MFA FREQUENTLY ASKED QUESTIONS

SUMMARY

This a summary of frequently asked questions regarding the roll-out of Multi Factor Authentication (MFA) for Office 365 at Fullerton College

Updated: 3/25/21

QUESTIONS AND ANSWERS

Q. Is MFA required by District Policy?

A. As of March 4th, it is not currently required by district policy.

MFA is being introduced to keep your accounts, and our student data safe against the the unprecedented number of phishing and hacking attempts we are currently experiencing. In discussion with District IS, a district wide policy regarding MFA is in the works. NOCE has already instituted MFA for all employees.

Q. Do I have to install an Authenticator App?

A. No.

The MFA system provided by Microsoft supports the use of automated phone calls, and SMS Text messaging. It is also possible to purchase physical hardware tokens that you can attach to your key chain that can provide MFA codes.

ACT recommends the use of the Microsoft Authenticator app w/ App Lock turned off, due to it's efficiency and ease of use once configured. Compatible Autenticator apps are available from other providers such Google, but they require entering 6 digit codes when performing MFA sign-in.

ACT recommends initially configuring SMS Text, and leaving it in place because it's the easiest method to setup and can be used as a backup should you encounter problems with your authenticator app.

Q. What if I'm traveling abroad, or am in a location without cell phone coverage?

A. The authenticator apps do not require cell phone service.

The full features of the Microsoft Authenticator app work best when you have WiFi or Cell Data Service, but the app will continue to function utilizing a 6 digit access code generation even if you do not have any network access available.

The campus is curenlty investigating the use of dedicated hardware tokens that negate for an Authenticator app, Voice Phone or SMS Text messaging.

Q. How do I get a dedicated hardware token, so I do not need to use a mobile phone or tablet?

A. ACT is still evaluating hardware vendors and options and hopes to have a solution available in the coming weeks.

If you believe you need a dedicated hardware token, please inform your Dean or Manager and have your department submit a Service Request ticket and we will add you to the wait list for devices.

Q. How do you know when you have completed the MFA process?

A. For an induvial to be completely transitioned to MFA it's a two-step process.

Step 1 The setup of their MFA preferences and MFA confirmation. (You may have already done this part by now).

Step 2 MFA being turned on for that employee and then MFA confirmation again just like during the test.

Below is a short explanation of this two-step process.

Once a user sets up their MFA preferences (in the Security Info section of their FCNet account jdoe@fullcoll.edu) the server will contact the user via the authentication method the user chose as their default method (Phone - Call, Phone - Text, Microsoft Authenticator – notification, or Authenticator app hardware token code) to confirm. Once the user confirms via that authentication method (for example by receiving a 6 digit code via text) and then they type in that 6 digit code when prompted for it upon login to their FCNet account the user will then be successfully logged in. This confirmation process should not occur again until MFA is turned on for the whole Division at a later date. All employees of a

Divisions should receive an email as to when MFA will be turned on for the whole Division. Once MFA is turned on for the whole Division the employee they will go through the authentication process again, just as they did during the test the first time. If they chose to receive a text in their MFA setup preferences they will again receive a 6 digit code via text and then they should put in that 6 digit code when prompted for it upon login to their FCNet account and the user will then be successfully logged in. If they chose Microsoft Authenticator – notification they will receive a notification form the Microsoft Authenticator App (on their phone) and they can click on Approve on their phone and the user will then be successfully logged in.

Q. Once I have completed MFA for one device (i.e. my campus laptop at home) will I need to MFA again if I access my Fullerton College email on another device like my iPad?

A. Once a user has setup their MFA preferences and after the confirmation process is complete this means that MFA is complete for the device the employee is using to login. (For example if I choose my cell phone # in my MFA setup preferences and I then try to log into my Fullerton College email on my Fullerton College Campus issued laptop I will receive a text to my cell phone with a 6 digit code and then I need to enter that code when I prompted for it on my Fullerton College Campus issued laptop and then I should be logged into my Fullerton College email on that Fullerton College Campus issued laptop. But then let's say I also decide to check my Fullerton College email on my iPad. I will then again receive another text to my cell phone with a different 6 digit code and then I need to enter that 6 digit code when I am prompted for it on my iPad to be able to access my Fullerton College email on my iPad). This is because the sever is trying MFA per device. Once the employee has done this at least once per device they should not have to do it again until the date that MFA is turned on for them. They will then need to MFA again (per device). Then after that date the employee should not have to MFA again (per device) until about another 30 days.

Q. What if I don't have a smart, phone can I still use MFA?

A. You can setup your MFA preference to receive text to your cell phone even if it is not a smart phone.

Q. What if my cell phone does not have text capability or I don't have a cell phone?

A. You can setup your MFA preference to receive a phone call to a different phone.

Q. I have an iPhone/iPad and would like to use the default email app to receive my Fullerton College email instead of the Microsoft Outlook App or the Gmail App.

