OFFICE OF INFORMATION TECHNOLOGY

OFFICE 365 MULTI-FACTOR AUTHENTICATION FAQ

Revised 12-3-2020

What is multi-factor authentication?

Multi-factor authentication provides an additional layer of security to protect your Salve Office 365 account credentials from unauthorized access. In addition to your username and password, a confirmation request is sent to a trusted device that a login is being attempted on your account. Once you use your preferred method of multi-factor authentication you will have access to your account. This login method confirms your password and another form of authentication to prove who you are and protect your identity.

Why is Salve enabling multi-factor authentication?

The University has seen an increasing number of attacks on faculty, staff, and student user accounts over the last few years. While the University has invested in and implemented several security tools that have reduced the amount of attacks and their effects, attacks are still occurring, and their sophistication continues to increase. Multi-factor authentication is a more proactive approach to security, where the end-user will automatically receive a notification when a new device attempts to login with a Salve username and password to any Office 365 services. If an end-user receives a multi-factor authentication request and is not attempting to logon actively to a new device, suspicion is raised, and action can be taken quickly by the end user or the Office of Information Technology if the logon is determined to be from an unauthorized person or device.

What services will be protected by multi-factor authentication?

The following services and applications are protected by multi-factor authentication, when enabled:

- All web-browser logins to the Office 365 web site (ie office.com, outlook.office365.com, etc).
- Microsoft Outlook 2016 for Mac/Windows when configured with a Salve e-mail account.
- Microsoft One Drive.
- Microsoft Office 2016 for Windows/Mac applications (Word, Excel, PowerPoint, etc) when configured to connect to Office 365 services, such as One Drive for Business.
- Microsoft Office apps for iOS and Android, when connected to your Salve e-mail/Office 365 account.
- Apple Mail/Contacts/Calendars apps in iOS 11 or later.
- Canvas
- Zoom
- Webex
- Campus.salve.edu

Other Salve online services, such as Portal, Colleague, etc, will not require or implement multi-factor authentication at this time.

Will a multi-factor authentication challenge occur every time I login?

When multi-factor authentication is first enabled, a challenge will occur on all the devices and applications that have your Salve Office 365 credentials configured. In the pop-up window that shows up during the multi-factor authentication process, you can authorize an application or web browser to be trusted and not require a re-authorization for 60 days.

When a login to Office 365 from a new device, application, or web browser that hasn't already been challenged occurs, you will receive a multi-factor authentication challenge at that time. You may also receive a challenge on a device that you have logged on with before if it occurs from a new location on the Internet that Microsoft considers unusual or suspicious.

Will multi-factor authentication challenges occur while I'm on campus?

Initially, multi-factor authentication challenges for Office 365 will occur regardless of whether you are on or off campus. After the multi-factor authentication roll-out has been completed for members of the University, on-campus challenges will be reduced or eliminated for devices connected to the Salve campus network. We will be working to reduce the number of challenges that occur when on-campus as quickly as possible.

How do I setup multi-factor authentication on my account?

The Office of Information Technology will enable multi-factor authentication on your Salve account. Once it has been enabled, you will be requested to setup "Additional Security Verification" on Microsoft's Office 365/Azure portal the next time a login occurs. Multi-factor authentication can occur through a combination of the following methods:

- An SMS text message with a numeric code to your mobile phone.
- A phone call to a mobile phone or other phone number of your choosing.
- A code or notification sent to the "Microsoft Authenticator" app installed on an iOS, Android, or Windows 10 device.

The Office of Information Technology recommends enabling and configuring as many methods as possible to complete multi-factor authentication, in the event of your preferred method is unavailable during a challenge event. We believe most end users will be content with the SMS text message or Microsoft Authenticator app options as their default method for completing multi-factor authentication challenges from Office 365.

How do I change my initial multi-factor authentication settings?

If at any point you want to change your multi-factor authentication settings, such as the phone number you receive alerts at, or updating the device and settings the Microsoft Authenticator app uses, you can go to this address:

https://aka.ms/setupsecurityinfo

Additional instructions are provided on the Setup Security Info page based on the selection of options you want to update or change.

Can I configure the Microsoft Authenticator app on multiple devices?

Yes. You can configure the app to provide codes and notifications on multiple devices at the same time.

I'm receiving multi-factor authentication challenges, but I'm not trying to use any Office 365 services at this time, what should I do?

Most applications and devices require a multi-factor authentication challenge once every 60 days. There may be a device that you are not near that requires re-authentication. In addition, there's always the possibility that someone else is attempting to login to your account in an unauthorized manner. When an unexpected multi-factor authentication occurs, we would recommend, denying any access (if using the Authenticator app) and then checking all devices you have configured with your Salve Office 365 credentials to see if re-authentication is required at your earliest convenience. If all devices are authenticated and working as expected, we would recommend you change your password as a precautionary measure.

My third-party application for accessing Salve e-mail/contacts/calendars has stopped working since multi-factor authentication has been enabled. How do I fix this?

Multi-factor authentication awareness is built-in to several applications for accessing Office 365 services. Unfortunately, there are some third-party applications, such as Apple Mail/Contacts/Calendars in macOS, Mozilla Thunderbird, and some built-in Android clients, that do not support this feature, including most other mail clients that use SMTP, IMAP, and POP methods for sending and receiving e-mail.

Please note that Salve Regina University officially supports the Microsoft Office application suite on the Windows, macOS, iOS, and Android platforms, and the built-in iOS 11 or greater Mail Contacts and Calendar apps for accessing Office 365 services. Web browsers that are supported by Microsoft for Office 365 can be found here:

https://support.office.com/en-us/article/which-browsers-work-with-office-online-ad1303e0-a318-47aa-b409-d3a5eb44e452

While other applications and browsers may work, support by the Office of Information Technology is limited to best effort. In addition, we have noticed in many cases that third-party applications have been used to bypass Microsoft's security protections in combination with compromised accounts for sending spam and other malicious e-mail. The TSC will work on a case-by-case basis with end users who wish to have a third-party application access Office 365 resources such as e-mail, calendaring, and address books. Please note that the support levels for third party applications, browsers, and older versions of the Office suite is determined by Microsoft and updated regularly.

I would like to learn more about multi-factor authentication, where can I find out more information?

Microsoft has provided several knowledge base articles that go into more detail on the setup and function of multi-factor authentication. They can be accessed at the following link:

Multi-factor authentication overview:
https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-two-step-verification-overview

Security information setup overview:
https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-security-info-overview

If you have any additional questions please reach out to the Help Desk by phone at (401) 341-7777 option 2, or by e-mail at helpdesk@salve.edu.