U. S. Steel MFA Set-Up Guide Using PC & Mobile

This guide will show you how to set up Multi-Factor Authentication (MFA). MFA requires you to setup authentication methods of your choice from the following: Microsoft Authenticator app on your mobile device, text message, or phone call. You will need access to a **computer and your mobile device** to complete the steps below.

- [Setup MFA Authentication Methods](#)
  - Authenticator App Example
  - Phone Example
- [Adding or Removing MFA Authentication Methods](#)
- [Changing the Default Authentication Method](#)
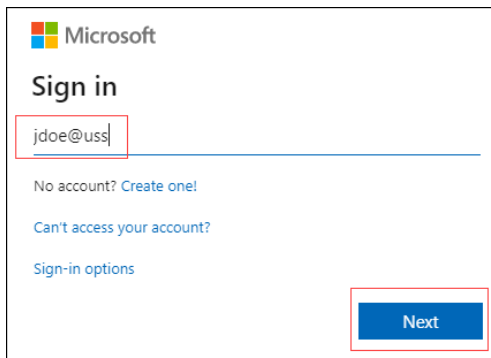
Setup MFA Authentication Methods

1. Navigate to the following website to set up your preferred methods for authentication.
   https://aka.ms/mfasetup

2. You will be prompted to sign in. If you have a U.S. Steel email address, enter it into the **Sign in** field.

   Example U. S. Steel email address: jdoe@uss.com

   If you do not have a U. S. Steel email address, enter your Windows user ID (ID used to log into your PC or log into applications) followed by @uss.com into the **Sign in** field.
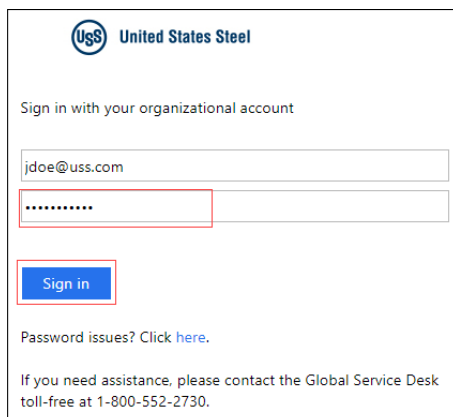
   Example U. S. Steel user ID: MDH1123EW@uss.com

   Then click **Next**.

   ![Microsoft Sign in screen showing jdoe@uss entered in the sign-in field with Next button highlighted]

3. If prompted, enter your Windows password and click **Sign In**.

   ![United States Steel organizational account sign-in screen with jdoe@uss.com and password fields, Sign in button highlighted. Text reads: Sign in with your organizational account. Password issues? Click here. If you need assistance, please contact the Global Service Desk toll-free at 1-800-552-2730.]

4. **If you previously went through an MFA setup process**, you will be prompted to verify your sign in request by a phone call, text or Authenticator App verification request. Complete the MFA request and skip to the [Adding or Removing MFA Authentication Methods](#) section of this document. If you have issues, please contact the GSD at 1-800-552-2730 (Steel Com 8-723-6000). Below is an example of a text notification.

If this is the first time setting up MFA, you will see a screen like the one below asking you to provide more information to keep your account secure. Click **Next**.

5. The **Keep your account secure** page appears where you will select the first of two authentication methods. The Microsoft Authenticator app is the first method by default. Click **Next** to begin the setup.
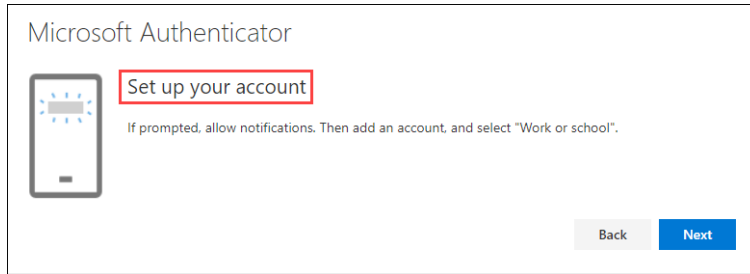

Note: You can select **"I want to set up a different method"** to change the first method from the Microsoft Authenticator app to another option such as a Phone.

We recommend you only use the Microsoft Authenticator app so please do not select **"I want to use a different authenticator app"**.

