myAuth Account Creation Guide

Production Date:

November 2025

Prepared For:

Department of Defense (DOD) Defense Manpower Data Center (DMDC)

Document History

Document Version	Production Date	Description
1.3	November 2025	Updates for myAuth 1.02, including Simplified CAC Registration
1.2	September 2025	Updates for myAuth 1.01.1, including adding new FAQs
1.1	June 2025	Updates for myAuth 1.01
1.0	May 2025	Initial downloadable guide

Downloadable Filename: myauth_account_creation_guide.pdf

Table of Contents

1.0 Introduction

myAuth is a new, multi-factor authentication application the Department of Defense (DOD) is using to manage access to various DOD web applications and provide enhanced protection of your data. With myAuth, you can access the DOD applications you normally use through a single, secure sign-on.

2.0 Creating a New myAuth Account

To start using myAuth, you will need to complete three (3) steps:

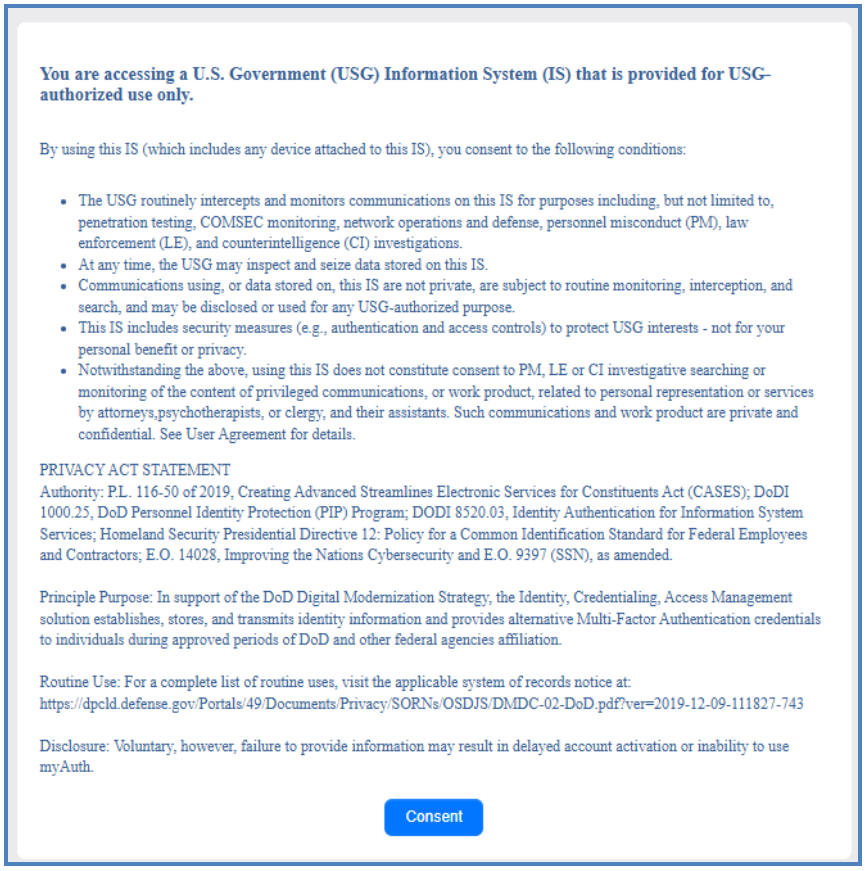
- Step 1 – Confirm Your Identity
- Step 2 – Create a myAuth Account
- Step 3 – Set up Your Security Methods

2.1 Step 1 – Confirm Your Identity

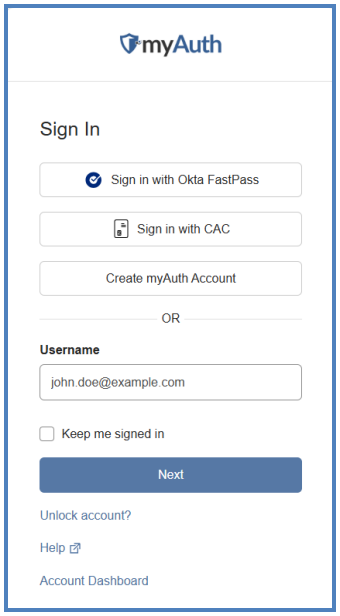
To create your new myAuth account, you will need to confirm your identity. This is an important part of making sure your personal information stays safe and secure. myAuth allows you to use your Common Access Card (CAC) or your DS Logon credentials to confirm your identity.

2.1.1 Confirm Your Identity with CAC

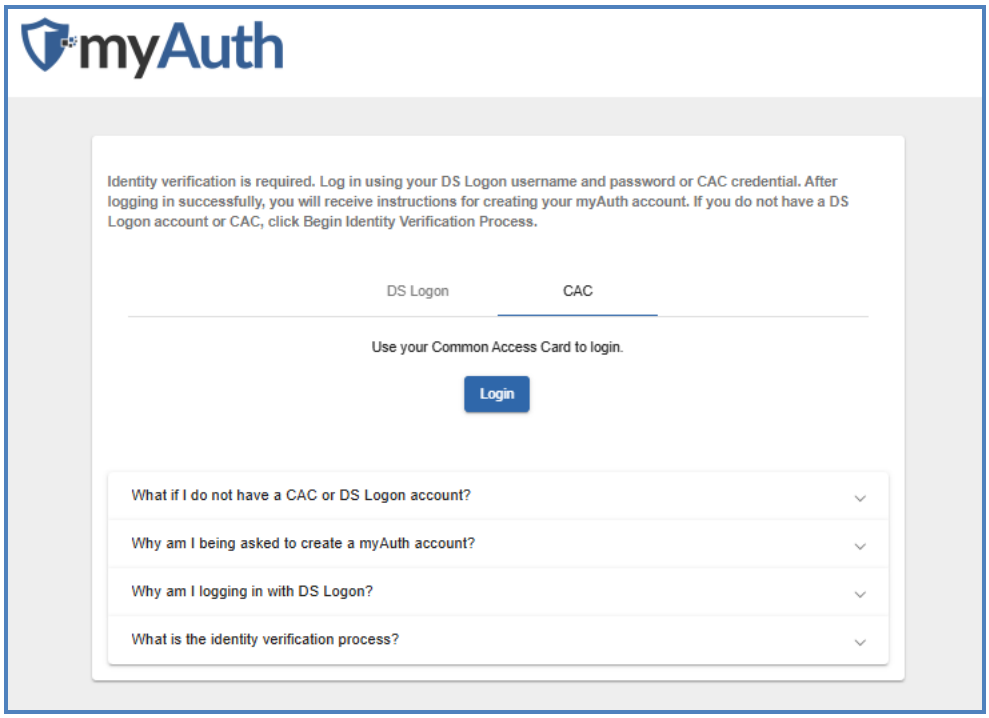
1. On the myAuth login page, read and click **Consent** on the DOD Consent to Monitor notification.



2. Click **Create myAuth Account** on the Login screen.

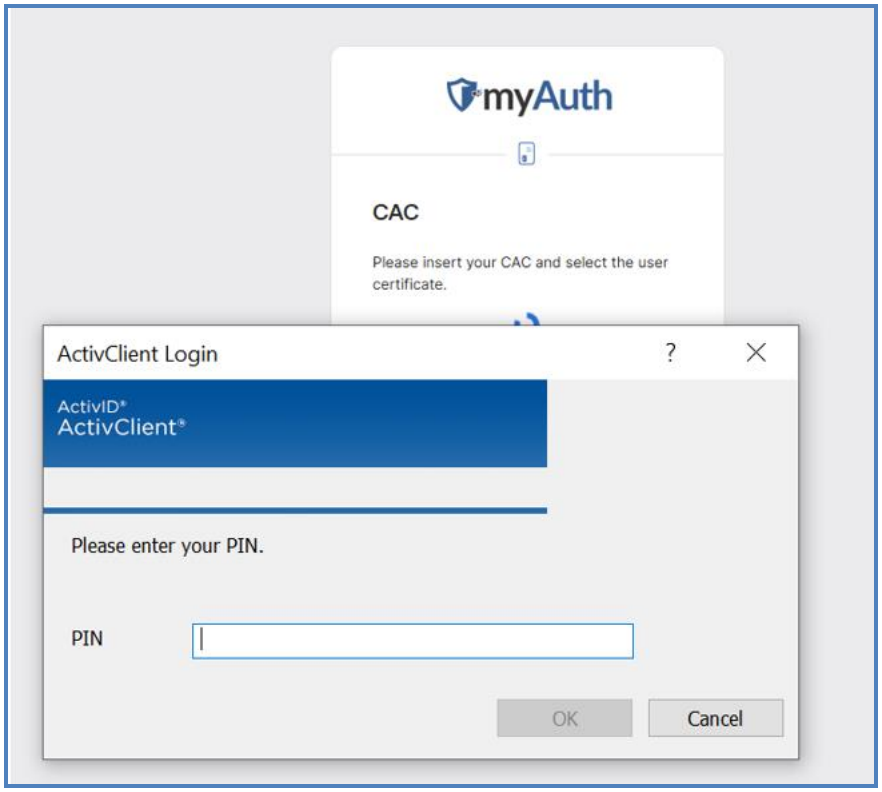


3. Click the **CAC** tab and click **Login**.



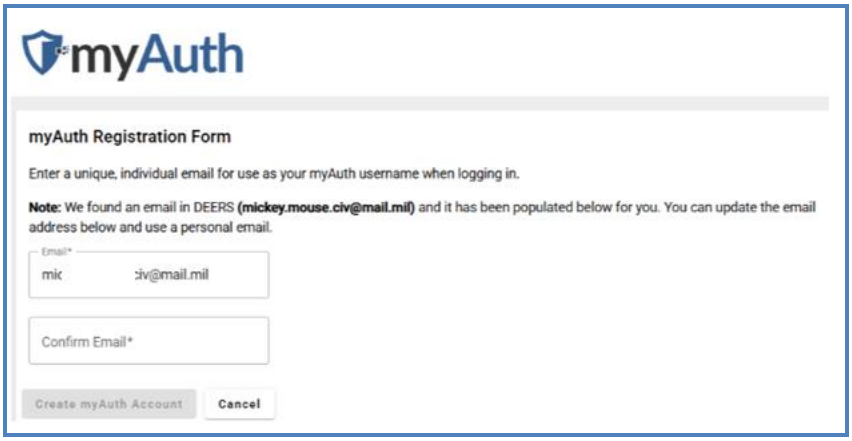
4. Select your CAC certificate if prompted and click **OK**.

5. Enter your CAC Personal Identification Number (PIN) and click **OK**, just like with a standard CAC login. The Registration Form opens.

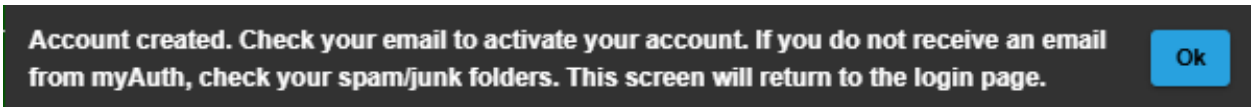


6. In the myAuth Registration Form window, enter an email address.

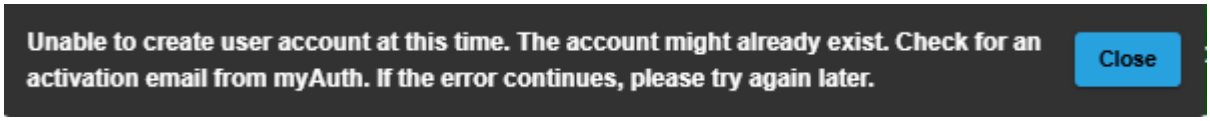
   Important: This email address will become your myAuth username and will receive the activation email. Enter a unique email address that no one else uses. Be sure to use an email address that you can access to receive the activation email. If you share an email address (for example, with a spouse), each person will need to enter a different email address for each account to be created.



