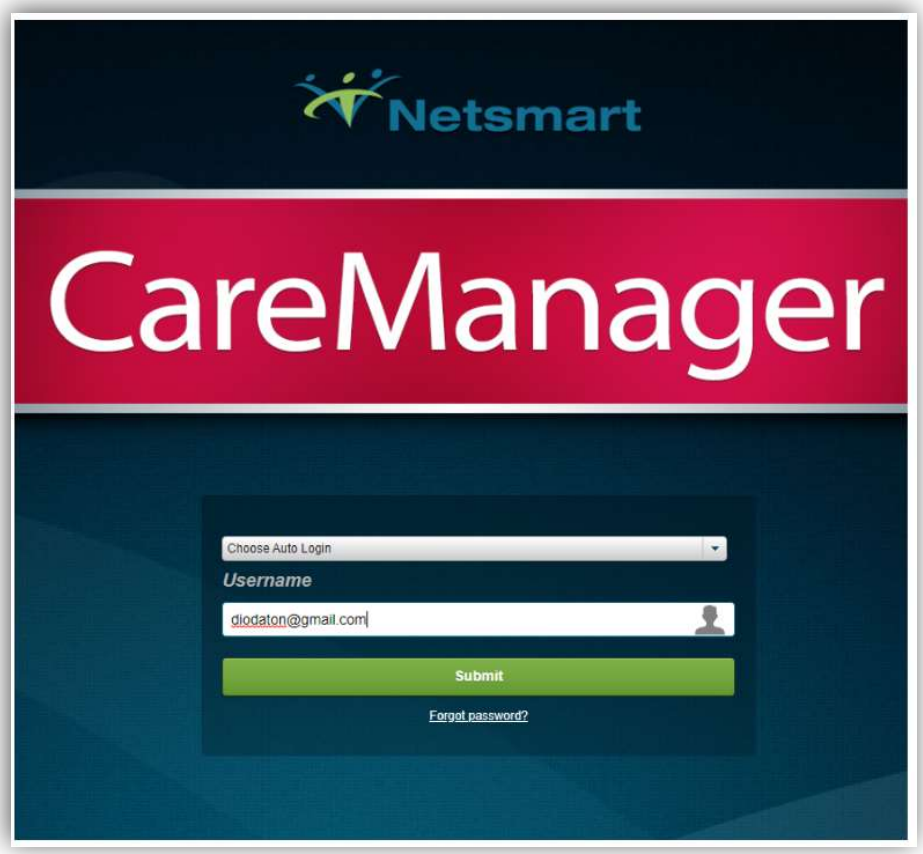
3. Once the process has completed, the following screen will be displayed. The user will then select the **'Sign Out'** option under the user menu. Now, the user will be able to log into CareManager using Multi-Factor Authentication.



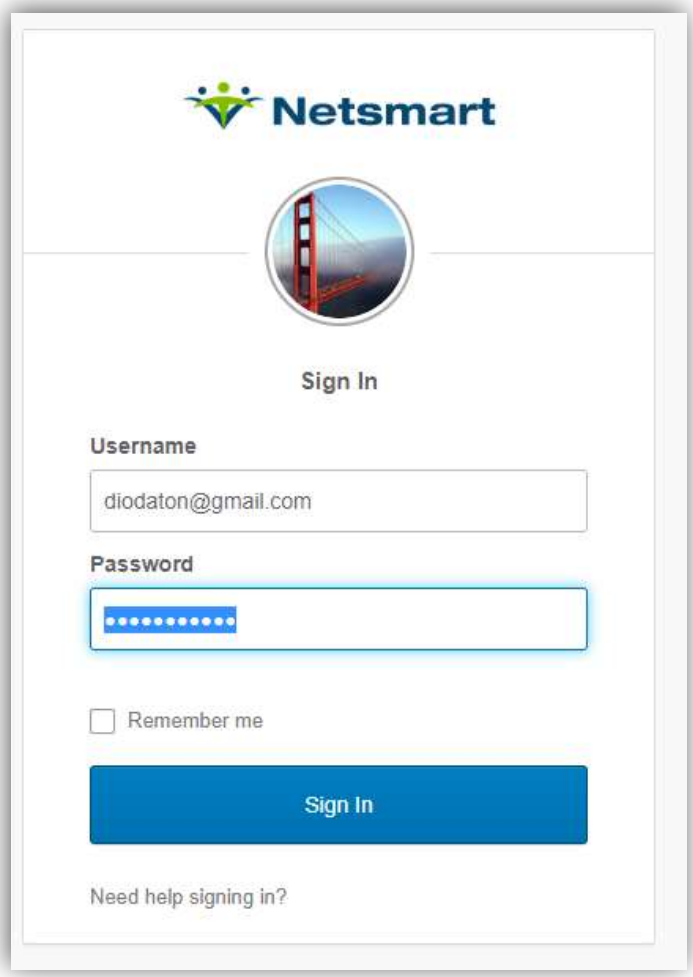
CareManager Account Login

Once the user account is set up in CareManager, users can now log into CareManager using their new user login. The multi-tenant capability will also be available.

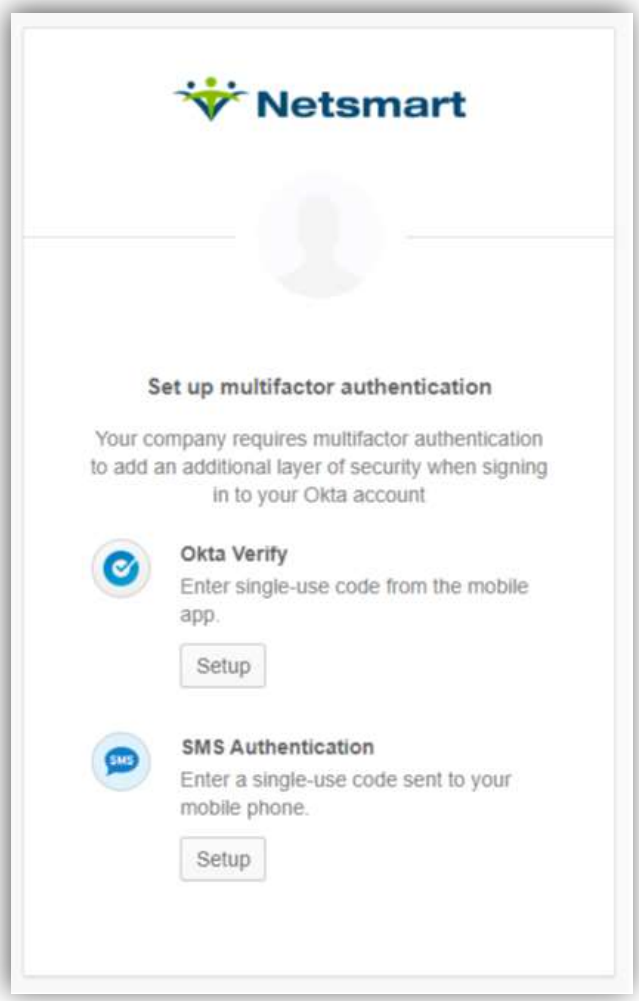
1. On the CareManager Login page, users will enter their username and select **'Submit'**.



2. The new **Okta** login screen will be displayed. Users will enter their password and select **'Sign In'**. After logging into CareManager successfully for the first time using the **Okta** login screen, users will begin seeing their security image on the Sign In page as shown in the screenshot below.



