

DAART AUTHENTICATION REGISTRATION USER GUIDE

This guide provides instructions for the new process to authenticate DAART users.

**** The URL for DAART has changed** to <https://govcloud.daart.us>. If you access <https://daart.us> you should be automatically redirected to the new URL. If you experience an error at <https://daart.us>, you may need to clear your browser cache in order to be redirected to <https://govcloud.daart.us>.

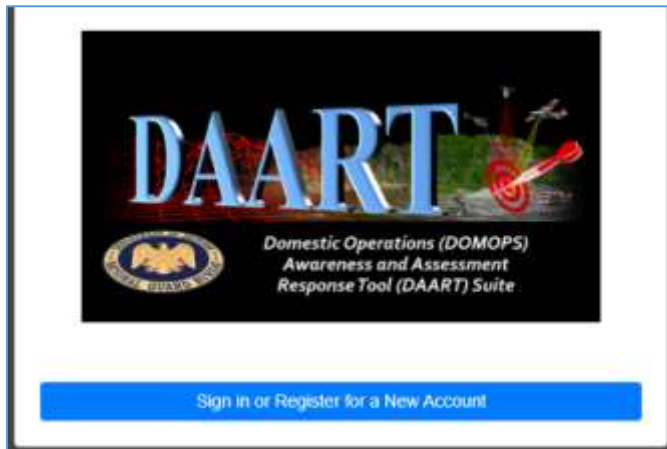
All DAART users will need to register an authentication method, Common Access card (CAC) and/or Mobile App. This will be a one-time registration for each/either method. You can register for both types (separately) and link them to a current DAART account.

The authentication registration process must be started and completed on a computer, not on a mobile device.

All desktop client and mobile app users will need to perform the authentication method registration for CAC and/or Mobile App token authentication **on the website** before using the client or mobile app.

Contents

Instructions.....	2
1. Existing User.....	2
Existing User CAC Registration.....	3
Existing User Non-CAC (mobile app) Registration.....	7
2. New User.....	13
New User CAC Registration.....	13
New User Non-CAC (mobile app) Registration.....	23
3. Mobile Authenticator App Set Up.....	30
Google Authenticator App Setup.....	30
Microsoft Authenticator App Setup.....	33
4. Log In to an Existing Account.....	39
Sign in with CAC.....	39
Sign in with Mobile App.....	39
5. Unable to Scan Barcode.....	42
Google Authenticator App.....	42
Microsoft Authenticator App.....	44



Follow the [instructions](#) below after clicking the **Sign in or Register for a New Account** button.

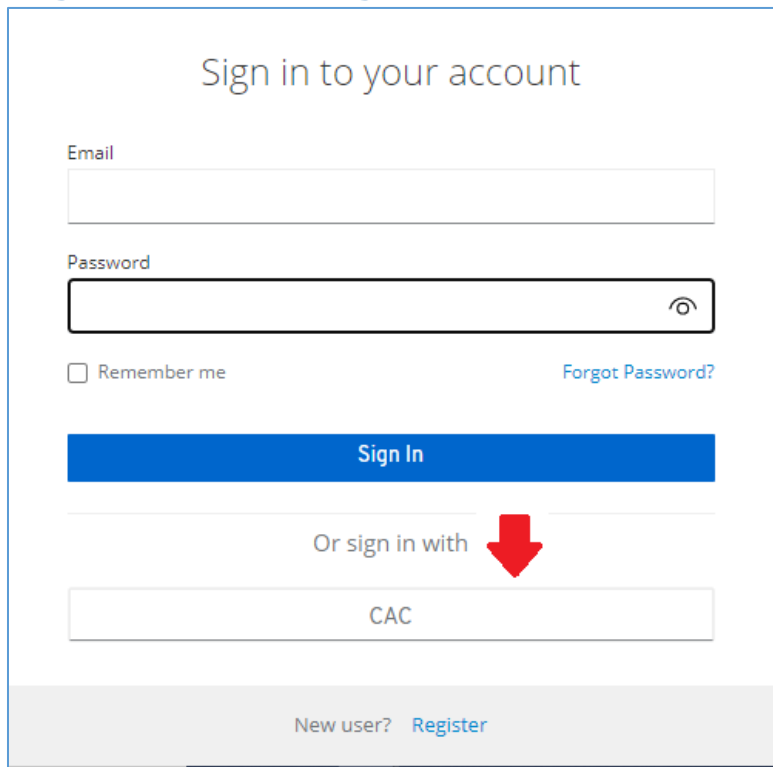
Instructions

Are you an existing DAART user? [YES](#) [NO](#) (go to page 13)

1. Existing User

Do you have a Common Access Card (CAC)? [YES](#) [NO](#) (go to page 7)

Existing User CAC Registration




Sign in to your account

Email

Password

☐ Remember me [Forgot Password?](#)

Sign In

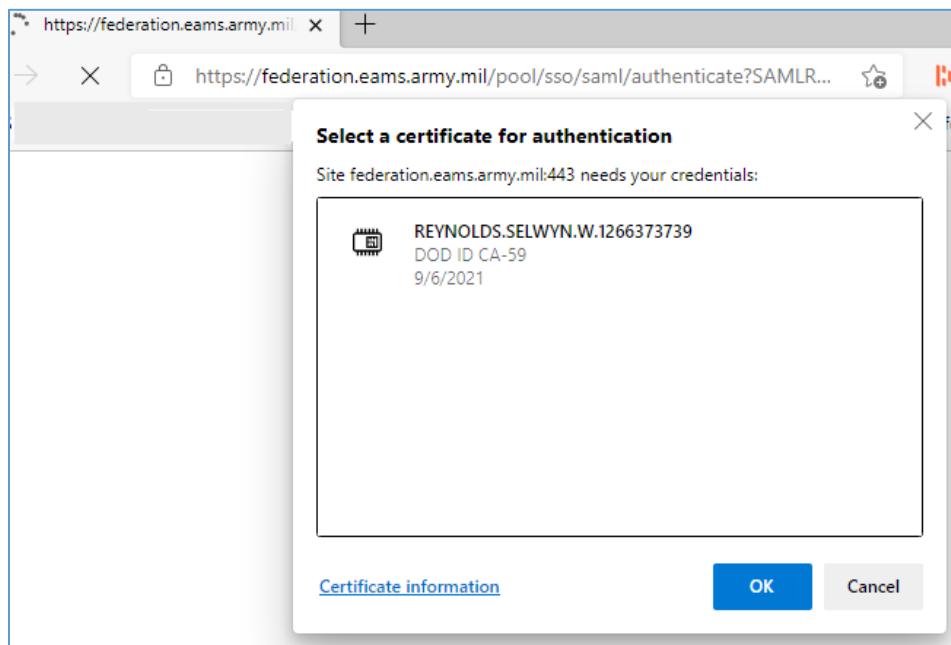
Or sign in with 

CAC

New user? [Register](#)

Click the **CAC** button

DAART utilizes EAMS-A (Enterprise Access Management Service-Army) for CAC authentication. You will be redirected to the EAMS-A to verify your CAC and PIN.



Select your certificate, click **OK**.



Enter your PIN, click **OK**.

Terms and Conditions

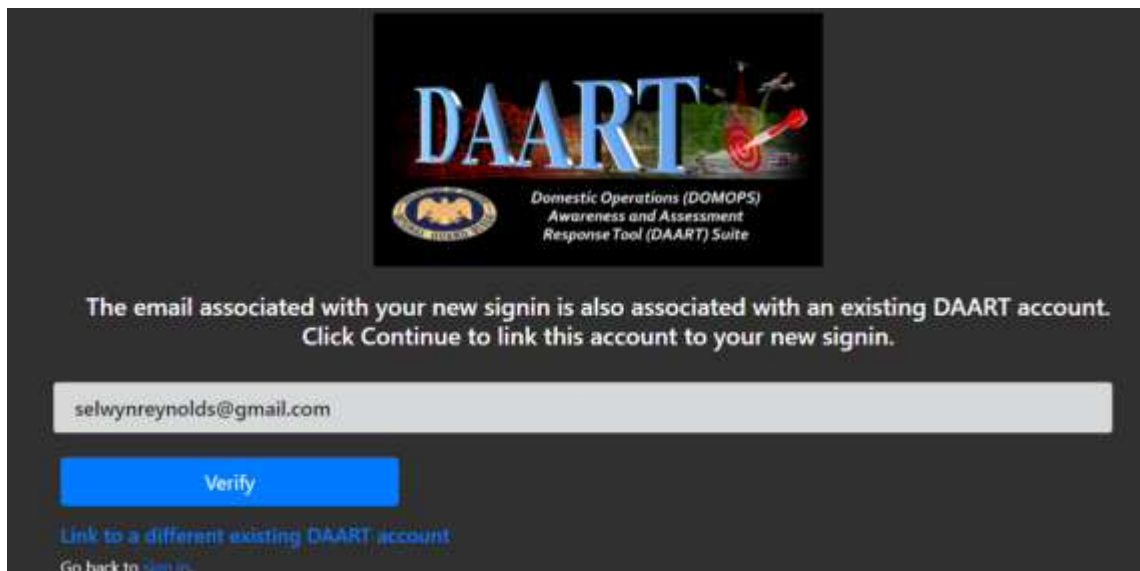
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

AcceptDecline

Read and **Accept** the Terms and Conditions of using DAART (displayed the first time you log in only). You will then be taken to the DAART Link/Continue Registration page.

If you have a DAART account that is associated with the same email used by your CAC you will be prompted to verify the email address.

