



DEPARTMENT OF JUSTICE

Office of Justice Programs

DIAMD

Frequently Asked Questions (FAQ's)

Version 1.3

Contents

- HOW DO I RESET MY PASSWORD? 3
- HOW DO I RECEIVE A CODE VIA SMS DURING LOGIN? 8
- I LOST MY WELCOME EMAIL. HOW DO I GET ANOTHER COPY SENT TO ME? 15
- MY LEGAL NAME HAS CHANGED, HOW DO I UPDATE IT IN DIAMD? 15
- MY EMAIL HAS CHANGED, HOW DO I UPDATE IT IN DIAMD? 15
- HOW DO I RESET MY PASSWORD RECOVERY QUESTIONS? 15
- WHAT DO I DO IF MY ACCOUNT IS LOCKED? 15
- HOW DO I REPLACE MYSELF AS AN ENTITY ADMINISTRATOR? 18
- HOW DO I INVITE NEW MEMBERS TO AN ENTITY? 21
- HOW DO I ADD OR REMOVE ROLES FROM A MEMBER? 23
- WHAT DO I DO IF I DON'T SEE THE DIAMD TILE? 25
- HOW DO I REMOVE MEMBERS FROM AN ENTITY? 26
- WHAT IF THE WRONG PERSON ON MY TEAM WAS INVITED AS ENTITY ADMINISTRATOR? 27

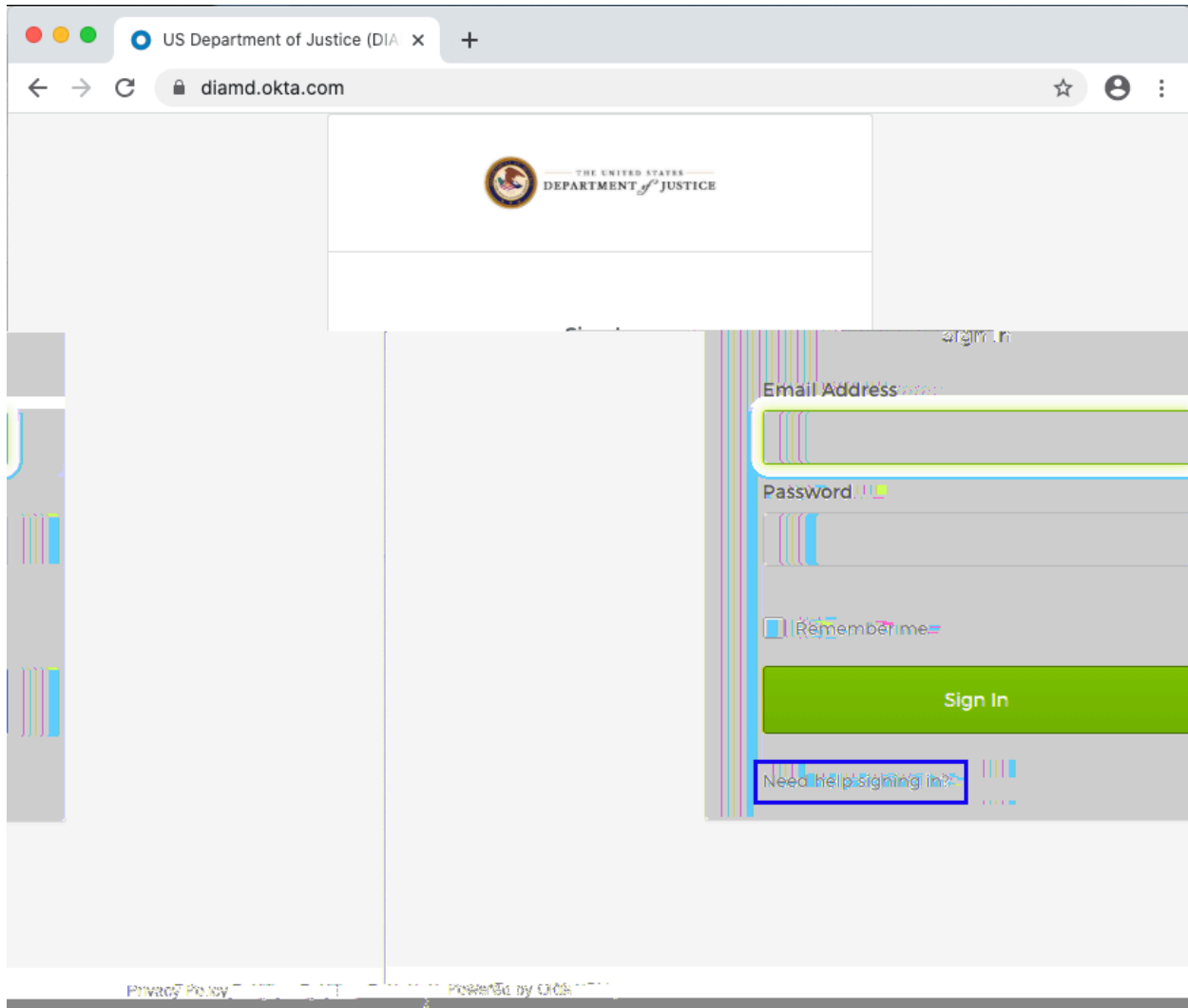
How do I reset my password?