7. Enter your email address again and click **Create myAuth Account**.
8. If you were successful, you will see a pop-up message at the top. Click **Ok**. You will be directed back to the login page.



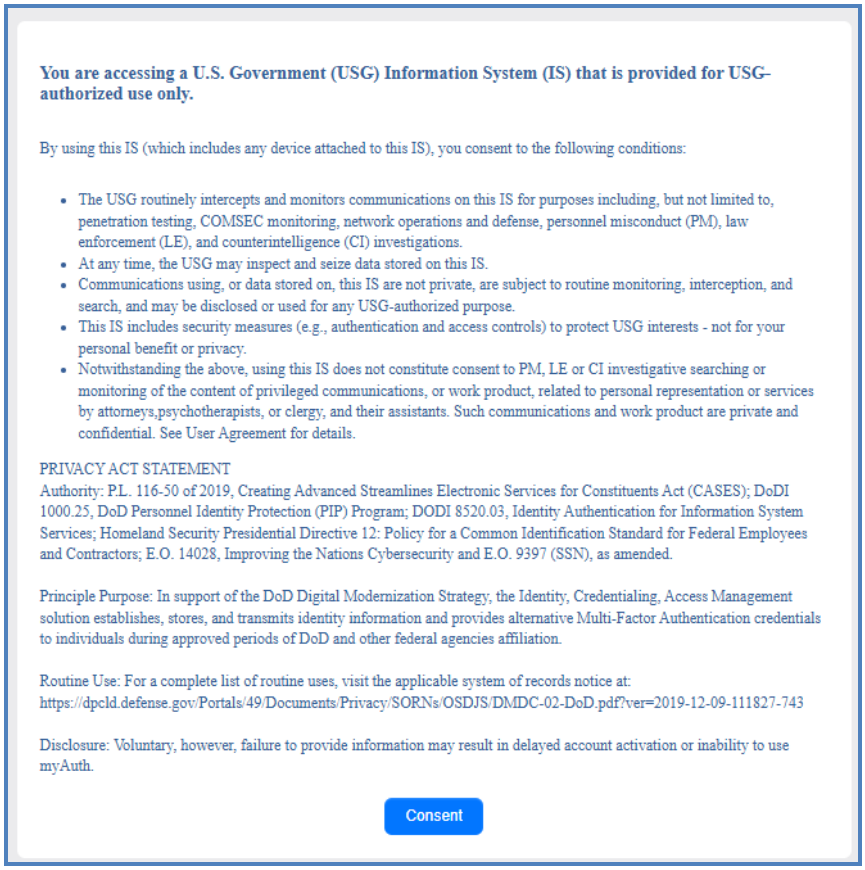
If the email has already been used to create a myAuth account, you will see a pop-up message at the top. Return to step 6 and enter a new email address. For additional assistance, see the "I see an error that says there might already be an account with my email. What can I do?" Frequently Asked Question (FAQ).



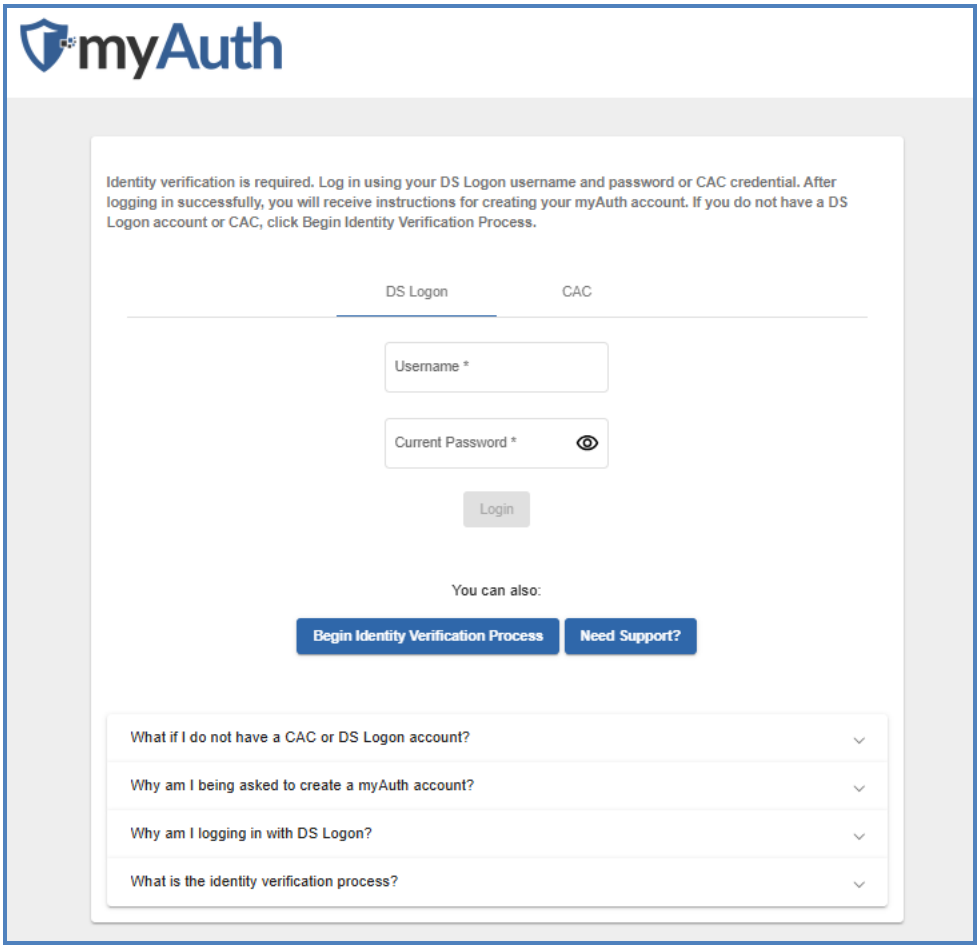
9. Identity verification is complete. You have two (2) options to finish creating your account:
   a. Once you have received an email from myAuth, use the activation email to create your account. If you did not receive the email, check your Spam or Junk folder. Continue to section 2.2, Step 2 – Create a myAuth Account.
   b. Click **Ok** on the pop-up message to return to the myAuth login screen. Click **Sign in with CAC** and follow the prompts to create your password. Continue to section 2.2, Step 2 – Create a myAuth Account.

2.1.2 Confirm Your Identity with DS Logon

1. On the myAuth login page, read and click **Consent** on the DOD Consent to Monitor notification.

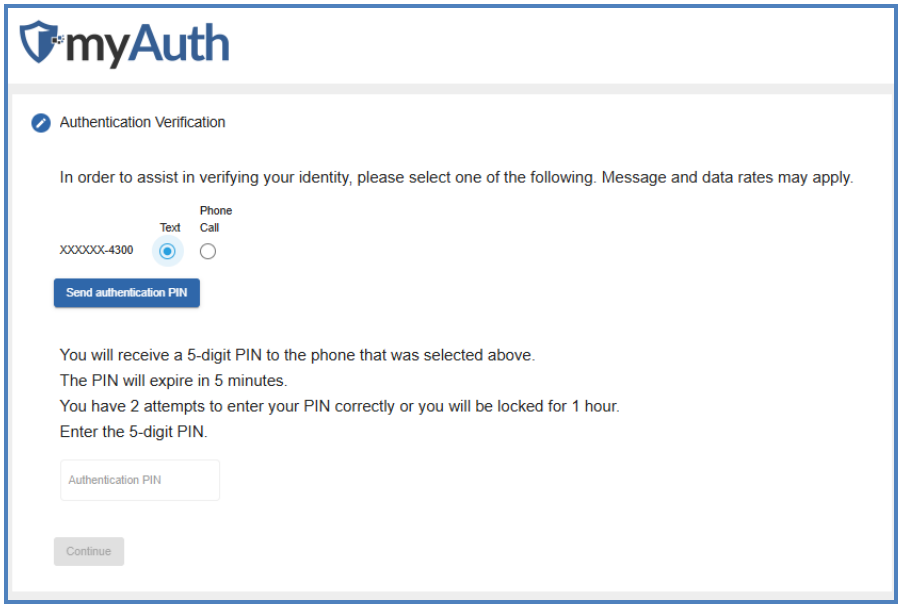


2. Click the **DS Logon** tab.

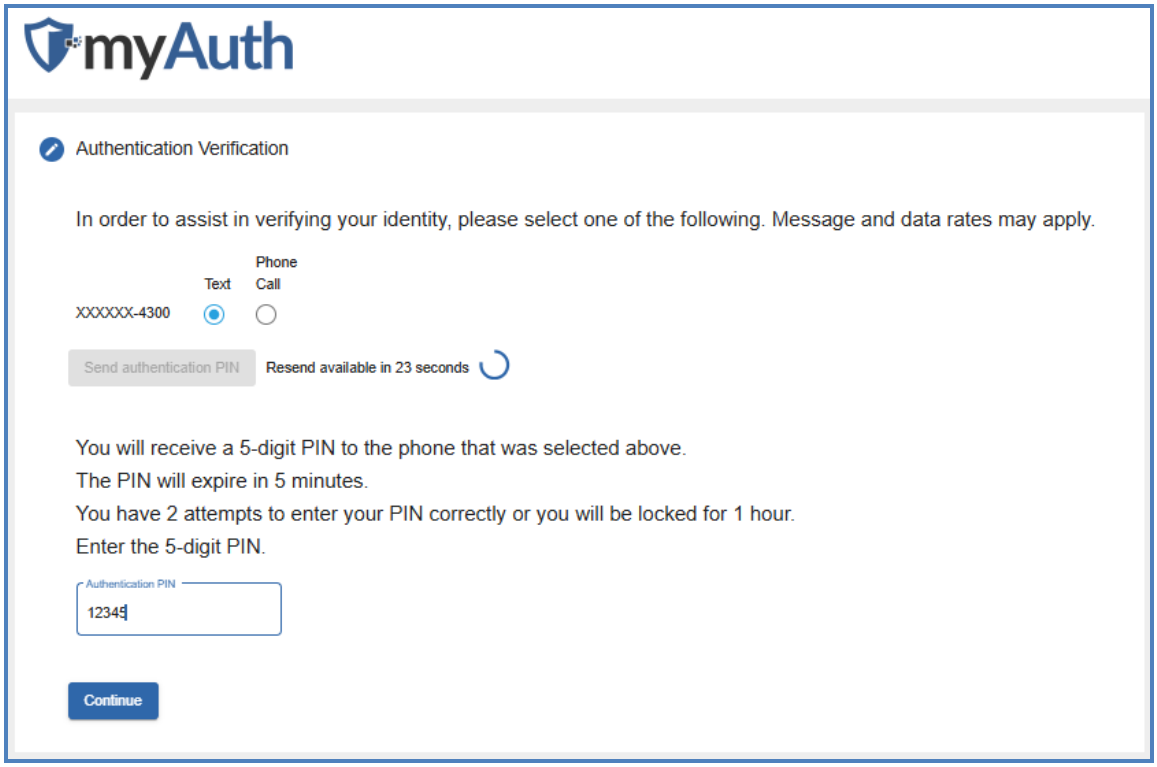


3. Enter your DS Logon username and password.

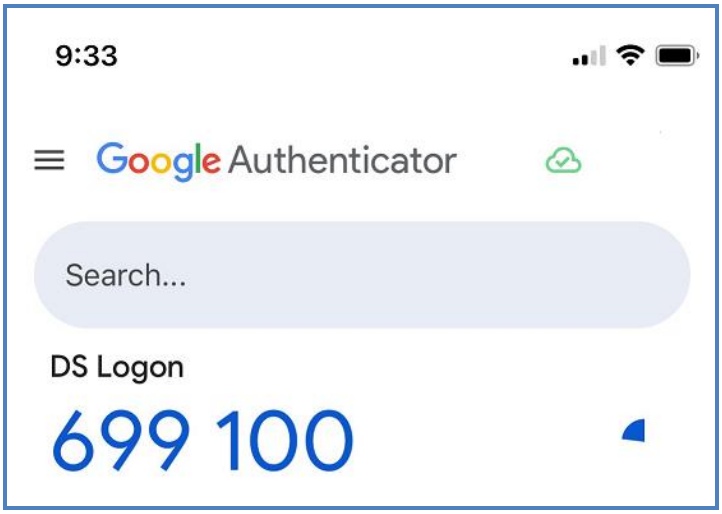
4. You will be required to complete Two-Factor Authentication (2FA). Choose a phone number and click **Send authentication PIN.**



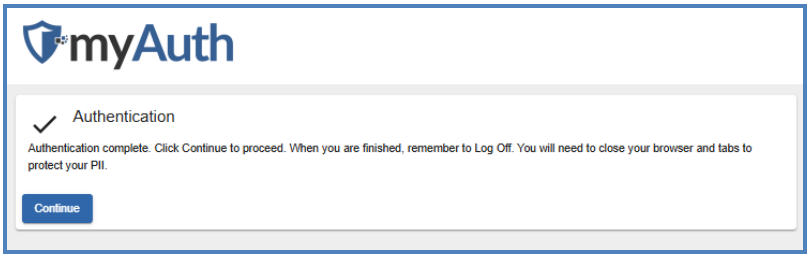
5. When you receive the message on your device, enter the 5-digit code and click **Continue**.



