



# MULTI-FACTOR AUTHENTICATION (MFA) GUIDE

## Information Security

Version 3

### DEFINITION

Multi-Factor Authentication (MFA) is a method of authenticating your account with something you have and something you know. An example would be your SSO account password, and a code sent to your mobile phone. Enabling MFA increases the security of your account and helps prevent it from being compromised.

### PURPOSE

To increase the District's security posture, MFA will add a layer of protection to your Single Sign-On (SSO) account. MFA helps protect against unauthorized access such as phishing attacks, social engineering, and brute force attacks.

## 1. REGISTER FOR MULTI-FACTOR AUTHENTICATION (MFA) ACCOUNT

Go to the <https://aka.ms/mfasetup>. You will then be taken to the Microsoft Online Sign in screen. Enter your full LAUSD **email address** and click **next**.

A screenshot of the Microsoft Online Sign in screen. The screen displays the "Sign in" heading, a text input field containing "jane.doe@lausd.net", a "Next" button, and links for "Can't access your account?" and "Sign-in options". Two red arrows point to the email field and the "Next" button. At the bottom, a grey box contains the text: "Enter your full LAUSD email address and password to Log in. e.g. (msmith@lausd.net, mary.smith@lausd.net)".

Enter your LAUSD email **password** and click **Sign in**. Next, you will receive a new window for **More information required**. Click on **Next**.

← jane.doe@lausd.net

**Enter password**

.....

[Forgot my password](#)

**Sign in**

Enter your full LAUSD email address and password to Log in. e.g. (msmith@lausd.net, mary.smith@lausd.net)

**Microsoft**

**More information required**

Your organisation needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

**Next**

The **Additional security verification** page will appear.

**Additional security verification**

Secure your account by adding phone verification to your password. [View video](#)

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

Authentication phone ▾

In the enrollment process, you will be able to specify your preferred method to verify your identity (**choose only ONE method**). This can be any of the following options listed in the table below.

Method	Description
1 Mobile App ( <b>RECOMMENDED</b> )	Pushes a notification to the Microsoft Authenticator mobile app on the user's smartphone or tablet. The user taps Verify in the app to authenticate.
2 Mobile Phone Call ( <b>Default</b> )	Places an automated voice call to the authentication phone number. The user answers the call and presses # in the phone keypad to authenticate.
3 Mobile Phone Text Message	Sends a text message containing a verification code to the user. The user is prompted to either reply to the text message with the verification code or to enter the verification code into the sign-in interface.

For additional information, you may access the Microsoft page: <https://docs.microsoft.com/en-us/enterprise-mobility-security/solutions/fasttrack-how-to-enroll-in-mfa#mobile-phone>

## Method 1: Mobile App (RECOMMENDED)

In the **Additional security verification** page. Under **Step 1: How should we contact you?** select **Mobile app**.

Check the **Receive notifications for verification** and click **Next**.

Figure 1.

This will start the configuration for your account to use the mobile application. You will see a QR code you have to scan with your phone to setup the app. (Figure 2)

On your mobile device, open the App Store (Apple iOS) or Google Play store (Android) app and search for **Microsoft Authenticator**. (Figure 3)

Download the **Microsoft Authenticator** application.

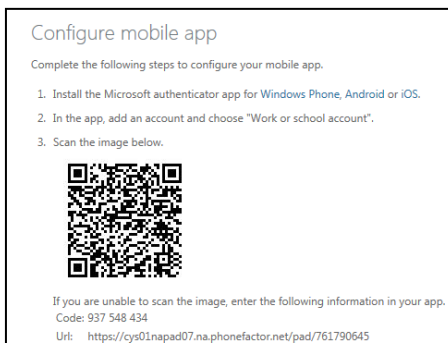


Figure 2

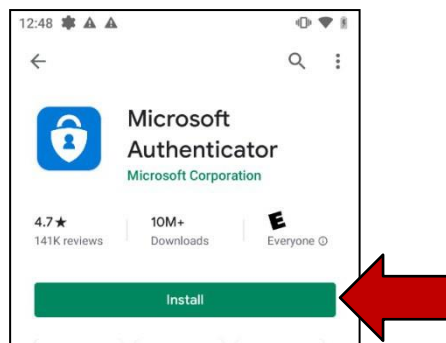


Figure 3

Open the **Microsoft Authenticator** mobile application. (Figure 4)