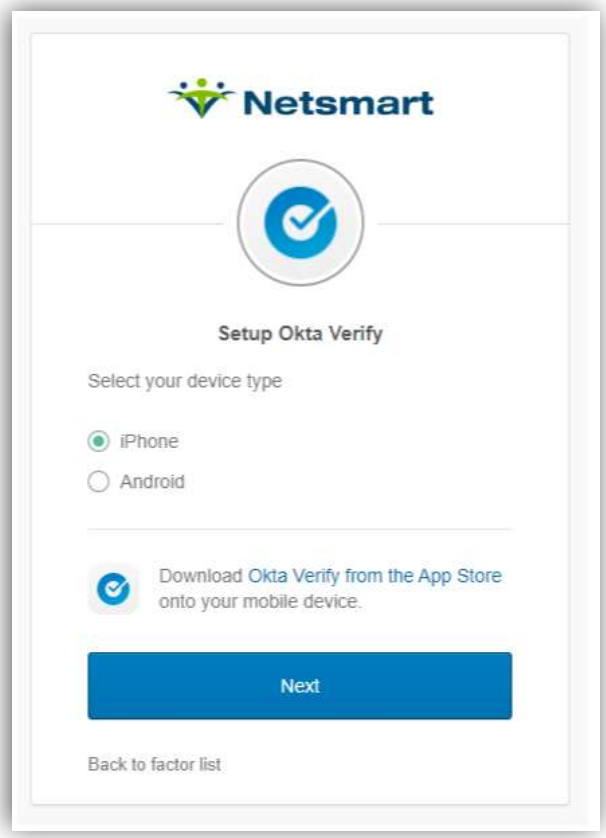
3. Users will then be required to configure multi-factor authentication option they want to use going forward. They will choose between the **Okta Verify** app or **SMS Authentication**. This is a one-time setup process and once an option is selected, the user will be required to use that option for all subsequent logins.



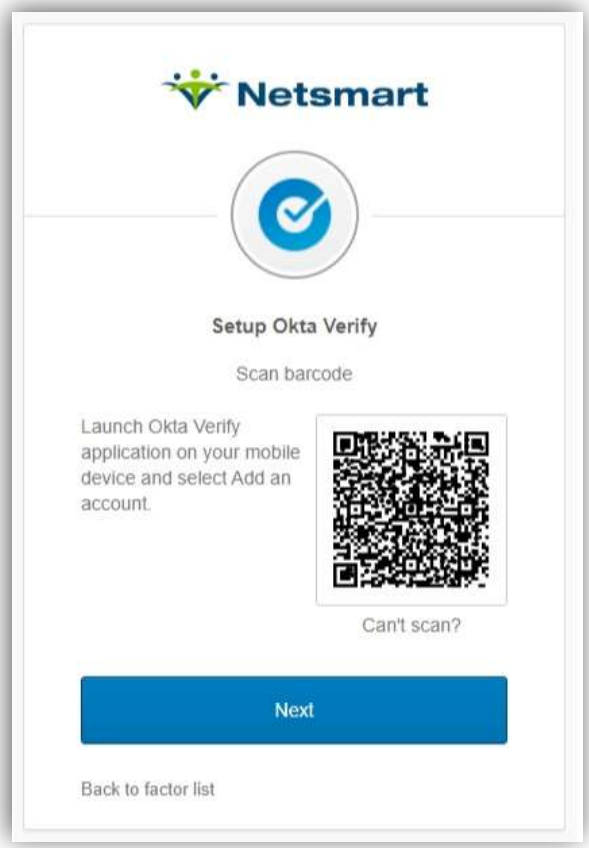
Okta Verify App

1. If the user wants to use the **Okta Verify** mobile app, they will click on the **'Setup'** button under **Okta Verify**. This will prompt the user to select the device type. After selecting the applicable device type for their mobile phone, they will click the **'Next'** button.

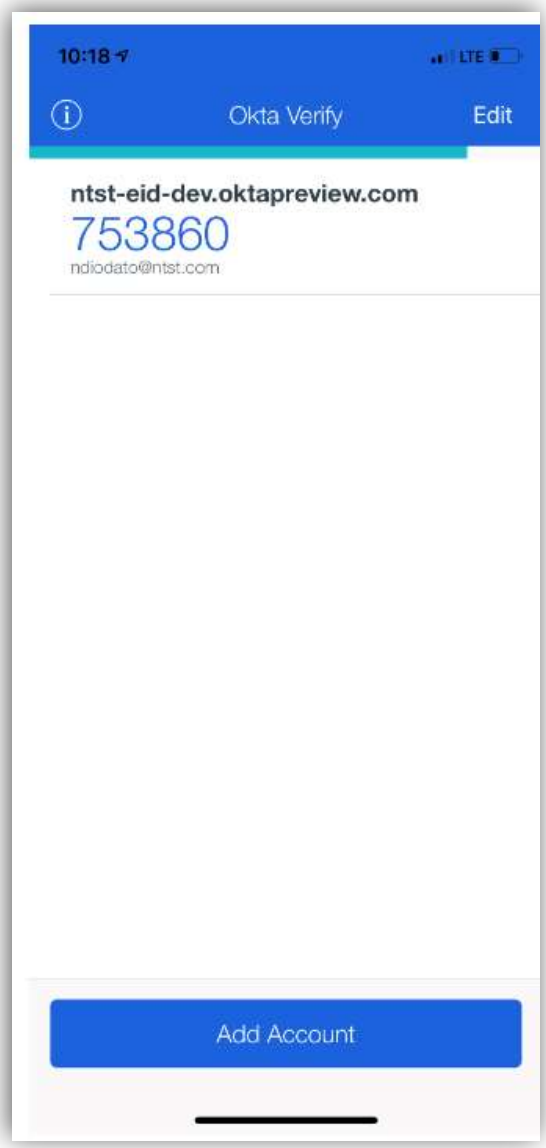
For users that may have limited mobile phone service, Netsmart advises users to use the **Okta Verify** mobile app. This app does not require cell or wifi/internet access.



2. A barcode will then be displayed for the user as shown below.

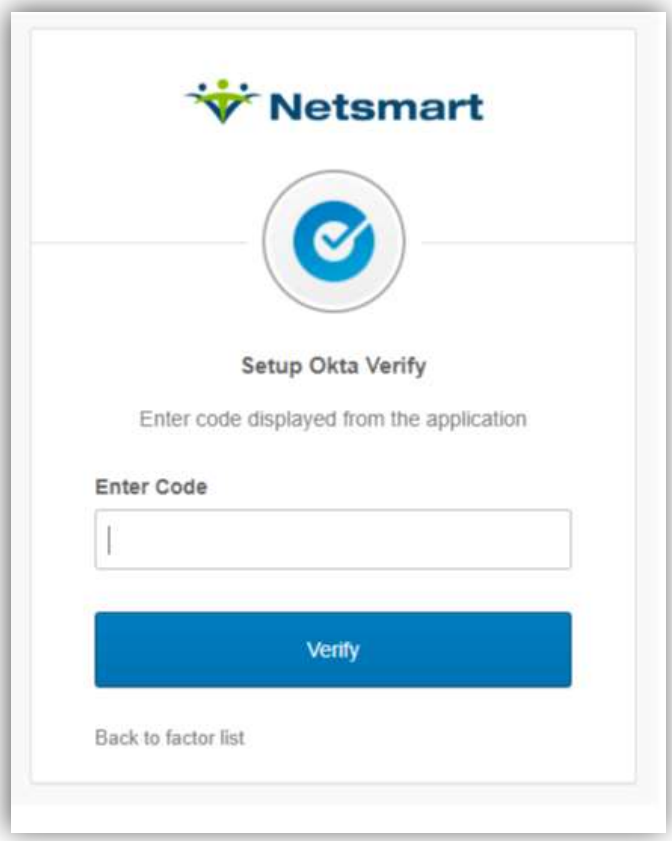


3. The user will then launch the **Okta Verify** app on their mobile phone and select **'Add Account'** as shown below. Selecting **'Add Account'**, the camera on the user's mobile phone will open automatically to bar scanning mode. The user will use their phone to scan the barcode on their screen.



4. After scanning the barcode in the **Okta Verify** mobile app, users will be presented with a code in the app as shown in the screenshot on the left. This code will be used to complete the login process for CareManager. Please note that the code changes every 30 seconds.

