NU SSO | Multi-Factor Authentication – Students

The purpose of this document is to provide National University student Single Sign-On users with instructions for how to configure and use Multi-Factor Authentication.

Contents

Multi-Factor Authentication Overview

Multi-Factor Authentication (MFA) is an additional authentication mechanism used in addition to your username and password in order to verify a user's identity. Because National University uses Okta as its SSO solution for its software systems, some of which contain sensitive financial, educational, and personal information, we want to ensure that the users accessing these systems are authorized to do so.

Available MFA Factors

There are currently 4 MFA factors available to students. Okta Verify, Google Authenticator, SMS/Text Message Verification, and Voice Call Authentication. Below is an overview of each factor. Detailed setup steps for each will additionally be provided. While only one additional factor is required, multiple factors can, and should be setup for redundancy should one of your factors become unavailable.

NU SSO | Multi-Factor Authentication – Students

Okta Verify

Okta Verify is mobile app available for iPhone, and Android. Okta Verify is like a standard authenticator app such as Google Authenticator, but it is exclusive to the Okta platform. Every 30 seconds a random 6-digit code is generated. After providing your username and password, you will be asked for the current 6-digit code. Enter the current code to complete the factor challenge. Once downloaded and configured, this factor can work offline and requires no data.

Google Authenticator

Google Authenticator is mobile app available for iPhone, Android, Blackberry and Windows devices. Google Authenticator is a standard one-time password (OTP) protocol authenticator app that many other sites and services support. Every 30 seconds a random 6-digit code is generated. After providing your username and password, you will be asked for the current 6-digit code. Enter the current code to complete the factor challenge. Once downloaded and configured, this factor can work offline and requires no data.

SMS/Text Message Verification

With SMS/Text Message Verification, after providing your username and password, a text message will be sent to the phone number specified during setup with a randomly generated code. Enter the code to complete the factor challenge. Text message and data rates may apply.

Voice Call Authentication

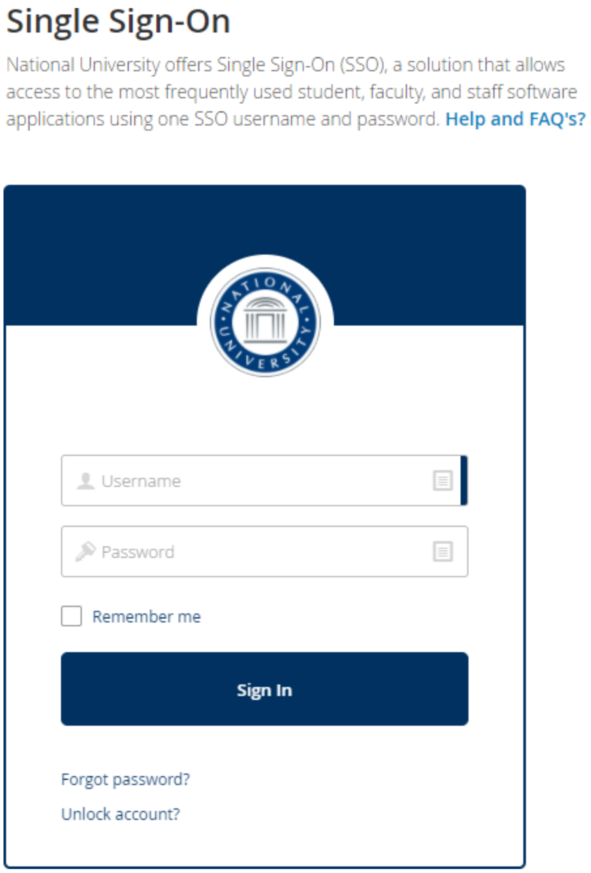
With Voice Call Authentication, after providing your username and password, a phone call to the phone number specified during setup will provide a randomly generated code. Enter the code to complete the factor challenge. Voice call and data rates may apply.

NU SSO | Multi-Factor Authentication – Students

Multi-Factor Authentication Setup Process Overview

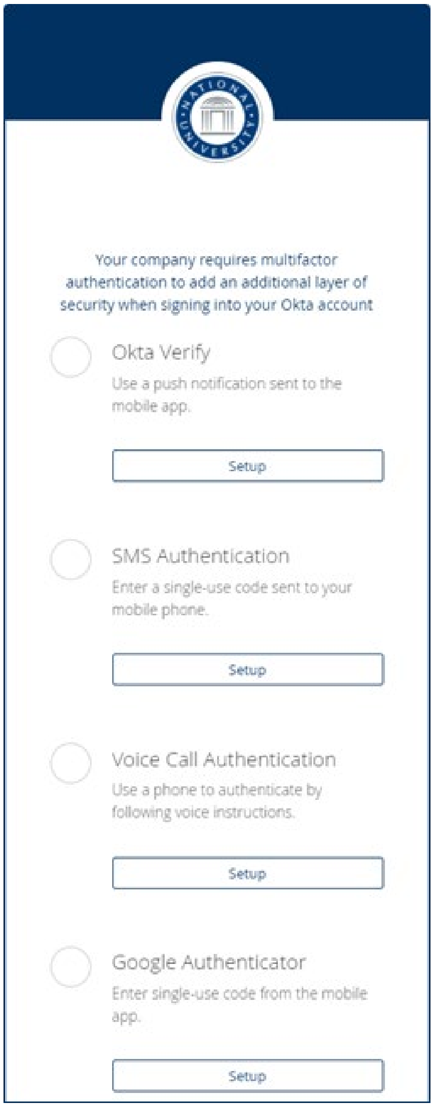
- Login to SSO by navigating to https://login.nu.edu.
- After performing the initial account setup process the **“Extra verification is required for your account”** page will be displayed.
- Select a desired MFA factor to configure.
- Complete the factor setup steps.
    - Detailed enrollment steps for each available factor will be provided below.
- Once a factor is setup, the authentication process is simply providing your username and password, with the addition of providing your second factor.