In the **Microsoft Authenticator** mobile application, press **Add account**. (Figure 5)

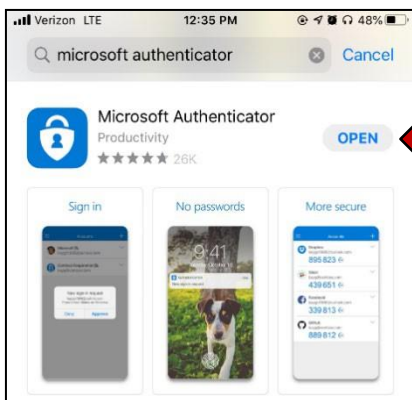


Figure 4

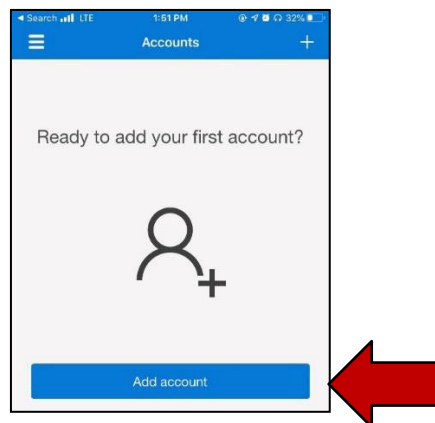


Figure 5

Next, press **Work or school account**. (Figure 6)

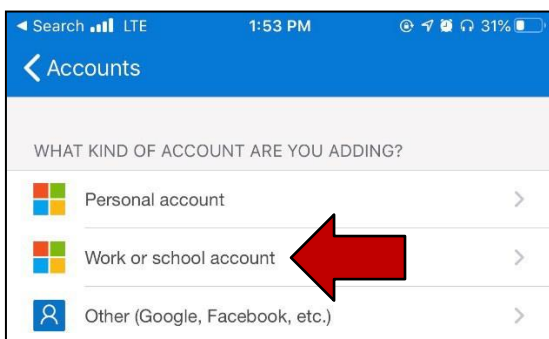


Figure 6

This will open the camera on your phone to scan the QR code on your computer screen.