6. **From your computer**, remain on the **Set up your account** page while you confirm that you have the Microsoft Authenticator app installed on your mobile device. The icon looks like a padlock shown below.
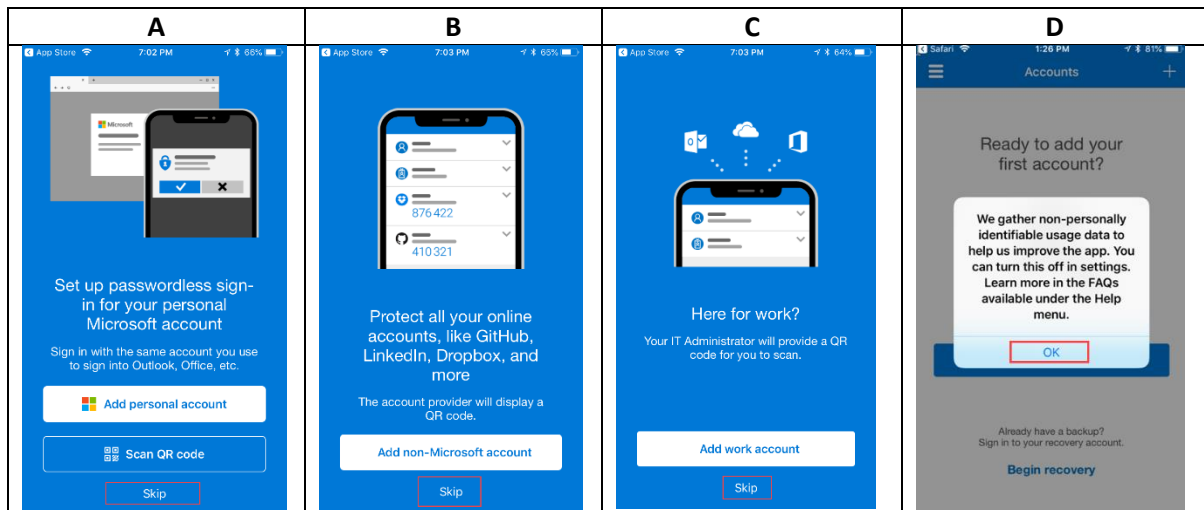

If you do not have the **Microsoft Authenticator** app installed, download it from the App Store or Google Play and install it on your mobile device.

7. Launch the **Microsoft Authenticator** app on your mobile device. The first time you launch the app, you will see three screens asking if you want to add accounts.
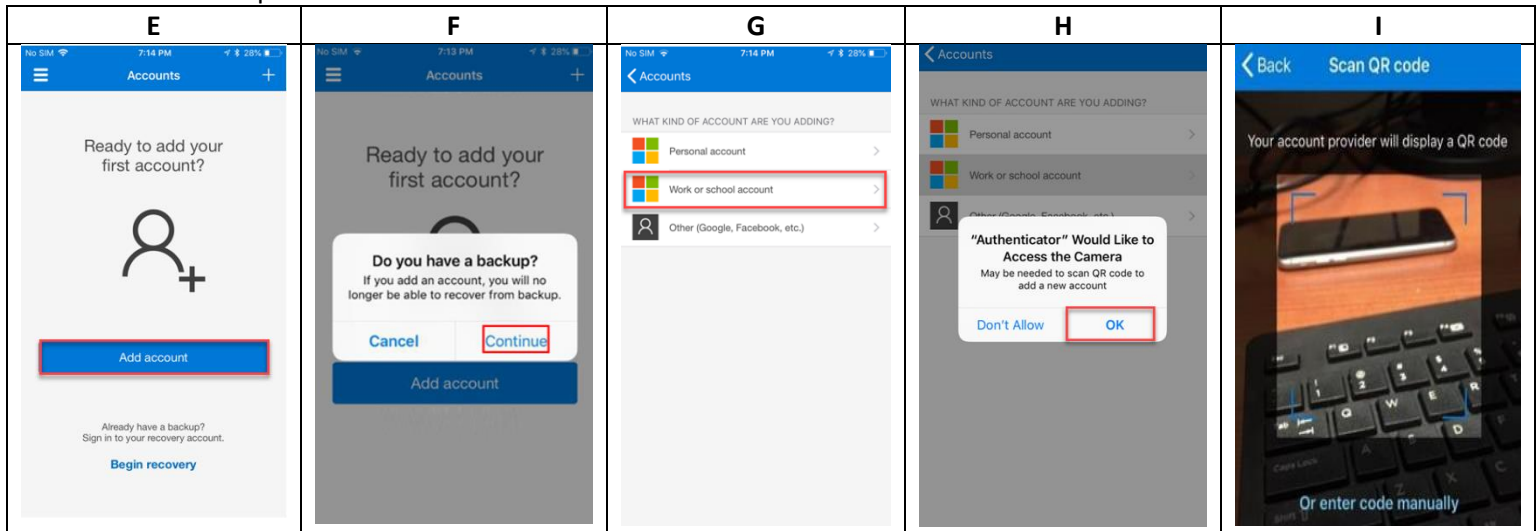
Tap **Skip** at the bottom of the screens shown in **steps A, B and C**. Then tap **OK** in **step D** when prompted that Microsoft will **gather non-personally identifiable usage data**.
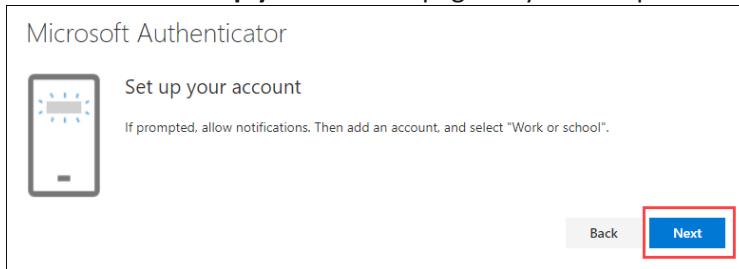
A	B	C	D