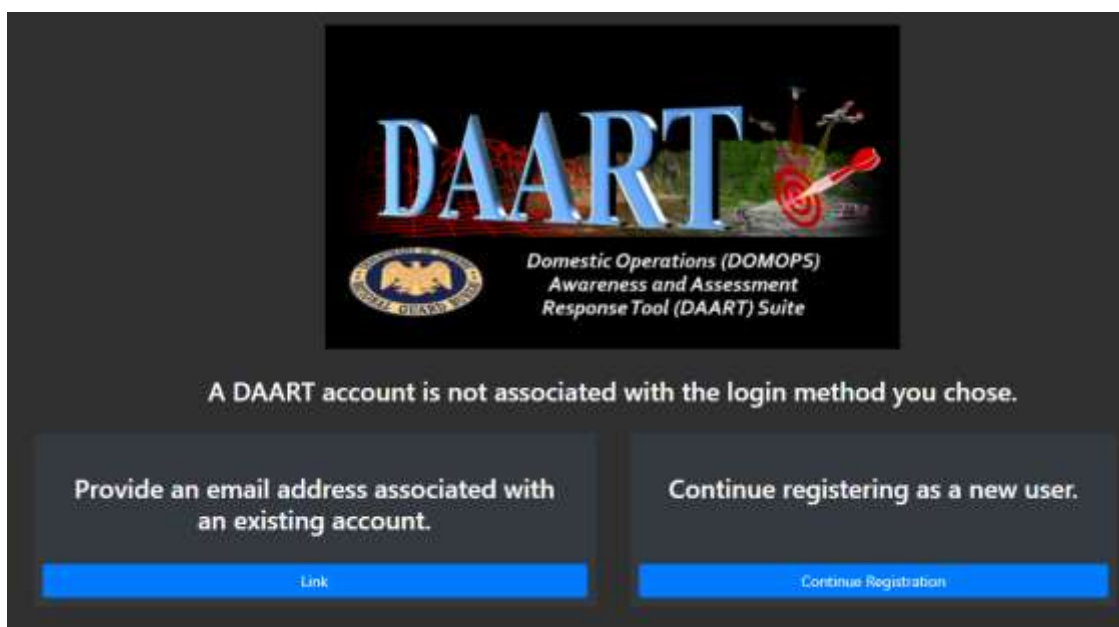


Click **Verify**. You will receive an email at this address.


Enter the 6-digit verification code from the email in the box on the right then click **Verify** to be taken to the DAART Event Page.

*If you have an expired Cyber Training Certificate or IO Training Certificate you will see a page stating you have been signed out of DAART. You can click the **Sign In** button or momentarily you will be redirected to the Sign in page. After signing in you will be taken to the Training Page to upload new certificates or take the cyber and/or IO training before entering DAART.*

If you do not have a DAART account that is associated with the email used by your CAC you will be prompted to enter the email address that is associated with your existing DAART account.



Click **Link** to provide the email address associated with your existing DAART account.



Provide the email of your existing DAART account and a verification code will be sent so you may complete the linking process.

Email

• The EmailAddress field is required.

[Send Verification Code](#)

Go back to [Link or Continue](#) or [sign in](#).

Enter the email address associated with your current DAART account then click **Send Verification Code**

You will be notified if an existing account does NOT match the email address provided.

Provide the email of your existing DAART account and a verification code will be sent so you may complete the linking process.

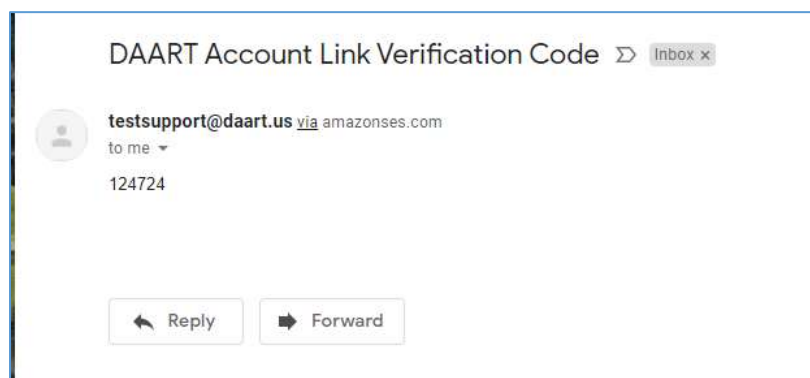
• Existing account was not found.

[Send Verification Code](#)

Go back to [Link or Continue](#) or [sign in](#).

Enter another email address or click **Link or Continue** to return to the Link/Register page to register for a new account. Go to [New User](#) (page 13).

If the correct email address was entered for an existing account you will receive an email with a 6-digit code from DAART Support at the email address entered.



Enter the verification code sent to the email listed in the Email address box.
****The verification code must be entered within 1 minutes of receiving the email****

Email address: selwynreynolds@gmail.com

Enter verification code: Verification Code

The VerificationToken field is required.

Resend Verification Code Verify

Enter the 6-digit verification code from the email in the box on the right then click **Verify** to be taken to the DAART Event Page.

Existing User Non-CAC (mobile app) Registration

DAART requires two factors of information in order to authenticate a user. Mobile device authenticator apps generate a unique code every 30 seconds that provides the second factor (second = something you have). Your username and password together are the first factor (first = something you know)

You will need an authenticator app installed on your phone to get the second factor (6-digit code) to log into and register for DAART. See [Mobile Authenticator App Setup](#) (page 30) for instructions if needed.

Sign in to your account

Email: |

Password:

☐ Remember me [Forgot Password?](#)

Sign In

Or sign in with

CAC

New user? **Register**

Click **Register**

Register

Minimum Password Requirements:

At least 15 characters

Any 2 of the following: & ! @ # \$ % ^ * _ - + = \ , . : ; / <

2 Numbers

2 Capital Letters

2 Lowercase Letters

First name

Last name

Email

Password

Confirm password

[« Back to Login](#)

Register

Enter your **first name**, **last name**, **email** and create a **password** (*according to the requirements listed in red*) then click **Register**.

Terms and Conditions

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Accept

Decline

Click Accept to accept the terms and conditions for use of DAART.

Email verification



You need to verify your email address to activate your account.

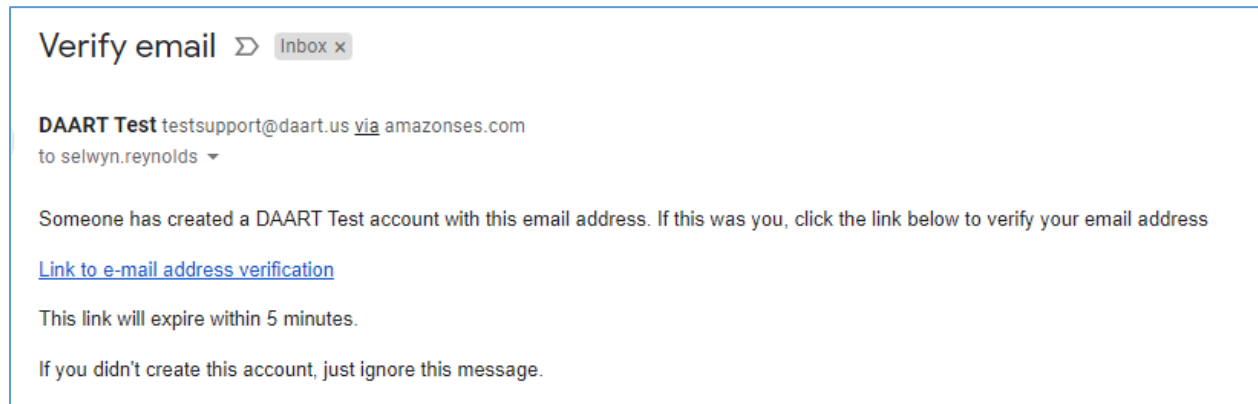
An email with instructions to verify your email address has been sent to you.

Haven't received a verification code in your email?

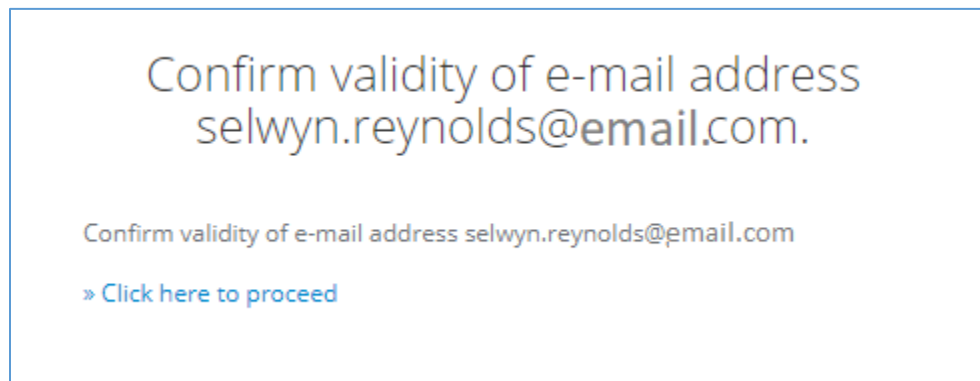
[Click here](#) to re-send the email.

DAART will need to verify your email address. An email will be sent to your address with a verification link in it. **** You must check your email on your computer, NOT your phone, to**

click the verify link. The authentication registration process must be started and completed on a computer, not on a mobile device.



Click the verification link to be taken to DAART to confirm the validity of your email address.



Click “»Click here to proceed”. At this point you will be taken to the DAART Mobile Authenticator Setup page to complete the authenticator app token registration by configuring the mobile authenticator setup.