Step 1 - Navigate to DIAMD Login page

Navigate your browser to the DIAMD home page: <https://diamd-auth.usdoj.gov>

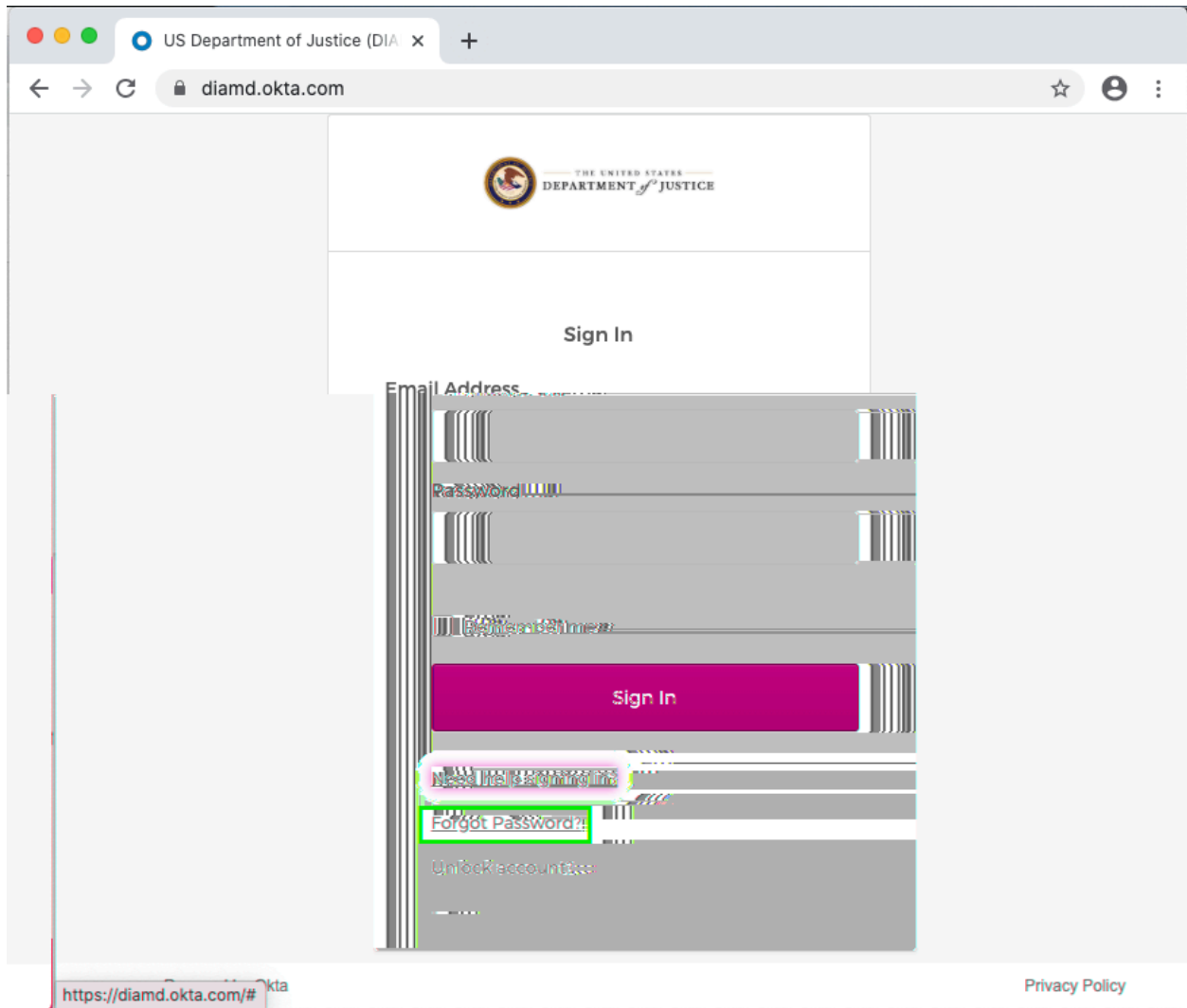
Step 2 – Click on “Need help signing in?”