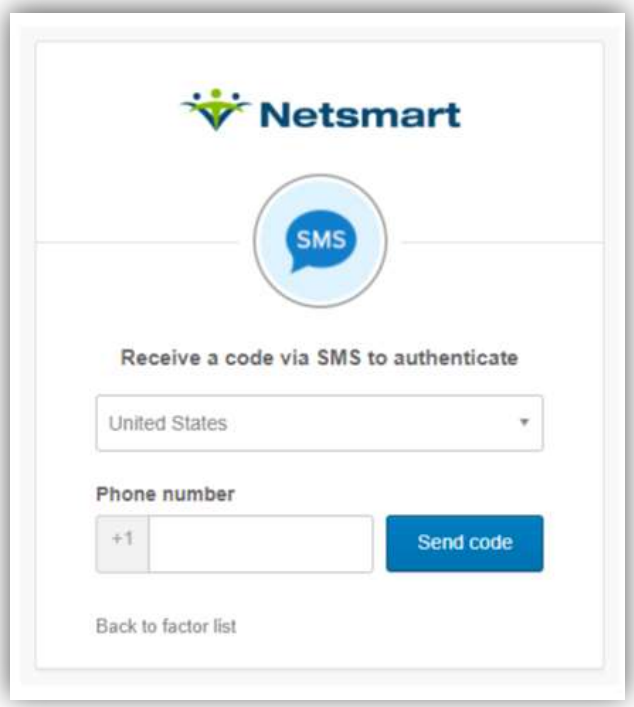
Users will enter the code in the **'Enter Code'** field and then select the **'Verify'** button. If the authentication process is successful, CareManager will be launched.



Note: Each time the user logs into CareManager going forward, they will be prompted to enter a code from the Okta Verify app as shown in the screen shots above.

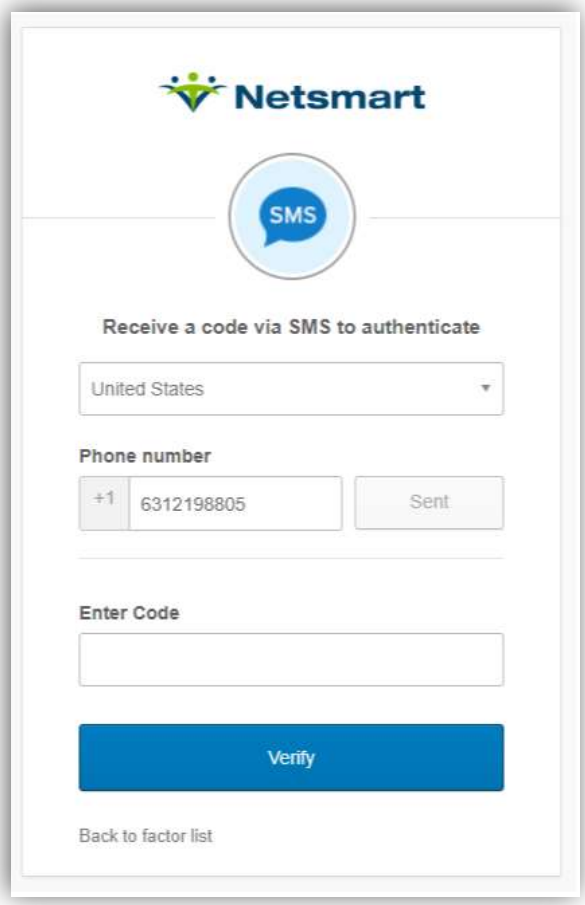
SMS Authentication

1. If the user wants to use the **SMS Authentication** process, they will click on the **'Setup'** button under **SMS Authentication**. This will prompt the user to enter their mobile phone number. After entering their mobile phone number, they will click the **'Send Code'** button.



2. An authentication code will be sent to the user's mobile phone.

3. Users will enter the code in the **'Enter Code'** field and then select the **'Verify'** button. If the authentication process is successful, CareManager will be launched.

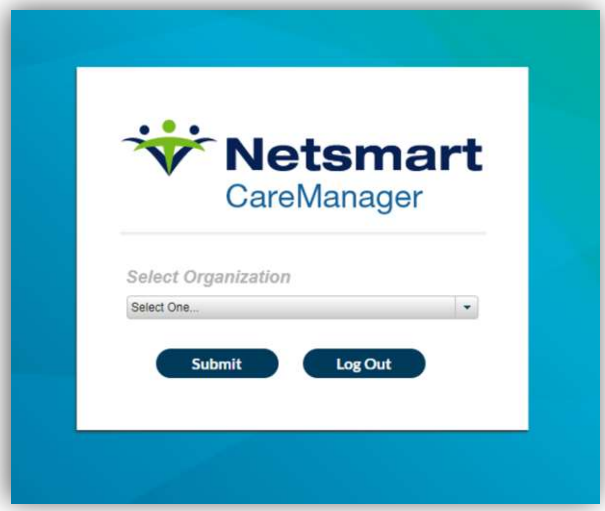


Note: Each time the user logs into CareManager going forward, they will be prompted to enter a code received via text message as shown in the screen shots above.

CareManager Multi-Tenant Login

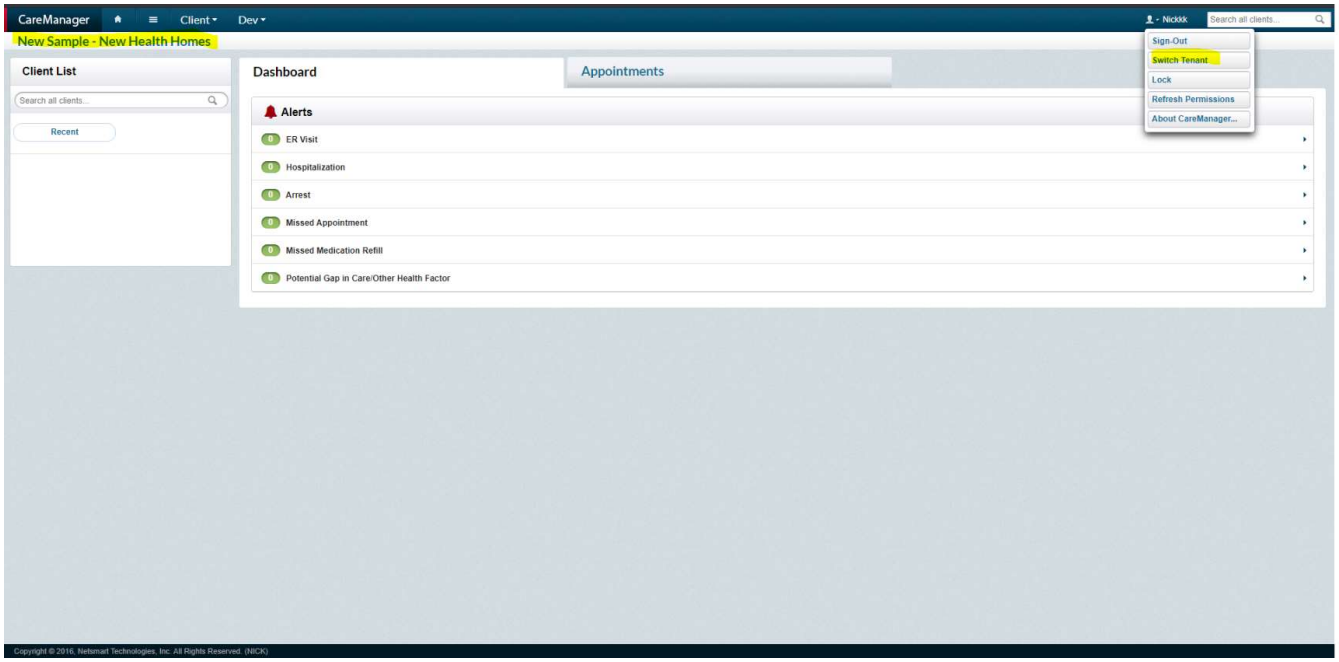
Once the user completes the multi-factor authentication process, CareManager will be launched. For users who are associated with multiple health homes, they will be prompted to select the health home they want to log into.