Mobile Authenticator Setup



You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications (or other authenticator app) on your mobile device:

Google Authenticator
Microsoft Authenticator

2. Open the application and scan the barcode:



[Unable to scan?](#)

3. Enter the one-time code provided by the application and click Submit to finish the setup.

Provide a Device Name to help you manage your OTP devices.

The one-time code must be entered within 10 minutes.

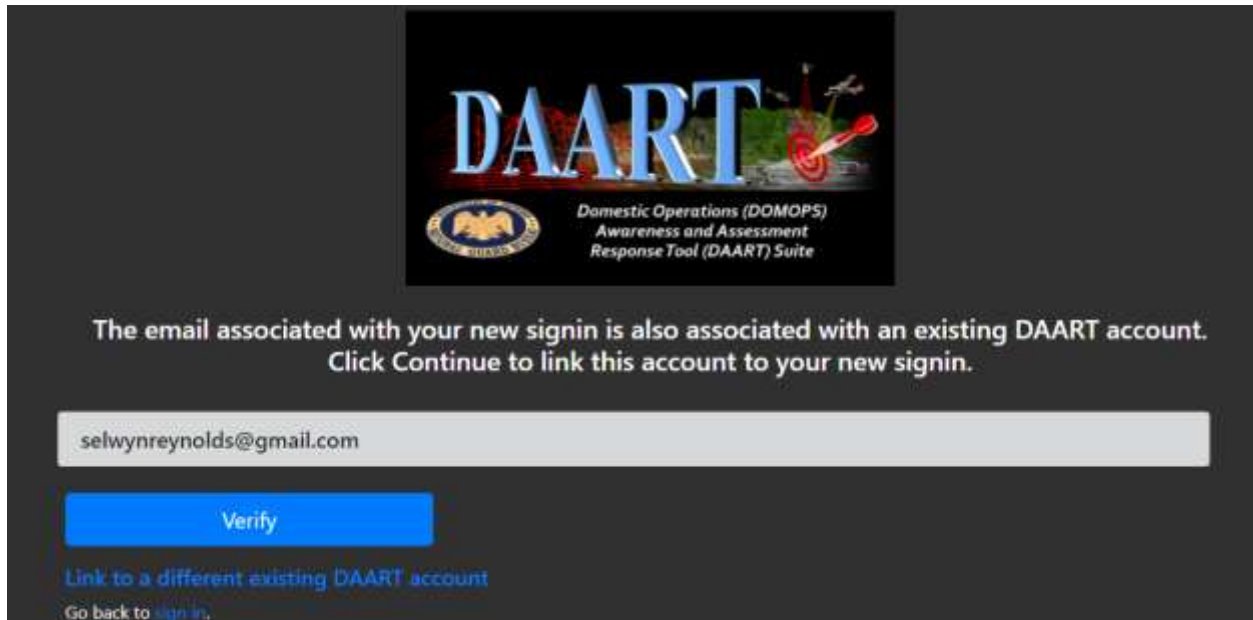
One-time code from mobile app * (Required)

Device Name (Optional)

Submit

Follow the instructions on the **Mobile Authenticator Setup** screen to establish a token authenticator provider.

1. Scan the barcode with the authenticator app installed on your mobile device
** See Unable to Scan for instructions if your app will not scan the barcode **
2. Enter the **6-digit one-time code** provided by the application on your mobile device in the box provided
3. **Optional:** enter a name for the device (named reference for your phone if you want)
4. Click Submit



DAART will look for an account that matches the email entered during the app authentication registration. If an account is found you can link the existing account to the app token registration by clicking **Verify**.

*If you have an expired Cyber Training Certificate or IO Training Certificate you will see a page stating you have been signed out of DAART. You can click the **Sign In** button or momentarily you will be redirected to the Sign in page. After signing in you will be taken to the Training Page to upload new certificates or take the cyber and/or IO training before entering DAART.*

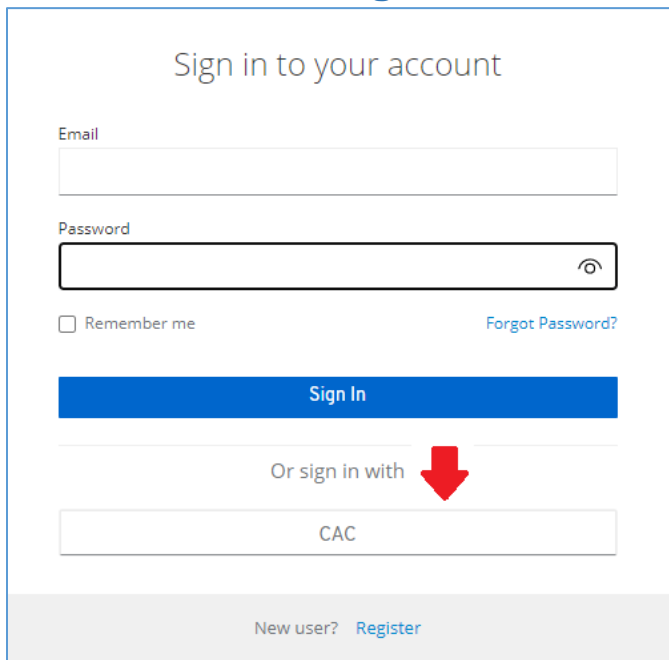
If this is not your account, you can click **Link to a different existing DAART account** to be taken to the [Link/Continue Registration page](#) (page 5).

You have been logged out of DAART, click Sign In if you aren't redirected to the sign in page. You can now sign into DAART.

2. New User

Do you have a CAC? [YES](#) (page 13) [NO](#) (page 23)

New User CAC Registration

A screenshot of a web form titled "Sign in to your account". It contains fields for "Email" and "Password". Below the password field is a "Remember me" checkbox and a "Forgot Password?" link. A blue "Sign In" button is positioned below these. A horizontal line separates this section from the next, which starts with "Or sign in with" followed by a red downward-pointing arrow and a "CAC" button. At the bottom, there is a "New user? Register" link.

Sign in to your account

Email

Password

☐ Remember me [Forgot Password?](#)

Sign In

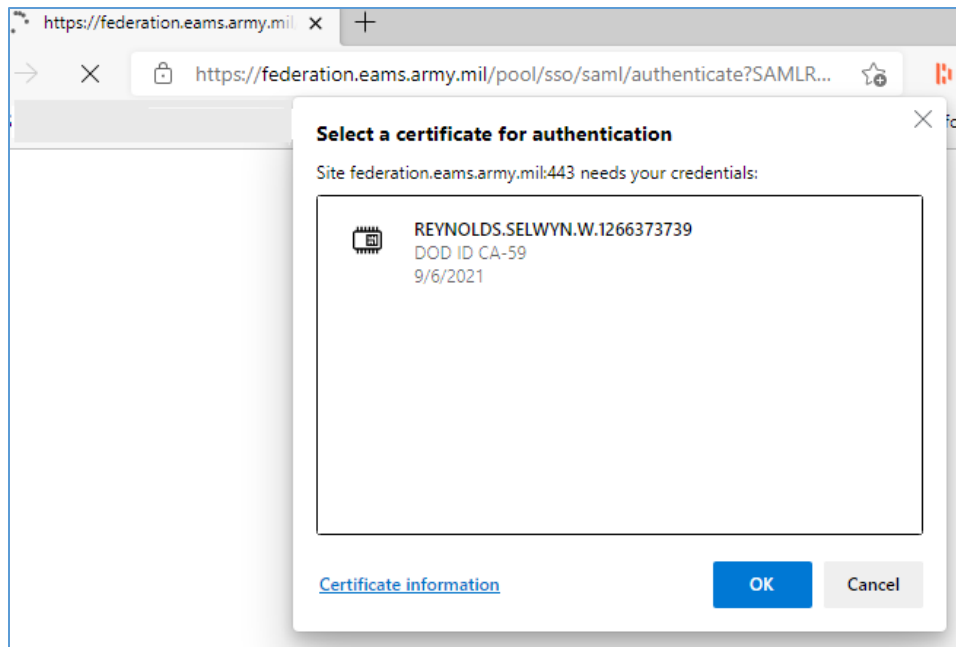
Or sign in with

CAC

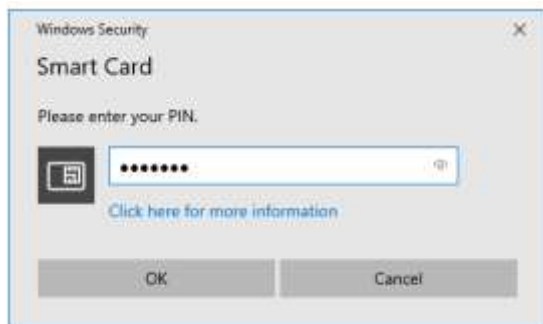
New user? [Register](#)

Click **CAC** button.

DAART utilizes EAMS-A (Enterprise Access Management Service-Army) for CAC authentication. You will be redirected to the EAMS-A to verify your CAC and PIN.



Select your certificate, click **OK**.



Enter your PIN, click **OK**.

Terms and Conditions


You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Accept

Decline

Read and **Accept** the Terms and Conditions of using DAART (displayed the first time you log in only). You will then be taken to the DAART Link/Continue Registration page.



A DAART account is not associated with the login method you chose.

Provide an email address associated with an existing account.	Continue registering as a new user.
Link	Continue Registration

Click **Continue Registration** to create a new DAART account.