6. If you have set up Multi-Factor Authentication (MFA), you will need to enter the code from your authenticator app.

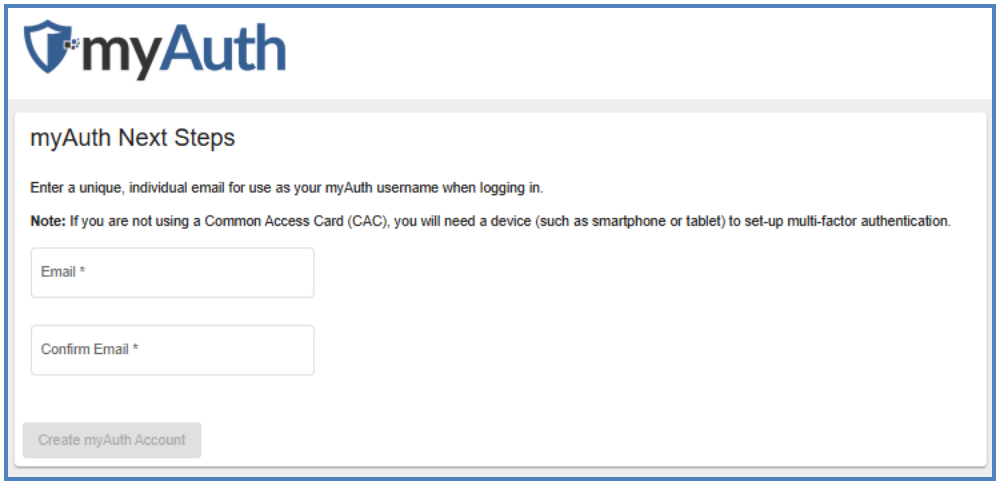


7. You will see the "Authentication Complete" message. Click **Continue**.



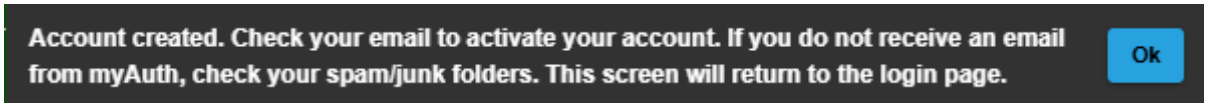
8. In the myAuth Next Steps window, enter an email address.

   Important: This email address will become your myAuth username and will receive the activation email. Enter a unique email address that no one else uses. Be sure to use an email address that you can access to receive the activation email. If you share an email address (for example, with a spouse), each person will need to enter a different email address for an account to be created.

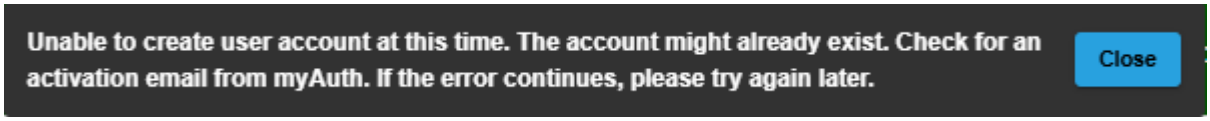


9. Enter your email address again and click **Create myAuth Account**.

10. If you were successful, you will see a pop-up message at the top. Click **Ok**. You will be directed back to the login page.



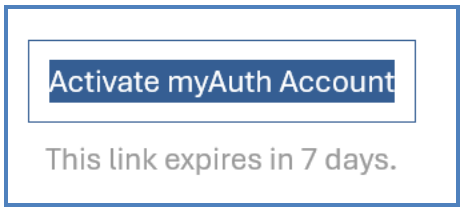
If the email has already been used to create a myAuth account, you will see a pop-up message at the top. Return to step 5 and enter a new email address. For additional assistance, see the "I see an error that says there might already be an account with my email. What can I do?" FAQ.



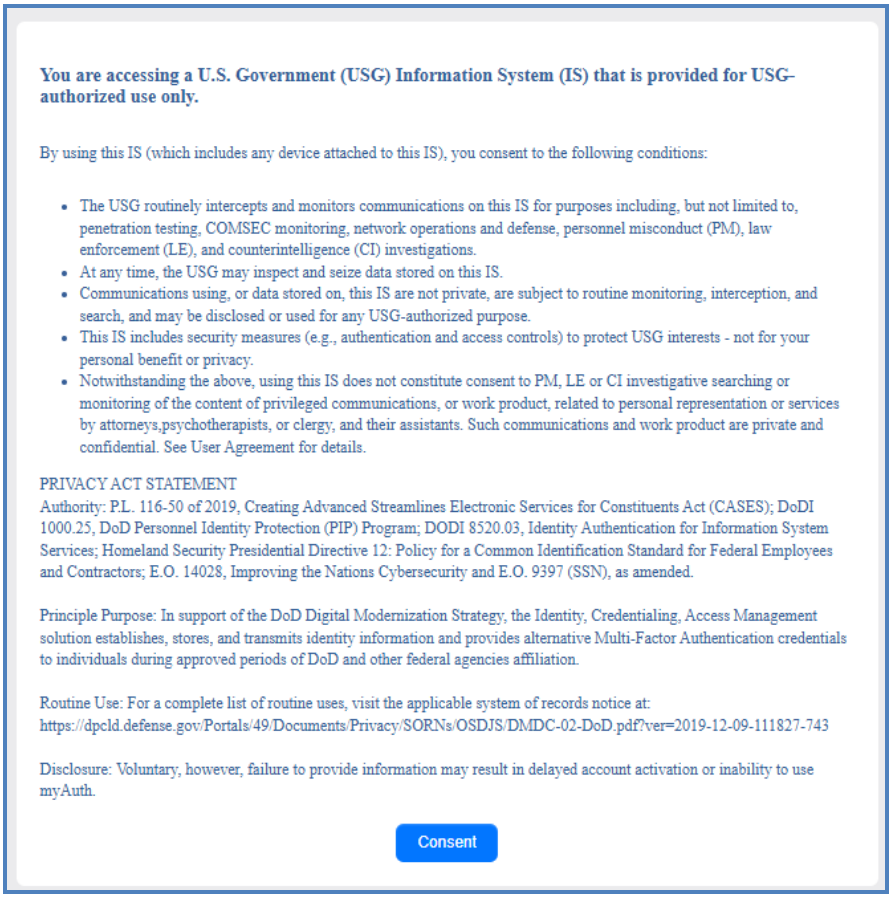
11. Identity verification is complete. Once you have received an email from myAuth, use the activation email to create your account. If you did not receive the email, check your Spam or Junk folder. Continue to section 2.2, Step 2 – Create a myAuth Account.

2.2 Step 2 – Create a myAuth Account

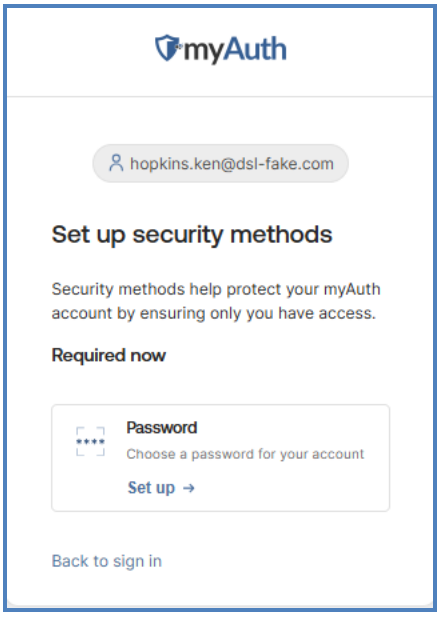
1. You will receive an email titled "Welcome to myAuth" at the email address you entered. This email will contain your username and a link for the myAuth login page.
2. Open the email and click **Activate myAuth Account**.



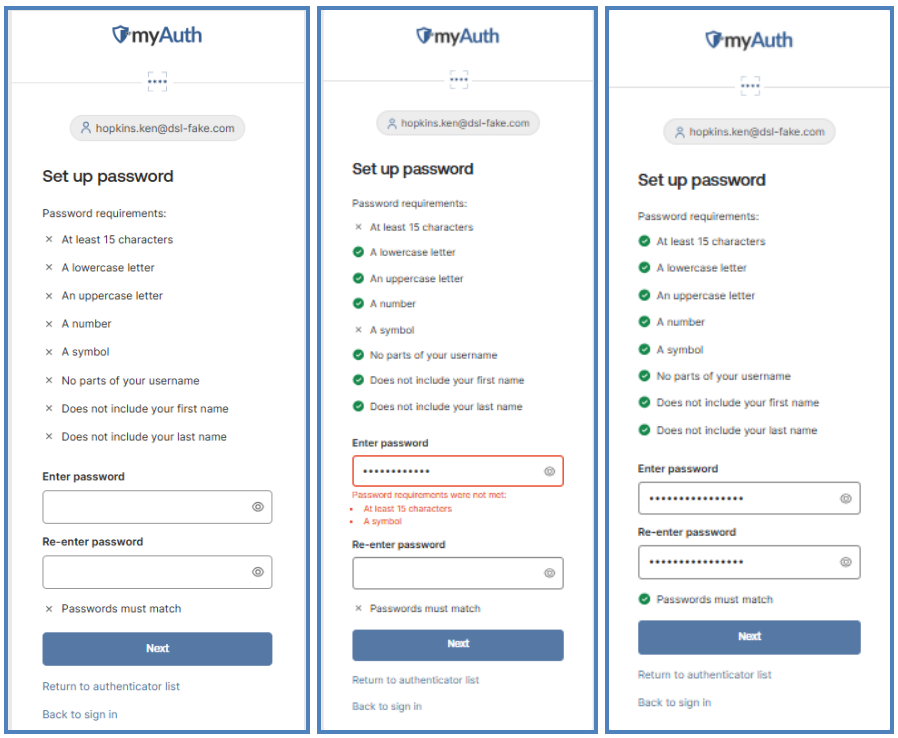
3. A new window will open in your browser. Click **Consent** to accept the standard DOD Consent to Monitor notification.



4. Click **Set up** under **Password**.



5. Create your password based on the listed requirements. Re-enter the password and click the blue **Next** button. Optionally, click the 'eye' icon to show the characters of your password. Continue to section 2.3, Step 3 – Set up Your Security Methods.

