



The School District of Osceola County, Florida  
Network and Information Security Department  
Every Child, Every Chance, Every Day



<u>Document Title:</u>	<b>Multifactor Authentication Registration</b>
<u>Responsible Team:</u>	Network and Information Security Department
<u>Intended Audience:</u>	All SDOC Employees
<u>Written By:</u>	Edward Murphy
<u>Written Date:</u>	2021-03-23
<u>Approved By:</u>	Angel Fonseca
<u>Approval Date:</u>	2024-08-07
<u>Revision Date:</u>	2024-08-07

### Summary:

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack. A factor in authentication is a way of confirming your identity when you try to sign in. The four most common kinds of factors are:

- **Something you know** - Like a password or a memorized PIN.
- **Something you have** - Like a smartphone or a secure USB key.
- **Something you are** - Like a fingerprint or facial recognition.
- **Somewhere you are** - Like your geolocation or IP address.

MFA is designed to ensure you are the only one who can access your account — even if someone knows your password. MFA is a proven and effective way to protect against many security threats that target passwords, such as phishing. MFA is a 2-step verification process that requires the use of more than one verification method whenever you are accessing district resources (e-mail, TEAMS, OneDrive, etc.) while away from campus.

For more information, you may visit the following Microsoft articles:

- [Multifactor Authentication First Time Setup](#)
- [Manage Your Security Info](#)





# The School District of Osceola County, Florida Network and Information Security Department

Every Child, Every Chance, Every Day



## Registration Procedure:

To help protect our Office 365 accounts, staff are required to setup additional verification options to help better secure their accounts and resources. Please follow the following steps to register for multifactor authentication.

1. Open a web browser and navigate to your **My Account** page by visiting:  
<https://myaccount.microsoft.com>
2. Staff will sign in with their @osceola.k12.fl.us email:

Microsoft  
Sign in  
[Redacted]@osceola.k12.fl.us  
[Can't access your account?](#)  
Next

3. You may be prompted to provide additional details if you have not already registered for multifactor authentication (MFA):

School District of  
**OSCEOLA COUNTY**  
FLORIDA  
*Celebrating 100 Years of Education Leadership*

[Redacted]

### More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

All users of the network are bound by SDOC policy. Any violation of the policy will result in the suspension of access, privileges or other disciplinary action, including student expulsion and employee, dismissal.



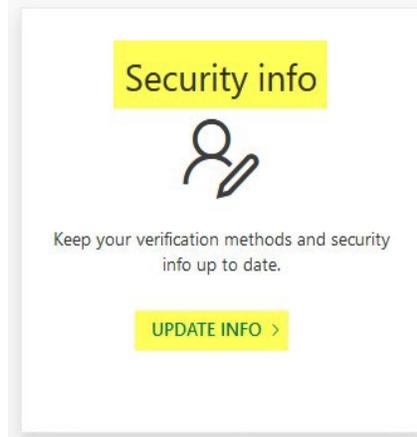


# The School District of Osceola County, Florida Network and Information Security Department

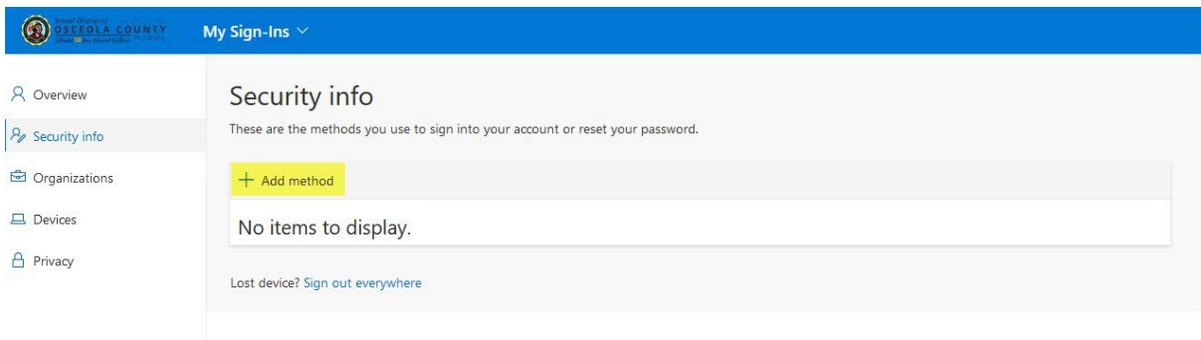
Every Child, Every Chance, Every Day



- Once logged-in, navigate and click on “Security Info” on the left pane.

