Information Technology Services

[Version 2.0 - Updated 07.09.2021]

UNE will begin using Multifactor Authentication (MFA) which requires a secondary verification after your password, either through the OKTA Verify app or SMS/Text messages. This increased security helps to protect your account and UNE.

SETTING UP MULTIFACTOR AUTHENTICATION

Starting on your desktop, go to https://okta.une.edu

NOTE: The "https://" is required. If you do not include it, you will be redirected to https://une.okta.com. This is by design.

After entering your password, go to your settings in the top right corner of the screen.

At the bottom right of the settings pages, you will find your Extra Verification options.

- Depending on how recently you logged in and your IP address, you may see Edit Profile button that you must click before editing your Extra Verification. This is normal.

Follow the steps below for either OKTA Verify (recommended) or SMS

OKTA VERIFY

If you click Setup under OKTA Verify, you will be asked to specify your phone’s operating platform & then prompted to download the app from the platform’s app store.

Download the OKTA Verify app from your app store

Click through the app’s initial set up screens

Choose Organization as Account Type

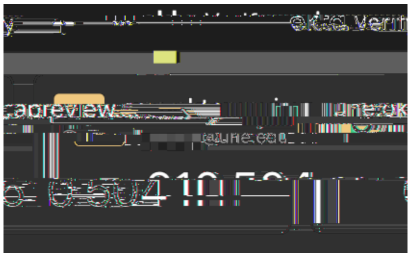
LOGGING IN WITH MFA

Once you've set up your Multifactor Authentication, you will go through the process you've chosen each time you login. After entering your password, you'll see the steps below (according to the verification used).

OKTA VERIFY

When logging in using OKTA Verify, you will receive a notification from the app when you sign in.

If OKTA Verify is already open and past the Yes, It's Me screen, you may also use a code shown within the app that changes every 30 seconds. The amount of time lapsed is shown in a blue bar across the top of the screen.



Okta Verify
@une.edu