STUDENT OKTA SIGN-ON PROCEDURES AND PASSWORD RECOVERY

TABLE OF CONTENTS

SUMMARY:

The University is consolidating usernames and passwords used to access University services (e.g. email, UIS) using a new single sign-on system called Okta. This system will make it easier for you to sign in, provide enhanced security, and give you the ability to reset your own password.

Starting in the Summer of 2020, all students please use signon.stjohns.edu to access your St. John's University email. After this date, if you try to access email through MySJU, you will be redirected to this new URL. Your user ID will be your Active Directory (AD) account and your password will be the same password you currently use for your St. John's e-mail and wireless.

Going forward, you will also be able to reset and change your current password through this new service. As a reminder, the credentials used for this service are what you use to log into St. John's email and wireless.

Also, we strongly recommend you bookmark **https://signon.stjohns.edu/** and use it going forward.

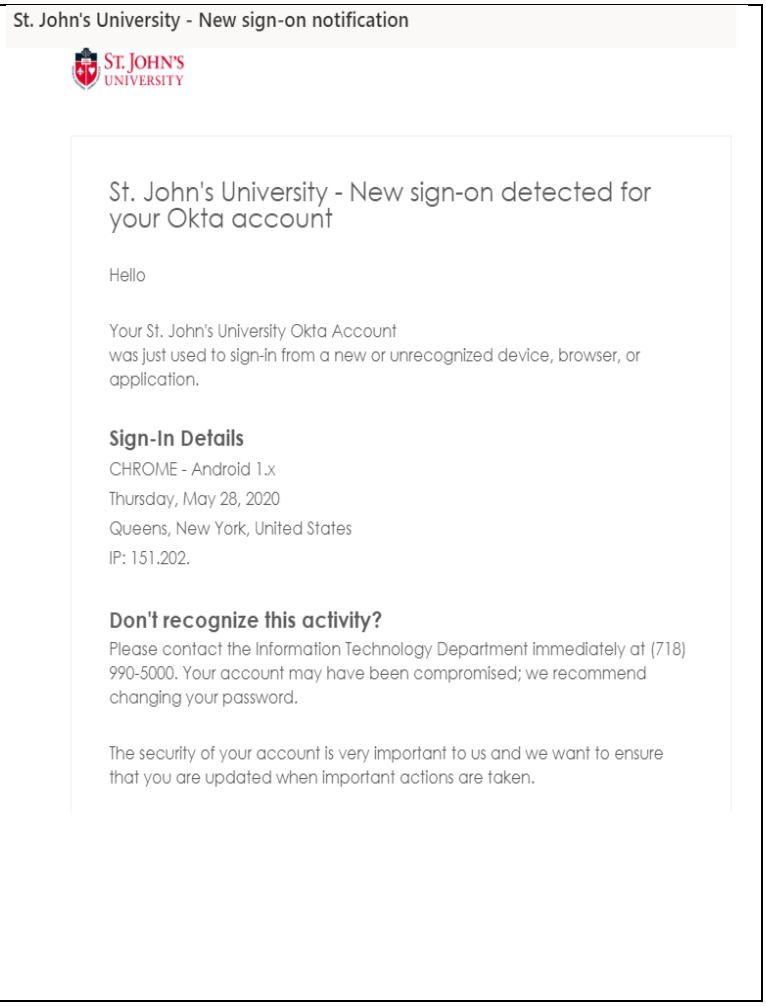
This PDF can also be found at https://www.stjohns.edu/IT

FIRST-TIME USER

First-time users of the new Sign-On system will be asked to complete some one-time actions to set up the enhanced security features. Like banks and other financial institutions, we reply to something that you know (your password) and something that you have (your phone) to periodically verify your identity. (This approach is also known as two-factor authentication.) You will need to select the secondary authentication method you'd like to use. The system can send a text message to your phone, rely on an app that runs on your mobile phone or call your desk phone.

OKTA E-MAIL NOTIFICATIONS

Upon first sign-on to a browser or a new device, you will receive an e-mail with the title "**St. John's University - New sign-on notification**". **This is not spam.** This is a normal behavior of the new Sign-On System. You will receive subsequent e-mails when you register a new device, enroll in a form of MFA and reset your password.


St. John's University - New sign-on notification

ST. JOHN'S UNIVERSITY

St. John's University - New sign-on detected for your Okta account

Hello

Your St. John's University Okta Account
was just used to sign-in from a new or unrecognized device, browser, or application.

Sign-In Details

CHROME - Android 1.x

Thursday, May 28, 2020

Queens, New York, United States

IP: 151.202.

Don't recognize this activity?

Please contact the Information Technology Department immediately at (718) 990-5000. Your account may have been compromised; we recommend changing your password.

The security of your account is very important to us and we want to ensure that you are updated when important actions are taken.