Users will select the **'Organization'** and then select the **'Submit'** button. This will launch CareManager for the selected health home.



When users associated with multiple organizations are logged into CareManager, they will see the Organization they just logged into in the banner in the top left of the screen.

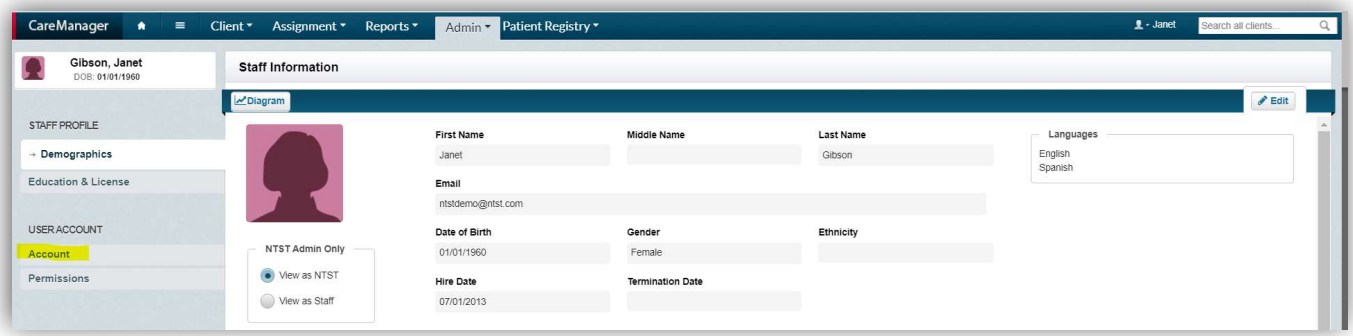
Users be able easily switch between health homes using the **'Switch Tenant'** option under the user menu.



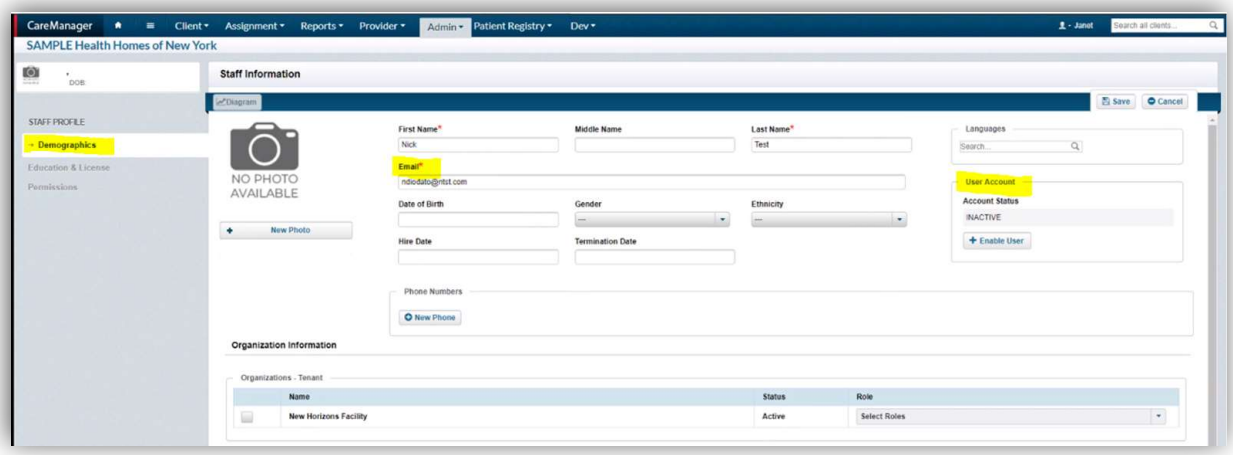
New Account Creation

After Netsmart releases the enhancements to support multi-tenant and multi-factor authentication, System Administrators will set up new accounts slightly different in CareManager. As mentioned before, staff members will have one user account that is linked together by their email address. So, going forward, System Administrators will no longer be able to use an invalid email address for staff members. It is very important that System Administrators use real email address for staff members when adding a new staff member working for a CMA that contracts with multiple Health Home organizations. If a valid email address is not used, then the user will not be able to set up their account or log into CareManager. If the staff member already has an account in CareManager for another Health Home organization when the organization create the new staff member account, CareManager will automatically link the accounts together using the email address, allowing the staff member to use the multi-tenant login process.

Prior to the change, there was an Account tab under User Account on the Staff Information screen in CareManager as shown below.



After these enhancements are released to Production, the User Account tab will be removed in CareManager. The Email and User Account Status fields will be moved to the Demographics tab as this is now part of the account creation process as shown below.



1. After entering the staff member information, with the valid email address, the System Administrator will select the 'Enable Account' button. When this is done, the User Account Status will be set to 'Pending' on the Staff Information screen as shown below.

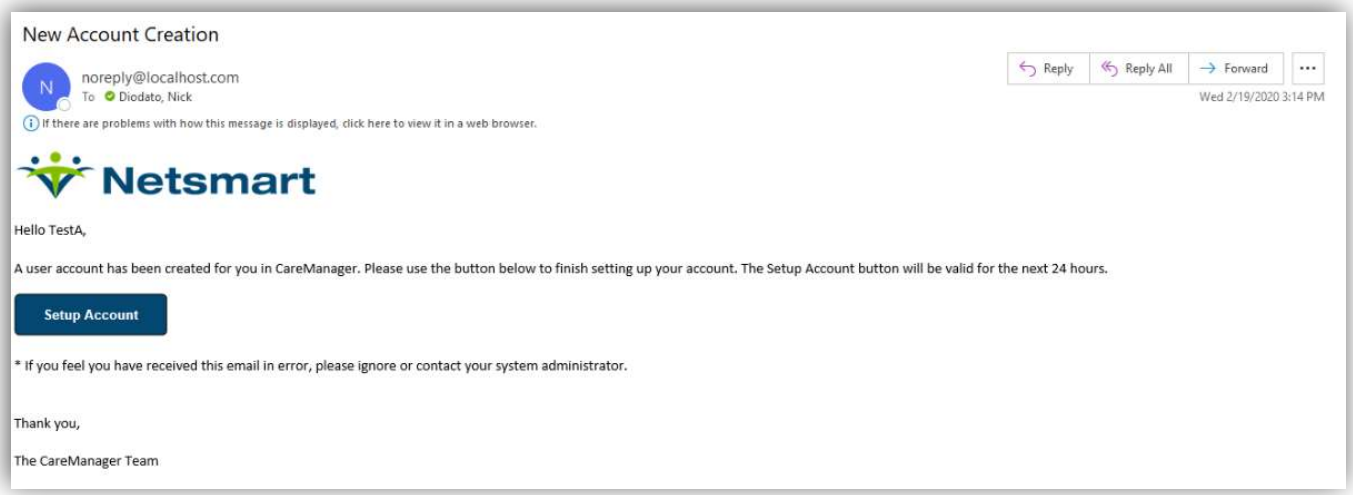
This will remain in **'PENDING'** status until the user completes the account creation process.

Until MFA is enabled on **April 20th**, any new accounts created after **April 6th** will receive one of two emails, depending on if the user already has an existing account. Once MFA is enabled on **April 20th**, they will receive the same email and will follow the process outlined under the **Okta Account Setup** section above.