Registration

First Name: <input type="text" value="Selwyn"/>	Title: <input type="text" value="N/A"/>
Last Name: <input type="text" value="Reynolds"/>	
Username: <input type="text" value="selwyn.reynolds"/>	Email: <input type="text" value="selwyn.reynolds@allionscience.com"/>
Street: <input type="text" value="11000"/>	City: <input type="text" value="Ft. Worth"/>
State: <input type="text" value="-- Choose State --"/>	Postal Code: <input type="text" value="76102"/>
Phone: <input type="text" value="817.250.1234"/>	Building Name: <input type="text" value="Building Name"/>
Organization: <input type="text" value="Organization"/>	Organization Type: <input type="text" value="-- select one --"/>
Affiliation: <input type="text" value="Affiliation"/>	

Justification:

Enter information then click **Continue Registration**.

• An account with email address selwyn.reynolds1@allionscience.com already exists. Please choose a different email address.

Note: the email address must be unique. Please contact support@daart.us if you need to use an existing email address.

Acceptable Use Policy

Username: selwyn.reynolds1 (please make a note of this)

[Download AUP](#)

DOMOPS Awareness and Assessment Response Tool (DAART)

General User Acceptable Use Policy (AUP)

1. Purpose. Controls are needed for the DAART System to ensure all users are accountable for their own actions and to protect mission-related data and equipment from either malicious and accidental loss or damage. The following AUP has been developed to govern the behavior of the DAART System users to ensure they know and accept their responsibilities with respect to the DAART System security. Individuals must agree to conform to these rules. This will be accomplished during the DAART System user registration process prior to being provided access to the DAART System. Consequences for violating the AUP vary according to the seriousness of the violation.
2. Understanding. I understand that I have the primary responsibility to safeguard the information contained in the DAART System from authorized or inadvertent modification, disclosure, destruction, denial of service, and use.
3. Access. Access to the DAART System is for authorized purposes as set for in DoD 5500.7-R "Joint Ethics Regulation" or as further limited by this policy.

10. I understand I am subject to disciplinary action if I violate DOD computer policy. For U.S. personnel, this means that if I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). If I am not subject to the UCMJ, I may be subject to adverse action under the United States Code or Code of Federal Regulations.

☒ I Agree

[Continue Registration](#)

Read the Acceptable Use Policy, check the **I Agree** box then click **Continue Registration**.

As a DAART user, you will belong to a primary State or Agency. You will request access to the State or Agency. An account manager for the State/Agency will be notified of your request via email and will either approve/disapprove your account request. You will be cc'd on the email to the account manager and will also receive an email when your account is approved. If the account request cannot be approved you will receive an email with the reason.

Primary State/Agency

Username: selwyn.reynolds1 (please make a note of this).

Please select your primary state or agency

USASMDC

[Request](#)

Select your **primary State or Agency** from the drop-down box then click **Request**.

Primary State/Agency

Username: selwyn.reynolds1 (please make a note of this).

Please select your primary state or agency

USASMDC

[Request](#)

State/Agency requested.

[OK](#)

Click **OK**.

If you require access to files containing Controlled Unclassified Information (CUI), please click here:

Request CUI Access

Continue Registration

If you will need access to Controlled Unclassified Information (CUI) click the **Request CUI Access** button.

Primary State/Agency

Username: tommie.reynolds1 (please make a note of this)

Please select your primary state or agency

USASMDC

Request

CUI Access Requested.

OK

Click **OK**, then click the **Continue Registration** button.

In order to have a DAART account you must provide a copy of a current **Cyber Security Training** certificate and a current **Intelligence Oversight Training** Certificate. If you do not have these certificates, you can take the training provided by DAART. The training and ability to upload certificates is provided in the Training Certificates page.

Training Certificates

Username: tommie.reynolds1 (please make a note of this)

A current Cyber Security Training certificate and a current Intelligence Oversight (IO) Training Certificate must be provided. You can upload one or both of these certificates if you have them. If you do not currently possess one or both of these you can take the training by clicking the links below. The cyber test takes about 15 minutes to complete and the IO training takes about 10 minutes. Certificates will automatically load to your account when training is complete. Please use the calendar link to set the expiration date of your training. Expiration date is 1 year from the date on your certificate.

Upload Current Cyber Certificate

[Take Cyber Training](#)

Expiration Date

Est. Time: 15 min

(Refresh page if Expiration Date does not appear)

Upload Current IO Certificate

[Take IO Training](#)

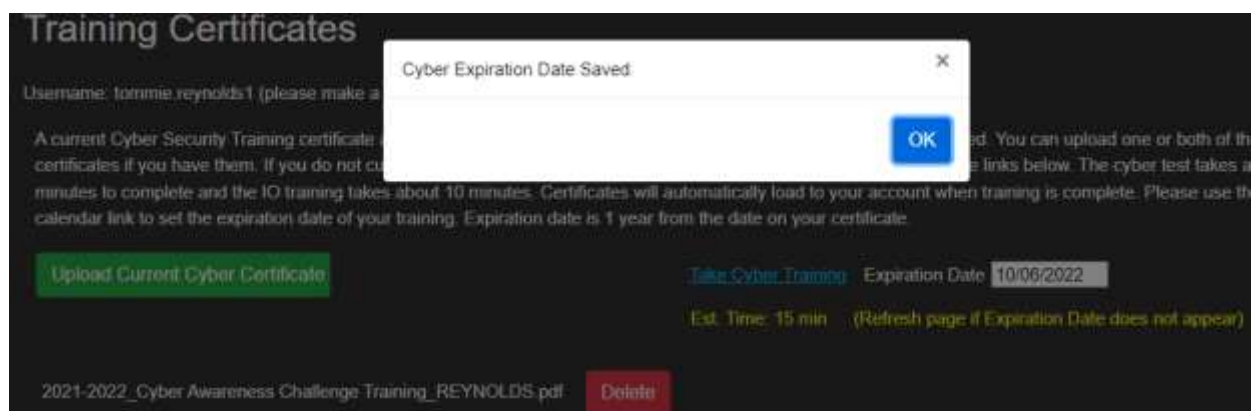
Expiration Date

Est. Time: 10 min

(Refresh page if Expiration Date does not appear)

Complete Registration

Upload a current cyber certificate and enter the expiration date of the certificate in the Expiration Date calendar box. Please note that the expiration date is 1 year out from the date on the certificate.



The screenshot shows a web interface titled "Training Certificates". A modal dialog box is open in the center with the title "Cyber Expiration Date Saved" and an "OK" button. The background page shows a user profile for "tommiereynolds1" and instructions about uploading a cyber security training certificate. It includes a green button "Upload Current Cyber Certificate", a link "Take Cyber Training", and an "Expiration Date" field set to "10/06/2022". Below this, it says "Est. Time: 15 min" and "(Refresh page if Expiration Date does not appear)". At the bottom, there is a file named "2021-2022_Cyber Awareness Challenge Training_REYNOLDS.pdf" with a "Delete" button.

You will be notified that you have successfully saved a valid cyber expiration date. Click **OK**.

If you do not have a current cyber security training certificate you can take the training provided by DAART. The training consists of reading cyber security information then taking a test of 10 questions. You must correctly answer 7 questions in order to pass the test and obtain a certificate.



The screenshot shows the "DAART Cyber Security Awareness Training and Exam" introduction page. It has a dark background with white text. The title "DAART Cyber Security Awareness Training and Exam" is at the top, followed by the subheading "Introduction". The main text explains that for security and DoD system security compliance, all DAART users must complete Cyber Security Awareness Training. Below this is "Module 1: Privacy Protection". Under "Module 1", there is an "Overview" section stating that upon completion, users should be able to define personally identifiable information (PII) and identify their privacy protection responsibilities. Finally, there is a "Topic 1: Why is Privacy Protection so important?" section, which begins by stating that an organization called IdentityTheftInfo reports that approximately 15 million U.S. residents have their identity stolen each year.

Read through the cyber training.

Topic 14: Wireless Vulnerabilities

Rogue (or unauthorized) wireless access points may not have adequate wireless security enabled and can be easily accessed by a hacker over a mile away using an antenna extender. In wireless transmissions, data is broadcast through the air over radio frequencies and can be captured by anyone within range of the signal, sometimes up to miles away. Another risk is that a laptop connected at home to a Linksys, D-Link, Belkin or other common hot spot Wireless Access Point (WAP) that uses the default Service Set Identifier (SSID) remembers this SSID and later automatically attempts to connect to another WAP with the same default SSID "leaking" into the workspace. Similarly, users can unknowingly connect to a fake WAP set up with a default SSID near normal Wi-Fi areas like hotels, libraries, or coffee shops. No wireless (or any) network is completely safe. However, a Wireless Local Area Network (WLAN) can be used with minimal risk. Usage of home, conference or hotel wireless networks is allowed when authorized. VPN or other approved authentication and encryption is essential.

Wireless Best Practices

An AirCard is a device for a laptop, tablet or cell phone that allows the user to connect to wide area wireless Internet access using an available USB port or PCMCIA slot. When used with a VPN and employing strict administrative procedures to ensure that the devices' internal wireless capability is disabled, this can be an acceptable method of using wireless Internet access for teleworkers or domestic travelers.

[Take Cyber Exam](#)

Click Take Cyber Exam to begin the exam.

[Submit Answers](#)

Click Submit Answers if you are sure you have answered all the questions. You must answer at least 7 questions correctly to pass the exam.

After answering all the questions, click **Submit Answers**.

DAART Security Awareness

Exam Name: DOMOPS Awareness and Assessment Response Tool (DAART) Security Awareness Training Exam

Total Questions: 10

You have failed the exam with a score of 20. A score of 70 is required to pass the exam.