Click on the “Need help signing in?” highlighted below.



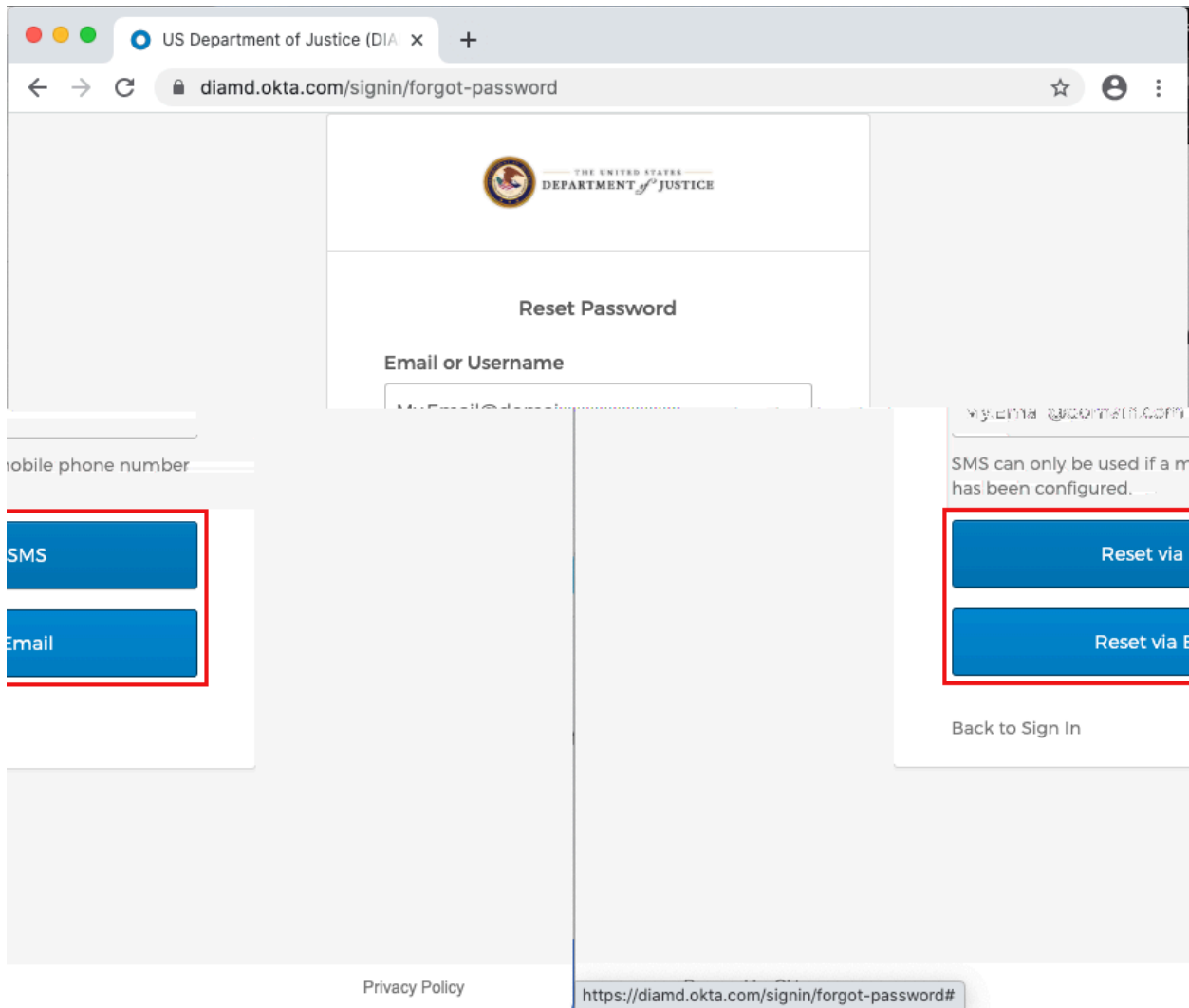
Step 3 – Click on “Forgot Password?”

