



# MULTIFACTOR AUTHENTICATION FOR HIGHER EDUCATION

Balance Between Access and Security



## OVERVIEW

Student Data Privacy Laws require all higher ed institutions to enforce complete protection of student information records. While you may have put standard procedures and solutions in place to assist in these efforts, sometimes, this is not enough. Colleges and universities have become prime targets for ransomware attacks as many attackers have realized the value of a student's personal information.

## WHAT IS MFA?

Multifactor Authentication (MFA) is a security process that requires two or more separate steps for a user to prove their identity. A combination of requirements allows the user to gain access to these resources. At the higher education level, this combination of criteria is described as something your student knows (login credentials), something they have (cell phone, One-Time Password (OTP)), and their location (on-campus).

Pairing MFA with Single Sign-On (SSO) provides an extra layer of security that dramatically decreases the risk of a ransomware attack on your college/university.

HelloID, Tools4ever's comprehensive cloud-based solution, provides a dashboard accessible by SingleSign-On and protected with the most current and advanced MFA options on the market. HelloID MFA options include Email, SMS, FIDO2, Push to Verify, OTP, etc.

HelloID already integrates with many Student Information Systems, including Ellucian. Furthermore, HelloID's Multifactor Authentication can be configured at the dashboard and individual application levels to protect your student data securely.

# HOW DOES IT WORK?

Multifactor Authentication requires that a combination of criteria need to be met in order for the user to gain access to their resources. MFA typically combines two or more of the following to enforce strict security during logins.



# PROTECT STUDENT DATA

Many colleges and universities have already implemented SSO solutions to help mitigate some of these security threats. With SSO, once the student has confirmed their identity using for example a smart card and PIN code, the required applications are loaded, and they will be logged in by the SSO solution automatically. This allows for students to have the benefit of additional security without the headache of completing the login process for each system or application. Additional security can be added by configuring SSO so that if the student walks away and the workstation locks, other users will not be able to log in.

By using SSO, higher ed institutions are tightening up the potential points of entry by limiting all access to a single spot. With one centralized portal for data, colleges and universities enforce strict access control and complex password policies that bolster security.

## ADVANTAGES OF MFA

There are many advantages to implementing multifactor authentication into your institution.

- 1 INCREASED PROTECTION**  
Implementing MFA provides an extra layer of security that dramatically decreases the risk of a ransomware attack.
- 2 OPTIONS TO CHOOSE FROM**  
There are many different types of MFA that your institution can choose from such as Push to Verify, Securty Key, or a Token.
- 3 PAIR WITH SINGLE SIGN-ON**  
MFA can be used in conjunction with Single Sign-On (SSO), so that students don't have to complete this process for each application.