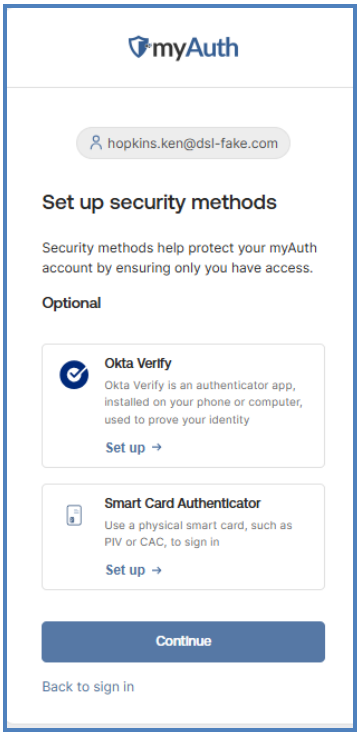


2.3 Step 3 – Set up Your Security Methods

You will be shown options for an additional security method. See the "Why do I need additional security methods? I already set up a password." FAQ for additional information.

- Choose a method (Okta Verify or Smart Card Authenticator) and click **Set up**.
  - **Okta Verify:** This free and secure app can be downloaded onto your phone. You can receive a one-time code in the app or a push notification.
  - **Smart Card Authenticator:** This option lets you link your CAC to your myAuth account.

Note: If you are not able to access either of these options, click **Continue** and you will be able to use the **Email One-Time Password** (OTP) option during login. An email will be sent to your myAuth primary email address with a link and a code you can use to authenticate.



2.3.1 For Okta Verify

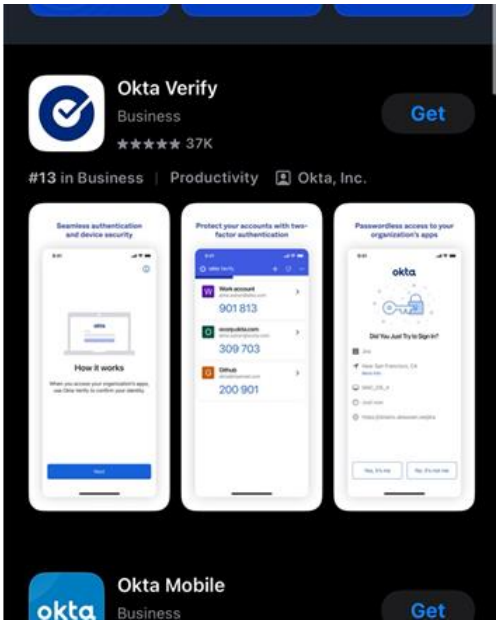
The following steps are only needed for users who choose to set up Okta Verify:

1. Click **Set up** under Okta Verify.

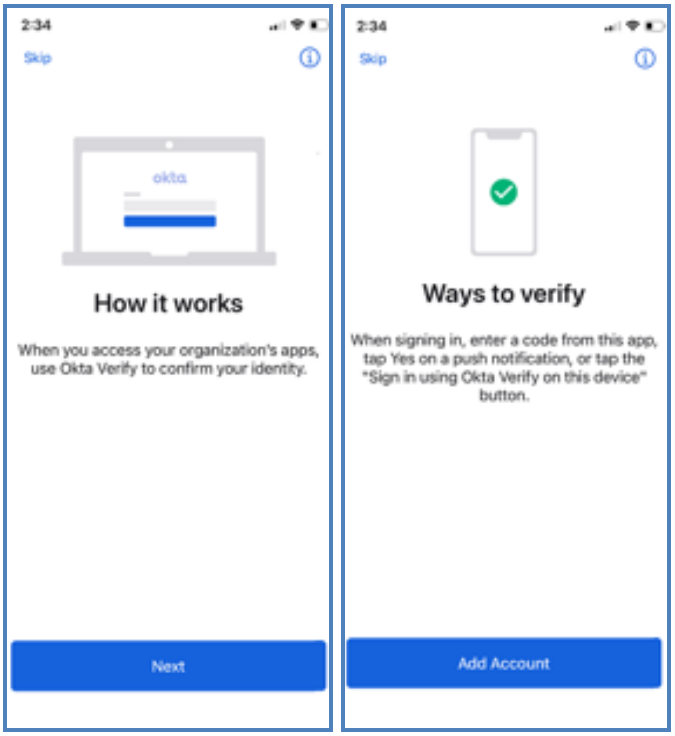
2. On the myAuth screen, you will see a QR code after you click **Set up**.

3. Download the free Okta Verify app onto your smartphone or device. You can search for **Okta Verify** in your device's app store.

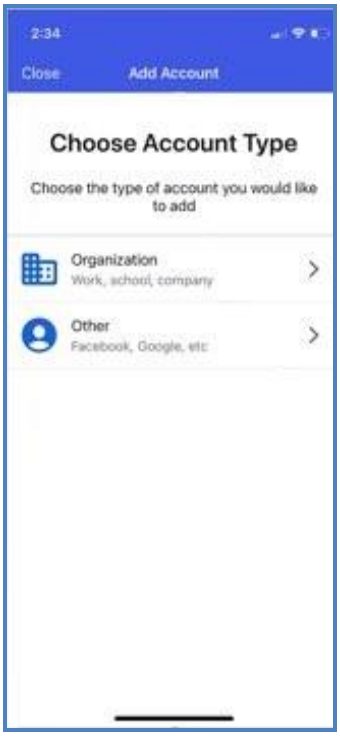
   Note: Be sure to download Okta Verify, not Okta Mobile or Okta Personal. There is no cost to download Okta Verify.



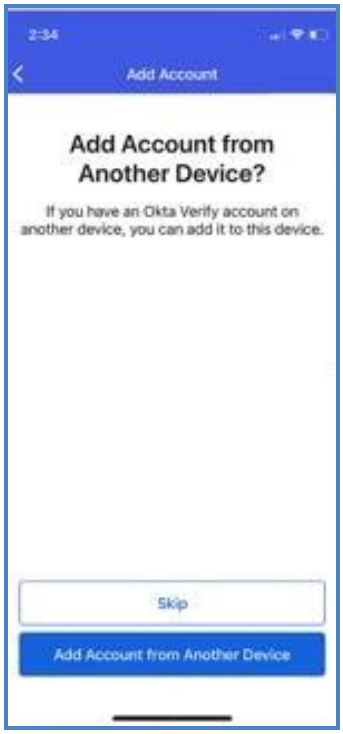
4. Open Okta Verify on your device. Okta will display informational screens to guide you through setup.



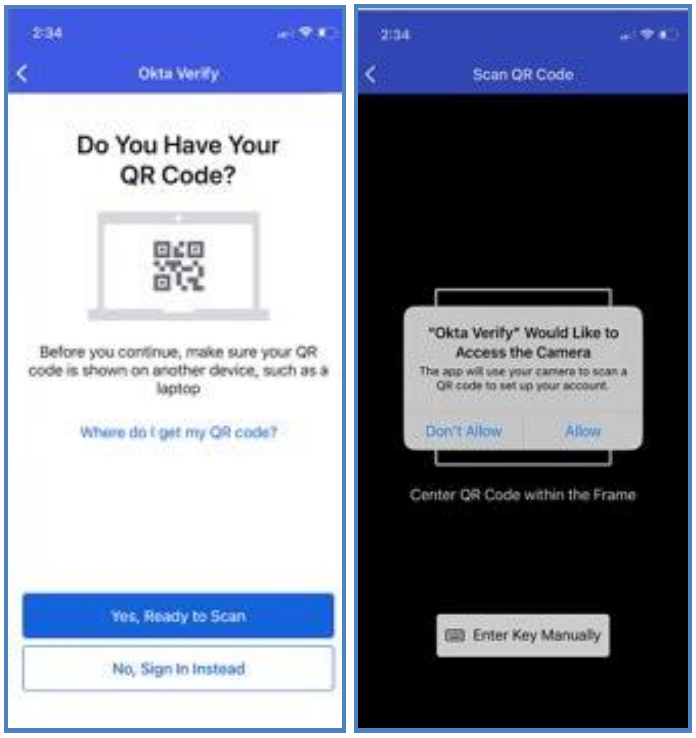
5. Select **Organization** for your **Account Type**. (Selecting **Other** will still allow you to add the account.)



6. **Optionally**, you can click **Skip** or choose to add an account from another device if you already use Okta Verify.



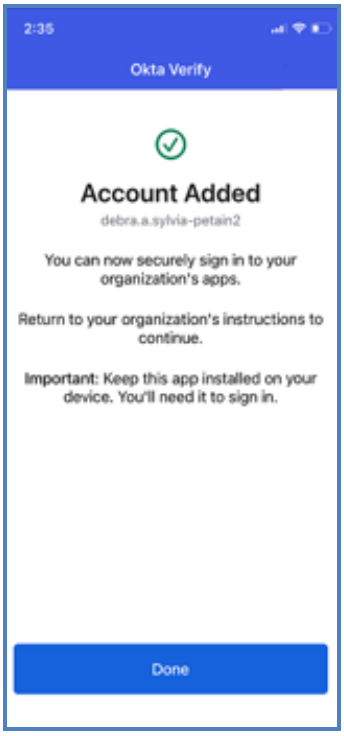
7. Okta Verify will ask you to scan the QR code on your other screen. Click **Allow** to allow the app to access your camera to scan the QR code. The app will automatically capture the QR code if you point the camera toward the code. You do not need to take a picture. See the "I am unable to scan the Okta Verify QR code. What can I do?" and "Okta Verify does not show me any codes or does not work on my device. What can I do?" FAQs if you need assistance.



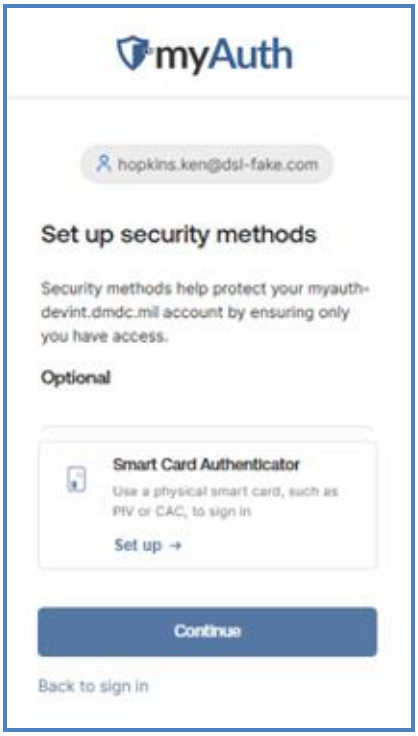
8. Okta Verify will let you choose whether you want push notifications turned on. A push notification is a notice that pops up on your device's screen, letting you authenticate without opening the app. You can choose **Allow** or **Skip**.

9. Okta Verify will ask if you want to use Face ID. Choose **Enable** or **Not Now**. Using Face ID adds an extra layer of security to your login and is recommended.