1. Click “Forgot Password?” highlighted below.



Step 4 – Enter Email Address

1. Enter your email address in the “Email or Username” box, select whether to reset your password via SMS or Email. The DIAMD system will then send you an SMS or Email communication based on your selection. Follow the instructions in the communication.



Step 5 – Check phone or email for instructions on resetting password

1. Follow the instructions provided to you via the SMS or Email you receive.
2. If you selected “Reset via SMS” you will see the below screen and receive a text message on your phone.



THE UNITED STATES
DEPARTMENT OF JUSTICE

Enter verification code sent via SMS

Enter Code

Sent

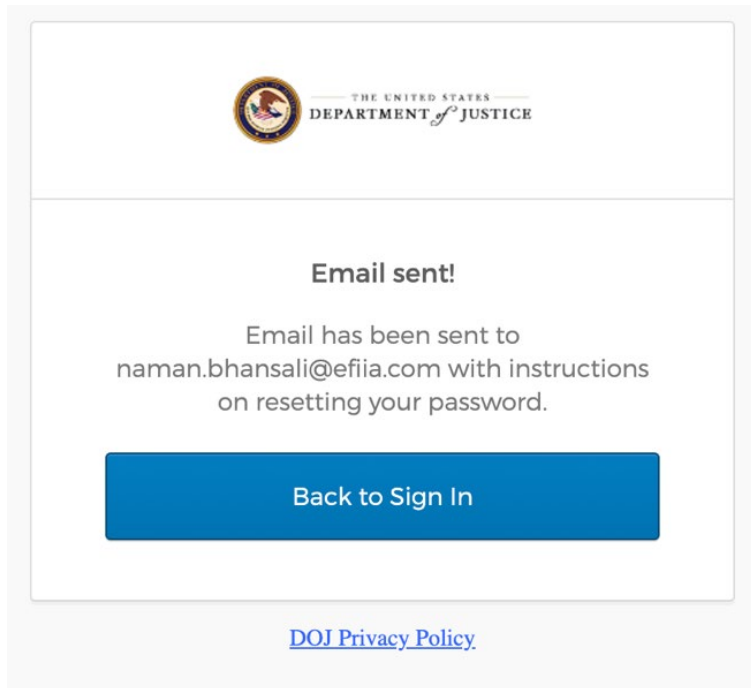
Verify

Didn't receive a code? [Reset via email](#)

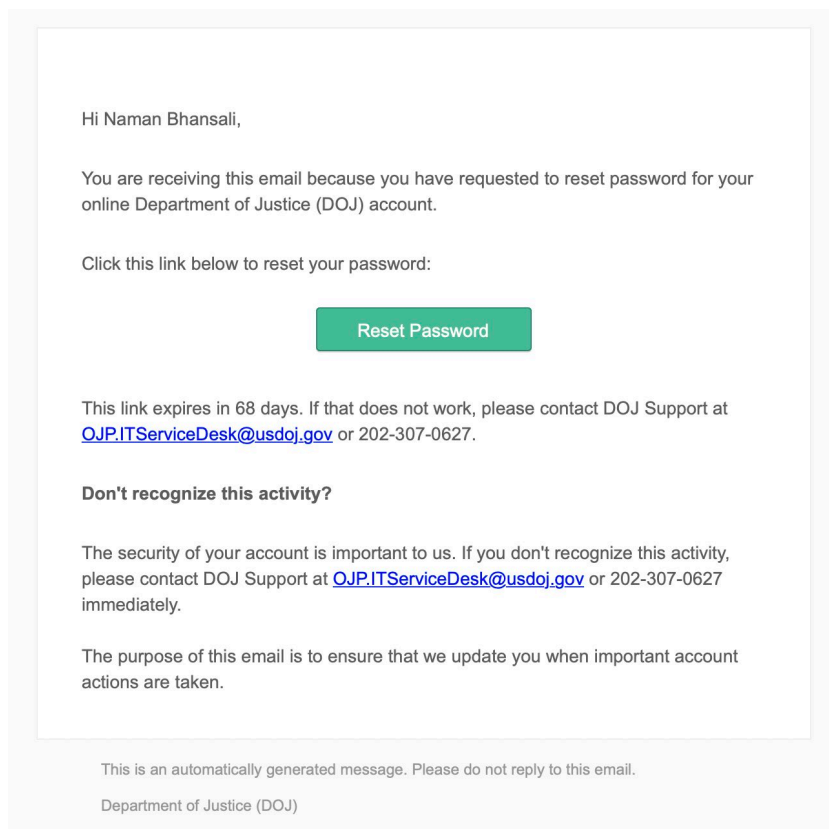
[Back to Sign In](#)