8. Next, respond to the prompts as shown below in steps E through I.
    E) Tap **Add Account**
    F) If you receive the prompt, **Do you have a backup?**, tap Continue
    G) Tap the **Work or school account** option
    H) Tap **OK** at the prompt to access the phone's camera
    I) The Authenticator app will launch your mobile device camera to scan a QR code that will be explained in the next section

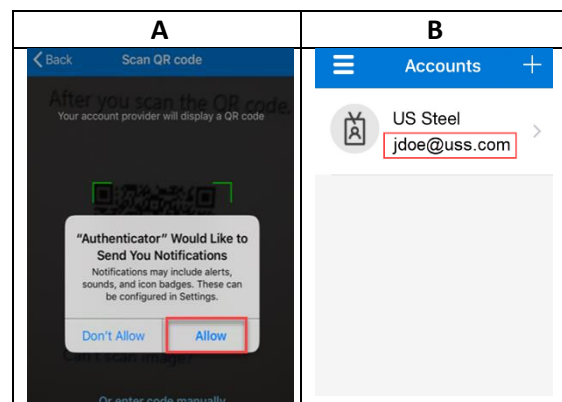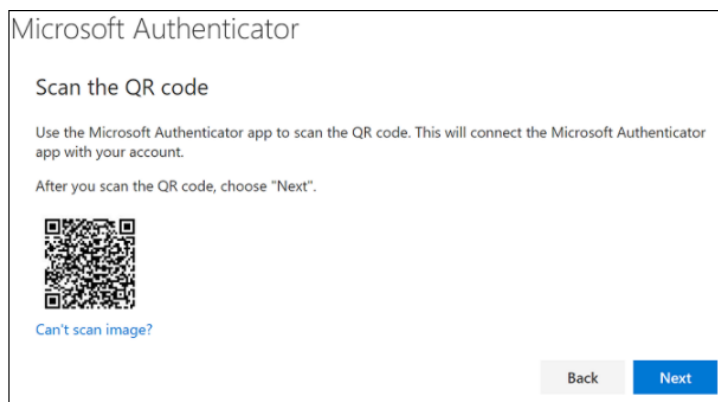| E	F	G	H	I