[Take the test again now](#)

[Not now, maybe later](#)

If you do not pass the exam you can take it again.

DAART Security Awareness

Exam Name: DOMOPS Awareness and Assessment Response Tool (DAART) Security Awareness Training Exam

Total Questions: 10

Congratulations, selwyn.reynolds, you have passed the DAART Security Awareness Exam! Date: 3/10/2022 7:58:17 PM

[Submit Certificate](#)

After passing the exam click **Submit Certificate**.

DAART Security Awareness

Exam Name: DOMOPS Awareness and Assessment Response Tool (DAART) Security Awareness Training Exam

Total Questions: 10

Congratulations, selwyn.reynolds, you have passed the DAART Security Awareness Exam! Date: 3/10/2022 7:58:17 PM

Certificate Submitted.

Close

A certificate will be generated and a valid expiration date will be entered automatically on the Training Certificates Page. Click **Close** to return to the Training Certificates Page.

Upload a current Intelligence Oversight Training Certificate in same manner as the Cyber Security Training certificate and enter a valid expiration date in the calendar box. Please note that the expiration date is 1 year out from the date on the certificate.

If you do not have a current Intelligence Oversight Training certificate you can take the training provided by DAART. Click the **Take IO Training** link to open the training.

NATIONAL GUARD BUREAU

2022 INTELLIGENCE OVERSIGHT AND PROTECTION OF NON-DOD AFFILIATED PERSON INFORMATION TRAINING

National Guard Bureau
Joint Intelligence Directorate
Intelligence Oversight Team
ng.ncr.ngb-armg.list.ngb-j2-intel-oversight@army.mil

Ms. GIGI Singleton NGB-J2 Intelligence Oversight Official	Mr. Bob Evans NGB-J2 Intelligence Oversight Policy Analyst
(703) 607-5502	(703) 601-8109
gigie.f.singleton.civ@army.mil	robert.g.evans12.civ@army.mil

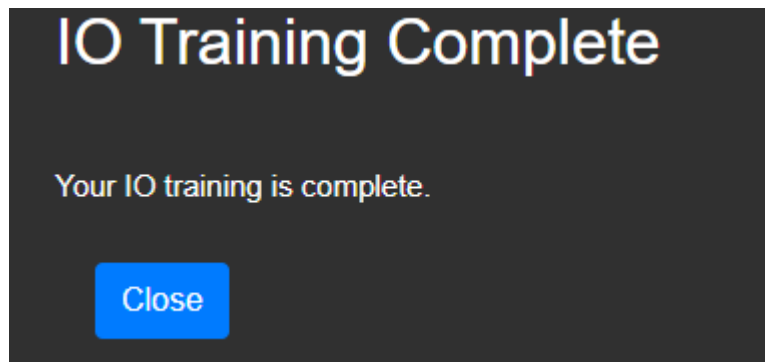
Agenda

- National Guard Information Users
 1. Intelligence Oversight Policy
 2. Protection of Non-DoD Affiliated Persons Information Policy

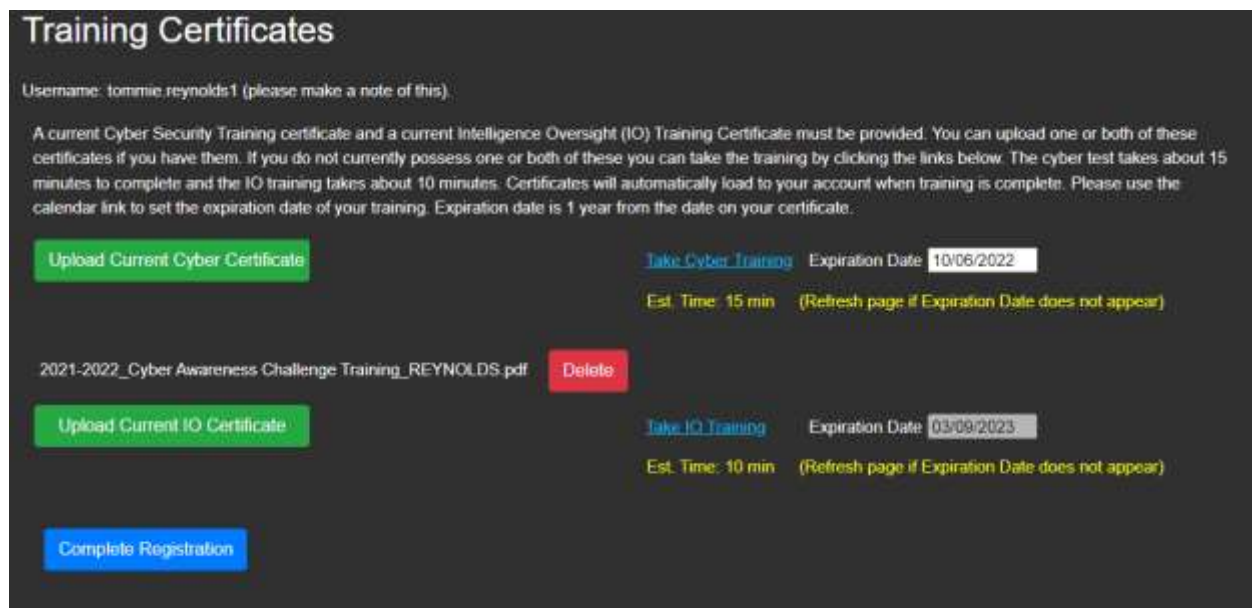
Submit

By clicking Submit, I agree that I have read and understand the Intelligence Oversight Training and will abide by the training in the use of the National Guard Bureau DOMOPS Awareness and Assessment Response Tool.

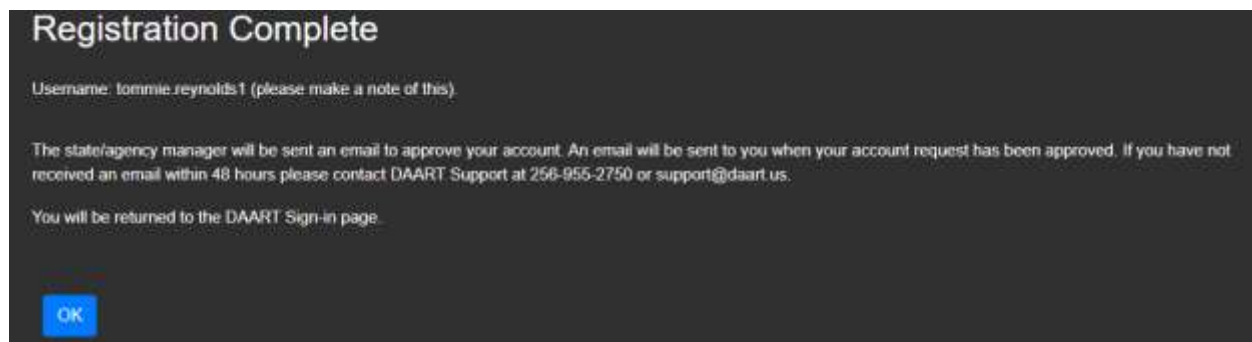
At the end of the training, click **Submit**. The system will automatically fill in the expiration date for you.



Click Close to be taken back to the Training Page.

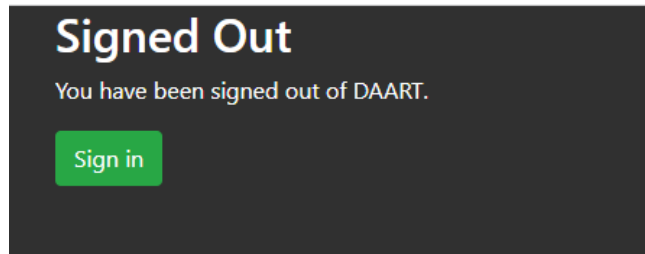
A dark gray rectangular box titled "Training Certificates" in white. Below the title, it says "Username: tommie.reynolds1 (please make a note of this)." followed by a paragraph of instructions. There are two main sections for uploading certificates. The first section has a green button "Upload Current Cyber Certificate", a blue link "Take Cyber Training", an "Expiration Date" field with the value "10/06/2022", and a yellow text "Est. Time: 15 min (Refresh page if Expiration Date does not appear)". The second section has a green button "Upload Current IO Certificate", a blue link "Take IO Training", an "Expiration Date" field with the value "03/09/2023", and a yellow text "Est. Time: 10 min (Refresh page if Expiration Date does not appear)". Between these sections is a file upload area showing a file named "2021-2022_Cyber Awareness Challenge Training_REYNOLDS.pdf" with a red "Delete" button. At the bottom is a blue button "Complete Registration".

The Complete Registration button will be enabled when all training certificates and expiration dates have been provided. Click **Complete Registration**.

A dark gray rectangular box titled "Registration Complete" in white. Below the title, it says "Username: tommie.reynolds1 (please make a note of this)." followed by a paragraph of instructions. At the bottom is a blue button "OK".

DAART will generate a username for you from your first and last name (and possible ordinal at end of a username already exists for the same first/last name). **IMPORTANT! This username is for display purposes only within the system.**

Click **OK**.



You will be signed out of DAART and taken back to the log-in page.

You will receive an email when your account is approved. If the account cannot be approved you will receive an email with the reason.

New User Non-CAC (mobile app) Registration

DAART requires two factors of information in order to authenticate a user.

Mobile device authenticator apps generate a unique code every 30 seconds that provides the second factor (second = something you have). Your username and password together are the first factor (first = something you know)

You will need an authenticator app installed on your phone to get the second factor (6 digit code) to log into and register for DAART. See [Mobile Authenticator App Setup](#) (page 30) for instructions if needed.