FOR EXISTING USERS

For existing users (those who have used this system to access Banner), you will no longer be able to authenticate via “Security Question”. You will be prompted upon log-on to update your Multi-factor Authentication to one of the following types: SMS, Voice Call or Okta Verify (Phone App)

If you have any questions or need assistance, please contact the Information Technology Service Desk at 718-990-5000 (x5000).

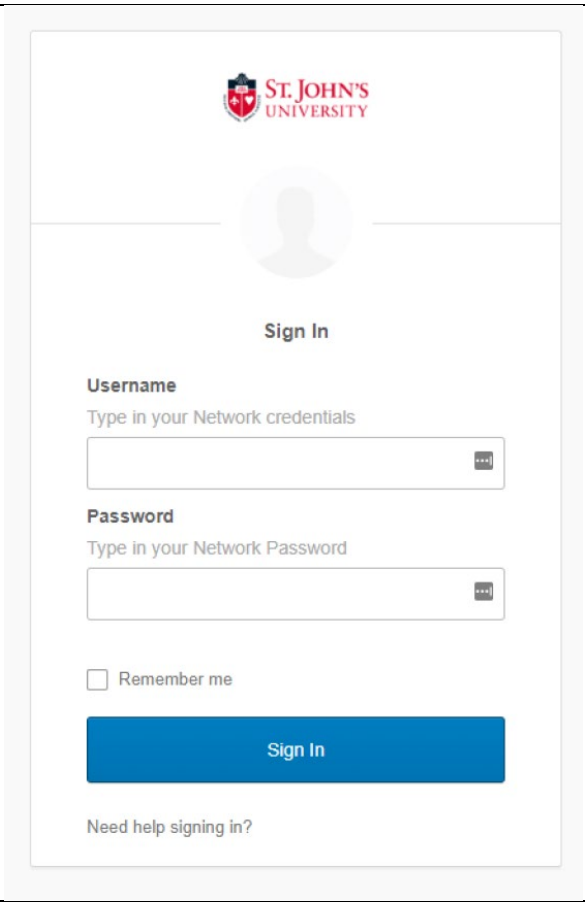
INITIALIZE OKTA SETUP

Through a web browser, enter https://signon.stjohns.edu to authenticate to your St. John’s email.

Username is your St. John’s email (Firstname.lastnameYY@my.stjohns.edu; e.g. John.doe15@my.stjohns.edu)

Default password:

SjXXXXXXXXX (where XXXXXXXXX is your Storm Card ID card number or PIDM)



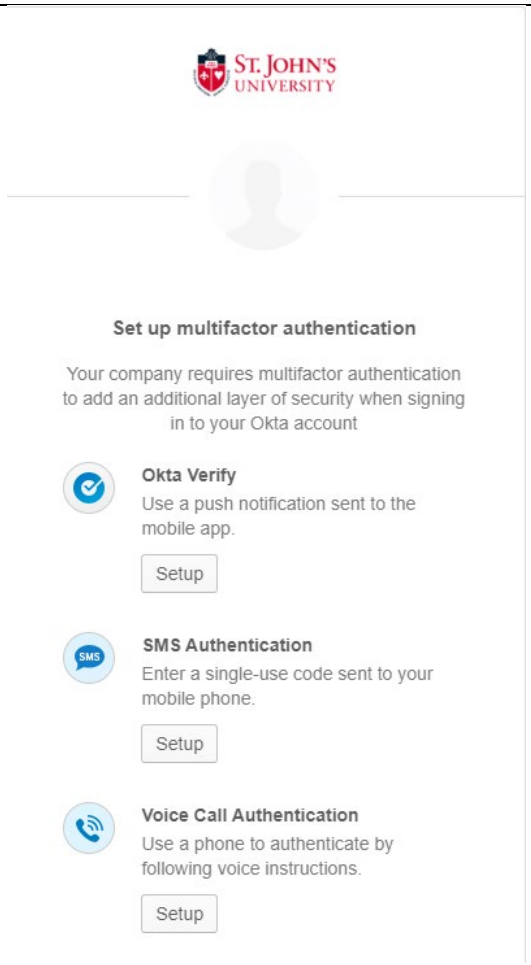
If this is the first time you are logging into this site, the system will ask you to configure at least one alternate way to verify your identity. This is also known as multi-factor or two-factor authentication. You probably have used most of these procedures with your financial institutions.

The University supports:

Okta Verify: This is an app on your iPhone or Android mobile phone which provides a six-digit pin number to supplement your username and password. Simply install the App on your phone and link it up to your account. Also note that Okta Verify is recommended for international travel.