[DOJ Privacy Policy](#)

3. If you selected "Reset via Email" you will see the below screen.

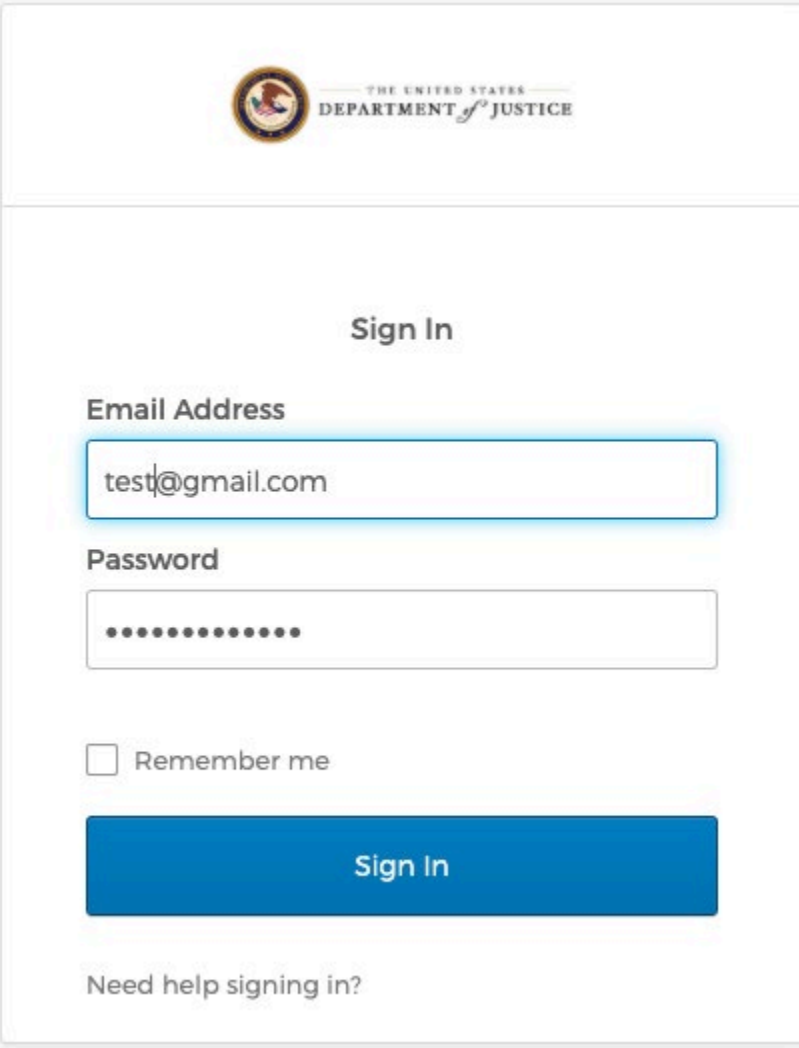


4. Here is a sample email that you will receive:



How do I receive a code via SMS during login?

