SOLUTION BRIEF

Passwordless MFA for
Higher Education Institutions

Removing vulnerable passwords with a phishing-resistant multi-factor authentication (MFA) stops the attacker's ability to exploit passwords and phish users.

- Delight students and staff with a streamlined passwordless MFA login
- Works with existing password apps and directories
- Eliminates password help desk calls

- Fast to start: It takes just an hour to configure and start onboarding users
- Low-cost site license to match dynamic student population
- Measurable ROI in the first year

Improve Security, Delight Students and Staff

Universities are one of the top 10 most attacked sectors in every cyberattack research report. However, IT leaders must balance security with student and staff academic freedom needs. After all, students become donor alumni, and educator-led grants build prestige for future growth.

Doing away with user passwords is the one affordable thing you can do for your institution that improves security, delights users, reduces operating friction, and pays for itself in the first year with measurable returns on investment (ROI).

Passwordless MFA Slashes the Attack Surface

IT leaders are realizing the MFA programs they have underway aren't good enough to stop the phishing threat. The Octopus passwordless MFA platform removes vulnerable passwords from the user's login process. Using a phishing-resistant approach, Octopus slashes the attack surface by shutting down attackers' ability to exploit passwords and phish users.

Passwordless MFA Pays for Itself in the First Year

Higher Education IT is known for being underfunded and overworked. That makes sense, as the business of Higher Ed is education, not IT. Therefore, their IT leaders need to innovate with high ROI modernization initiatives.

Passwordless MFA is less: less steps for the user, less work for IT, less risk with the Octopus, but more security with high ROI. But "less is more": Stronger security, a better user experience (UX), and a financial payoff that comes from making staff and admins more productive.

How it works

Octopus passwordless MFA works with existing applications and directories, supporting the broadest use cases to meet the needs of students, staff, and IT alike. Use cases include fulfilling regulatory and cyber insurer criteria for local privileged user desktop MFA and strong authentication for every network access from university-managed assets and students' BYOD devices.

							Method	Phishing Resistant
Desktop	Mac	Windows	Linux	Shared	BYOD (Bring Your Own Device)		Mobile Push	✓
Workforce Apps & Services	Cloud/ Mobile SSO	Remote VPN	Remote VDI	Custom/ Legacy	Air Gap		FIDO2	✓
							Smartcard	✓
Privileged Access	>_SSH SSH	>_ PsExec/WMI/ PowerShell	⋝ RDP				OTP **** Traditional MFA	
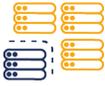
Octopus Passwordless MFA Use Case and Method Flexibility

Benefits

- Flexible deployment: Octopus Cloud SaaS or self-managed on-premises
- Simple integration: Works with existing directories, no rearchitecting infrastructure or recoding apps
- Phishing-resistant MFA: FIDO2 tokens, mobile push, and adaptive MFA
- Supports custom and legacy apps

Summary

Passwordless MFA is one of the few technologies that pays for itself right away. Taking password management off users' plates and replacing it with MFA that fits into existing password-centric infrastructure makes the Octopus platform ideal for Higher Ed.

Change always means a leap into the unknown, but passwordless MFA delivers an obvious conclusion: better security, self-sufficient users, and an IT department able to innovate faster without having to coordinate shared secrets with an entire new population every semester.

SECRET DOUBLE OCTOPUS

Learn more at **doubleoctopus.com**