A. You can use the default email app that comes with iPhone/iPad to access your Fullerton College email but you will need to delete your Fullerton College email account from your iPhone/iPad and then add it back again. After you have added your Fullerton College email account back on the iPhone/iPad then you will need to turn off your iPhone/iPad and turn it back on again and MFA and then wait about 10 min. It takes about 10 min for your Fullerton College email to re-populate on your phone. You can contact the Fullerton College Help Desk for assistance.

Q. I have a Samsung phone and would like to use the Samsung email app to receive my Fullerton College email instead of the Microsoft Outlook App or the Gmail App.

A. Unfortunately the Samsung email app is not currently supported by MFA. Currently Samsung phone users who wish to access their Fullerton College email will need to download the Microsoft Outlook App or the Gmail App to access their Fullerton College on their Samsung phone.

Q. Will MFA be turned on for Departmental FCNet accounts like Mathmatics@fullcoll.edu or PhysicalEducation@fullcoll.edu ?

A. All users of Departmental FCNet accounts should not be logging into that account to use it. This makes the account more venerable to a security breach. All users of a Departmental FCNet accounts should be able to access the email of that Departmental account by adding that email box to their own email box. (If you would like to know how to add a Departmental account email box to your own FC email please contact the Fullerton College Academic Computing Technologies Help Desk). If you have file drive shares that are specifically available to this Departmental account please put in a service request so that you may be granted access to those drive shares under you own FCNet account.

Q. Will MFA be turned on for Retirees.

A. MFA will be turned on for retirees at a later date. The retirees will receive an MFA notice email at their FCNet email address (i.e. jdoe@fullcoll.edu) with all the MFA instructions and a description of what will happen and when MFA will be turned on for them. In addition, they will also be given the FC ACT Help Desk contact information and operation hours.

Q. What if I am unable to use a personal device for Multi-Factor Authentication (MFA)?

A. These are the options for employees that are unable, or chose not to use a personal device for Multi-Factor Authentication (MFA):

1. The campus has ordered physical hardware tokens that are capable of producing login codes, so that a mobile phone or tablet is not needed. ACT is currently testing these devices, and working out procedures for their use. Once the devices are approved for use, divisions/departments may then order these devices for their employees.

Employees that would like one of these devices, should have their division/department submit a SRS Request ticket requesting "MFA Hardware Token for {Employee's name}." The employee will be placed in the queue to receive devices, once they become available. The employee will need to use an alternative MFA process until they receive their hardware token device such as a personal device, office phone, or MFA exemption.

Estimated cost per device is $20 to $50.

2. An employee's division may purchase an Android or iOS mobile device for the employee to use for MFA. Employees that would like such a device, should discuss this option with their division and submit an RQ for the purchase of an Android or iOS tablet. Any device ordered for this purpose, must have access to the Google Play Store, or Apple App Store which precludes the use of some tablets such as Amazon Fire devices.

Estimated cost per devices $100-$400 (Android), $300-$1000 (iOS).

https://www.cdwg.com/search/computers/tablets/?key=android&w=CC&enkwrd=android+tablet&akr=0&instock=1&ln=0&SortBy=PriceAsc

https://www.cdwg.com/search/computers/?key=ipad+tablet&w=C&instock=1&SortBy=PriceAsc

3. [Not Recommended] The employee can use their office phone number to receive an automated voice call from the MFA system that provides a six digit code for authentication. This means the employee must have access to receiving a phone call at their Office Phone number. If the employee is working remotely, they can attempt to use the Cisco Softphone software to receive these calls. Although this method is currently available, it may be phased out in the future.

4. [Not Recommended] An employee's dean may request an exemption from MFA for the employee. To request an exemption to MFA, the employee's division must submit a SRS Request ticket requesting the exemption, and the division's Dean must submit a memo to Co Ho Manager, Academic Computing Technologies indicating their approval of the exemption, and indicating if the exemption is to be temporary until a physical hardware token can be provided, or is to be a permanent exemption.

Due to the increased security threats faced by district employees, being exempt from MFA places both the employee's and the campus' data and systems at increased risk compared to employees utilizing MFA. Employees not using MFA may be restricted to utilizing campus & district provided services on only campus provided devices, and may not be able to access those services on any personal devices.

Please note: future administrative policies may require MFA for all employees.

ADDITIONAL INFORMATION AND SUPPORT

If you have any other questions regarding Multi-Factor Authentication (MFA), need assistance with readying your account for MFA, or are experiencing difficulties access your Email, OneDrive, or Microsoft Teams after MFA has been enabled for your account, please visit the FCNet website at https://fcnet.fullcoll.edu. In addition the Fullerton College Academic Computing Technologies Help Desk is available Monday through Friday 8:00 am to 4:30 pm to assist with any questions at helpdesk@fullcoll.edu or 714-992-7111.