

Customer Center & Partner Portal MFA/Security Method FAQ  
Summer 2025

## Table of Contents

What is MFA/Security Method? .....	2
Why is MFA being implemented? .....	2
Can I or my institution opt out of MFA? .....	2
What are first and second factors? .....	2
What MFA second factors are supported? .....	2
Can I have more than one factor and can I use different devices? .....	3
What if I don't have a smartphone or I choose not to use my personal device? .....	3
Do I have to use all of the factors? .....	3
What if I have questions about setting up MFA or troubleshooting issues? .....	3
What if I previously setup MFA? .....	3
Setup steps: .....	4
Setup Google Authenticator .....	6
Setup Email Authentication .....	8
How long does it take to setup the factors? .....	9
What if I lose my smartphone, have a new phone or its' out of charge, how to I reset my second factor? .....	11
Who can help me setup my factors? .....	12

*Important consideration: MFA Security Method enrollment occurs once. If you think there is a possibility you may want to use other factors you MUST set them up initially. Once enrollment is complete the only way to adjust is to create a support case and the team will remove your factors and you can re-establish.*

## What is MFA/Security Method?

Multifactor Authentication (MFA) Security Method is an authentication approach that requires the user to provide two or more verification factors to gain access to a resource such as an application or online account. Within the application and various components it is also referred to as “Security Methods”.

## Why is MFA being implemented?

In order to provide the most secure experience for our customers and partners, MFA is being implemented for all.

## Can I or my institution opt out of MFA?

MFA applies to all customers and partners. An individual or an institution cannot opt out of MFA.

## What are first and second factors?

For the Customer Center and the Ellucian Partner portal, the first factor is your username and password. The second factor is one you can select and configure yourself using a device or account that is linked specifically to you.

## What MFA second factors are supported?

The factors that are supported are:

- Email verification
- Google authenticator app
- OKTA verify app

The criteria in determining the supported factors were determined by Ellucian security standards and policy, guidelines from the StateRAMP initiative and industry best practices.

\*\*\*Note: Ellucian may adjust the supported factors given the always changing guidelines in the security arena. The most secure second factor is an app on a smartphone.

## Can I have more than one factor and can I use different devices?

You may choose to setup all three factors if you wish. You may set them up on one device or you may choose multiple devices, for example your smartphone or tablet and/or an institution issued device or a combination of the two.

## What if I don't have a smartphone or I choose not to use my personal device?

"Email Authentication" is a second factor that does not require a smartphone.

## Do I have to use all of the factors?

You may use more than one factor if you wish, but only one is required. ***Once you complete the initial second factor setup you will no longer be prompted to setup other factors, so complete all factor enrollment during initial setup.***

## What if I have questions about setting up MFA or troubleshooting issues?

If you have any questions about MFA setup and configuration you can send an email to: [csenablement@ellucian.com](mailto:csenablement@ellucian.com)

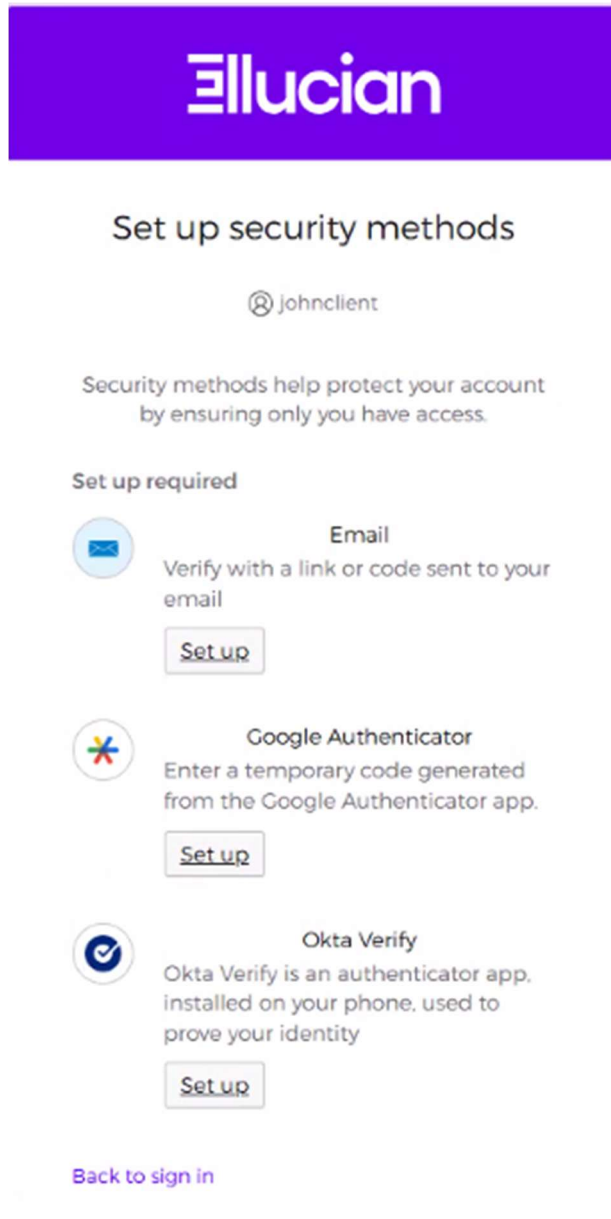
## What if I previously setup MFA?