9. Return to the **Set up your account** page on your computer and click **Next**.

10. The **Scan the QR code** page appears. With the Microsoft Authenticator app open, point your mobile device camera towards the QR Code on your computer screen. Tap **Allow** when prompted on your mobile device as shown in image **A** below. The Authenticator app should automatically add your account as shown in image **B**. Click **Next** back on the **Scan the QR code** page on your computer.
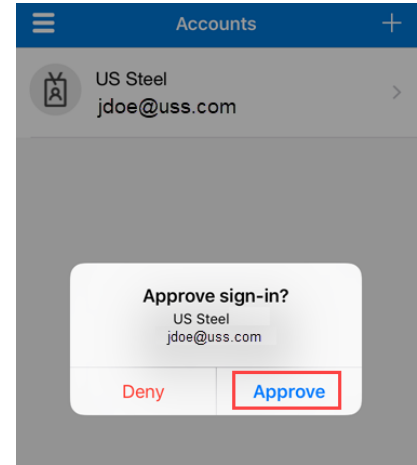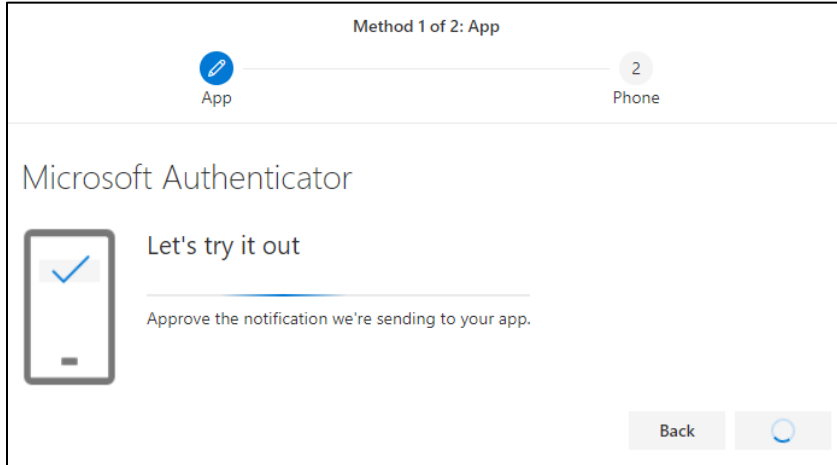
    Note: If the QR code reader cannot detect the code, you can select the **Can't scan image?** link to manually enter the QR code and URL into the Microsoft Authenticator app.
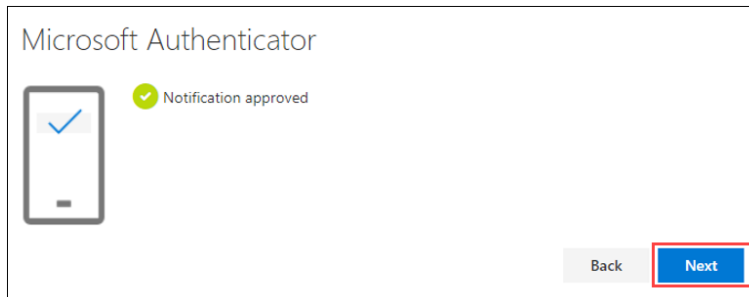

A	B

11. The **Microsoft Authenticator** page displays with a message to "try it out". You will then be prompted in the Microsoft Authenticator app on your mobile device to approve the notification. Tap **Approve** to test your account.
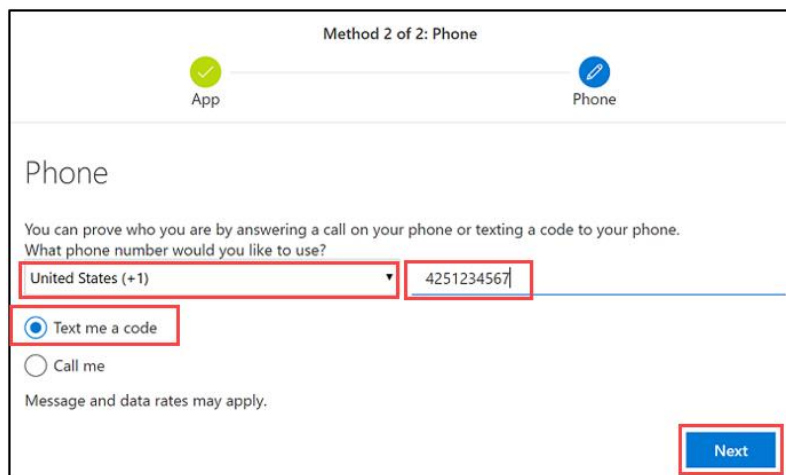

12. Once you approve the notification, the **Microsoft Authenticator** page on your computer will display a **Notification approved** message. This completes the setup of your first authentication method. Click **Next** to continue.

13. Now you will need to set up your second authentication method.

From the **Phone** set up page on your computer, choose whether you want to receive a text message or a phone call, and then click **Next**. If you choose to receive a code via text, you must use a phone number for a device that can accept text messages. Switch the country code to the "**United States (+1)**" using the drop-down and enter in your mobile number. Do not include spaces or dashes.

Note: You must set up two different methods of authentication. (Example: If Authenticator is selected for the first method, then you cannot select it again for the second method.)

Note: If you select the **Call me** option instead of **Text me a code**, you will receive a phone call asking you to press # as the notification approval method.