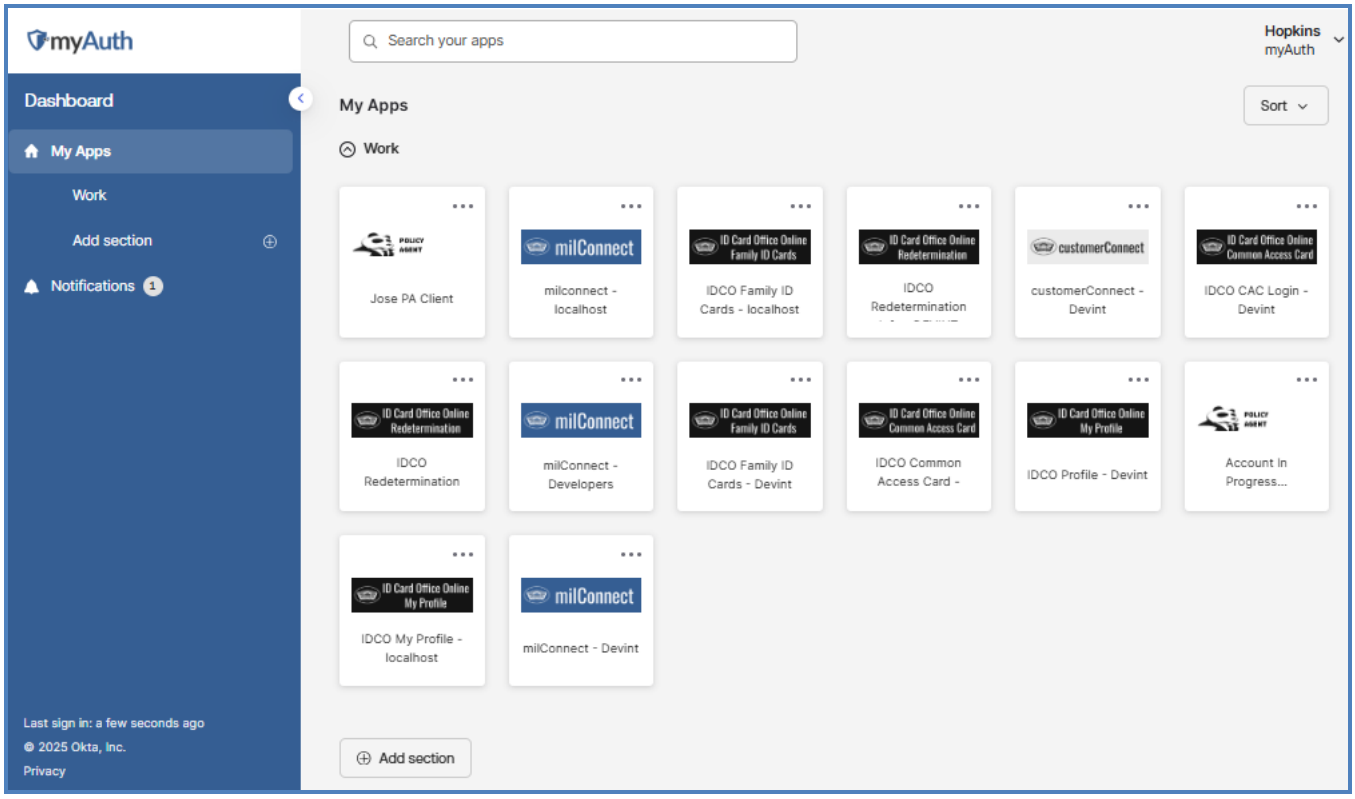
10. Okta Verify will confirm that your myAuth account has been added. You can close the app.



11. On your myAuth screen, you will have the option to connect a CAC as a security method. If you do not have a CAC, click **Continue**.



12. You will see your dashboard and the apps to which you have access. When you click on an app, you will be taken to the app and automatically logged in. The process is complete!



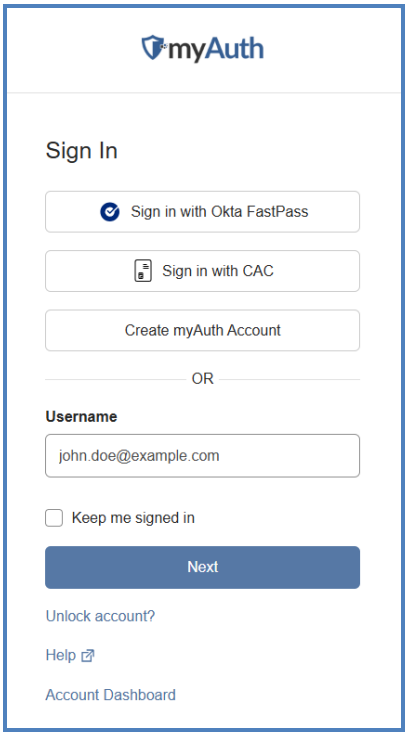
3.0 Logging In With myAuth

3.1 Logging In

You can authenticate through myAuth using your CAC, a username and password, or Okta FastPass. You can log in directly from a partner site (e.g., milConnect or Identity Card Online [IDCO]) or you can log into your myAuth dashboard and access partner sites with a single click.

3.1.1 Login with CAC

1. On the myAuth login screen, click **Sign In with CAC**. You may need to select your certificate and enter your CAC PIN.

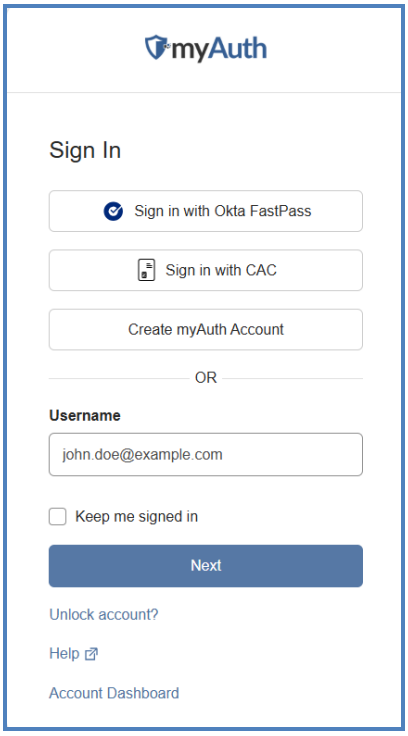


2. Depending on where you started the login process, you will see your myAuth dashboard, or be taken back to the partner site and logged in.

   Note: If you logged in through a partner site, you may need to read and click **Consent** on the site's DOD Consent to Monitor notification.

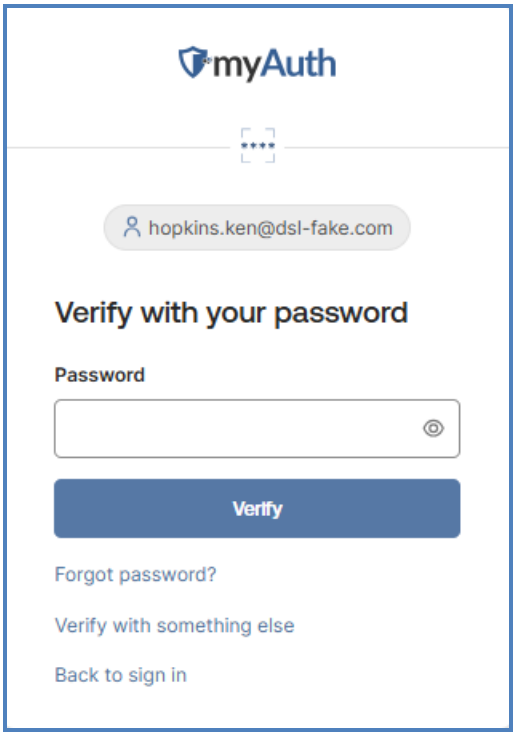
3.1.2 Login with Username

1. On the myAuth login screen, enter your **Username** and click **Next**.



2. Enter your password and click **Verify**.

   Note: Click the 'eye' icon in the password field to see the password as you type it.



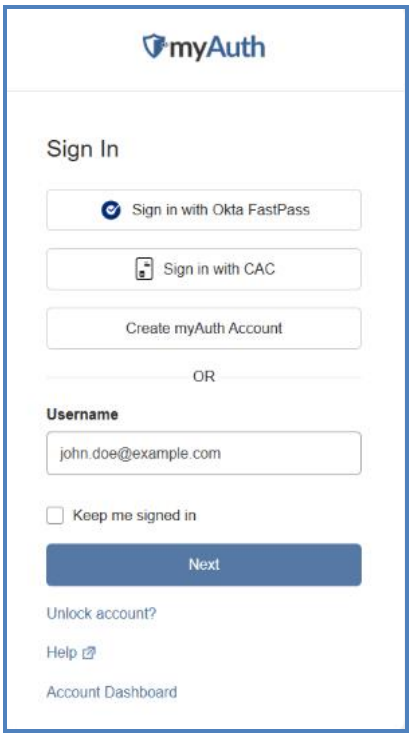
3. To maintain high levels of security for your personal information, you will always be asked to enter your password and one additional security method. Select an additional security method to complete the login. See section 3.2, Authenticating Using Security Methods, to learn more about each option.
4. Depending on where you started the login process, you will see your myAuth dashboard, or be taken back to the partner site and logged in.

   Note: If you logged in through a partner site, you may need to read and click **Consent** on the site's DOD Consent to Monitor notification.

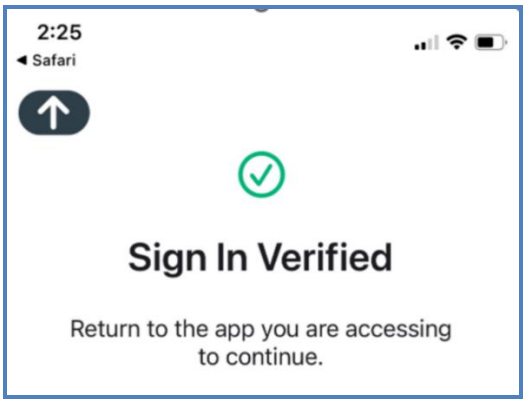
3.1.3 Login with Okta FastPass

1. On the myAuth login screen, click **Sign In with Okta FastPass**.

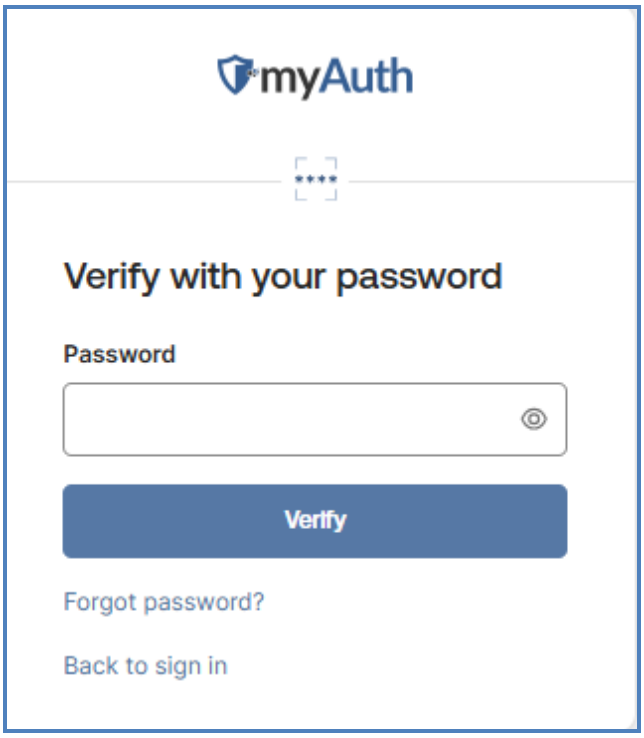
   Note: To use Okta FastPass, you must have the free Okta Verify app installed on the device from which you are logging in. When you enroll in Okta Verify, you automatically have access to FastPass. There is no cost for using FastPass.



2. Open the Okta Verify app on your device. If you have Face ID or Passcode Confirmation enabled in the Okta Verify app, the app will automatically verify your identity.



3. Close the Okta Verify app and return to your browser.
4. If you do not have Face ID or Passcode Confirmation enabled in the Okta Verify app, you will be prompted to enter your password. Enter your password and click **Verify**.



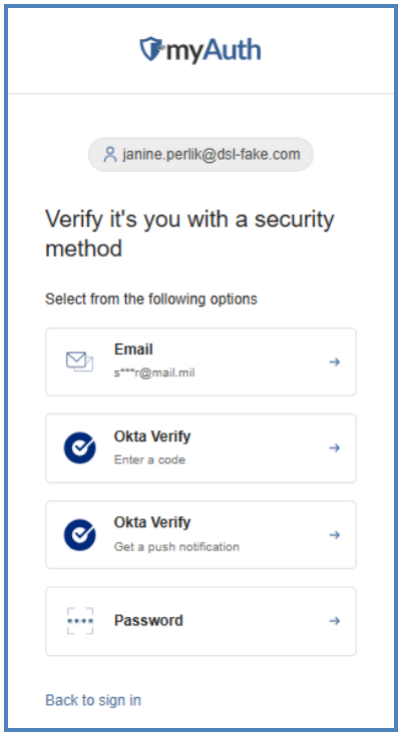
5. You are now authenticated. Depending on where you started the login process, you will see your myAuth dashboard, or be taken back to the partner site and logged in.