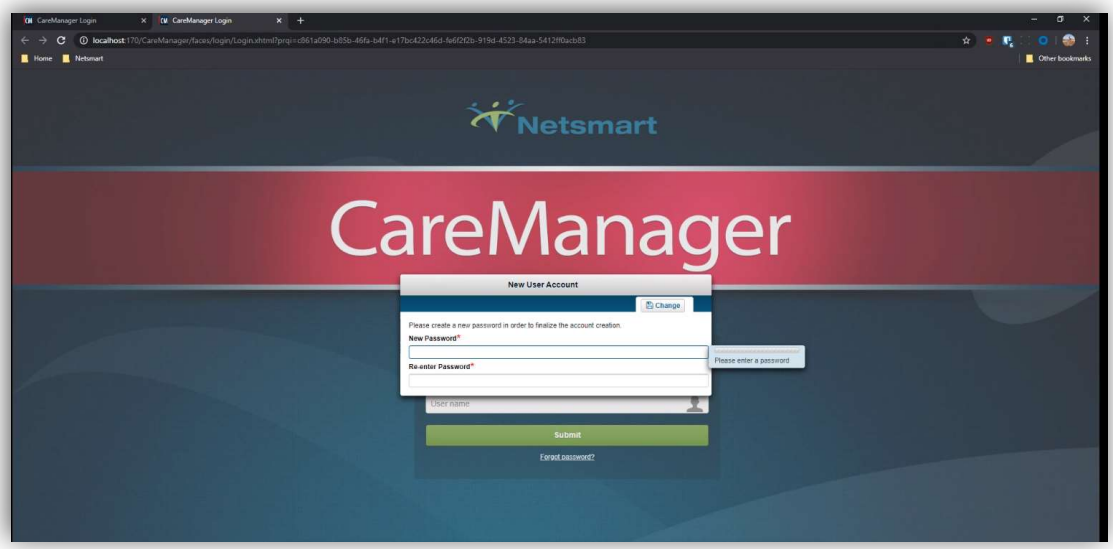
Account Creation Process for Single Tenant

If the staff member created does not have an email matching another staff member across any Health Home organization, then the staff member will be considered a **'Single Tenant'** user and will receive the email below to set up their account.

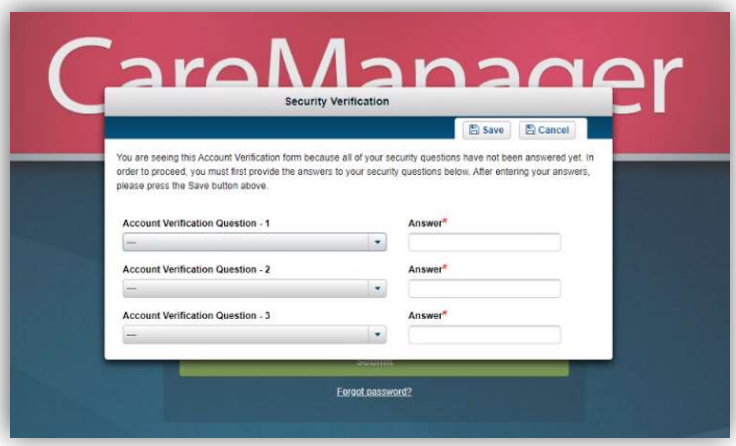
1. Users will click the **'Setup Account'** button on the email to start the account setup.



2. The user will be taken to the CareManager login screen and prompted to enter their new password. After entering their password in both fields, they will click the **'Change'** button.



3. The user will then be prompted to select 3 security questions and enter their answers. Once entered, the user will click the **'Save'** button.



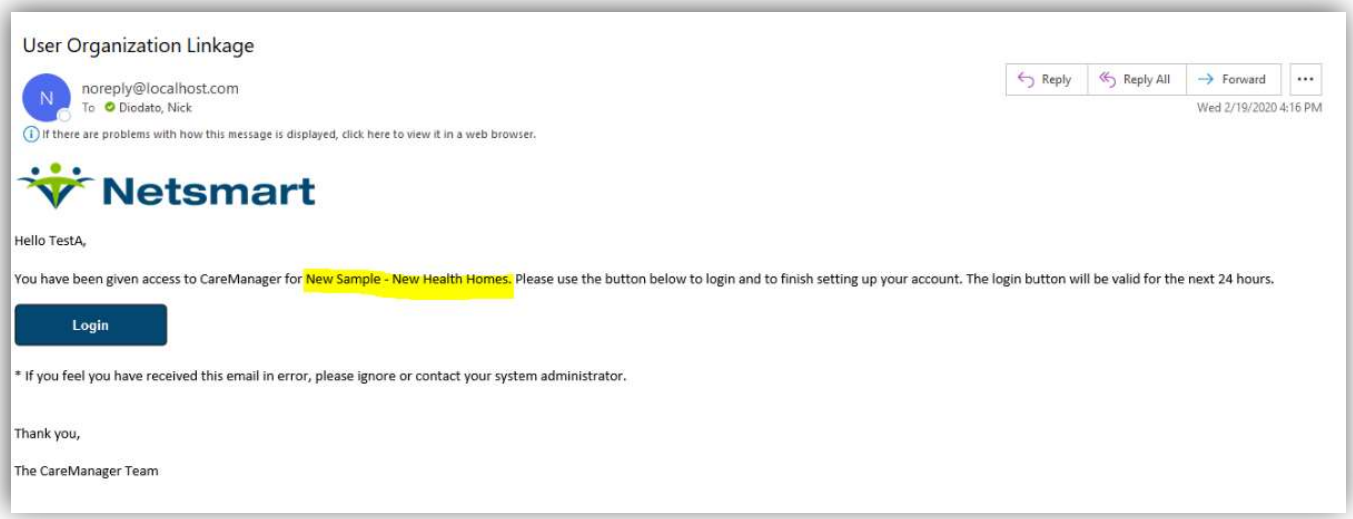
The user will now be able to log into CareManager with the password they just configured.

System Administrators will be able to tell when the user has completed their account as the User Account Status will now be set to **'ACTIVE'**.

Account Creation Process for Multiple Tenant

If the staff member created has an email matching active staff member across any Health Home organization, then the staff member will be considered a **'Multiple Tenant'** user and will receive the email below to set up their account. The email will reference the 'Health Home' for which the account is being configured.

1. Users will click the **'Login'** button on the email to start the account setup.

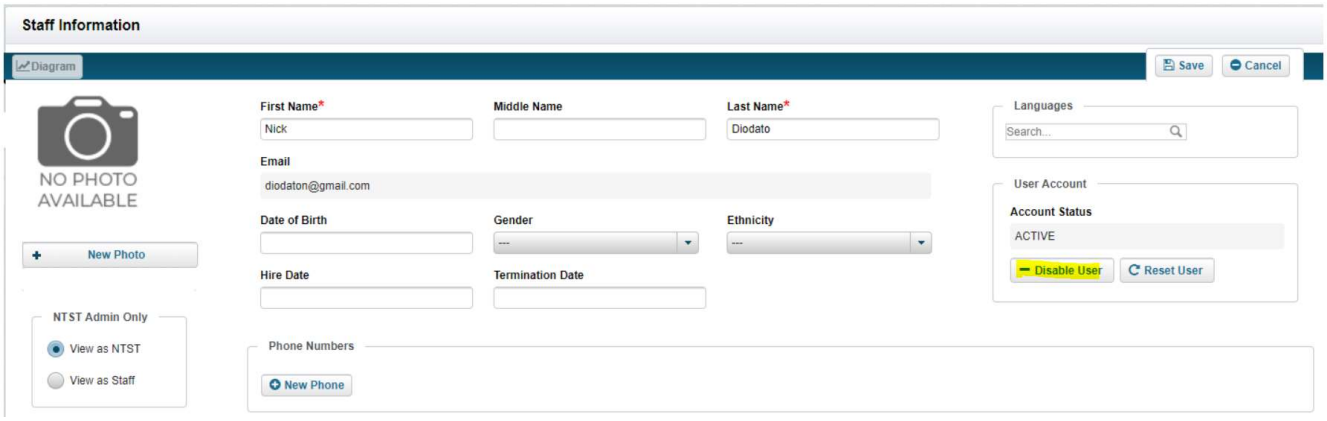


2. Users will be prompted to enter their username. After entering their username, they will the **'Submit'** button.

The user will then enter their password associated with the email address and then be logged into CareManager for the associated health home. Users will be able to use the 'Switch Tenant' option on the user menu to switch easily between each health home in which they are associated.