Sign in to your account

Email

Password

☐ Remember me [Forgot Password?](#)

Sign In

Or sign in with

CAC

New user? [Register](#)

Click **Register**

Register

Minimum Password Requirements:

At least 15 characters

Any 2 of the following: & ! @ # \$ % ^ * _ - + = \ , . : ; / <

2 Numbers

2 Capital Letters

2 Lowercase Letters

First name

Last name

Email

Password

Confirm password

[« Back to Login](#)

Register

Enter your **first name**, **last name**, and **email** and create a **password** (*according to requirements listed in red*) then click **Register**.

Terms and Conditions

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Accept

Decline

Click Accept to accept the terms and conditions for use of DAART.

Email verification



You need to verify your email address to activate your account.

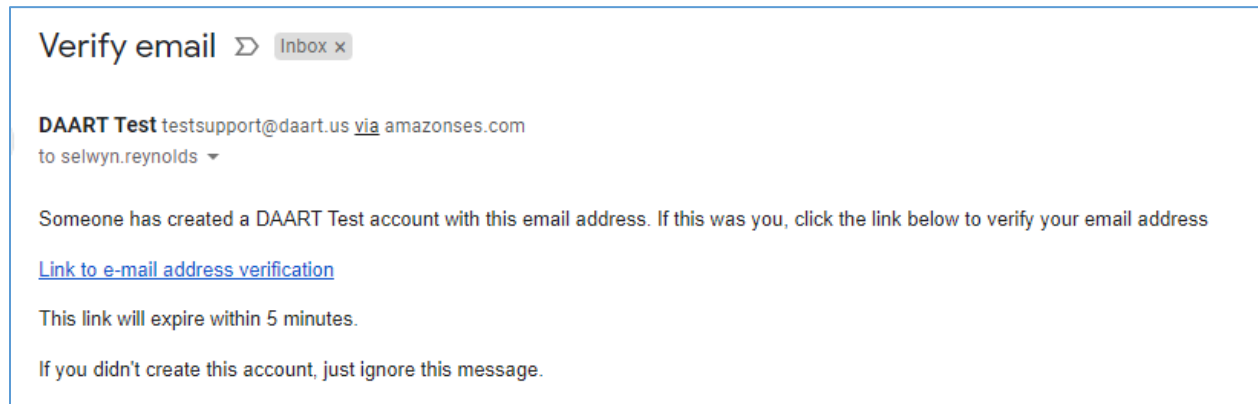
An email with instructions to verify your email address has been sent to you.

Haven't received a verification code in your email?

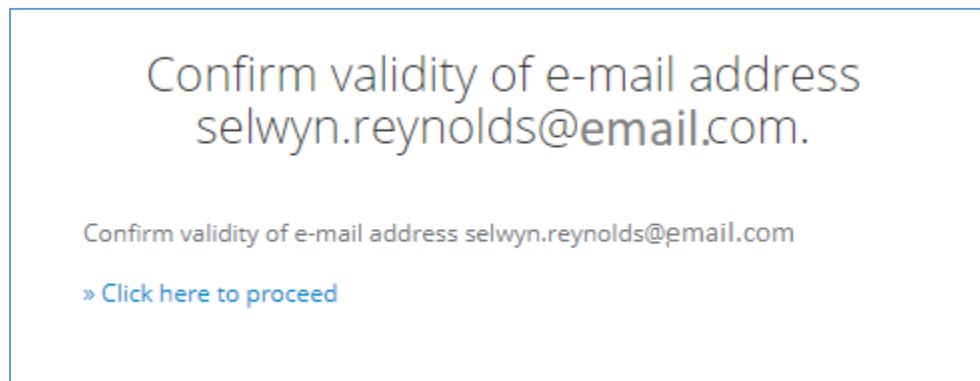
[Click here](#) to re-send the email.

DAART will need to verify your email address. An email will be sent to your address with a verification link in it. **** You must check your email on your computer, NOT your phone, to**

click the verify link. The authentication registration process must be started and completed on a computer, not on a mobile device.



Click the verification link to be taken to DAART to confirm the validity of your email address.



Click "Click here to proceed". At this point you will be taken to the DAART Mobile Authenticator Setup page to complete the authenticator app token registration by configuring the mobile authenticator setup.

Mobile Authenticator Setup



You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications (or other authenticator app) on your mobile device:

Google Authenticator

Microsoft Authenticator

2. Open the application and scan the barcode:



[Unable to scan?](#)

3. Enter the one-time code provided by the application and click Submit to finish the setup.

Provide a Device Name to help you manage your OTP devices:

The one-time code must be entered within 10 minutes.

One-time code from mobile app * (Required)

Device Name (Optional)


Submit

You will need an authenticator app installed on your phone to get the second factor (code) to log into and register for DAART. See [Mobile Authenticator App Setup](#) (page 30) for instructions if needed.

Follow the instructions on the **Mobile Authenticator Setup** screen to establish a token authenticator provider.

1. Scan the barcode with the authenticator app installed on your mobile device.
2. Enter the **6-digit one-time code** provided by the application on your mobile device in the box provided.

3. **Optional:** enter a name for the device (named reference for your phone if you want).
4. Click Submit.



The email associated with your new signin is also associated with an existing DAART account.
Click Continue to link this account to your new signin.

selwynreynolds@gmail.com

Verify

[Link to a different existing DAART account](#)

Go back to [sign in](#).

DAART will look for an account that matches the email entered during the app authentication registration. If an account is found you can link the existing account to the app token registration by clicking **Verify**. *You may be automatically directed to the Events Page or you may be taken to a page with a Sign In button. Sign in with the email you linked, password you created and a one-time code from the authenticator app.* If this is not your account, you can click **Link to a different existing DAART account** to be taken to the [Link/Continue Registration page](#) (page 5).

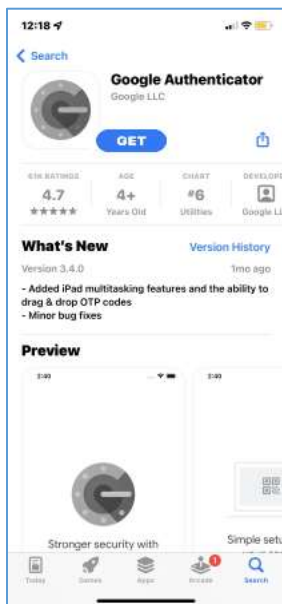
3. Mobile Authenticator App Set Up

You can use any mobile authenticator app. This document will provide instructions for installing and configuring the [Google Authenticator](#) (page 30) and [Microsoft Authenticator](#) (page 33) apps. *Screenshots are from an iPhone.*

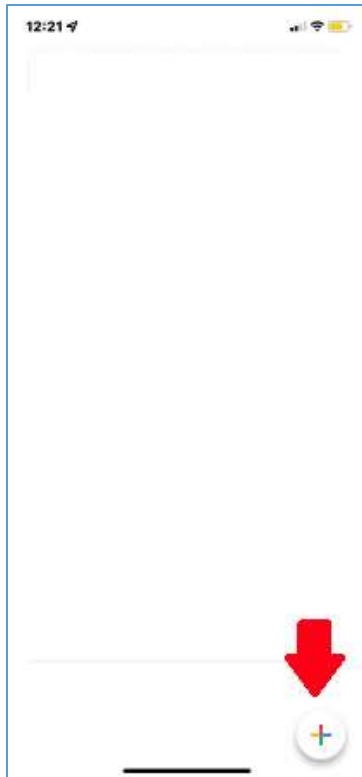
Google Authenticator App Setup

In the iPhone App Store or in Google Play Store, search for **Authenticator**.


Select the **Google Authenticator App** and install it (click **GET**).



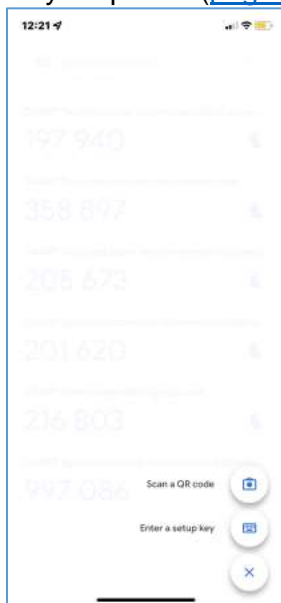
Open the app



The authenticator app will list the accounts that have been set up

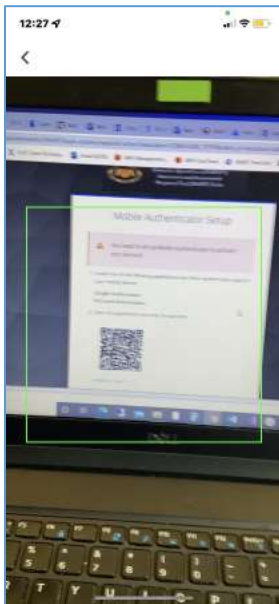
for your phone. On first use you will not have any accounts listed. Click the  **button** at the bottom to create a new account. The app will wait for you to scan a QR code.

During DAART registration, you will be provided a QR code to scan with the authenticator app on your phone ([page 28](#) of these instructions).




When DAART presents the QR code to scan, click the **Scan a QR code camera** button.

Point your phone at your computer screen and position the green box around the QR code displayed on DAART.




The app will automatically create an account that is only associated with DAART.