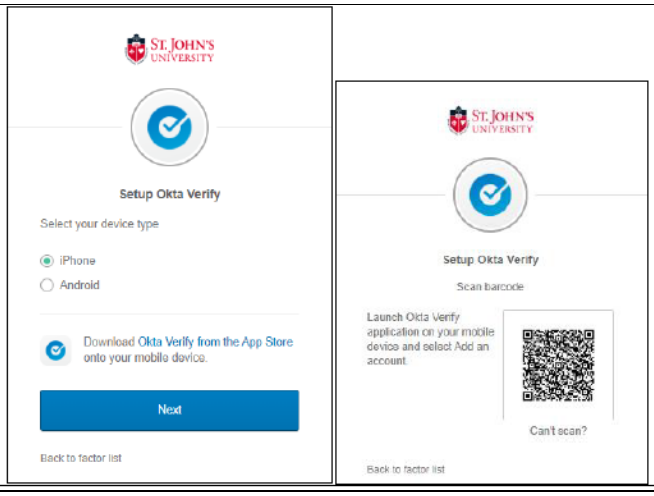
SMS Authentication: Similar to Okta Verify, this supplemental authentication approach uses a six-digit pin which is texted to you. To use, you must supply the mobile phone number.

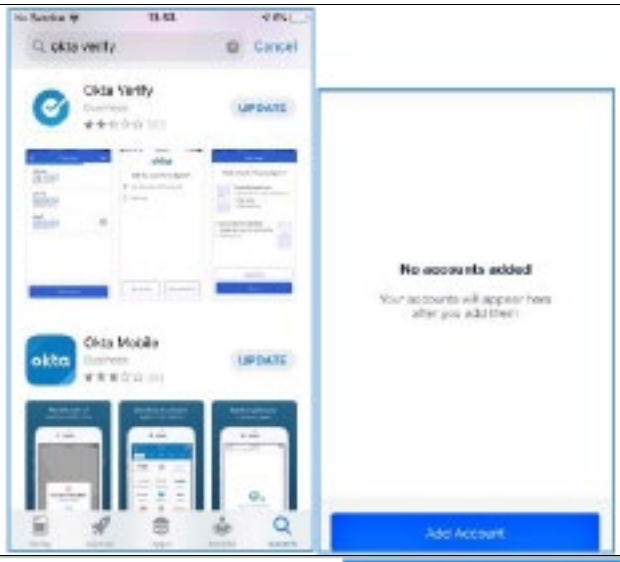
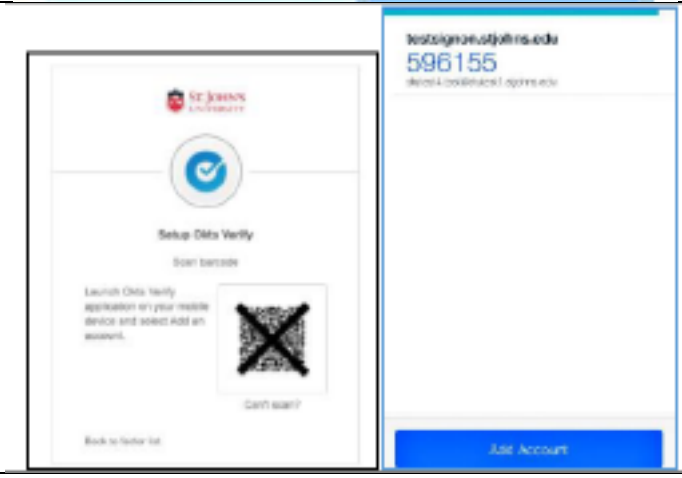
Voice Call Authentication: This allows you to authenticate using a five-digit code by receiving an automated phone call. To use, you must provide a phone number that you can be called at.



OKTA VERIFY SETUP

Step 1: Go to a web browser not on a mobile device (e.g. laptop or desktop computer). Select your mobile phone type and click "Next". A screen with a barcode will appear.



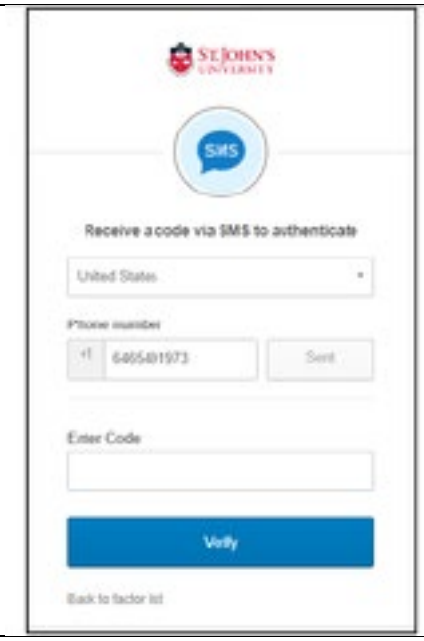
Step 2: From your mobile device, install the free Okta Verify app from the App Store. **Step 3:** Open the app and click “Add Account”. Apple App Store for iPhones Google Play Store for Android	
Step 4: The app will start your phone’s camera and show a square frame. **Step 5:** Point your camera’s frame toward the barcode (QR code) on your laptop or desktop browser. The code will be automatically scanned and display a number after. **Complete:** Okta Verify is now set up and will show a six-digit authentication pin whenever it is started.	