Deactivate Account

System administrators will deactivate a staff member's account using the **'Disable User'** button on the Staff Information screen. If a user is associated with multiple tenants, this will only impact the account for the staff member associated to the health home.

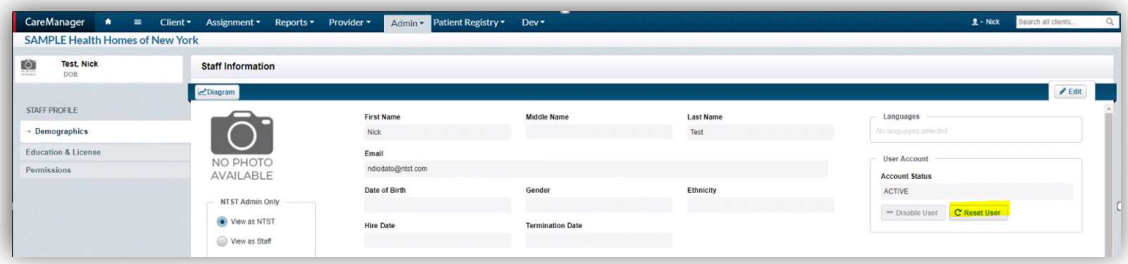


Password Resets

After **April 6th**, password resets can be performed by the user, or can be initiated by a System Administrator as outlined in the sections below. Although, System Administrators will still be able to reset passwords, the process will be different. System administrators will also no longer have access to add/update a user's password or view/edit a user's account verification questions.

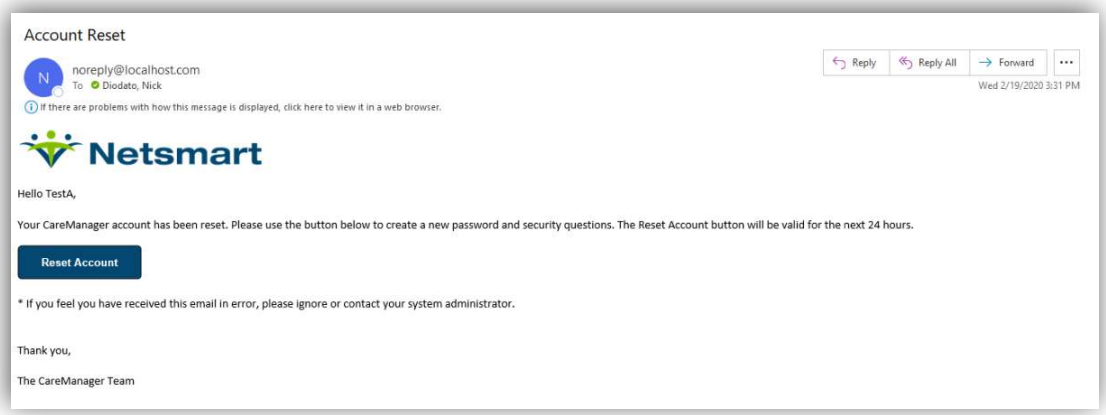
System Administrator Initiated Password Reset

1. System Administrators can also initiate a password reset for their staff members. To do this, the System Administrator will select the 'Reset User' button on the Staff Information screen.

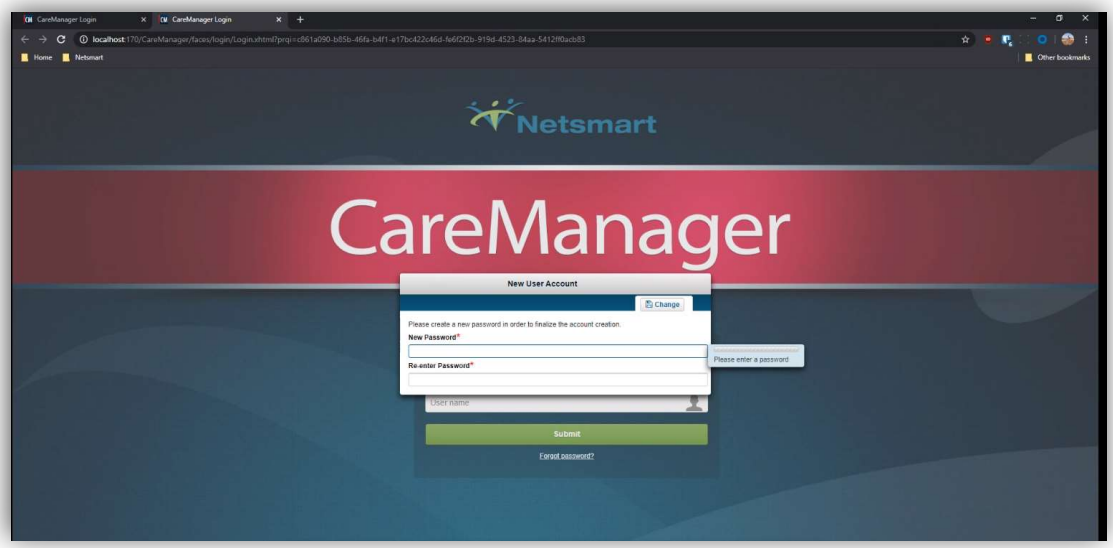


2. The prompt to the right will be displayed. The System Administrator will select **'Yes'** to reset the password. Selecting **'Yes'** will delete the existing password and the user will not be able to log into CareManager for ANY health home they are associated until they complete the password reset process.

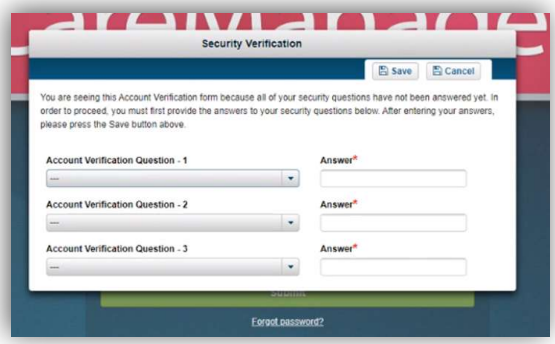
3. Selecting **'Yes'** will also send an email to the user to reset their password. The user will then click on the **'Reset Account'** button.



4. The user will be taken to the CareManager login screen and prompted to enter their new password. After entering their password in both fields, they will click the **'Change'** button.



5. The user will then be prompted to select 3 security questions and enter their answers. Once entered, the user will click the **'Save'** button.