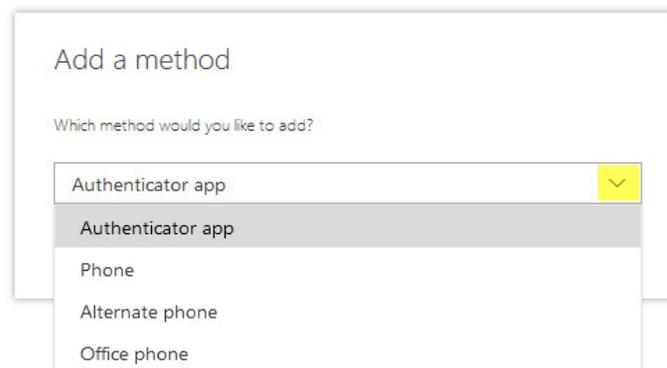


- Under Security Info, select **Add method**:



- Click on the drop-down arrow in the “Add a method” window to select your preferred method to authenticate.

**\*\*\* Please note: The available options may vary slightly as Microsoft updates them, but the general instructions apply. \*\*\***

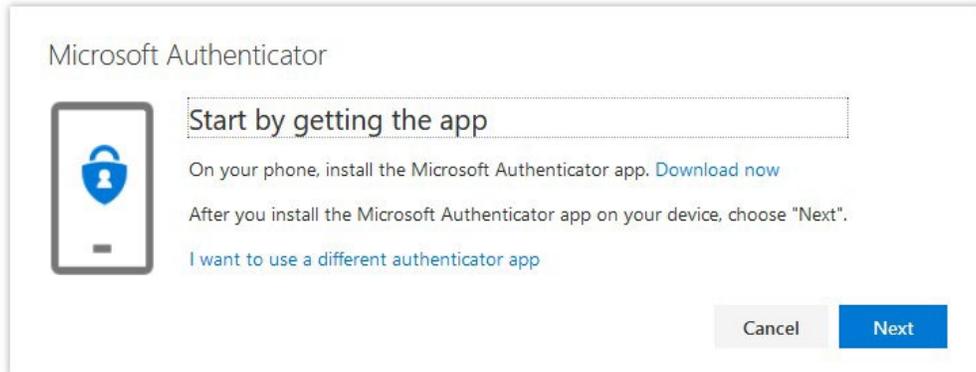




The School District of Osceola County, Florida  
Network and Information Security Department  
*Every Child, Every Chance, Every Day*



7. There are multiple Authentication options available to choose for Multifactor Authentication:
- a. Authenticator App – Microsoft Authenticator, Google Authenticator, etc. (**This is the most secure and recommended option**).

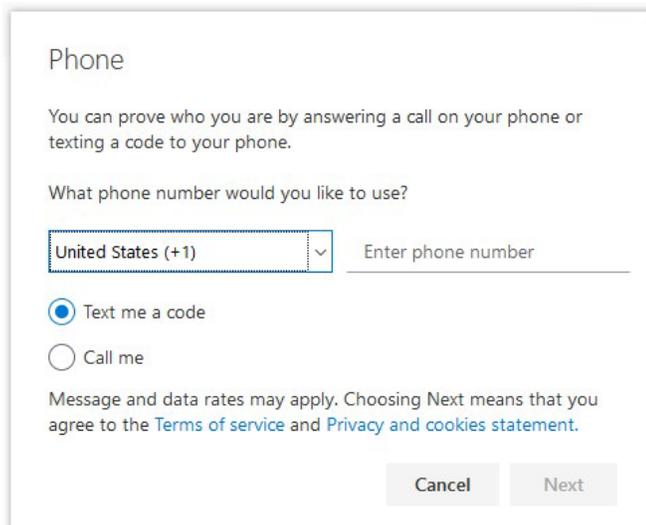


Using your smartphone, you may download the Microsoft Authenticator app from the Google Play store for Android devices, or App Store for Apple iOS devices.

Alternatively, you may also choose to use a different authenticator app.

For either case, follow the remaining steps to complete the setup of your chosen authenticator app.

- b. Phone – This is your Primary Phone option to receive a call or code sent through Text Message (SMS).



- i. For the “Text me a code” option, which is only available on the primary phone, you will receive a text message with a code to enter to complete the setup process.
- ii. For the “Call me” option, you will receive a call from a Toll-Free number, which will guide you through the rest of the setup process.





The School District of Osceola County, Florida  
Network and Information Security Department  
*Every Child, Every Chance, Every Day*



c. Alternate Phone/Office Phone – Phone Call Verification Only, No Text Message Option.

Phone

You can prove who you are by answering a call on your phone.

What phone number would you like to use?

Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

i. Similar to the previous section, for the “Call me” option, you will receive a call from a Toll-Free number which will guide you through the rest of the setup process.

**Note:** It is not recommended to use your Office Phone for MFA. If you are accessing resources from outside the office, you will not be able to answer your office phone.

This concludes the overview and instructions for registering for Multifactor Authentication.