SMS AUTHENTICATION SETUP

Step 1: Enter the SMS mobile phone number and press “Send Code”

Step 2: Enter the code that was sent to your phone and press “Verify”.

Complete: You may now continue to use St. John’s services.



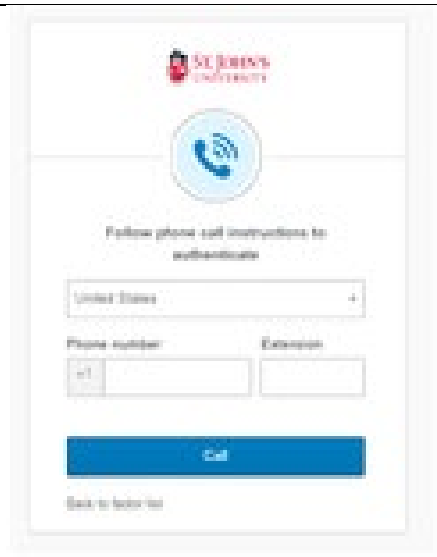
PHONE CALL AUTHENTICATION

Step 1: Enter the phone number and press “Send Code”.

Step 2: Answer the phone call.

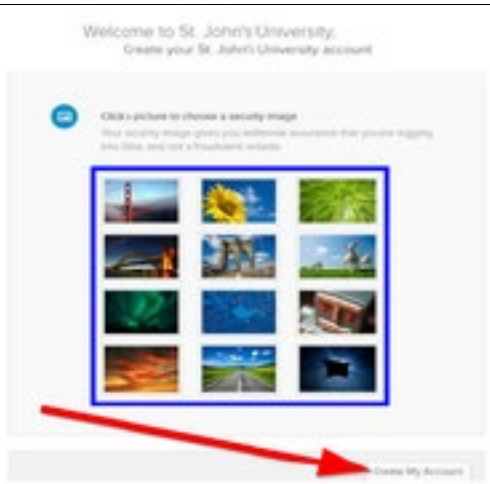
Step 3: Enter the 5-digit code that was spoken over the phone and press “Verify”.

Complete: You may now continue to use St. John’s services.



SELECT SECURITY IMAGE

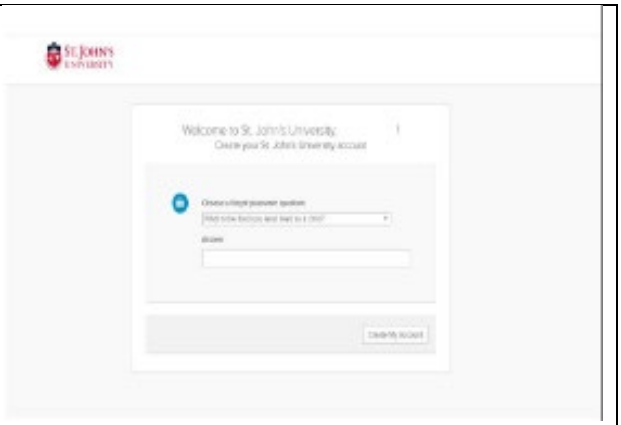
You will now be asked to select a security image. This will help you identify which login credentials you are using during login. Select an image from the list (blue box below), and the select the “Create My Account” button (see red arrow) to complete account setup.



SET UP FORGOT PASSWORD QUESTION

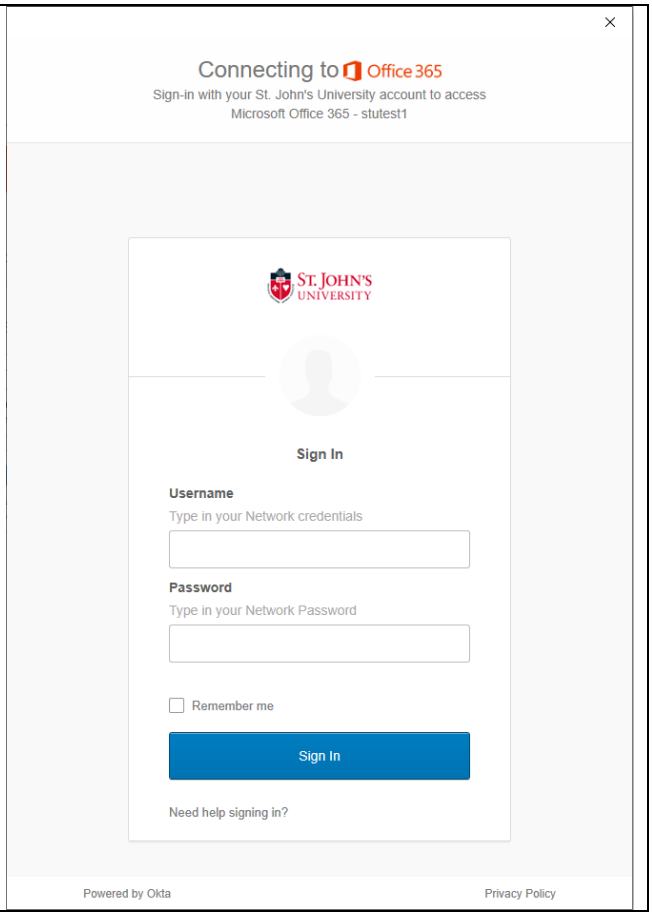
You will now be asked to setup a forgot password question. Please select a question from the list of questions and type in your answer. Please note, the answer is case sensitive.