**** If the app is unable to scan the barcode, return to the main screen, click the  button then follow the instructions at [Unable to Scan Barcode on Google Authenticator App \(page 42\)](#) to manually configuring the mobile app account.**



This account will be updated with a new code (blue numbers) every 30 seconds. You will use this code whenever DAART prompts you to enter a one-time code (window below).

selwyn.reynolds@email.com



One-time code from mobile app

The one-time code must be entered within 10 minutes

Sign In

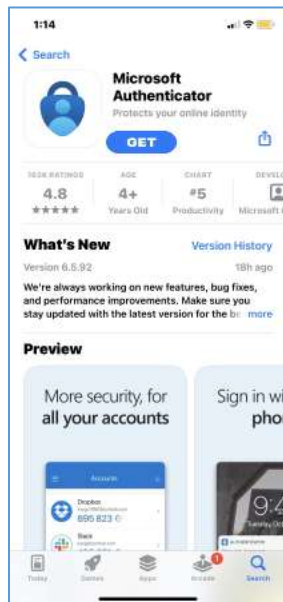
You will also use the code during initial account registration (and subsequent logins) as shown on [page 28](#) of these instructions.

End Google Authenticator App setup, return to [Existing User Non-CAC registration](#) (page 7) or [New User Non-CAC registration](#) (page 23) if in the process of registering this authentication method.

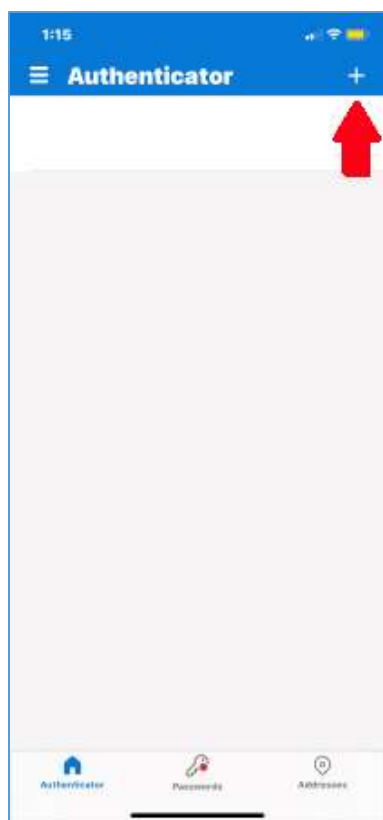
Microsoft Authenticator App Setup

In the iPhone App Store or in Google Play Store, search for **Authenticator**.

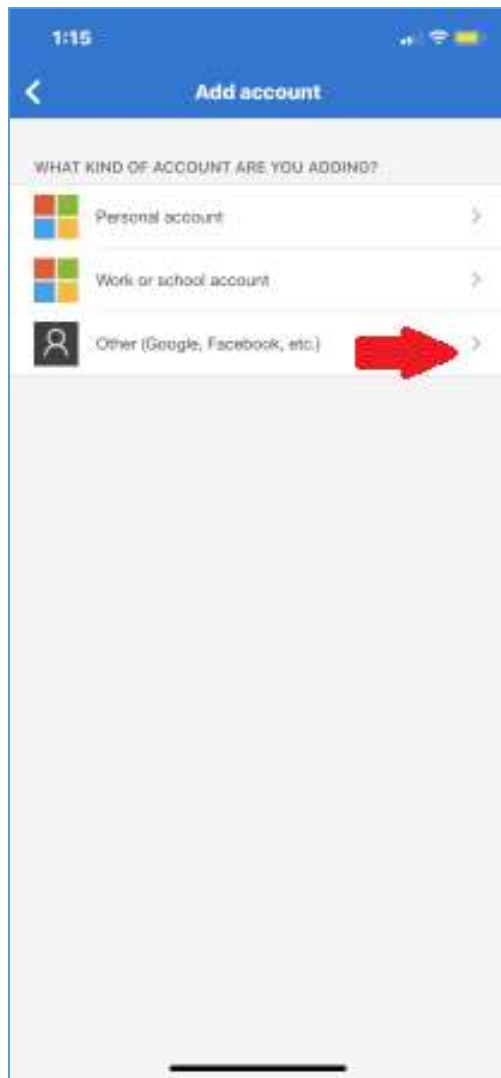
Select the **Microsoft Authenticator App** and install it (click **GET**).



Open the app

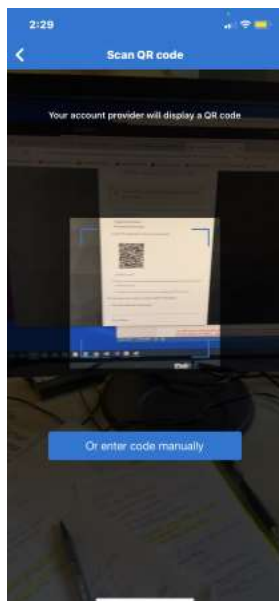


The authenticator app will list the accounts that have been set up for your phone. On first use you will not have any accounts listed. Click the **+** button at the top to create a new account.



Select **Other (Google, Facebook, etc.)** for the type of account. Click the ➤ on the right.

During DAART registration, you will be provided a QR code to scan with the authenticator app on your phone ([page 28](#) of these instructions).

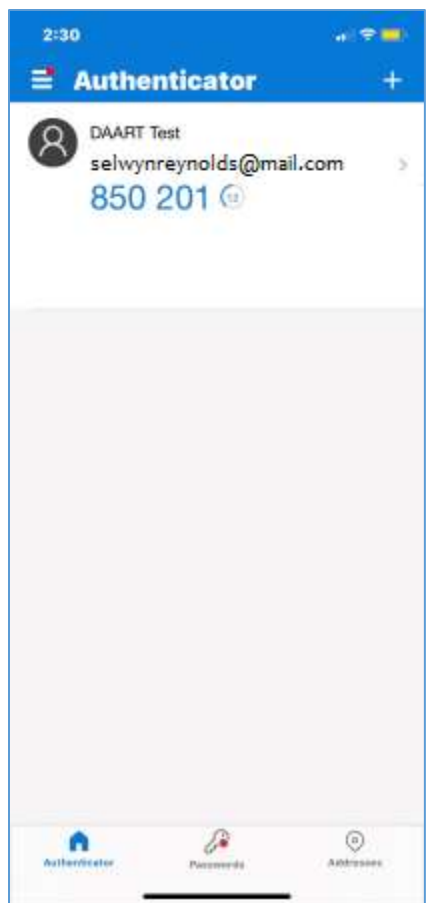


The app will wait for you to scan a QR code.

When DAART presents the QR code to scan, point your phone at your computer screen and position the box with blue corners over the QR code displayed on DAART.

**** If the app is unable to scan the barcode, click the “Or enter code manually” button then follow the instructions at [Unable to Scan Barcode on Microsoft Authenticator App \(page 44\)](#) to manually configuring the mobile app account.**

The app will automatically create an account that is only associated with DAART.



This account will be updated with a new code (blue numbers) every 30 seconds. You will use this code during registration and subsequent logins when DAART prompts you to enter a one-time code (window below).

selwyn.reynolds@email.com

One-time code from mobile app

The one-time code must be entered within 10 minutes

Sign In

You will also use the code during initial account registration (and subsequent logins) as shown on [page 28](#) of these instructions.

End Microsoft Authenticator App setup, return to [Existing User Non-CAC registration](#) (page 7) or [New User Non-CAC registration](#) (page 23) if in the process of registering this authentication method.

4. Log In to an Existing Account

If you have registered for CAC and/or Mobile App authentication you will take the following steps to log in to DAART.



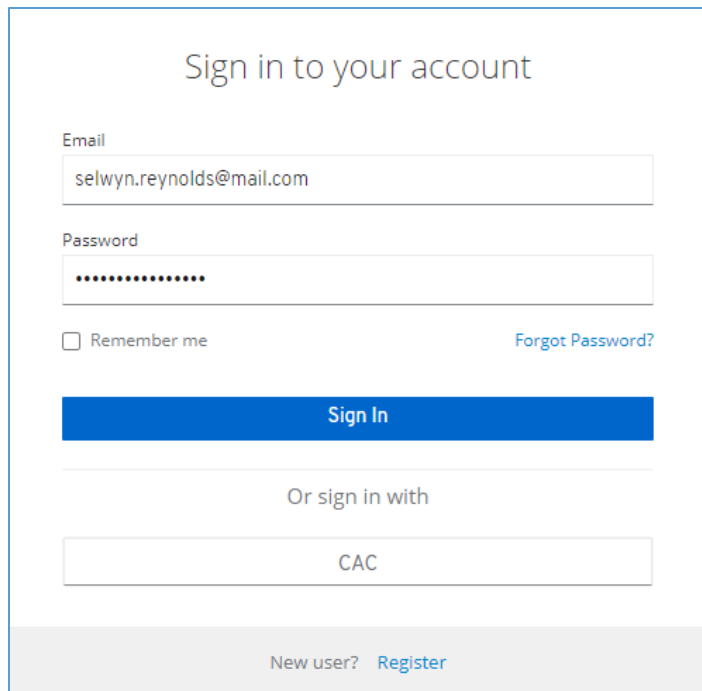
Click the **Sign in or Register for a New Account** button.

Sign in with CAC

You will follow the same instructions used to register your CAC. Click the CAC button, select your certificate, enter your PIN when prompted, and click OK to enter DAART.

Sign in with Mobile App

You will need to open the mobile app on your phone.



Sign in to your account

Email
selwyn.reynolds@mail.com

Password
.....