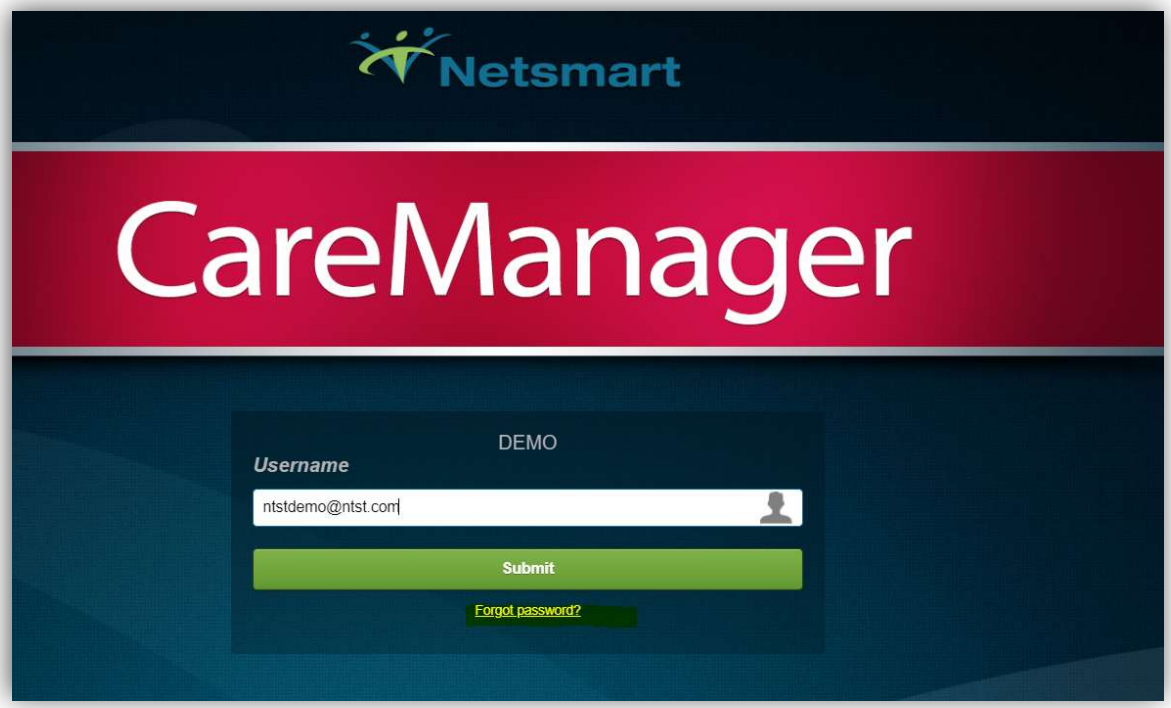


The user will then be logged into CareManager or be prompted to select the tenant if they are a multi-tenant user.

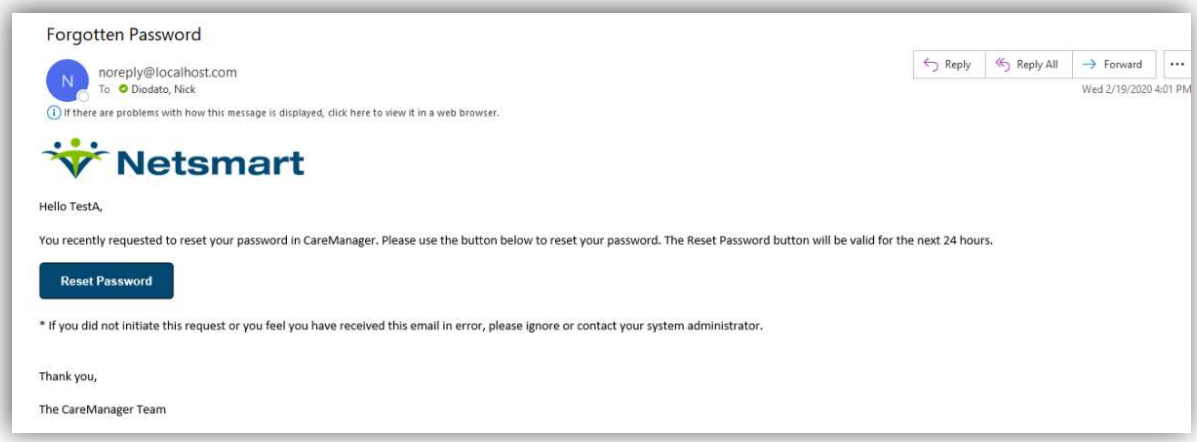
User Initiated Password Reset Before MFA is Enabled.

Once the latest version is released on **April 6th** but before MFA is enabled on **April 20th**, users can reset their password using **'Forgot Password'** link on the CareManager login page.

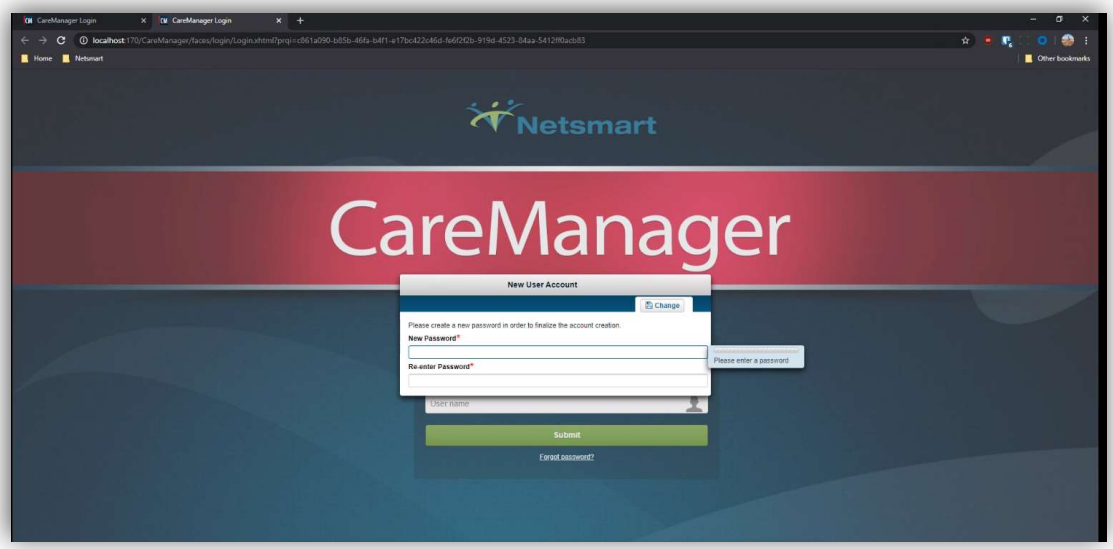
1. If a user needs to reset their password before their Okta, they enter their username and then click on the **'Forgot Password?'** link below the Submit button on the CareManager login screen.



2. Clicking the link will send an email to the user. The user will then select the **'Reset Password'** button on the email.



3. The CareManager login page is launched and the user will be prompted to enter their new password. Once they enter a matching password in each field and click **'Change'**, the user will be logged into CareManager.

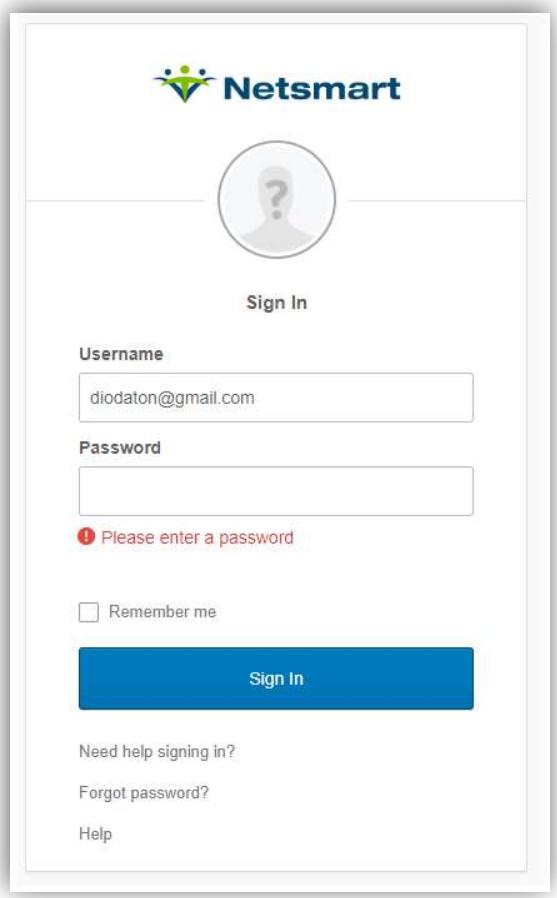


The user will then be logged into CareManager or be prompted to select a tenant if they are a multi-tenant user.