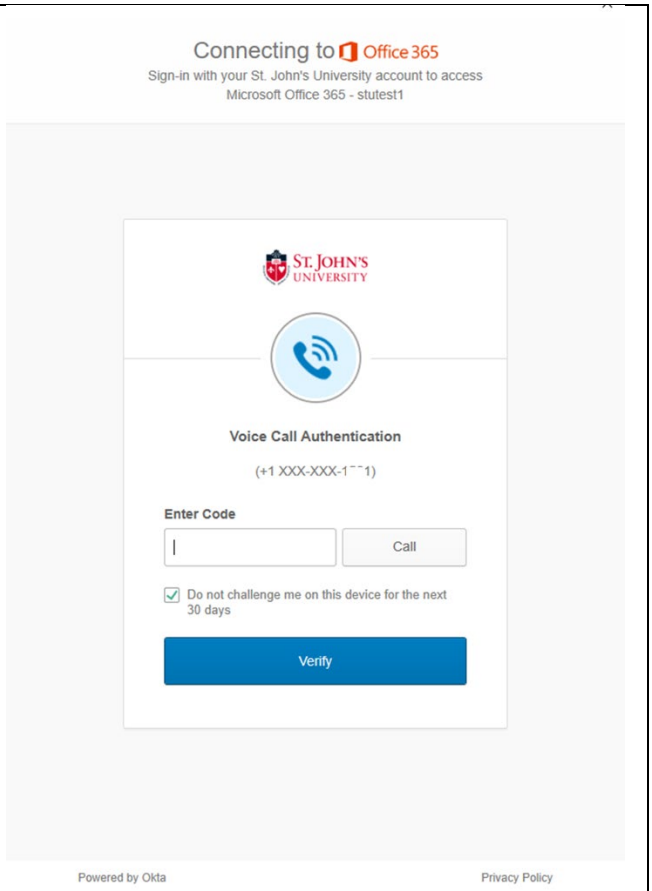
It is very important to remember your answer to your forgot password question. If you forget your password answer, please call 718-990-5000 (x5000) for assistance in recovering it.



E-MAIL AUTHENTICATION FOR OUTLOOK

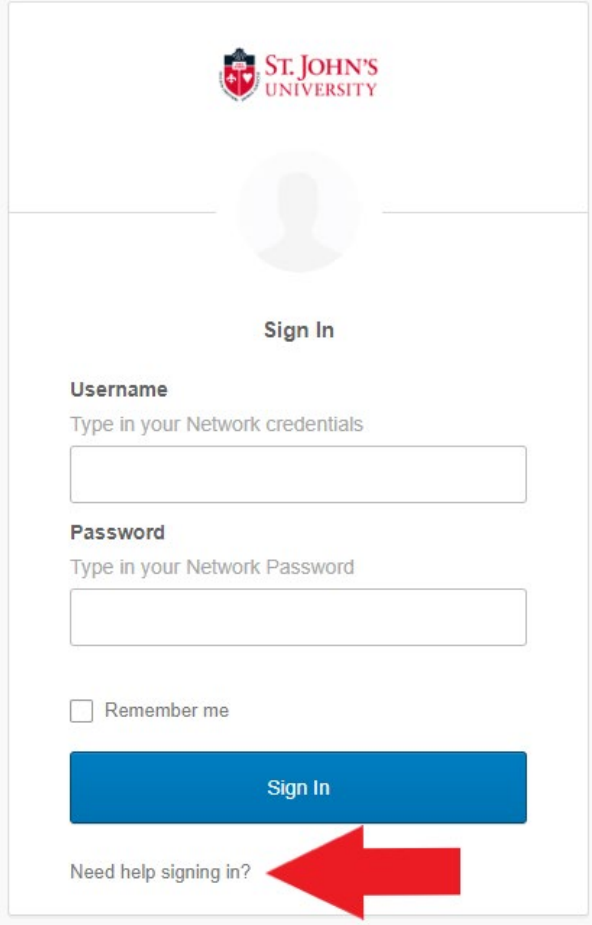
If you use Microsoft Outlook client on your desktop or laptop to check and send emails, you will be prompted every 30 days to re-authenticate.