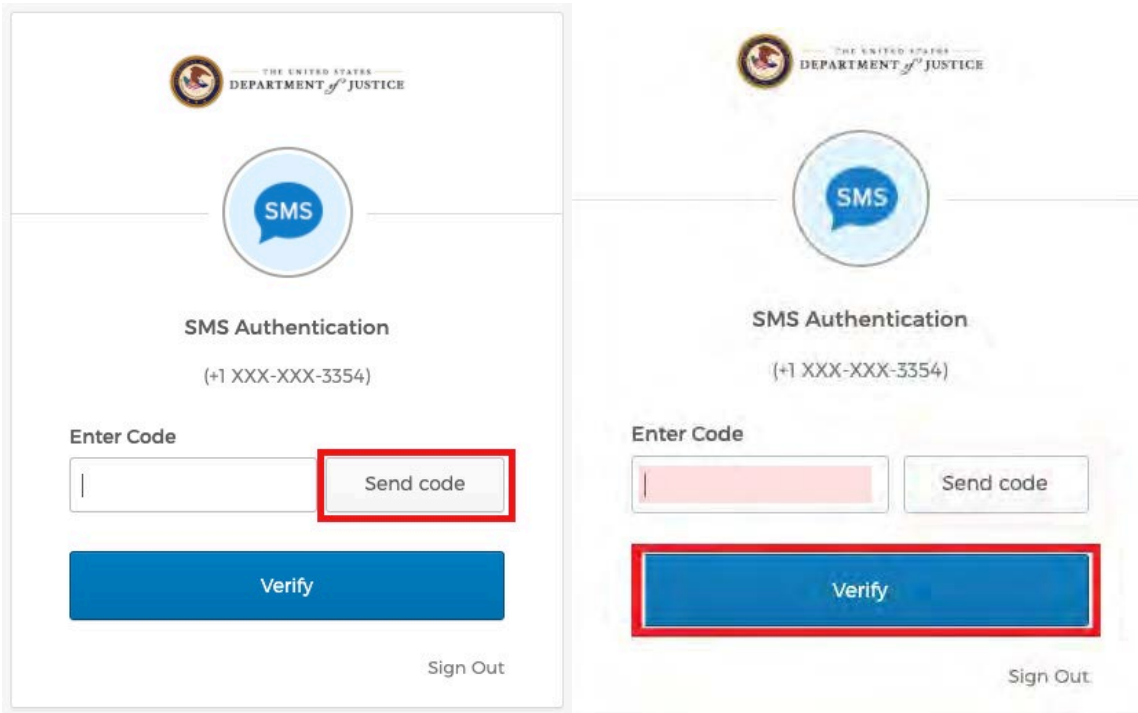
Step 1 – On the DIAMD login screen, enter your username and password



The screenshot displays the login interface for the Department of Justice. At the top, the Department of Justice seal and name are visible. The main heading is "Sign In". Below this, there are two input fields: "Email Address" containing "test@gmail.com" and "Password" which is masked with dots. A "Remember me" checkbox is present below the password field. A prominent blue "Sign In" button is located at the bottom of the form. A link for "Need help signing in?" is positioned at the very bottom of the page.

Step 2 – On the SMS Authentication screen, click the “Send Code” button. Enter the code you receive via SMS and click “Verify”

Step 3 – Enter the code you received via SMS and click “Verify”



A note of critical importance. When a customer calls in and says “it doesn’t work” – there are many different reason why “it” might be failing:

- 1) The carrier has not delivered the text in extreme cases, the carrier can deprioritize the traffic (SMS/VOICE) call and it will take anywhere from seconds to minutes for the code to arrive. If during this time the user clicks the button many times multiple codes will be sent and result in different arrival times of the codes. Because there is no way to know which code was sent first or last – entering the code will likely result in a failure.
- 2) Carrier roaming is also a possibility – as the carrier roaming option can cause SMS delivery to suffer.

I can't receive SMS or VOICE for MFA what other options do I have?

Step 1 – Login to your account.

- 1) If you are completely unable to login you will need to call the service desk for a password reset which will allow you to reinitialize the process and choose a different MFA option.

Step 2 – Go to the bottom left hand side of the screen and click on the “Settings”



Step 3 – In the new window that is presented you will now have the following options available including a Security Key or Biometric Authenticator option if phone service or internet service is not available.

✓ Extra Verification	
Extra verification increases your account security when signing in to Okta and other applications you use	
Okta Verify	Remove
Security Key or Biometric Authenticator	Set up
Google Authenticator	Set up
SMS Authentication	Remove
Voice Call Authentication	Remove

How do I setup Biometric or Security Key Authenticator?

Step 1 – Login > settings > Security Key or Biometric Authenticator

The screenshot shows the Okta Account settings page. On the left is a navigation sidebar with 'My Apps', 'DOJ Apps', 'Add Section', 'Notifications', 'Admin', 'Preferences', 'Settings', and 'Sign out'. The main content area is titled 'Account' and contains several sections:

- Personal Information:** Fields for First name, Last name, Okta username, and Primary email, with an 'Edit' button.
- Extra Verification:** A section with a checkmark icon, explaining that extra verification increases account security. It lists several authentication methods with 'Remove' or 'Set up' buttons: Okta Verify, Security Key or Biometric Authenticator, YubiKey 5, Google Authenticator, SMS Authentication, and Voice Call Authentication.
- Change Password:** A section with a lock icon, listing password requirements (12 characters, lowercase/uppercase letters, number, symbol, no parts of username, no first/last name, not one of last 6 passwords, and at least 1 day since last change). It includes input fields for Current password, New password, and Confirm new password, along with a 'Change Password' button.
- Forgotten Password Question:** A section with a lock icon and an 'Edit' button, asking the user to select a question to reset their password. The question shown is 'Where did you meet your spouse/significant other?'.