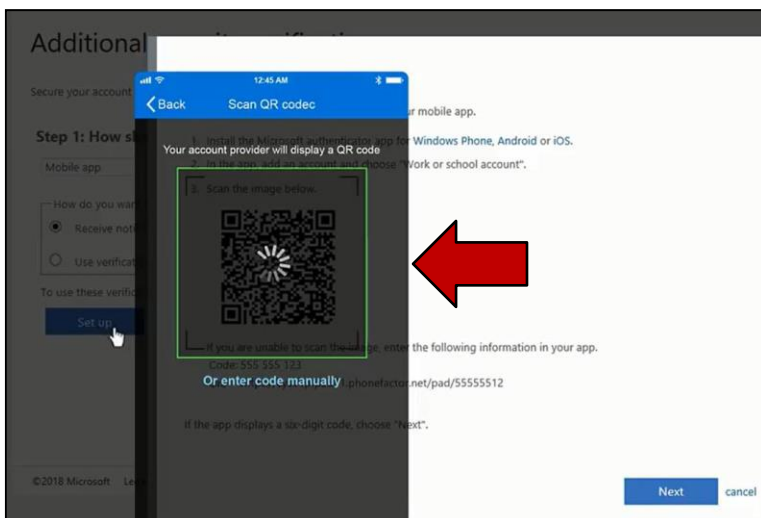
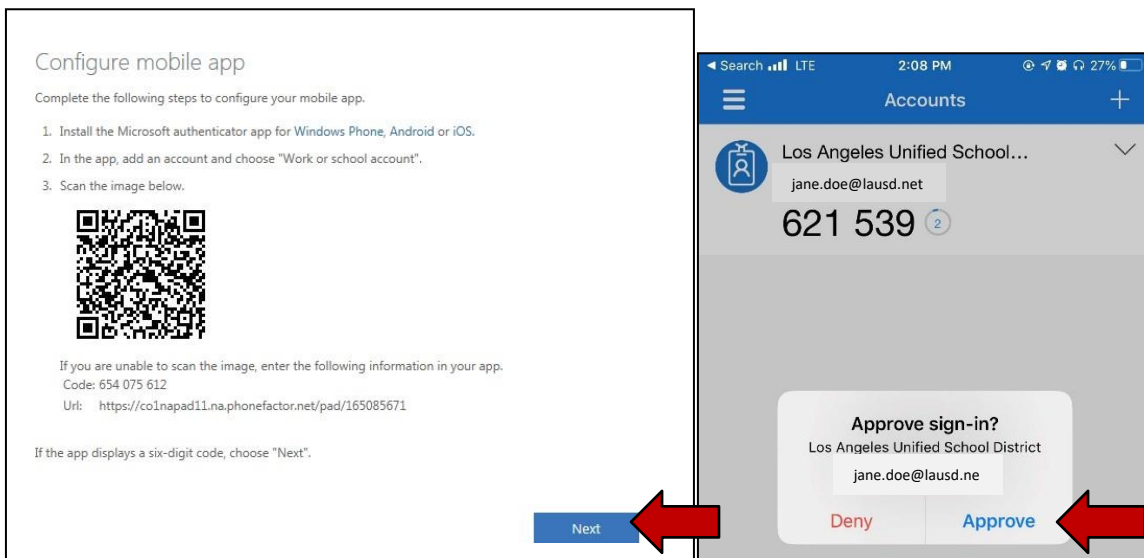
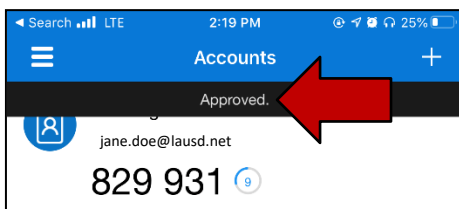


Figure 7

When the account has been added, the **Microsoft Authenticator** app will display an **Approved** message. On the browser screen, click **Next**. The system will then send a notification to your phone to approve the sign-in. Press **Approve**.



Last, enter a **phone number** in case you lose your mobile application. Click **Done** when finish.

A screenshot of a web page titled 'Additional security verification'. Below the title, it says 'Secure your account by adding phone verification to your password. View video to know how to secure your account'. Underneath, there is a section titled 'Step 3: In case you lose access to the mobile app'. This section contains a dropdown menu set to 'United States (+1)' and a text input field containing '111-111-1111'. A red arrow points to the input field. Below the input field is another red arrow pointing left. At the bottom right of the form is a blue 'Done' button with a red arrow pointing to it. At the bottom of the page, there is a small text box that says 'Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.'

Congratulations! You are now configured to MFA through the mobile app method.

## Method 2: Mobile Phone Call

In the **Additional security verification** page. Under **Step 1: How should we contact you?** select **Authentication phone**.

In the **country or region** box, select **United States (+1)**. In the box next to the country or region box, type your **10-digit mobile phone number** (include the area code – no dashes).

Select **Call me** as the method and click the **Next** button.

The screenshot shows the 'Additional security verification' page. Under 'Step 1: How should we contact you?', there is a dropdown menu for 'Authentication phone' with a red arrow pointing to it. Below it is a dropdown for 'United States (+1)' with a red arrow pointing to it, and an adjacent text input field for the phone number with a red arrow pointing to it. Under the 'Method' section, there are two radio buttons: 'Send me a code by text message' and 'Call me', with a red arrow pointing to the 'Call me' option. A blue 'Contact me' button is on the right with a red arrow pointing to it. A disclaimer at the bottom states: 'Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.'