If you previously setup MFA you won't have to reestablish it again. However, if you wish to add additional factors you may contact [csenablement@ellucian.com](mailto:csenablement@ellucian.com) and the team can reset your account so that you can recreate your MFA factors.

***NOTE: If your factors are reset you should delete the previous factors entries in Google Authenticator and/or OKTA Verify to avoid any confusion about the valid MFA factors.***

## Setup steps:

Once MFA has been enabled, the first time you sign in, you will be prompted to setup your factors. Once you complete the enrollment process you will proceed to the Customer Center/Partner Portal homepage. For subsequent logins, the MFA prompt will occur after you enter your username and password on the login widget.






**Ellucian**

### Set up security methods

@ Johnclient

Security methods help protect your account by ensuring only you have access.

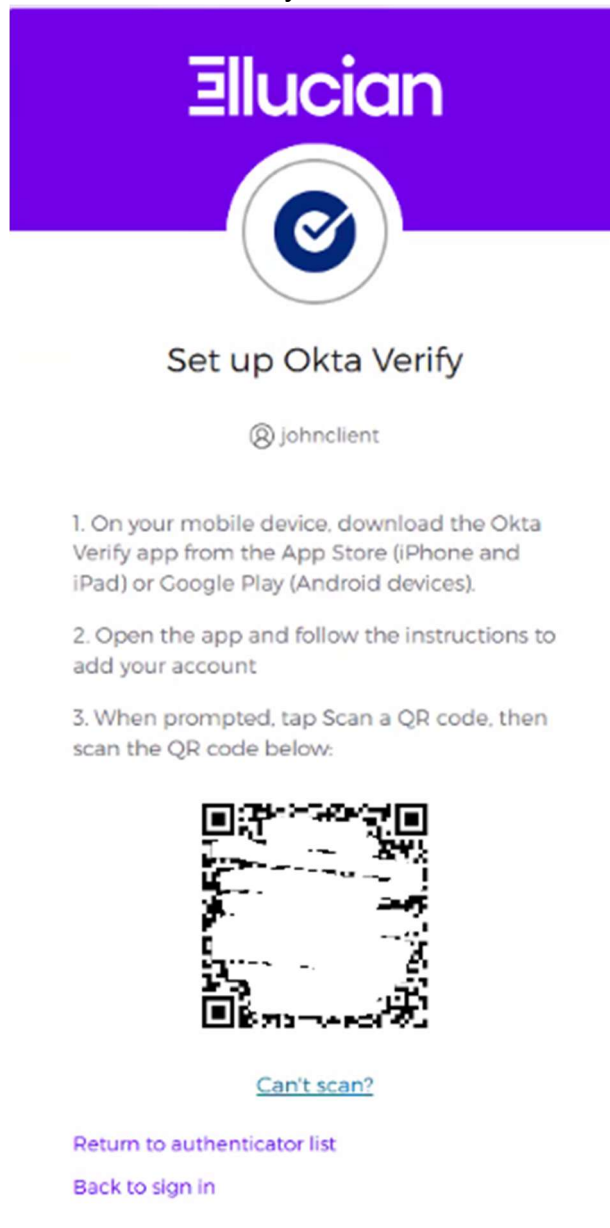
**Set up required**

-  **Email**  
Verify with a link or code sent to your email  
[Set up](#)
-  **Google Authenticator**  
Enter a temporary code generated from the Google Authenticator app.  
[Set up](#)
-  **Okta Verify**  
Okta Verify is an authenticator app, installed on your phone, used to prove your identity  
[Set up](#)