☐ Remember me [Forgot Password?](#)

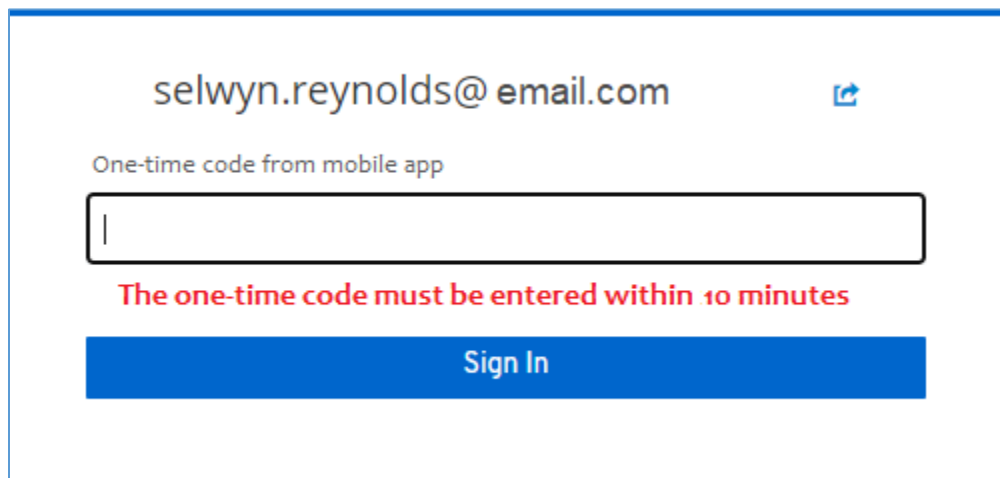
Sign In


Or sign in with

CAC

New user? [Register](#)

Enter your email address and password (created when you registered). Click **Sign In**.



selwyn.reynolds@email.com 

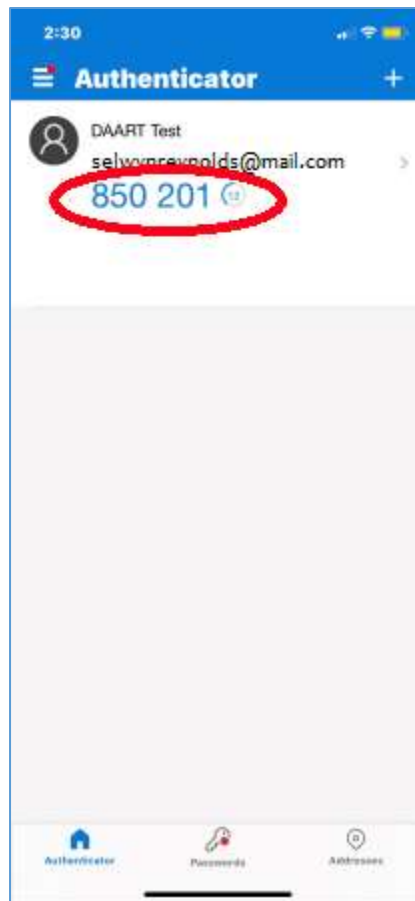
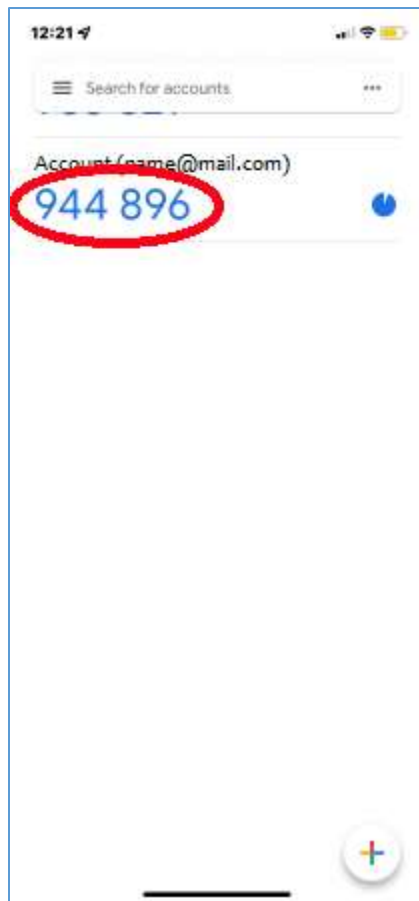
One-time code from mobile app

|

The one-time code must be entered within 10 minutes

Sign In

From the mobile app, enter the code displayed by your DAART account (blue numbers for Google and Microsoft Authenticator apps).



selwyn.reynolds@email.com

One-time code from mobile app

525252

The one-time code must be entered within 10 minutes

Sign In


Click **Sign In** to enter DAART.

5. Unable to Scan Barcode

Google Authenticator App

If the Google Authenticator App could not successfully scan the barcode on your computer, you should see the following screen after clicking the “[Unable to scan barcode?](#)” link.

Mobile Authenticator Setup

 You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications (or other authenticator app) on your mobile device:
Google Authenticator
Microsoft Authenticator
2. Open the application and enter the key:
K43H CQ3Q O54D G3TX IZJW 66DM MZLE MUKJ
[Scan barcode?](#)
3. Use the following configuration values if the application allows setting them:
Type: Time-based
Algorithm: SHA1
Digits: 6
Interval: 30
4. Enter the one-time code provided by the application and click Submit to finish the setup.
Provide a Device Name to help you manage your OTP devices.

The one-time code must be entered within 10 minutes.

One-time code from mobile app * (Required)

Device Name (Optional)

Submit

Open the Google Authenticator App



Click **Enter a setup key** button

2. Open the application and enter the key:

K43H CQ3Q O54D G3TX IZJW 66DM MZLE MUKJ

The key (unique for your registration) above should be manually entered into the Google Authenticator App on the screen below in the Secret key box. You must include the spaces between the groups of characters.

Enter Account name (can be DAART or anything you want), then enter the Secret key from the computer screen. Capitalization does not matter but the spaces between the groups of characters is required.

Click **Add** when key is entered.

The code that is displayed in the app after this should be entered in the One-time code from mobile app box.

The one-time code must be entered within 10 minutes.

One-time code from mobile app *

End Microsoft Authenticator App setup, return to [Existing User Non-CAC registration](#) (page 7) or [New User Non-CAC registration](#) (page 23) if in the process of registering this authentication method.

Microsoft Authenticator App

If the Microsoft Authenticator App could not successfully scan the barcode on your computer, you should see the following screen after clicking the “[Unable to scan barcode?](#)” link.

Mobile Authenticator Setup



You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications (or other authenticator app) on your mobile device:

Google Authenticator

Microsoft Authenticator

2. Open the application and enter the key:

K43H CQ3Q O54D G3TX IZJW 66DM MZLE MUKJ

[Scan barcode?](#)

3. Use the following configuration values if the application allows setting them:

Type: Time-based

Algorithm: SHA1

Digits: 6

Interval: 30

4. Enter the one-time code provided by the application and click Submit to finish the setup.

Provide a Device Name to help you manage your OTP devices.

The one-time code must be entered within 10 minutes.

One-time code from mobile app * (Required)

Device Name (Optional)

Submit

2. Open the application and enter the key:

K43H CQ3Q O54D G3TX IZJW 66DM MZLE MUKJ

The key above should be manually entered into the Microsoft Authenticator App on the screen below in the Secret key box. You must include the spaces between the groups of characters.

1:26

< Add account

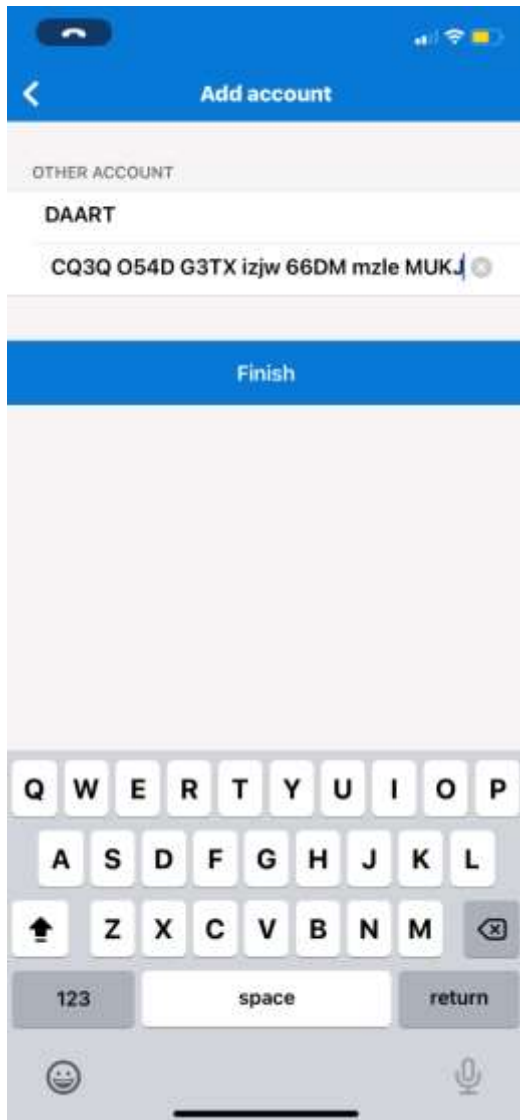
OTHER ACCOUNT

Account name

Secret key

Finish

Enter Account name (can be DAART or anything you want), then enter the Secret key (unique for your registration).



Capitalization does not matter but the spaces between the groups of characters is required.

Click **Finish** when key is entered.

The code that is displayed in the app after this should be entered in the One-time code from mobile app box.

The one-time code must be entered within 10 minutes.

One-time code from mobile app *

End Microsoft Authenticator App setup, return to [Existing User Non-CAC registration](#) (page 6) or [New User Non-CAC registration](#) (page 22) if in the process of registering this authentication method.