Next, you will receive a phone call from a **1-855-XXX-XXXX** number to confirm the request.

The screenshot shows the 'Additional security verification' page. Under 'Step 2: We're calling your phone at...', there is a phone number field with a red arrow pointing to it. Below the number is a red arrow pointing to the text 'Answer it to continue...'. A 'View video' link is visible on the right.

The automated message will request you to **Press # key** to finish your verification. Once you have verified the request, the browser page will display **Verification successful!** Click the **next** button to complete the setup.

The screenshot shows the 'additional security verification' page. Under 'Step 2: Let's make sure that we can reach you on your Mobile Phone', there is a message 'Verification successful! Hit next to continue.' with a red arrow pointing to it. A blue 'next' button is at the bottom with a red arrow pointing to it. A 'View video' link is visible on the right.

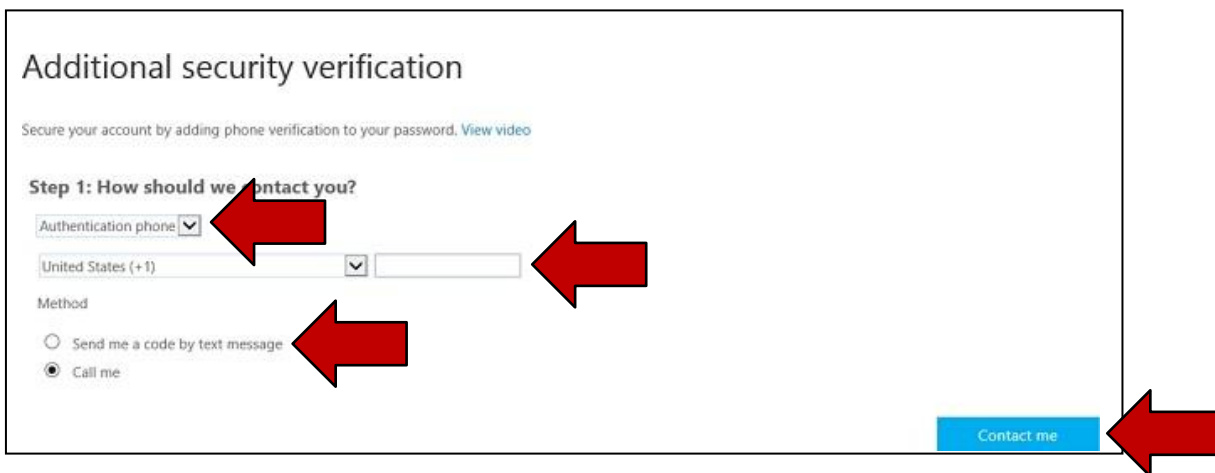
Congratulations! You are now configured to MFA through the mobile phone call method.

### Method 3: Mobile Phone Text Message

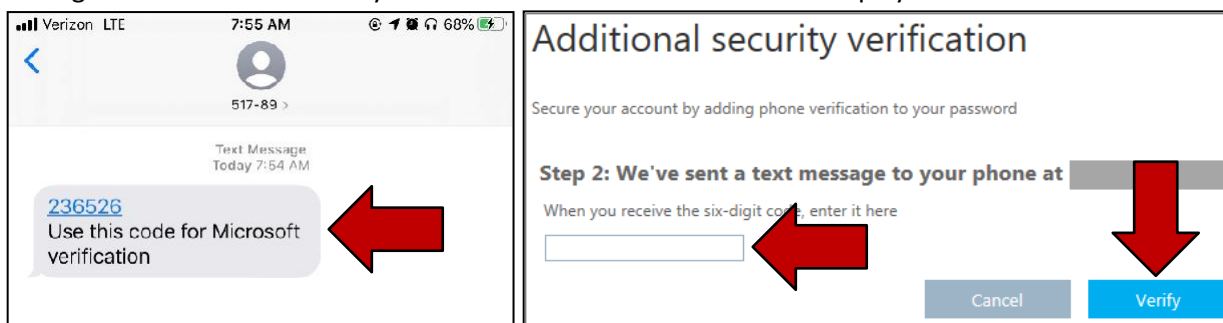
In the **Additional security verification** page. Under **Step 1: How should we contact you?** select **Authentication phone**.