[Back to sign in](#)

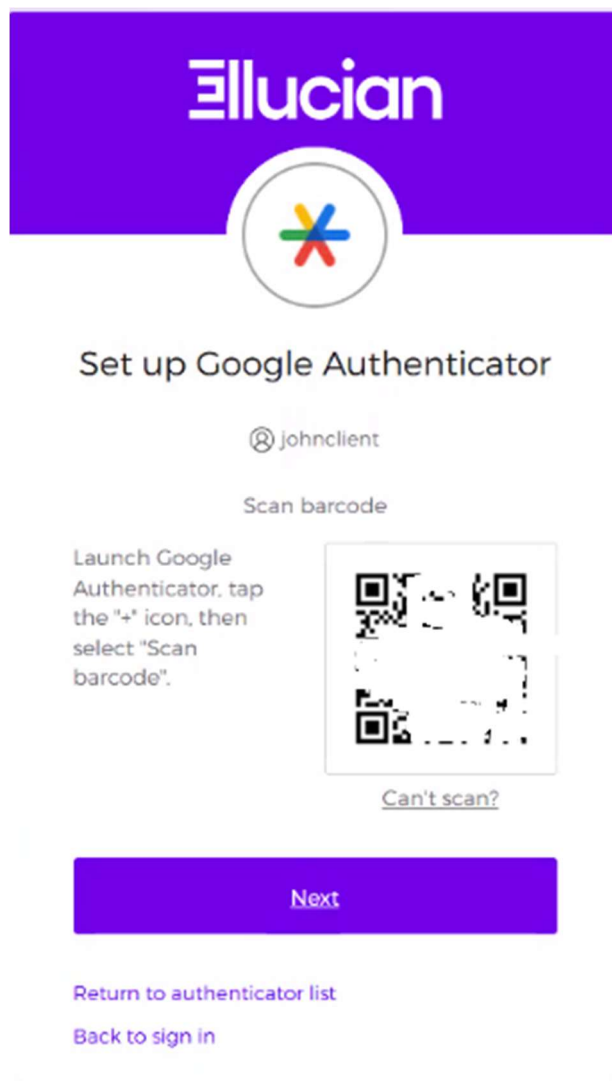
## Setup Okta Verify

Download the OKTA Verify app from the relevant app store unless you already have it installed on your device



The factor will be listed in the Okta verify app labeled “sso.ellucian.com”

## Setup Google Authenticator



Download the Google Authenticator app from the relevant app store unless you already have it installed on your device. The factor will be listed in the Google Authenticator app labeled "sso.ellucian.com"



## Set up Google Authenticator

 johnclient

Enter code displayed from application

Enter code

[Verify](#)

[Return to authenticator list](#)

[Back to sign in](#)

## Setup Email Authentication



Verify with your email

@johnclient

 Haven't received an email? [Send again](#)

We sent an email to \*\*\*\*@\*\*\*\*.com. Click the verification link in your email to continue or enter the code below.

[Enter a verification code instead](#)

[Return to authenticator list](#)

[Back to sign in](#)

An email will be sent to the email that you used to register your account.



---

Ellucian - Action Required: Confirm your email address

Hi 

You are receiving this email so we can confirm this email address for your account.

Please use the following one-time code to complete verifying your email address:

