



Two-Factor Authentication FAQs

Page 1 of 2

VSU Division of Information Technology

Rev. 4/4/2017

Answers to frequently asked questions (FAQs) regarding Valdosta State University implementation of the advanced digital security method known as two-factor authentication (2FA).

1. What is Two-Factor Authentication (2FA)?

2FA provides an extra layer of security to your online accounts by requiring a second form of log-in verification. The authentication process provides a variety of ways for you to access your account, which include requesting a text message or phone call verification or using the Microsoft Authenticator app.

2. Why is VSU implementing 2FA?

While IT's Office of Information Security regularly reviews areas for improvement to bolster proactive security monitoring, 2FA was introduced in response to a growing demand from faculty and staff for additional peace of mind when logging in to their online VSU accounts. Information Security reports more than 300 compromised VSU email accounts in the last two years, 23 of which have been repeat compromises. While we strongly encourage all users to remain vigilant and safeguard personally identifiable information (i.e. 870 numbers and account passwords) at all times, this two-step log-in process prevents attackers from gaining access to email accounts and sensitive academic, financial and human resources information in the event that password credentials are compromised. 2FA has become a best practice at other universities as well as many online email providers and financial institutions.

3. Do I have to authenticate every time I log in?

While on campus, you will have to authenticate each time you log in for the **first seven (7) days after enrollment**. Following the enrollment period, you will only have to authenticate if you log in to **MyVSU** or the **Outlook Web** on the **wireless network or off-campus**. This includes accessing these resources through the V-State Mobile App (please make sure your app is updated to the most recent version). 2FA will **NOT** be required when using the Outlook desktop client (including using the desktop client via remote access) and legacy email clients such as Mail on Apple devices.

4. What if I do not have a cell phone? or I lose my cell phone? or I change my phone number? or I am out of the country?

You can verify your MyVSU account by receiving calls from a designated landline phone and entering your PIN or by answering your security questions. To initiate the security questions prompt, wait 60 seconds after attempting one of the three primary methods and then choose 'Use a different verification option'.

The [Two-Factor Management](#) link on the MyVSU homepage allows you to easily change your authentication method and update your phone numbers.

DIVISION of INFORMATION TECHNOLOGY

LOCATION Pine Hall • PHONE 229.333.5974 • FAX 229.245.4349 • WEB www.valdosta.edu/it • ADDRESS 1500 N. Patterson St. • Valdosta, GA 31698-1095



Two-Factor Authentication FAQs

Page 2 of 2

VSU Division of Information Technology

Rev. 4/4/2017

5. What if I receive an Authenticator mobile app notification when I'm not trying to log in?

This would only happen if someone else was trying to log in to your account, and that person knew your MyVSU password. The Authenticator mobile app notifications are only sent after the username and password are entered and verified. So, if this happens, two-factor authentication has just saved your account from illicit access! To report the incident, you can press the **'Deny and Report Fraud' button** in the app and future authentication attempts will be blocked until the issue is resolved. [Contact VSU Solutions Center](#) for additional assistance.

[Visit Information Security site to learn how to create a more challenging password.](#)

6. Can I write my own security questions or change my answers?

No, you cannot write your own questions; but you can log in to the [Two-Factor Management](#) portal at any time to change your question options (*and answers*) by selecting 4 questions out of 11 prescribed questions. Note, when attempting to log in to MyVSU using the question method, you will only be prompted to answer two of your selected four questions.

7. Can 2FA be configured to run on a Mac computer or Apple device?

Yes, and you should not experience compatibility issues when using a Mac computer or Apple device. 2FA is web/server-based and applies when you attempt to log in to your MyVSU account via a web-based app or web browser, including Apple's Safari web browser, when you are off campus or are using VSU WiFi. Additionally, the optional Microsoft Authenticator App is designed for both iPhones and iPads and is available for download at the [iTunes App Store](#).

For Android devices, you can download the Microsoft Authenticator app at [Google Play](#).

8. What if I already have an authenticator app (i.e., Google Authenticator) installed on my device?

If you choose to be contacted via the app, you will need to install the Microsoft Authenticator App for MyVSU login to be successful. You, of course, can still use your existing authenticator app as you had before for other applications. Once you have installed and setup the Microsoft Authenticator, you will not need to interact with it again or even have the App open on your device(s) in order to receive the verification prompts. Note, if you log in to MyVSU using multiple mobile/tablet devices, you will need to install MS Authenticator on each.

9. Where can I find additional information on the 2FA process?

For more information, visit the 2FA webpage at <http://www.valdosta.edu/administration/it/helpdesk/2FA.php>.