3.2 Authenticating Using Security Methods

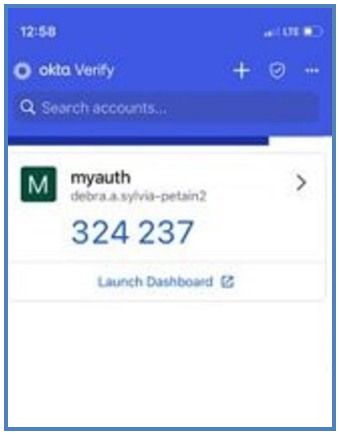
To maintain high levels of security for your personal information, you will always be asked to enter your password and one additional security factor.

3.2.1 Authenticate with Okta Verify Code

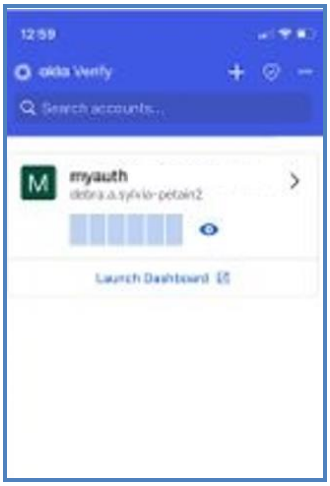
1. Click the blue arrow next to **Okta Verify - Enter a code**.



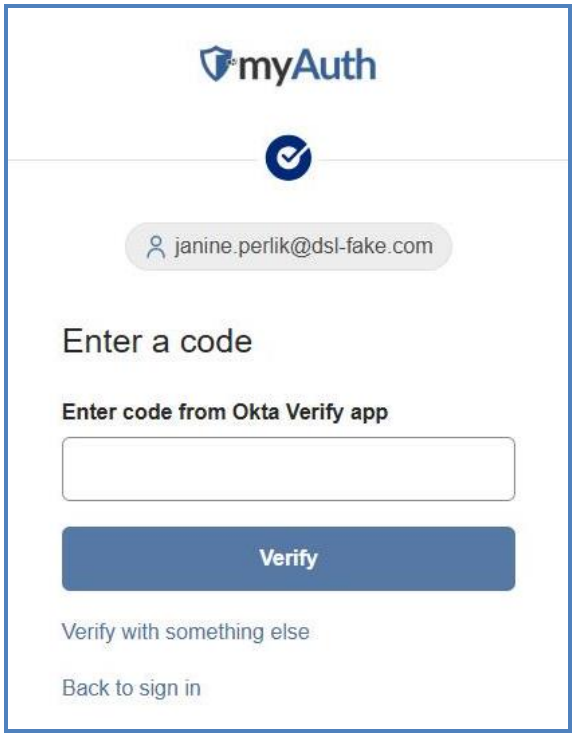
2. Open the Okta Verify app on your device. You will see a six-digit code.



If you have Face ID enabled, the numbers will be cloaked. Click the 'eye' icon to verify with Face ID and reveal the numbers.



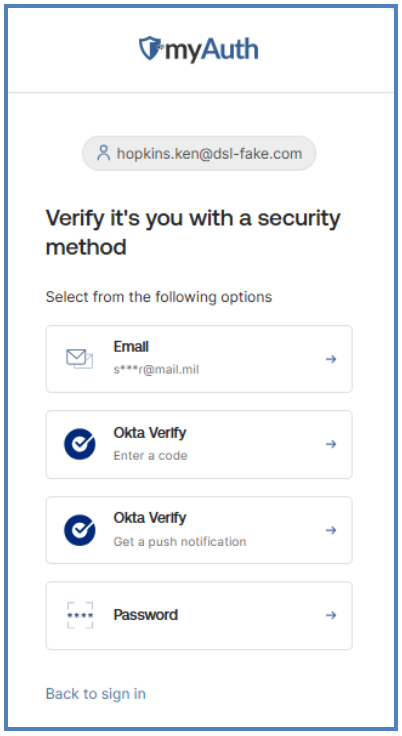
3. Enter the code on your myAuth login screen and click **Verify**.



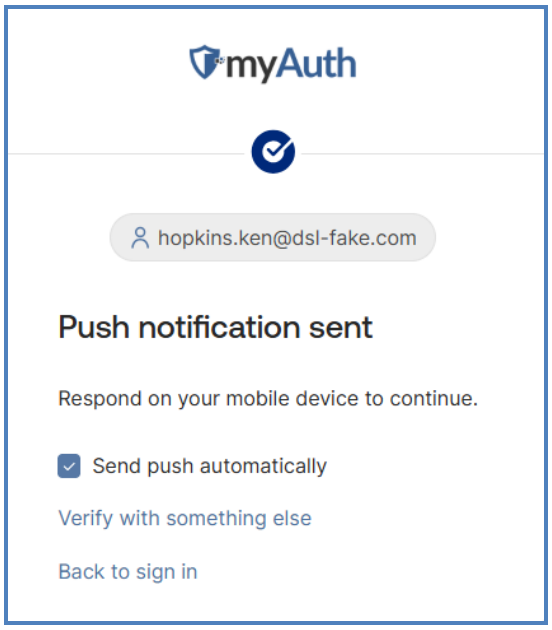
4. Close the Okta Verify app and return to your browser. Depending on where you started the login process, you will see your myAuth dashboard, or be taken back to the partner site and logged in.

3.2.2 Authenticate with Okta Verify Push Notification

1. If you have push notifications enabled, you can click the blue arrow next to **Okta Verify - Get a push notification**.

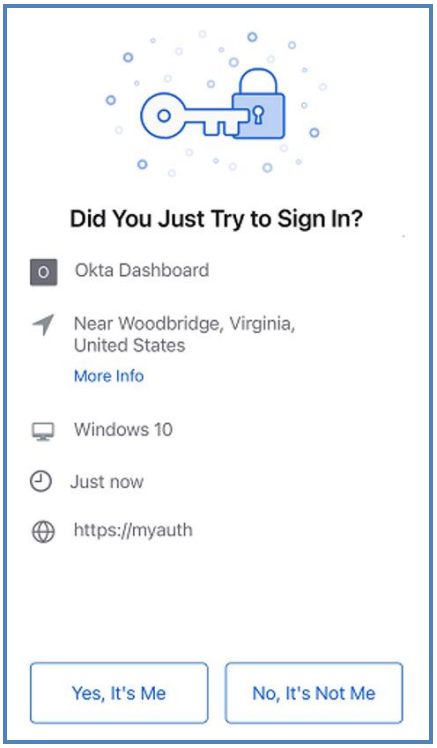


2. Optionally, you can select or de-select the **Send push notifications automatically** check box if you want to receive push notifications any time you log into myAuth.



3. Check your device and select the notification. You can also verify the notification without opening the app by touching and holding the notification or swiping down (on supported devices) and tapping the approve option.

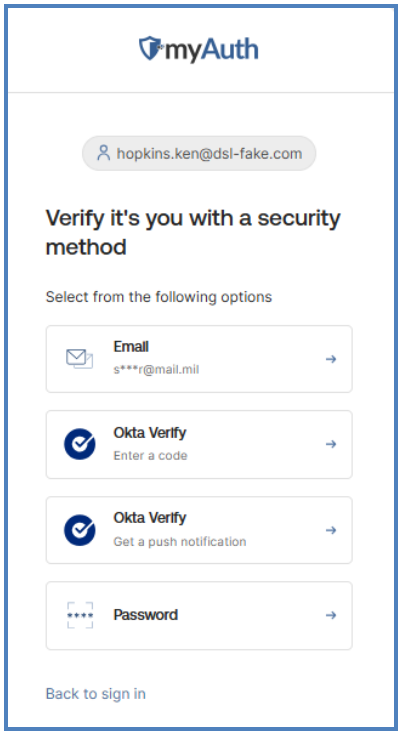
4. You will be taken to the Okta Verify app. Select **Yes, It's Me** to confirm.



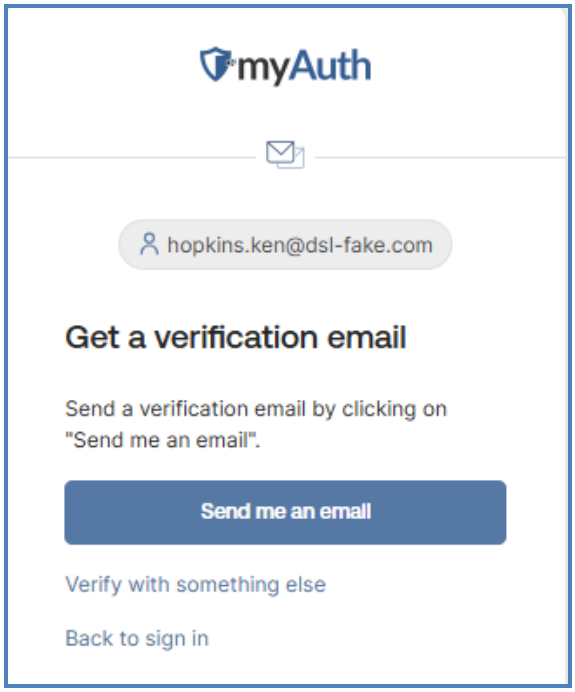
5. Close the Okta Verify app and return to your browser. Depending on where you started the login process, you will see your myAuth dashboard, or be taken back to the partner site and logged in.

3.2.3 Authenticate with Email OTP

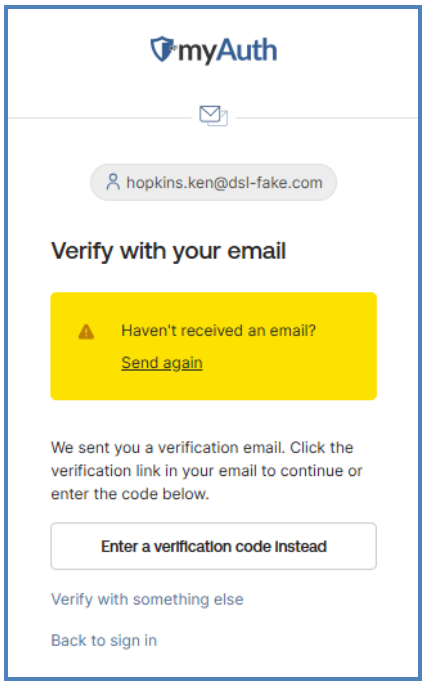
1. Click the blue arrow next to **Email**.



2. Click **Send me an email** to confirm that you want to receive an email.



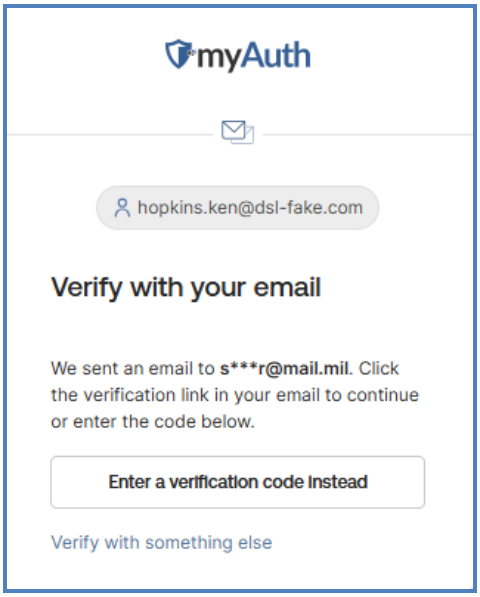
Note: Emails are usually sent out within two (2) minutes. The screen will update after one (1) minute with a link to click to resend the email. Click **Send again** to have the email sent out again.