14. A text message is sent to your phone number. Enter the code from the text message on the **Phone** page on your computer and click **Next**.

Phone

We just sent a 6 digit code to +1 1234567890. Enter the code below.

142124

Resend code

Back   Next

15. The **Phone** page will display a **SMS verified** message that your phone was successfully registered. Click **Next**.

Method 2 of 2: Phone

App   Phone

Phone

✅ SMS verified. Your phone was registered successfully

Next

16. The **Success!** page will indicate that both the Microsoft Authenticator app and Phone authentication methods have been successfully set up. Click **Done**.

Method 2 of 2: Done

App   Phone

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method: Microsoft Authenticator - notification

📞 Phone
+1 412

🛡 Microsoft Authenticator
Pixel 4

Done

Upon clicking **Done**, the **Security info** page displays allowing you to add or make changes to your authentication methods.

My Sign-Ins   ?

👤 Overview

🔑 Security info

📇 Organizations

💻 Devices

🔒 Privacy

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification Change

➕ Add method

📞 Phone   +1 412   Change   Delete

🛡 Microsoft Authenticator   iPhone 6s   Delete

Adding or Removing Authentication Methods

You must configure **two methods** for two-factor authentication. We recommend setting your default method to Push Notification via the Microsoft Authenticator app. You can register additional methods such as multiple phones or email following the steps below.
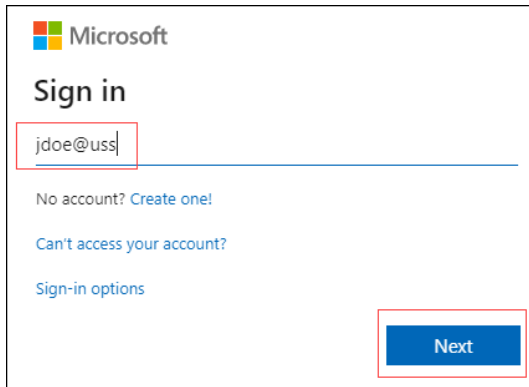
1. Navigate to the following website to view your current MFA authentication methods.
   https://aka.ms/mfasetup

2. You will be prompted to sign in. If you have a U.S. Steel email address, enter it into the **Sign in** field.

   Example U. S. Steel email address: jdoe@uss.com

   If you do not have a U. S. Steel email address, enter your Windows user ID (ID used to log into your PC or log into applications) followed by @uss.com into the **Sign in** field.

   Example U. S. Steel user ID: MDH1123EW@uss.com

   Then click **Next**.

3. If prompted, enter your Windows password and click **Sign in**.

4. You will be prompted to verify your sign in request based on the default authentication method that you currently have selected. Below is an example of a Microsoft Authenticator app notification. Complete the verification process and proceed to the next step.
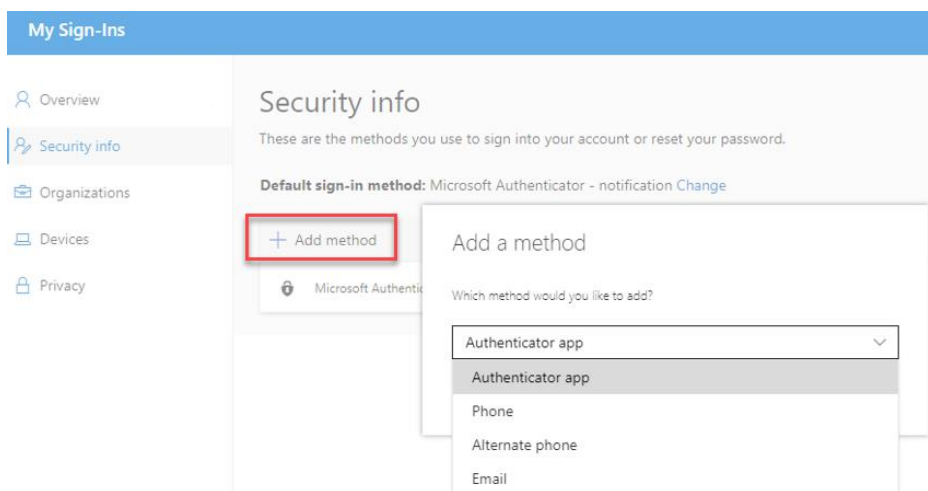

5. The **Security info** page displays your current authentication methods and default preferences.

6. To **add** an authentication method, click the plus sign next to **Add method** and select the method you would like to add from the drop-down list.

