Microsoft Two-Factor Authentication (MFA or 2FA)

This page is dedicated to information and support for Microsoft Two-Factor Authentication (2FA) at Syracuse University, also referred to as multi-factor authentication (MFA), two-step authentication, or ‘added security verification’ used by services like SUmail and Office 365, managed at msmfa.syr.edu.

Table of Contents

- About Microsoft 2FA
- Available Authentication Methods
- Configuring Your Account - Setup and Management
  - First-time Setup
  - Get The App
  - Set up the Microsoft Authenticator app
  - Modify Existing Microsoft MFA Configuration
- Traveling with Microsoft 2FA including Syracuse Abroad
- Microsoft Support Documents
- Getting Help

About Microsoft 2FA

Microsoft 2FA is currently enabled for all Syracuse University Faculty, Staff, and Students accessing Office 365 applications accessed or downloaded through https://portal.microsoft.com. 2FA is an added verification step during authentication that helps to prevent the unauthorized use of University NetIDs and passwords by ensuring that only the account owners themselves use their credentials on systems hardened with 2FA, in this case, Office 365. Typically, 2FA is described as “something you know and something you have” where the “something you know” is your username and password, and the “something you have” (often called a “second factor”) is a private, unique code generated just for you.

Additional information about two-factor authentication can be found on the Two-Factor Authentication home page. You can manage your security verification methods at at msmfa.syr.edu.

Can’t Use These Methods? If you have any limitations which prohibit the use of the listed methods, please contact the ITS Help Desk by calling at 315-443-2677, by emailing help@syr.edu, or by stopping into 1-227 CST.

Available Authentication Methods

There are current 4 available methods for authenticating with Microsoft 2FA. You can configure or manage your security verification methods at msmfa.syr.edu.

<table>
<thead>
<tr>
<th>Method</th>
<th>Process</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify me through the app</td>
<td>Uses Microsoft Authenticator app to push notification</td>
<td>Recommended option for general use. Allows you to press &quot;Approve&quot; as your second factor.</td>
</tr>
<tr>
<td>Use verification code from app or token</td>
<td>Uses Microsoft Authenticator app to provide verification code</td>
<td>Recommended option for when internet connectivity is unavailable.</td>
</tr>
<tr>
<td>Text code to my authentication phone</td>
<td>Text to mobile device</td>
<td>Country code must be provided and international rates may apply.</td>
</tr>
<tr>
<td>Call my authentication phone</td>
<td>Call to configured phone number</td>
<td>Country code must be provided and international rates may apply.</td>
</tr>
</tbody>
</table>

Configuring Your Account - Setup and Management

Follow the steps below for 2FA configuration.

First-time Setup

DMC and MySlice Financial Applications

Note that this page is intended for use with two-factor authentication related to Microsoft Office 365 products and applications including SUmail. Support for DUO, the two-factor authentication used for the Delegated Management Console (DMC) and MySlice financial applications, can be found on the Installing and Using 2-Factor Authentication DUO page.
Follow the [How To Configure Microsoft Two-Factor Authentication page](#)

**Get The App**

Download and install the Microsoft Authenticator app for [Android](#), [iOS](#), or [Windows Phone](#).

**Set up the Microsoft Authenticator app**

Follow the [6 Steps provided by Microsoft](#) to set up the Authenticator app with your account.

**Modify Existing Microsoft MFA Configuration**

You can manage or update your authentication settings at [msmfa.syr.edu](#).

**Traveling with Microsoft 2FA including Syracuse Abroad**

If you are traveling and plan to access your account, be sure to configure authentication methods you will have available *prior to traveling*. You can manage or update your security verification methods at [msmfa.syr.edu](#).

ITS recommends the mobile application version as it *does not* require an internet connection once configured. Note that for call or text authentication, your mobile device will require service at your destination. Additionally, if you use the office phone method, an alternative method will be required while traveling.

**Going Abroad?**

Syracuse Abroad students should configure their 2FA as soon as possible, download and configure the Microsoft app on their mobile device, and take their mobile device when they go abroad. Configuring before you leave enables your continuing access to protected University accounts regardless of location. Students should ensure their authentication methods function correctly, and should be sure to have their configured mobile device when they go abroad.

**Country Code and Costs**

Please note that country code(s) must be provided for phone options, and standard/international message and data rates apply.

**No Methods Available While Traveling or Abroad?** If you have any limitations which prohibit the use of the authentication methods while traveling, please contact the [ITS Help Desk](#) by calling at 315-443-2677, by emailing [help@syr.edu](mailto:help@syr.edu), or by stopping into 1-227 CST.

**Microsoft Support Documents**

- [How to Use Two-Step Verification with Your Microsoft Account](#)
- [Microsoft Account Security Information](#)

**Getting Help**

For support of the information above, contact the [ITS Help Desk](#) by calling at 315-443-2677, by emailing [help@syr.edu](mailto:help@syr.edu), or by stopping into 1-227 CST.

Microsoft two-factor authentication is active for all Syracuse University students and is required to access Office 365 applications including SUmail. If you are traveling and plan to access your account, be sure to configure authentication methods you will have available *prior to traveling*. You can manage or update your authentication methods at [msmfa.syr.edu](#).

ITS recommends the mobile application version as it *does not* require an internet connection once configured. Note that for call or text authentication, your mobile device will require service at your destination.