



## Multi-factor Authentication USB Token Frequently Asked Questions

Brad Christ - 2023-09-07 - Comments (0) - Multi-factor Authentication

### **Q.What are USB multi-factor authentication tokens?**

A. Sometimes referred to as usb security keys, a token, when the button is pressed, automatically enters a passcode at the Duo multi-factor authentication prompt.

A variety of tokens are shown here:



### **Q. Can I use a token as my primary multi-factor authentication method?**

A. Yes, but if one or both of the following circumstances are true:

- You have a physical disability that makes using other methods burdensome
- You do not own or have access to a university-owned mobile device

Tokens are only provided to faculty or staff. Students may purchase their own tokens. We recommend Yubikeys, which can be purchased through Amazon.

### **Q. Are there limitations on using a token?**

A. Yes, there are some limitations to tokens.

First, you must be using a device with a compatible USB port and the USB port must not be disabled (some kiosks and computer labs disable USB ports for security reasons). At this time, only USB A tokens are available.

Second, you must use a supported browser. Google Chrome and Opera support tokens natively. Firefox plans to support multi-factor tokens sometime in the middle of 2018.

**Q. How do I obtain a token?**

A. Please contact your [IT Computing Coordinator](#).

**Q. My token is lost, damaged, or stolen. What do I do?**

A. Report damaged, stolen, or lost tokens immediately to the Information Technology department so the token can be disabled. Departments are responsible for any replacement charges.

**Q. I am a departing employee, what do I do with my token?**

A. Much like other university property, you are required to return your multi-factor token.

Departments will be charged for any tokens that are not returned by departing employees.