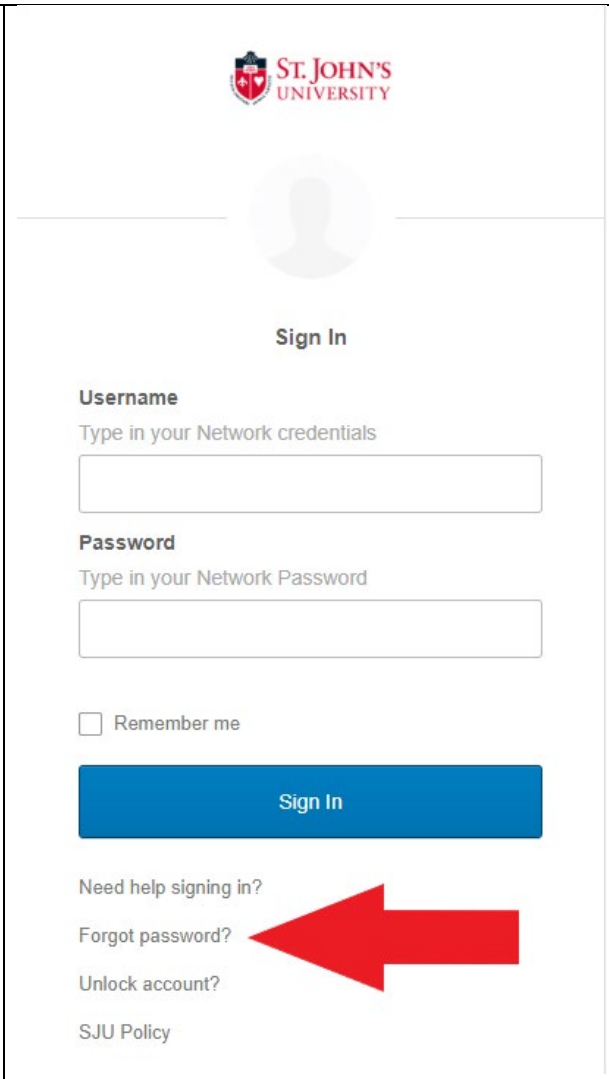
Step 1: A log-in box like the one pictured to the right will prompt you to put in your username and password and click “Sign In.”	

Step 2: After you have signed in, you will be prompted to answer your multi-factor authentication prompt (as an example, “Voice Call Authentication” is depicted to the right). You can also check the checkbox for “Do not challenge me on this device for the next 30 days”. Verify your authentication method via Phone Call or SMS and enter the code then Click “Verify”.	

SELF-SERVICE PASSWORD RECOVERY

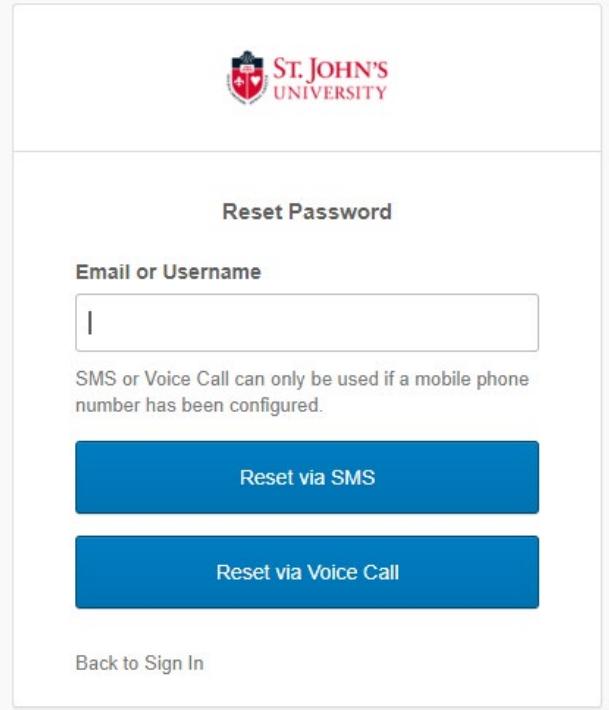
If you have forgotten your password, please visit signon.stjohns.edu and follow the instructions below to reset your password via Self-Service Password Recovery.