Note: The email verification screen will time out after 10 minutes. You will be able to attempt to sign in again.

3. Check your email. You should receive an email titled "myAuth Email One-Time Passcode." Click the blue **Sign in** link.

You can also type the 6-digit code into the myAuth login screen after clicking **Enter a verification code instead**.



4. Return to your browser. Depending on where you started the login process, you will see your myAuth dashboard, or be taken back to the partner site and logged in.

4.0 Updating Your myAuth Account

Your myAuth account gives you access to DOD sites securely with one click. To maintain your access, you can manage your account with self-service tools.

Note: For your security, you will be prompted to enter a security method (such as password, Okta Verify, or email one-time passcode) every time you make updates to your account.

4.1 Updating Your Password

For your protection, you will need to update your password every 60 days.

Important: Passwords cannot be changed more than once every 24 hours.

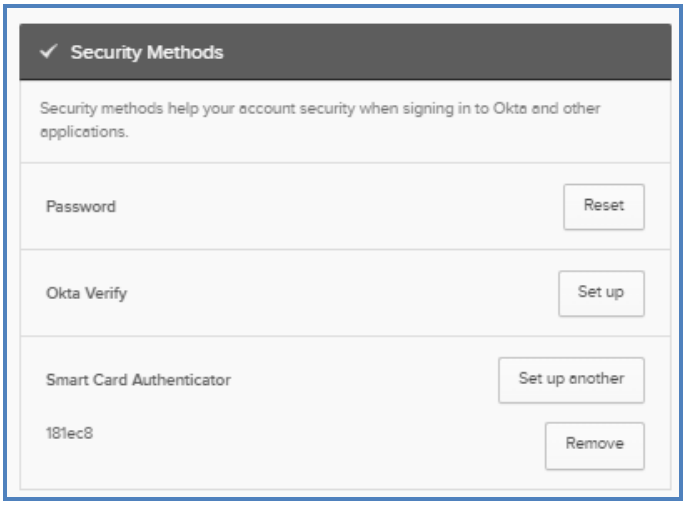
1. On the myAuth dashboard page, click your name in the top right corner.
2. Click **Settings**.
3. In the **Security Methods** box, click **Reset** next to Password.
4. Click **Yes** to confirm that you want to change your password.
5. Select a security method, such as email OTP, password, or Okta Verify.
6. Enter your new password. The requirements will show green checks when your password meets all the requirements. Click **Reset Password**.

   Your password has been successfully updated.

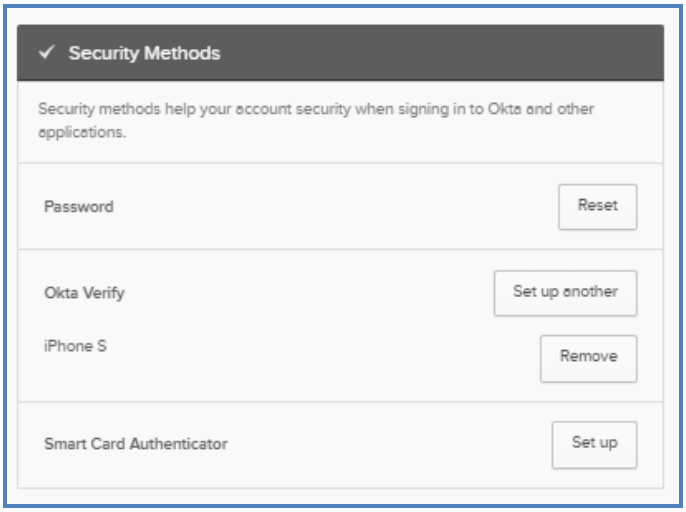
4.2 Adding a Security Method

1. On the myAuth dashboard page, click your name in the top right corner.

2. Click **Settings**.



3. In the **Security Methods** box, you can click **Set up** next to any method you would like to add to your account. If you already have Okta Verify set up on one device, but would like to add another, click **Set up another**.



4. Follow the directions to set up any method you would like to add (see section 2.3, Step 3 – Set up Your Security Methods).

4.3 Removing Security Methods

1. On the myAuth dashboard page, click your name in the top right corner.
2. Click **Settings**.
3. In the **Security Methods** box, click **Remove** next to any method you would like to remove from your account.
4. For your security, you will be prompted to enter a security method (such as password or email OTP) every time you make updates to your account.

4.4 Updating an Expired or Forgotten Password

If your password has expired or you cannot remember it, you will need to create a new password before you can log into myAuth and partner sites.

Important: Passwords cannot be changed more than once every 24 hours.

1. Enter your username on the myAuth login screen and click **Next**.
2. Click **Forgot password?**.
3. Select a security method, such as email OTP, password, or Okta Verify.
4. After you verify your identity, the Reset Password page displays.
5. Create a new password that fulfills the requirements that are listed. As each requirement is satisfied, you will see a green check next to it.
6. Re-enter the password and click **Reset Password**.
7. You will now be authenticated into myAuth and can access partner sites.

4.5 Updating Your Phone Number

1. On the myAuth dashboard page, click your name in the top right corner.
2. Click **Settings**.
3. In the **Personal Information** box, click **Edit Profile** in the top right corner.
4. Click **Edit** in the top right of the **Personal Information** box.
5. Enter updated information in the **Mobile Phone** field.
6. Click **Save** in the bottom right of the **Personal Information** box.
7. Confirm that your information has been updated.

   Note: Updating your information in myAuth does not change your information in the Defense Enrollment Eligibility Reporting System (DEERS). Only myAuth will be affected by the update.

4.6 Updating Your Email

1. On the myAuth dashboard page, click your name in the top right corner.
2. Click **Settings**.
3. In the **Personal Information** box, click **Edit Profile** in the top right corner.
4. Click **Edit** in the top right of the **Personal Information** box.
5. Enter updated information in the **Primary Email** or **Secondary Email** field.
6. You will receive an email titled “Confirm Email Address Change” at the new email address you entered.
7. Click **Confirm Email Change** in the email to verify that it is the correct address.
8. You will see a confirmation on the screen that says “Email Change Confirmed.” You can close this window; your email has been updated.

   Note: Updating your information in myAuth does not change your information in DEERS. Only myAuth will be affected by the update.

Appendix A: Acronyms and Abbreviations

The following table defines the acronyms and abbreviations used in this guide.

Table 1: Acronyms and Abbreviations

Acronym	Definition
2FA	Two-Factor Authentication
CAC	Common Access Card
CCC	Customer Contact Center
DEERS	Defense Enrollment Eligibility Reporting System
DMDC	Defense Manpower Data Center
DOD	Department of Defense
IDCO	Identity Card Online
MFA	Multi-Factor Authentication
OTP	One-Time Password
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
RAPIDS	Real-time Automated Personnel Identification System
SSO	Single Sign-On
VA	Department of Veterans Affairs
VPN	Virtual Private Network

Appendix B: Frequently Asked Questions (FAQs)

B.1 myAuth Login FAQs

Why am I being asked to create a myAuth account?

myAuth is a new, multi-factor authentication application supported by the Defense Manpower Data Center (DMDC) to provide enhanced protection of your data. myAuth utilizes high levels of security to create a safe and convenient sign-on.

Why are only some apps showing in my dashboard?

myAuth has completed the pilot phase and will continue to partner with additional DOD applications. As more applications are added, you will be able to access all your regular DOD sites with one sign-in through your myAuth account. You can still use your DS Logon account to access applications that are not using myAuth yet.

Can I log in with my PIV card?

myAuth is set up for the use of CACs, but not other types of Personal Identity Verification (PIV) cards. Additional PIV functionality is expected to be added. If you do not have a CAC, you can create a username and password to log in to myAuth.

myAuth says “Unable to Sign In” when I try to log in. What can I do?

For your protection, myAuth will not sign you in if your username is entered incorrectly, or your security methods are entered incorrectly. You can click **Back to sign in** on any of the login screens to return to the initial screen. Try logging in again:

- Double-check that you entered your username correctly. Your username is included in the myAuth welcome email.
- Ensure that your password is entered correctly. You can click the ‘eye’ icon to display the password characters and ensure that it is correct.
- For your security, if you fail authentication too many times, your account will be locked. You can follow the directions on the screen to unlock your account.

I keep getting logged out. What can I do?

For your protection, your session will end after a period of inactivity. If you are getting logged out of the system frequently, confirm that you are not connecting with a commercial (non-DOD/non-DMDC) Virtual Private Network (VPN). It is recommended to not use commercial VPNs to access myAuth.

2.0Creating a New myAuth AccountI forgot my username. What can I do?

Your myAuth username is same as the email address that you entered when setting up your myAuth account. Check your email, including trash and spam or junk mail folders, for an email with the subject line “Welcome to myAuth.” Your username is included in the email. If you no longer have the email, you can create a new account (see section 2.0, Creating a New myAuth Account).

B.2 myAuth Account Creation FAQs

Why am I using DS Logon to create a myAuth account?

Users with a DS Logon account have already completed the identity verification process. myAuth is set up so that new users can quickly and easily verify their identity through DS Logon and create a myAuth account without repeating the process.

I am having trouble creating a new DS Logon account. What can I do?

View a detailed walkthrough of the remote proofing process in the online help.

Some users will not be able to verify their identity remotely due to their devices or a lack of credit history. For those users, in-person proofing at a Real-time Automated Personnel Identification System (RAPIDS) office is the best option. Contact a RAPIDS office to confirm what will be required (typically two [2] forms of ID).

I logged into DS Logon's Identity Management page, but I do not see anything about myAuth.

Logging in from the regular DS Logon page will not connect you to myAuth. Go to the myAuth website to connect your DS Logon identity. Log into DS Logon as you normally would. When you are authenticated, you should see a myAuth screen that prompts you to enter your email. If you see your DS Logon dashboard instead, try closing your browser and pasting the myAuth website link (https://myaccess.dmdc.osd.mil/identitymanagement/api/auth/myauth) into a new tab.

I have a DS Logon account, but I am getting an error when I log in.

For security purposes, DS Logon accounts may be deactivated, suspended, or locked. Depending on the error message you see, try the following:

- **Deactivated:** Accounts that have not been used in 180 days are automatically deactivated to prevent unauthorized access. You will see Error Code 5 when you try to log in.

On the myAuth login page, click **Create New DS Logon Account**, and complete the identity verification process (see the online help for additional information).

Once you have authenticated, you will automatically be directed to the myAuth account process.

- **Suspended:** An account can be suspended due to incorrect password attempts. You will see Error Code 8 when you try to log in.
    1. Click **Unsuspend my Account** in the error message.
    1. Enter your Personally Identifiable Information (PII) to confirm your identity.
    2. Answer the challenge questions correctly.
    3. Change your password.
    4. Update your challenge questions.
    5. Click **Continue**.
    6. Create a new myAuth account and connect your DS Logon identity verification (see section 2.0, Creating a New myAuth Account).
- **Locked:** DS Logon accounts can be locked to protect user security, including unusual activity.
    1. Contact the DMDC Customer Contact Center (CCC) at 1-800-368-3665 to request instructions on how to have your account unlocked.

2. You may be asked to contact the Department of Veterans Affairs (VA) if the CCC is unable to remove a lock placed by the VA. The CCC will provide you with the necessary information.

Can I use my DEERS official email address as the myAuth email address?

Yes. If you choose to use your DEERS email address as your myAuth email address, all myAuth notifications will be sent to this email. Please note that myAuth requires a unique email address for all accounts; email addresses shared between family members will not work for multiple myAuth accounts. If you are about to separate or retire, it is recommended that you use a personal email to maintain your access.

Can I use an email address for myAuth that is different than my DEERS official email address?