Note: You can forego MFA prompts for up to 7 days after successfully authenticating in with your factor. To do this, check the **“Do not challenge me on this device for the next 7 days”** box when completing the MFA challenge. This is exclusive to the device and browser session in which it was saved.



Single Sign-On

National University offers Single Sign-On (SSO), a solution that allows access to the most frequently used student, faculty, and staff software applications using one SSO username and password. Help and FAQ's?



Your company requires multifactor authentication to add an additional layer of security when signing into your Okta account

○ Okta Verify
Use a push notification sent to the mobile app.

○ SMS Authentication
Enter a single-use code sent to your mobile phone.

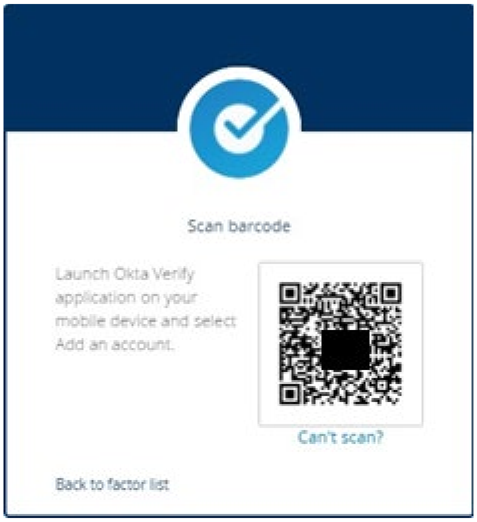
○ Voice Call Authentication
Use a phone to authenticate by following voice instructions.

○ Google Authenticator
Enter single-use code from the mobile app.

Okta Verify

To begin the setup process, select **Setup** under the **Okta Verify** extra verification option:

- From your mobile device, follow the instructions to download and install the **Okta Verify** app, and then click **Next**.
- Configure the Okta Verify app to link it to your Okta account.
  - This can be done by scanning a QR code or manually entering a code.



Scan barcode

Launch Okta Verify application on your mobile device and select Add an account.

Setup Using QR Code

- On your phone, start the Okta Verify app, tap **Add Account** on iOS, or **+** on Android.
- Scan the QR code displayed on your computer screen using the device camera.
- Enter the generated code in the setup prompt to complete the enrollment process.

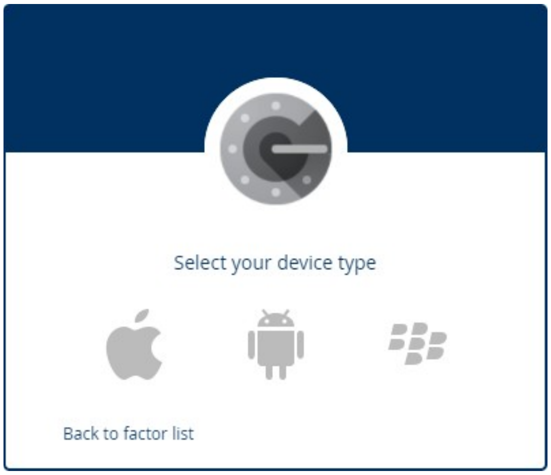
Manual configuration

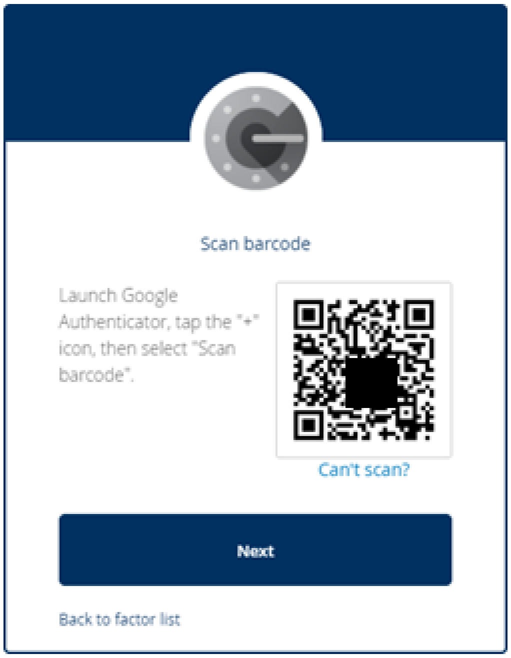
- On your mobile device, start the Okta Verify app, then tap **Add Account** on iOS, or **+** on Android.
- From the barcode page, tap **No barcode?**.
- In the **Okta Account** field, enter your SSO username.
  - 9-digit@student.nu.edu
- From your computer, click the **Can't scan the QR code** link to obtain the secret key which you enter in the **Secret Key** field on your mobile device.
- Tap **Save**.
- Enter the generated code in the setup prompt to complete the enrollment process.

