**ITS Procedure**
**MFA Registration**

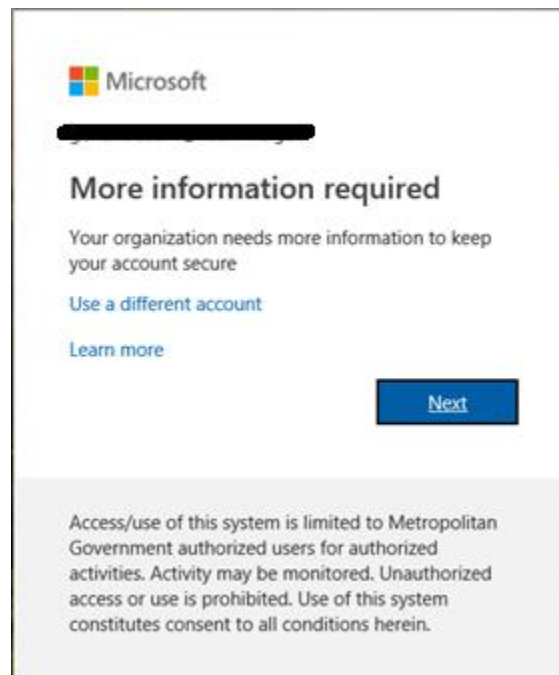| Document ID | |
|---|---|
| **Effective Date** | 7/13/2020 |
| **Owner** | ITS Identity and Access Management |
| **Info Classification** | Internal |
| **Page No.** | Page 1 of 4 |

**AUDIENCE**

Any users requiring MFA to authenticate to Metro resources.  This includes Office 365 users, Federated Azure users and Cisco AnyConnect VPN users.

**PURPOSE**

Provide step by step instructions on completing Multi-Factor Authentication (MFA) registration.

**DETAILS**

1) Navigate to http://mfasetup.nashville.gov in a web browser to begin MFA registration.

2) Log in to the MFA Registration page using your Metro email address.  If you have not been assigned a Metro email account, then you will need to log in with your UPN.  The UPN format is your current username with "@nashville.org" on the end. Example: If you log into workstations, servers or Cisco VPN using "jsmith" as your username, then the UPN you will use is jsmith@nashville.org

3) On the "More information required" prompt click "Next"



4) On the "Additional security verification" page select the contact method you would like to configure. If you have completed Self-Service Password Reset (SSPR) registration, then some of this data may be provided already.

**ITS Procedure**
**MFA Registration**

| Document ID | |
|---|---|
| Effective Date | 7/13/2020 |
| Owner | ITS Identity and Access Management |
| Info Classification | Internal |
| Page No. | Page 2 of 4 |

**Step 1: How should we contact you?**

Authentication phone
Office phone
Mobile app

Method

**Note: MFA is triggered when logging into the Cisco VPN connection or an Office 365\Azure resource is accessed while outside the Metro Network. As a result, DO NOT register an office phone for use with MFA.**

5) To configure the "Mobile APP" (preferred)

Note: You will need to download and install the "Microsoft Authenticator" on your mobile device to configure MFA using the mobile app. It is available on the Apple App Store and Google Play. Look for the icon below. If you have already installed the Mobile app you do not need to install it a second time.



a. How do you want to use the mobile app?
   i. The option "Receive notifications for verification" notifies you through the app that you have an MFA request. When opening the app, you can approve or deny the request.
   ii. The option "Use verification code" requires that you open the app and type a six-digit code to complete MFA.
b. Click "Set up" to configure the mobile app
c. A window will come up with steps to follow to complete the MFA setup.

## Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

**Step 1: How should we contact you?**

Mobile app

How do you want to use the mobile app?
○ Receive notifications for verification
○ Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up    Please configure the mobile app.

d. If you are not prompted to add an account, you can do so by following the steps below depending on your phones operating system
e. For IOS press the + sign in the upper right corner
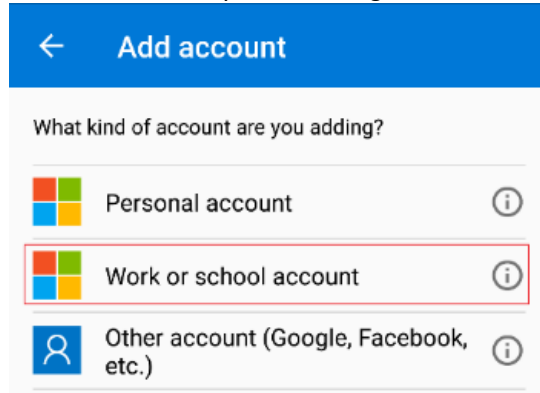
**ITS Procedure**
**MFA Registration**

| Document ID | |
|---|---|
| Effective Date | 7/13/2020 |
| Owner | ITS Identity and Access Management |
| Info Classification | Internal |
| Page No. | Page 3 of 4 |
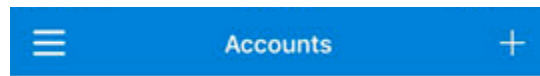
f. For Android press the three dots in the upper right corner and select "Add account"



g. When asked what kind of account you are adding select "Work or school account"



h. Finally, use your phones camera to take a picture of the QR code on your computer screen

6) To configure an "Authentication phone"
    a. Select your Country code and enter your mobile phone number
    b. Select if you want to receive a text or a phone call and click "Next"
    c. The wizard will give you a six-digit code based on your preferred contact method.
    d. Enter the code into the page and click "Verify"
    e. Once verification is successful click "Done"



7) You have now completed MFA registration.

**ITS Procedure**
**MFA Registration**

| | |
|---|---|
| **Document ID** | |
| **Effective Date** | 7/13/2020 |
| **Owner** | ITS Identity and Access Management |
| **Info Classification** | Internal |
| **Page No.** | Page 4 of 4 |

**CISCO AnyConnect VPN Users:**  Users may receive the following error when attempting to establish a VPN connection to the Metro network with Cisco Any Connect.
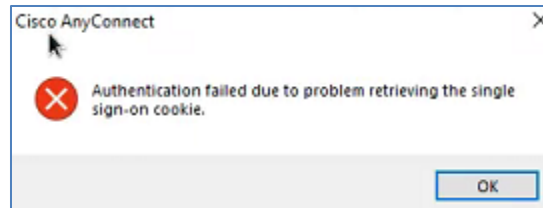


This error indicates that the user will need to set up MFA.  Please use the instructions above to do so.


**ADDITIONAL INFORMATION** *(optional)*

If you are unable to find the "Microsoft Authenticator" App, Microsoft will text you a download link. Simply go to the link below and enter your phone number.
https://www.microsoft.com/en-us/account/authenticator

Manage your settings for two-step verification
https://docs.microsoft.com/en-us/azure/active-directory/user-help/multi-factor-authentication-end-user-manage-settings


**REVISION HISTORY**

| REVISION | DATE | CHANGES |
|---|---|---|
| 1.00 | 7/13/2020 | Final |