    Note: When selecting "**Email**" as the authentication method, you should use a non-USS email address. Email is not an available default sign-in method offered by Microsoft, but it can be used as a secondary method.

When you finish adding your new authentication method it will appear in the list of available methods.

To **delete** an authentication method, click the **Delete** link to the right of the item.

Changing the Default Authentication Method

1. Navigate to the following website to view your current MFA authentication methods.
   https://aka.ms/mfasetup

2. You will be prompted to sign in. If you have a U.S. Steel email address, enter it into the **Sign in** field.

   Example U. S. Steel email address: jdoe@uss.com

   If you do not have a U. S. Steel email address, enter your Windows user ID (ID used to log into your PC or log into applications) followed by @uss.com into the **Sign in** field.
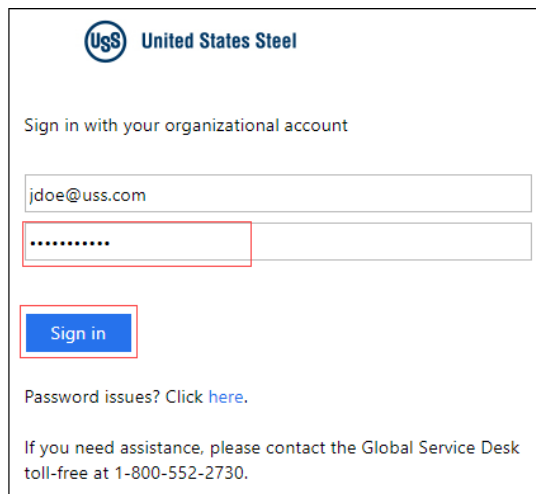
   Example U. S. Steel user ID: MDH1123EW@uss.com

   Then click **Next**.

3. If prompted, enter your Windows password and click **Sign in**.

4. You will be prompted to verify your sign in request based on the default authentication method that you currently have selected. Below is an example of a text notification. Complete the verification process and proceed to the next step.

5. The **Security info** page displays your current authentication methods and default preferences.

   To change your **Default sign-in method**, click **Change**.

6. A prompt will appear allowing you to select a new default sign-in method. Click the drop-down and select from the list of methods you currently have set up. In the example below, **Microsoft Authenticator - notification** is selected.

   Note: The list of available methods will only display the methods you have set up. If you do not see the method you want, you will need to add the method first by following the <u>Adding or Removing Authentication Methods</u> *section in this document. When selecting "Email" as the authentication method, you should use a non-USS email address. Email is not an available default sign-in method offered by Microsoft, but it can be used as a secondary method.*

7. Once you have selected your preferred authentication method, click **Confirm**.
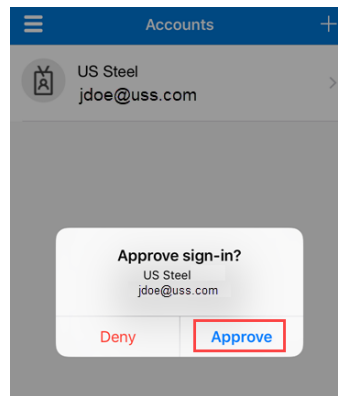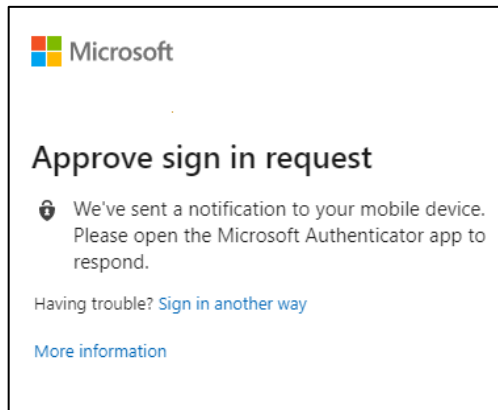
Change default method

Which method would you like to use to sign in?

Microsoft Authenticator - notification

Back   Confirm

8. The next time you sign-in, MFA will use the new preferred authentication method.

Microsoft

Approve sign in request

We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.

Having trouble? Sign in another way

More information

Accounts

US Steel
jdoe@uss.com

Approve sign-in?
US Steel
jdoe@uss.com

Deny   Approve

IMPORTANT: If you encounter any issues with the process described, please contact:
Global Service Desk
Steel Com: 8-723-6000
Pittsburgh: 412-433-6000
Toll Free: 1-800-552-2730