Yes. If you use an email address for myAuth that is different than your DEERS official email address, you will receive myAuth notifications at that address. DMDC will continue to send benefits-related information to your official DEERS email address.

I see an error that says there might already be an account with my email. What can I do?

If you started to create a myAuth account but did not complete the process, your email username is already set up. The account creation process may not have been completed, or another person, such as a family member, may have created an account using the email address.

1. Check your email. Look in the trash and spam or junk mail folders for an email titled “Welcome to myAuth.” That email has a link that will let you complete the process.
2. If you share your email address with anyone else, like a child or a spouse, check to see if they already used the email address to create their own myAuth account. You may need to use a different email to create your own account.

I have a CAC. Do I still have to create a myAuth username and password?

Yes, for the purpose of one-time account creation. Once you have created your myAuth account and set up Smart Card Authentication, you will be able to log in using just your CAC.

Having a username and password also allows you to maintain access to your myAuth account after separation of service or when you do not have access to a CAC reader.

I have not received the email to finish setting up my account. What can I do?

- Emails typically take less than one (1) minute to arrive. Occasionally, emails will take up to 20 minutes to arrive.
- Check your trash and spam or junk mail folders. The subject line will read “Welcome to myAuth.”
- Add noreply@okta.mil to your trusted senders or contact list in your email settings to ensure that myAuth notifications are delivered to your inbox.
- It is possible that the email address had an error or typo. Follow the to create a new myAuth account using your DS Logon (see section 2.1.2, Confirm Your Identity with DS Logon). After you are authenticated, you will be asked to enter an email address. Enter your email address and the myAuth email will be sent to you. If you receive an error message that there is already an account with that email, see the “I see an error that says there might already be an account with my email. What can I do?” FAQ above.

  Note: If you share the email account with anyone, such as a spouse, check if they already created an account with your shared email. If they did, you can create an account with the same process using a different email address.

- This email is valid for seven (7) days. If it has been longer than (7) days, please contact the CCC at 1-800-368-3665 to have the welcome email resent.

Does myAuth protect my accounts against fraudulent access?

Yes, myAuth is designed to be safe and secure to protect your information. myAuth uses the latest industry standard fraud detection and prevention tools. Consequently, to protect your identity and information, myAuth may require you to log in with more secure methods if it determines that your log in request is at a higher risk of being fraudulent.

B.3 Setting Up and Using Security Methods FAQs

Why do I need additional security methods? I already set up a password.

Maintaining the privacy of your personal data is a shared priority for you and myAuth. For the security of your information, myAuth requires additional security methods to protect your account.

In addition to providing your username and password, you will be required to provide a second security method, such as a code or push notification using the free Okta Verify app, or OTP via email. The extra step keeps your information secure while giving you Single Sign-On (SSO) access to various apps.

Having additional security methods in place helps you recover your account if your password is forgotten or stolen.

How do I link my CAC after setting up my myAuth account?

To link your CAC to your myAuth account, you should be logged in. In your user dashboard, click your name in the top right corner and click **Settings**. In the Security Methods box, click **Set up** next to the **Smart Card Authenticator** option. Insert your CAC and select the appropriate certificate in the pop-up window. You will now be able to choose Smart Card to authenticate from the login screen on future sign-ins.

What is the correct Okta app to install?

From the app store on your device, search for **Okta Verify**.

Note: Choose Okta Verify and **NOT** Okta Mobile or Okta Personal. There is no cost to download Okta Verify.

I am unable to scan the Okta Verify QR code. What can I do?

If you are not able to scan the QR code to set up Okta Verify, you can click **Can't Scan** under the QR code. You will be given the option to set up Okta Verify with email. Select **Email me a setup link** and click **Next**. You will receive an email with a link. Click the **Activate Okta Verify Push** link. See section 3.2, Authenticating Using Security Methods, for additional information.

Can I use a tablet to log in with Okta Verify or is a smartphone required?

Yes, you can use a tablet to log in with Okta Verify. The Okta Verify app can be downloaded on devices using Android, iOS, and iPadOS operating systems. Chrome, Safari, and Firefox are all supported browsers. If you are having trouble downloading the free Okta Verify app, check that you are using the latest versions of your operating system and browser.

How do I add Okta Verify to my myAuth account after it is initially set up?

You can easily add Okta Verify from your user dashboard. When you are logged into your myAuth dashboard, click your name in the top right corner and click **Settings**. In the Security Methods box, click **Set up** next to the **Okta Verify** option. The system will prompt you to enter a security method to verify your identity. Once you have entered a security method (email passcode, CAC authentication, or password), click **Set up** when presented with the Okta Verify option.

To proceed, you will need to download the free Okta Verify app on your device. You can search for Okta Verify in your device's app store and download the app. Once the download is complete, open the Okta Verify app on your device and complete the setup (see section 2.3.1, For Okta Verify).

Okta Verify does not show me any codes or does not work on my device. What can I do?

If you have face or fingerprint recognition (such as Face ID) set up with Okta Verify on your device, Okta Verify will cloak the numbers until you successfully complete the face or fingerprint verification. Once your phone has completed the check, the numbers will be displayed.

It is possible that Okta Verify might not be set up correctly on your device. You can remove Okta Verify from your security methods and try setting it up again (see section 4.3, Removing Security Methods). You can log in using Email OTP and password for your security methods. Click **Verify with something else** if they are not presented as options.

You can also check the health of your device within the Okta Verify app to ensure that your device is secure and up to date. Click the icon in the top right of the app to access **Settings** and click **Device health.**

If your device passes all checks, each security requirement has a green check mark. You will see suggestions on the **Device health** screen to resolve any issues that were identified.

Can I add Face ID to my Okta Verify app?

Yes. If you did not choose to set up Face ID during the Okta Verify setup, you can add it later. Open the Okta Verify app and click on the myAuth account. You will be directed to the Account Details screen.

Under **Security**, you can toggle **Face ID or Passcode Confirmation** on. You will need to verify your identity to complete the setup. The Okta Verify app will present a code that you will enter on the following myAuth screen to complete the setup.

What if I lose my phone and cannot log in with Okta Verify?

You can use the Email OTP security method (see section 3.2.3, Authenticate with Email OTP) to log in and change your security methods. In your Settings, you can add Okta Verify to a new device (see 4.2, Adding a Security Method) any time you are logged into myAuth. You can also remove Okta Verify (see section 4.3, Removing Security Methods) from your myAuth security methods completely or just from selected devices if you no longer have access to that device.

What is Okta FastPass, and can I use FastPass to log in?

Okta FastPass is part of the free Okta Verify app and allows passwordless authentication. You automatically have access to FastPass once you download the Okta Verify app and enroll your myAuth account. You must have the Okta Verify app installed on the device you are using to log in for FastPass to work. The **Face ID or Passcode Verification** setting must be enabled in the Okta Verify app for passwordless authentication to work. Users logging in with FastPass without **Face ID or Passcode Verification** enabled will still need to enter a password to authenticate (see section 3.1.3, Login with Okta FastPass).

I am seeing a message in my Chrome browser that myAuth wants to connect to my local network. What should I do?

Click **Allow** to ensure that FastPass will work with the newest version of Chrome. This one-time action is due to an update in Chrome. This process is secure and only communicates with the device where Okta Verify is installed. myAuth will not look for or connect to any other device on your local network. If you already clicked **Block**, you can take the following steps to ensure that you can authenticate with FastPass:

1. While on the myAuth sign-in page, click the icon (padlock or tune icon) on the left side of the address bar.
2. Select **Site Settings** to open the Site Settings menu.
    - For Chrome on Mac or Windows: Click **Privacy & Security**
    - For Chrome on Android: Click **Permissions**.
3. Find the setting for **Local Network Access**.
4. Use the toggle or drop-down menu to change the permission from **Block** to **Allow.**
5. Refresh the page. Okta FastPass should now work correctly.

Note: FastPass users accessing myAuth with Google Chrome browser on a Mac, Windows, or Android device will see this pop-up and be required to allow the one-time connection. Users who are using iOS/iPhone or a different browser, such as Edge, will not be affected.

B.4 myAuth Account Maintenance FAQs

Can I change my username?

Your username is the same as the email you entered during account creation. Users can change their primary email address (the address that will receive notifications from myAuth) without affecting the username. Users cannot change their username at this time.

Can I change my password?

Users are required to update their password every 60 days. You can change your password in the myAuth dashboard. See section 4.1, Updating Your Password, for instructions. Please note that passwords cannot be changed more than once every 24 hours.

Can I change my email address?

Yes. Changing your email address will not change your username at this time. Any notifications from myAuth will go to the primary email address on file. See section 4.6, Updating Your Email, for instructions.

How do I update my myAuth account when I transition out of the military?

Before you transition out of the military, you will want to complete the following:

- Make sure your primary email address is one that you will be able to access after separation. If your primary email address ends with ".mil" you can update it to a personal email address. Your username does not need to be updated. You can keep your existing username, even if it is a .mil email address.
- If you having been using your CAC to log in to myAuth, consider adding Okta Verify as a security method. By downloading the free Okta Verify app, you will be able to log into myAuth using a convenient one-time passcode, push notification, or FastPass.

I see an event I do not recognize in my Recent Activity. What can I do?

If you see activity that you do not recognize, it is recommended that you immediately update your password (see section 4.1, Updating Your Password). Review your MFA security methods under **Settings** and make sure that they are up to date. Verify that your contact information (such as phone number and email addresses) has not changed.

You can also click **Sign out** in the **End All Sessions** box in your Settings. This will log your account out of any open sessions across any devices, including your current session, that have accessed your account.

If you suspect fraudulent activity, you can report the activity to suspend your account. This will prevent all account access, including your own. To report a fraudulent Sign-In and suspend all access to the account, click the **Report** button in the **Report to Admin** column. To report a fraudulent Security Event and suspend all access to the account, click the blue dots in the top right of the event's box. This will open a panel with additional details and a **Report** button.

To recover an account that has been hacked or hijacked or suspended in error, please call the DMDC CCC at 1-800-368-3665. After confirming your identity, an operator will be able to help you unsuspend your account or close out the compromised account and create a new account.

I am getting emails from myAuth. Do I need to do anything?

myAuth will send automated emails regarding account actions that you have taken that could affect your account access (such as when you change your email or update your password). Any time you receive an email with activity that you do not recognize, you can secure your account by logging in, clicking on your name in the top right corner, and going to **Settings**. You can take the following actions:

- Update your password
- Make sure your contact information is accurate
- Review your security methods to make sure they are up to date

If you receive a suspicious message or call, do not respond. Verify the contact information of the organization and contact them directly.

Never give out your password or personal information to unsolicited messages or calls.

Remember that DOD, DMDC, and myAuth will **never**:

- Call to ask you to respond to a text or for your password
- Contact you to take control of your computer

I received an email that my account is locked. What can I do?

Your account will be locked after too many failed sign-in attempts. Any time this happens, you will receive an email. Click the **Unlock Account** button in the email. You will be prompted to enter security methods and unlock the account. None of your information or applications will be changed while your account is locked.

I received an email that my password was changed, but I did not change it and now I cannot access my account. What can I do?

To recover an account that has been hacked or hijacked, please call the DMDC CCC at 1-800-368-3665. After confirming your identity, an operator will be able to help you close out the compromised account and create a new account.

I am not able to sign in and I see a message that says, “Reset password is not allowed at this time."

Your account may be in “Suspended” status. Please call the DMDC CCC at 1-800-368-3665. After confirming your identity, an operator will be able to help you. Please note that passwords cannot be changed more than once every 24 hours.

What operating systems and browsers does myAuth support?

myAuth supports the latest versions of Android, iOS, and iPadOS, macOS, and Windows operating systems. The latest versions of Chrome, Safari, Edge, and Firefox are all supported browsers. If you are having trouble accessing your myAuth account, check that you are using the latest versions of your operating system and browser.