004427

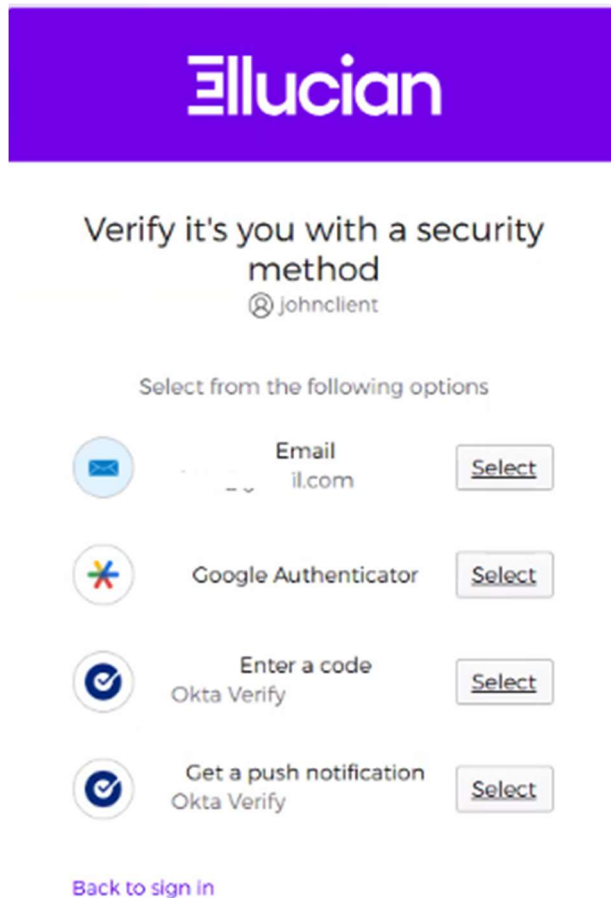
If you believe you have received this email in error, please reach out to your system administrator.

## How long does it take to setup the factors?

It should only take 10 minute or less to complete factor enrollment. **NOTE:** Do not stop and pause during the enrollment process. If you are idle for 5 minutes, the process will timeout and you will have to start over. Once you have one or more factors established you can select which one to use at the time of login.

## MFA/Method Prompt During Login





After you enter your Username/Password, the below screen will appear, giving you the opportunity to select the factor/method you wish to use for that logged in session.



**Ellucian**

Verify it's you with a security  
method  
@johnclient

Select from the following options

	Email johnclient@ellucian.com	<a href="#">Select</a>
	Google Authenticator	<a href="#">Select</a>
	Enter a code Okta Verify	<a href="#">Select</a>
	Get a push notification Okta Verify	<a href="#">Select</a>

[Back to sign in](#)

## What if I lose my smartphone, have a new phone or its' out of charge, how to I reset my second factor?

### Primary option: Zoom Id Verification

1. Contact [csenablement@ellucian.com](mailto:csenablement@ellucian.com) or create a support case. Select the product line = Customer Success, product = Multifactor. (If you email us, a case will be created for you)
2. In both scenarios a member of our Customer Experience Center will contact you
3. A Zoom link will be created and shared with you and once logged into the zoom, your video camera must be on.
4. Be prepared to speak to the support agent and show one of the following forms of identification containing your name and photo: State, province or international driver's license, government issued passport, global entry card, other state, province or country issued identification.
5. Once the support team member has validated your identity an email will be sent to the email address on file for the account you are looking to reset.
6. Upon receipt of the email, please respond to the agent with a "confirmed"
7. The agent will at that point re-set your factors so that you may proceed to Sign In.

### Secondary option: Institution confirmation of your identity

1. If for whatever reason you choose not to or are unable to verify via Zoom, we can contact your institutions' Technical Security Contact(s).
2. Contact [csenablement@ellucian.com](mailto:csenablement@ellucian.com) or create a case if you have access rights to create cases. Select the product line = Customer Success, product = Multifactor. (If you email us a case will be created for you)
3. In both scenarios a member of our Customer Experience Center will contact you
4. A support team member will email the Technical Security Contact (TSC) at your institution for verification of identity.
5. The support team member will provide the TSC to you so that you may follow up if necessary.
6. Upon verification your factors will be reset, and you may proceed to re-establishing your second factor.

## Who can help me setup my factors?

If you have any questions or need assistance with your factor setup, you may email us at: [csenablement@ellucian.com](mailto:csenablement@ellucian.com)

**\*\*Support Note:** *Ellucian will provide support on MFA issues related to the three currently supported second factor options (Google Authenticator, Email and OKTA Verify).*

*We cannot support other combinations of MFA such as DUO or other OTP devices used in combination with Google Authenticator, Email or OKTA Verify.*

*If access issues arise as a result of a non-standard configuration, the Ellucian support team can reset the second factor indicator on your account and you will be able to reestablish your MFA/Security Methods.*