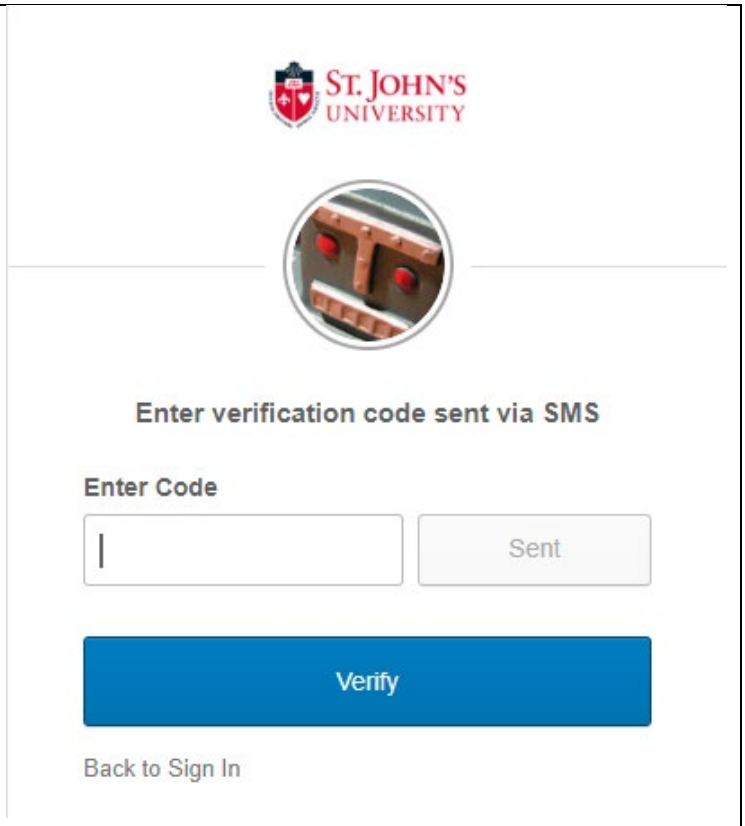
Step 1: To recover your password, please Click on the "Need help signing in?" link.	

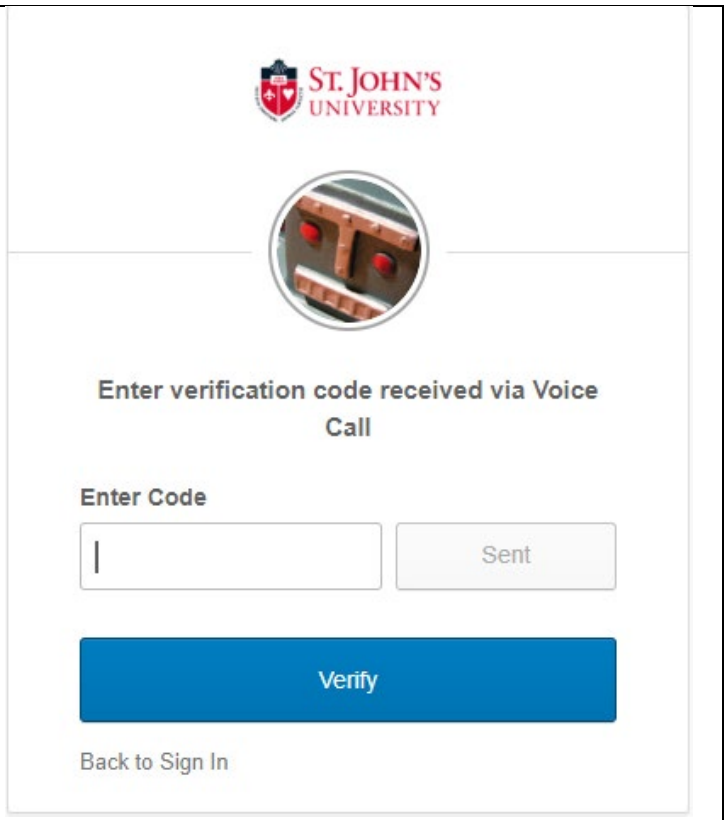
Step 2: A menu of options will appear below this current link. Please click the “Forgot password?” link.	

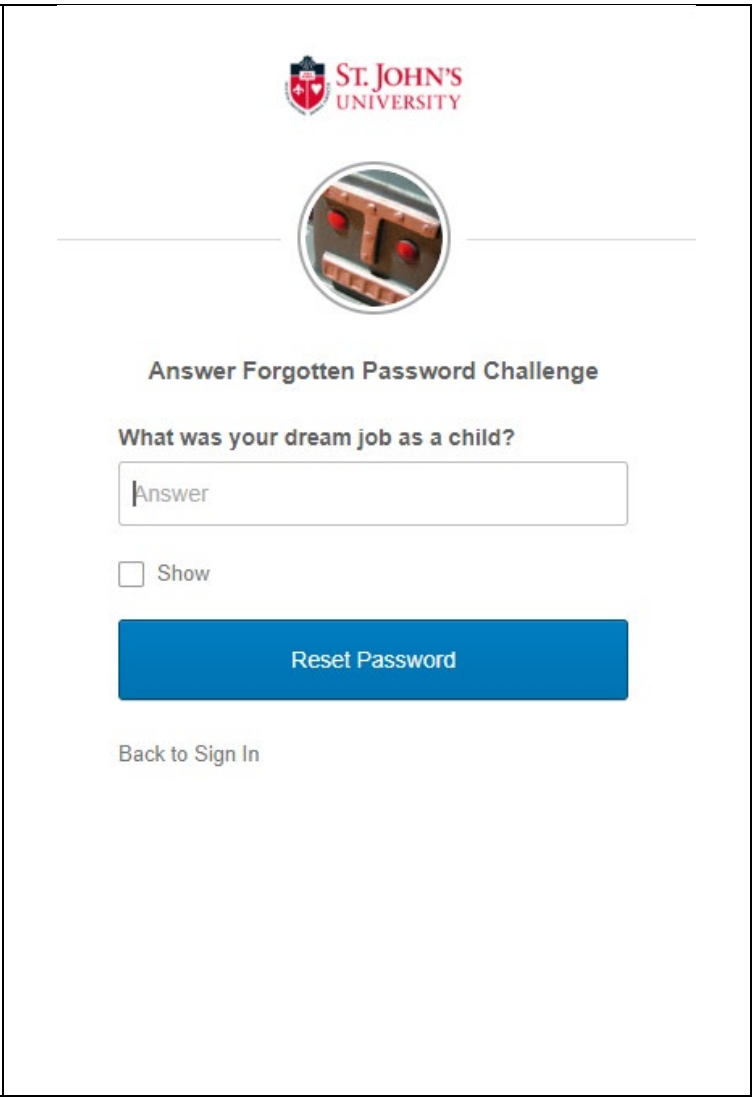
Step 3: Enter your e-mail address or username and choose your reset method:

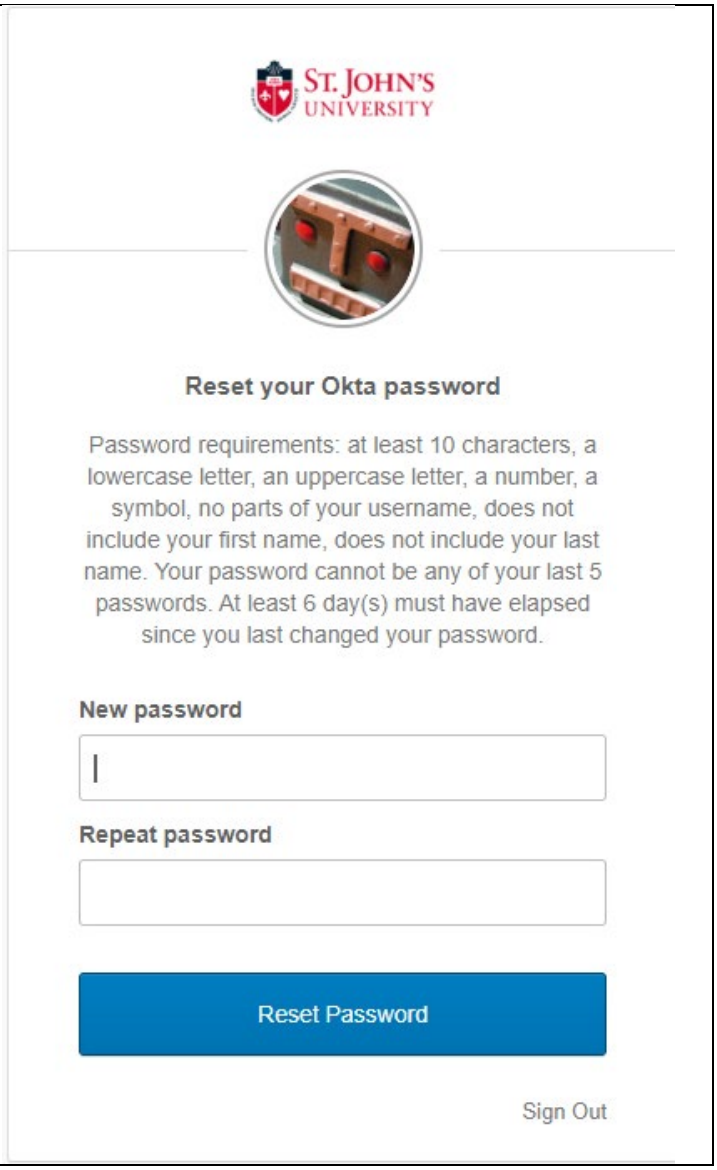
- Click “Reset via SMS” for text message or
- Click “Reset via Voice Call” for a phone call.



Step 4a: For SMS verification, you will receive a six digit verification code. Enter the code from the text message and Click “Verify”.	

Step 4b: For Voice Call verification, you will receive a phone call where a five-digit code is spoken. This code will be repeated twice and then the call will disconnect. Enter the five-digit code and Click “Verify”.	

Step 5: Answer the Forgotten Password Challenge and Click “Reset Password”. *You set up this forgotten password challenge during the initial setup of your account. If you have forgotten your password challenge answer, please contact the Service Desk at 718-990-5000 (x5000) for assistance in resetting your Forgotten Password Challenge.*	

Step 6: Please read the password requirements and enter your new password in the “New password” field. Then enter the same password in the “Repeat password” field and click “Reset Password”.	

Step 7. You will be logged in and you now can access your applications. *Please note, that your password needs time to synchronize throughout all your St. John's accounts and this can take up to 15 minutes to access other applications that are not in the sign-on portal.*	

REFERENCE

Knowledge article: *164134952*
Date: May 20, 2020