

# Employee DUO for Gmail setup

MATC has implemented Cisco Duo for Two-Factor Authentication, also known as MFA (Multi-Factor Authentication), to provide an extra level of security to protect the college's employees and sensitive information.

To provide that additional security (and meet the requirements of our Auditors and Insurance vendor), we are requiring all employees accessing Google Apps products to utilize the Duo Two-Factor Authentication process to login to Gmail, Calendar, Drive, etc.



The MATC Portal has additional information on Duo and MFA via this FAQ:

<https://portal-prod.ec.matc.edu/departments/it/Pages/Multi-Factor-Authentication.aspx>

**To ensure you are ready, please make sure you have completed the following:**

**Step 1: In June 2022, all employees we required to begin using the Duo enrollment process**

If you are already a MATC Duo user, go to Step 4

**Step 2: Pick your Duo MFA authentication device**

Duo authentication requires either a smartphone app or a Hard Token also known as a 'Fob' as the 2<sup>nd</sup> authentication factor in the login process.

Duo offers a FREE smartphone app that you can download from your phone vendor's app store for your model of smartphone. There is NO cost to you for this app. ***This is the recommended solution for MATC employees***

***The Duo FAQ (see link above) has instructions to download the smartphone app.***

If you do not have a smartphone, employees can receive one free DUO Hard Token (Fob). You will need to contact the IT Helpdesk to request a Fob. You will be contacted by IT when your Fob has been setup, and given information on where to pick it up. *There is a \$8.00 charge for a replacement Fob, if you lose it.*

Here is a short YouTube video showing how the Cisco Duo Fob works:

<https://www.youtube.com/watch?v=EYWUO7p5s88>



**Step 3: Enrolling your smartphone in Duo**

You will receive an email from Duo Security [no-reply@duosecurity.com](mailto:no-reply@duosecurity.com) with information to enroll your smartphone to use Duo for Google authentication. *Here is an example of that email:*

From: Duo Security <[no-reply@duosecurity.com](mailto:no-reply@duosecurity.com)>  
Date: Tue, Feb 15, 2022 at 10:07 AM  
Subject: Duo Security Enrollment  
To: \_\_\_\_\_

This is an automated email from Duo Security.

Your organization invites you to set up a user account for Duo. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or helpdesk team.

Hello,



MATC is now rolling out "Duo Security", a friendly and secure way for you to log into your Desktop or applications. MATC Information Technology has invited you to set up your account for Duo so you can start logging in.

To begin, click this link to enroll a phone, tablet, or other device:

<https://api-3db2081b.duosecurity.com/portal?code=045c253250cc8f13&akey=DAFYX7PIDD154GTNTHQH>

Duo Security is a two-factor authentication service that strives to be easy to use and secure. To learn more about Duo authentication, visit the guide here:

<https://guide.duo.com/enrollment>

Click on the URL link in this email to complete the enrollment process.

**This should be completed ASAP, but needs to be completed within 30 days of receipt of this email. If the link has expired, you can contact this IT Helpdesk ([helpdesk@matc.edu](mailto:helpdesk@matc.edu) or 414-297-6541) to request a new enrollment email message.**

**You will not be able to access your Gmail / Calendar / Drive apps until this is completed.**

#### Step 4: (optional) – Duo self-service portal

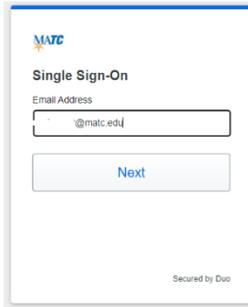
You can verify your Duo enrollment status and view/change your authentication device and preferred method of communication (Push Notification, SMS text or call) by going to: <https://duo.matc.edu>

#### Step 5: New DUO MFA for Google Apps login process

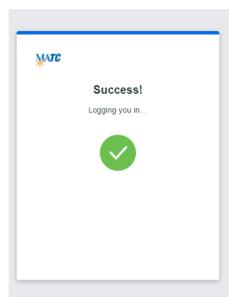
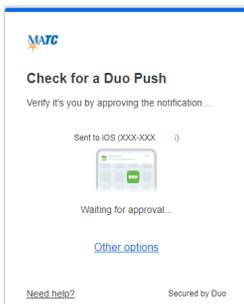
- 1) You can continue to use whatever process you were using to get to the Gmail Login prompt
- 2) Enter your full Email address (as you did in the past)

A screenshot of the Google sign-in page. At the top is the Google logo. Below it, the text reads "Sign in to continue to Gmail". There is a text input field with a blue border containing the text " :@matc.edu". Below the input field are links for "Forgot email?", "Not your computer? Use Guest mode to sign in privately. Learn more", and "Create account". A blue "Next" button is located at the bottom right of the form area.

- 3) You will see the new Duo Google Apps login screen, enter your full Email address and then your MATC Network password



- 4) You will be prompted by Duo to complete your 2<sup>nd</sup> Factor for authentication (*in this case we are using a smartphone with Duo Push notifications*)  
*Note: If you are using a Fob or selected SMS text notification during your Duo Enrollment setup, you will be enter the 6 digit code you received*  
If you successfully completed the 2<sup>nd</sup> Factor Authentication, you will see 'Success' / green checkmark on your phone

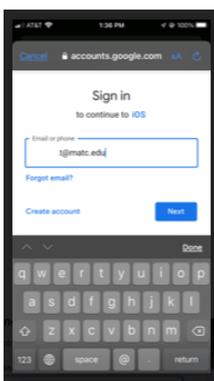


- 5) You will now see your normal Gmail application.  
*Note: Once you complete the Duo MFA process for Gmail, you will have access to your other Google Apps during this browser session. If you logout of Google Apps, you will need to use Duo again to authenticate.*

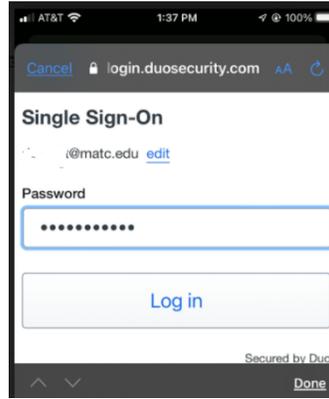
## Step 6: If you have installed the Google Mail app on your smartphone

If you use the Google Mail / Calendar app on your smartphone, it will also require a similar login process using Duo Two-Factor Authentication. See the screen shots below.

Enter your full Email address (as you did in the past)



- 1) You will see the new Duo Google Apps login screen, enter your full email address and then your MATC network password.



2) You will be prompted by Duo to complete your 2<sup>nd</sup> Factor for authentication (*in this case we are using Push Notification on our smartphone*)

*Note: If you are using a Fob or selected SMS text notification during your Duo Enrollment setup, you will be enter the 6 digit code you received*

If you successfully completed the 2<sup>nd</sup> Factor Authentication, you will see 'Success' / green checkmark on your phone