In the **country or region** box, select **United States (+1)**. In the box next to the country or region box, type your **10-digit mobile phone number** (include the area code – no dashes).

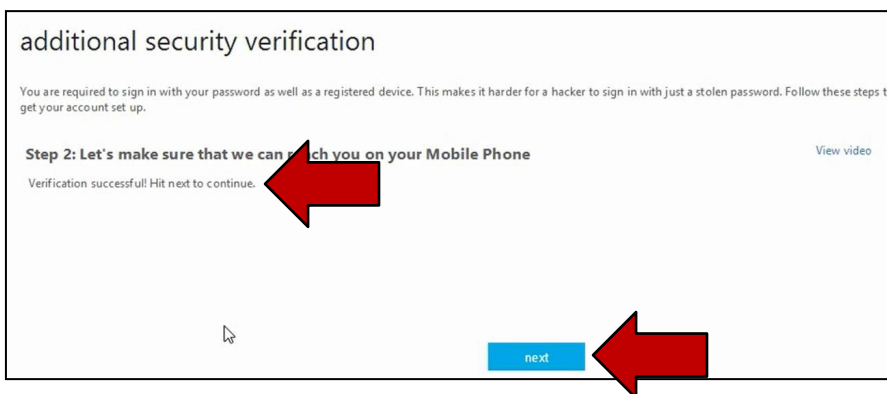
Select **Send me a code by text message** as the method and click the **Next** button.



A 6-digit code will be texted to you. Enter this code in the box that is displayed in the browser.



Once you have verified the request, the browser will display **Verification successful!** Click the **next** button to complete the setup.



Congratulations! You are now configured to MFA through the mobile phone text message method.

## OPTIONAL: CHANGE SECURITY VERIFICATION METHOD

If you want to review or make changes to your security verification information, click on **Additional security verification** under the **manage account** profile. If you have already closed your browser, you can access your profile page here:

<https://account.activedirectory.windowsazure.com/r/#/profile>

Profile

DOE, JANE  
Teacher  
School Elementary

Email: jane.doe@lausd.net  
Alternate email:  
Phone: 222-222-2222 (work)  
Office: DISTRICT SCHOOL OFFICE, LOS ANGELES

Manage account  
[Change password](#)  
[Set up self service password reset](#)  
[Additional security verification](#)  
[Review terms of use](#)  
[Sign out everywhere](#)

You will be taken to the **Additional security verification** page. In this page, you can update the verification option, authentication phone number or alternate authentication phone number. Press the **Save** button to confirm the request.

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. View video to know how to secure your account

what's your preferred option?  
We'll use this verification option by default:  
Notify me through app

how would you like to respond?  
Set up one or more of these options. Learn more

Authentication phone United States (+1)

Office phone Select your country or region  Extension

Alternate authentication phone United States (+1)

Authenticator app or Token [Set up Authenticator app](#)

Authenticator app - iPhone [Delete](#)

restore multi-factor authentication on previously trusted devices

[Restore](#)

[Save](#)

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

Updates successful

Your settings were configured successfully.



Should you have any questions on this guide or have issues connecting to VPN and/or accessing District Applications after connecting, please contact the ITD Helpdesk at 213-241-5200 or the ITD Helpdesk Chat (Monday-Friday, 7:00am-4:00pm) at <https://achieve.lausd.net/chat>.