Google Authenticator

To begin the setup process, select **Setup** under the **Google Authenticator** extra verification option:

- Select your mobile device, follow the instructions to download and install **Google Authenticator**, and then click **Next**.
- Configure Google Authenticator to link it to your Okta account.
  - This can be done by scanning a QR code or manually entering a code.





Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".

Setup Using QR Code

- On your mobile device, start Google Authenticator and select **Scan a barcode.**
- Scan the QR code displayed on your computer screen using the device camera.
- Click **Next**.
- Enter the generated code in the setup prompt to complete the enrollment process.

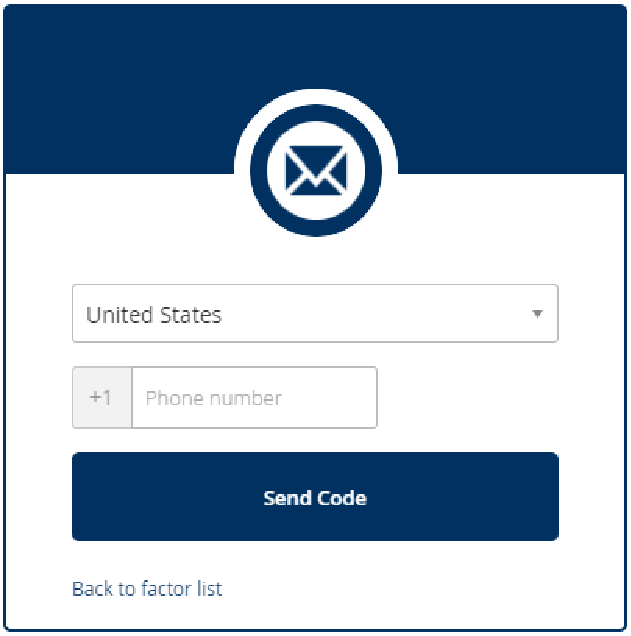
Manual Configuration

- On your mobile device, start Google Authenticator and select **Enter a provided key.**
- In the **Account name** field, enter your SSO username.
  - For example, 9-digit@student.nu.edu
- On your computer, click the **Can't scan** link so that you can access the secret key and enter it in the **Key** field.
- Click **Done**.
- Enter the generated code in the setup prompt to complete the enrollment process.

SMS/Text Message Verification

To begin the setup process, select **Setup** under the **SMS Authentication** extra verification option:

- Enter the mobile phone number where you want your security tokens sent.
- Click **Send Code.**



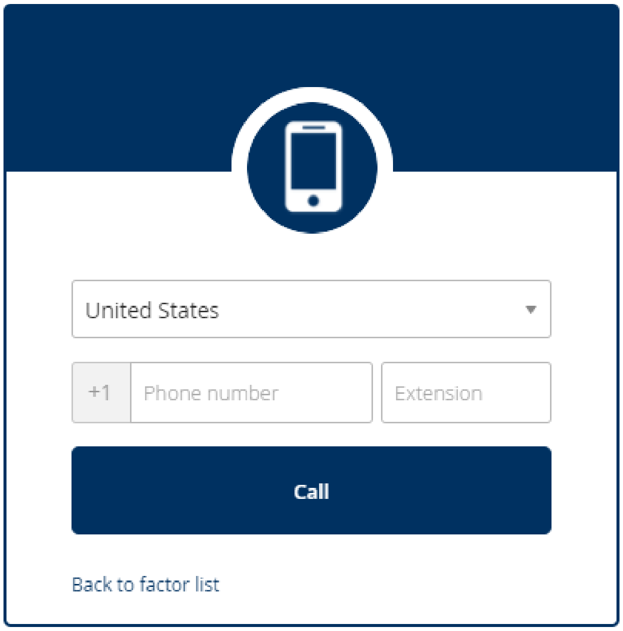
- You will receive a text message containing a verification code to the number specified.
- Enter the verification code that was sent to your phone.
- Click **Verify.**

Note: Standard text messaging and data rates may apply for this method.

Voice Call Authentication

To begin the setup process, select **Setup** under the **Voice Call Authentication** extra verification option:

- Enter the mobile phone number where you want your security tokens sent.
- Click **Call.**



- You will receive an automated voice call that will provide a verification code to the number specified.
- Enter the verification code provided by the automated voice call.
- Click **Verify.**

Note: Standard voice call and data rates may apply for this method.

Troubleshooting

For additional information or assistance, please contact the IT Helpdesk at (858) 309-3580 or helpdesk@nu.edu.