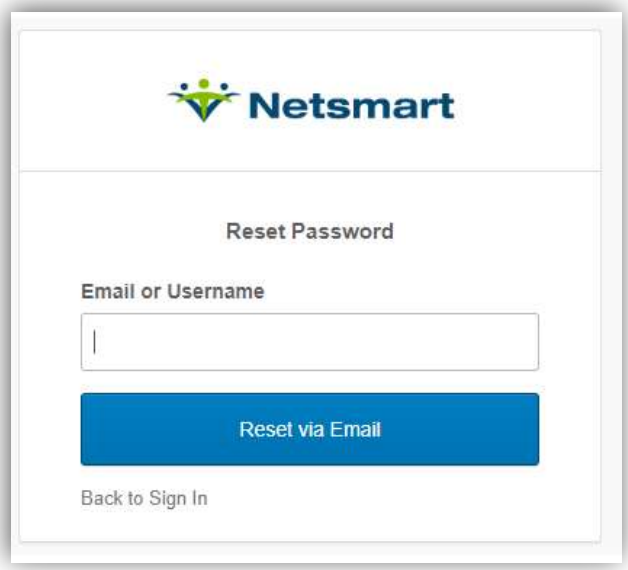
User Initiated Password Reset After MFA is Enabled

Once MFA is enabled on **April 20th**, users now need to reset their password on the **Okta** login screen.

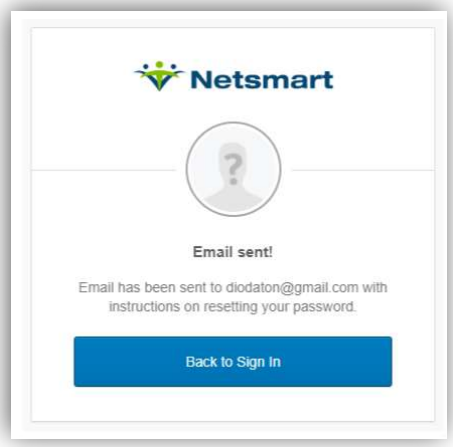
1. If a user needs to reset their password after their Okta login has been activated, they will do this by selecting the **'Need help signing in?'** link on the Okta login screen.



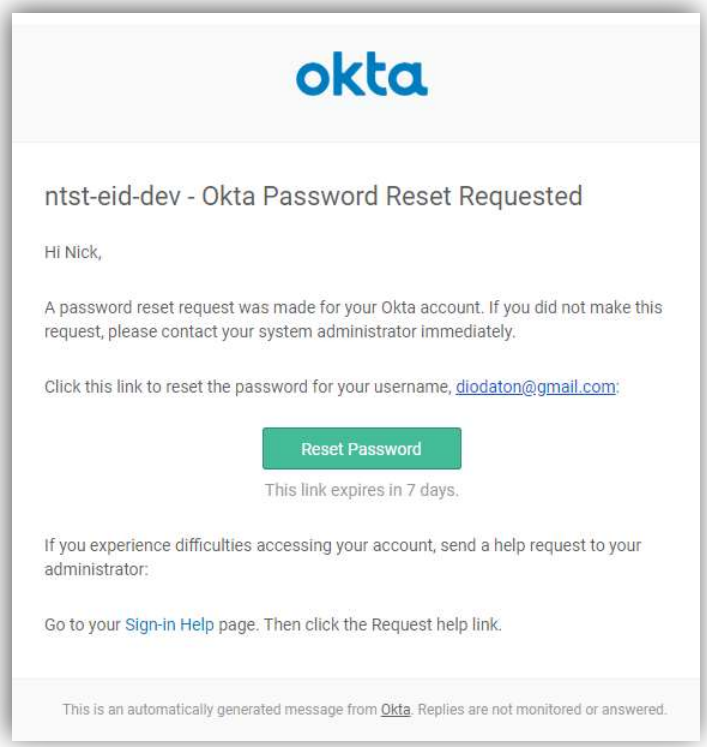
2. Clicking the link will display the following screen. The user will enter their email address and click the **'Reset via Email'** button.



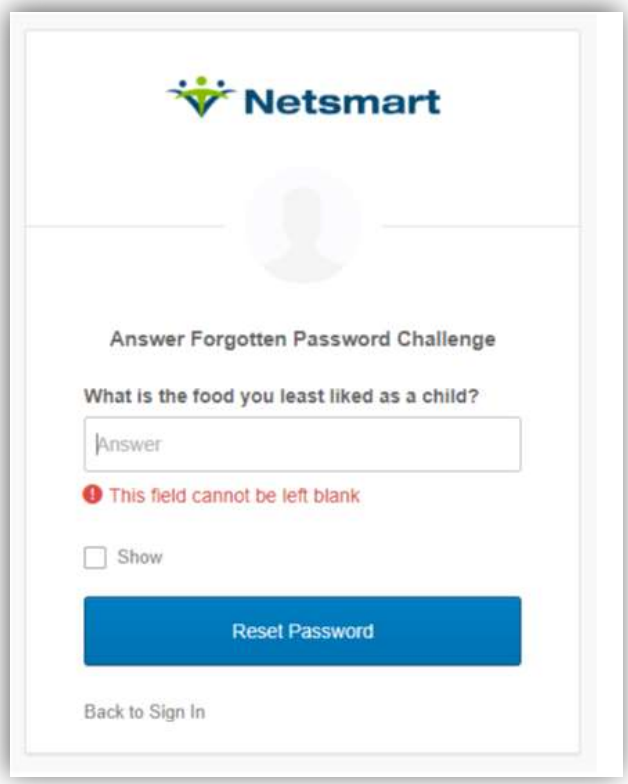
3. The user will be notified that an email has been sent.



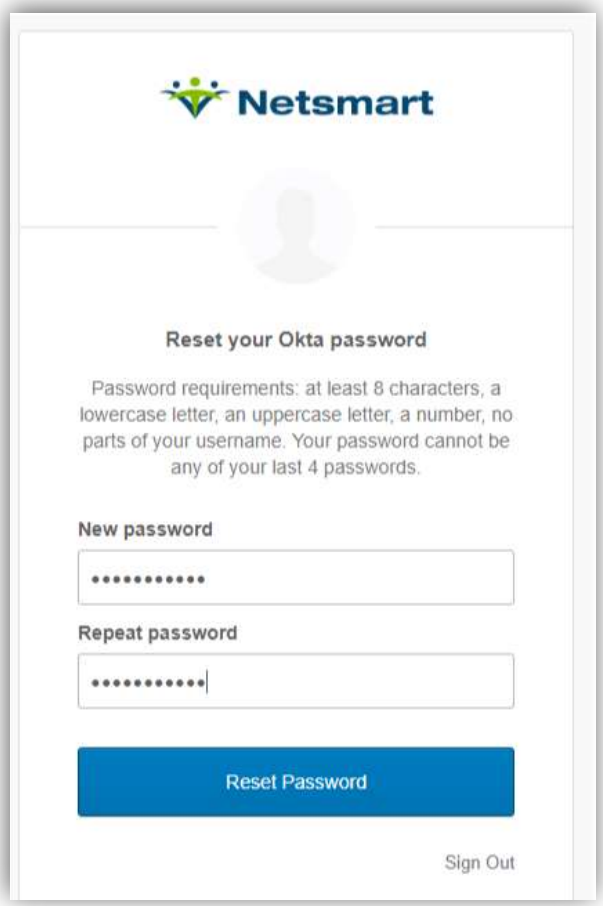
4. When the user receives the Okta email, they will click on the **'Reset Password'** button.



5. The user will be prompted to enter the answer to their security question. Once entered, they will select the **'Reset Password'** button.



6. The user will then be prompted to enter a new password. Once entered, they will select the **'Reset Password'** button. The user will then be returned to the **Okta** profile page. The user will be required to navigate back to CareManager and start the login process again using the new password.



UAT Testing

Netsmart will allow testing of the Okta account configuration and multi-factor authentication process between **March 31st** and **April 4th**. Organizations will need to send a list of test users with valid email addresses to be used during this testing period. Users will be able to follow the same instructions outlined in the **User Guide** section to provision their **Okta** account in UAT and log into CareManager UAT. Organizations will also be able to test the new account activation and password resets. Netsmart encourages this testing process so that system administrators become familiar with the process so they can answer questions from staff.

Once the MFA capabilities are release to Production on **April 6th**, the Okta MFA process will be turned off in UAT, so users will no longer need to go through authentication. This will allow those user accounts configured with invalid email addresses to be used for testing.