Step 2 – Setup Enrollment

The screenshot shows the 'Setup multifactor authentication' enrollment screen. At the top, there is a 'NOTICE TO USERS' section with the following text:

You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties.

By logging in to this information system you are acknowledging that you understand and consent to the following:

- You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transmitting or stored on this information system.
- Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

For further information see the Department order on Use and Monitoring of Department Computers and Computer Systems.
[Privacy Act Statement](#)

The main content area is titled 'Set up multifactor authentication' and states: 'Your company requires multifactor authentication to add an additional layer of security when signing in to your account'. It features a 'Security Key or Biometric Authenticator' option with a 'Setup' button. Below this is a link to the 'DOJ Privacy Policy'.

Step 3 – Begin Authenticator Enrollment

NOTICE TO USERS



You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties.

By logging in to this information system you are acknowledging that you understand and consent to the following:

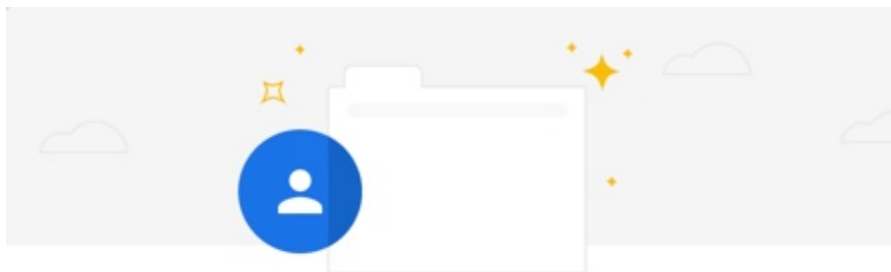
- You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transmitted or stored on this information system.
- Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

For further information see the Department order on Use and Monitoring of Department Computers and Computer Systems.

[Privacy Act Statement](#)





Set up security key or biometric authenticator
Your browser will prompt to register a security key or biometric authenticator (Windows Hello, Touch ID, etc.). Follow the instructions to complete enrollment.
[Enroll](#)
[Back to factor list](#)
[DOJ Privacy Policy](#)

Step 4 – Verify identity with selected type (Select the type you wish to use)



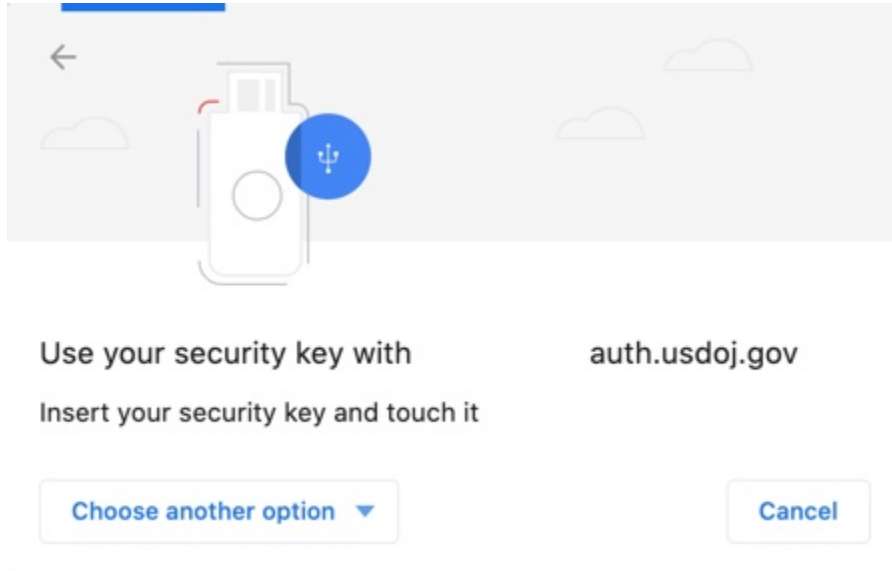
Verify your identity with **auth.usdoj.gov**

Pick an option

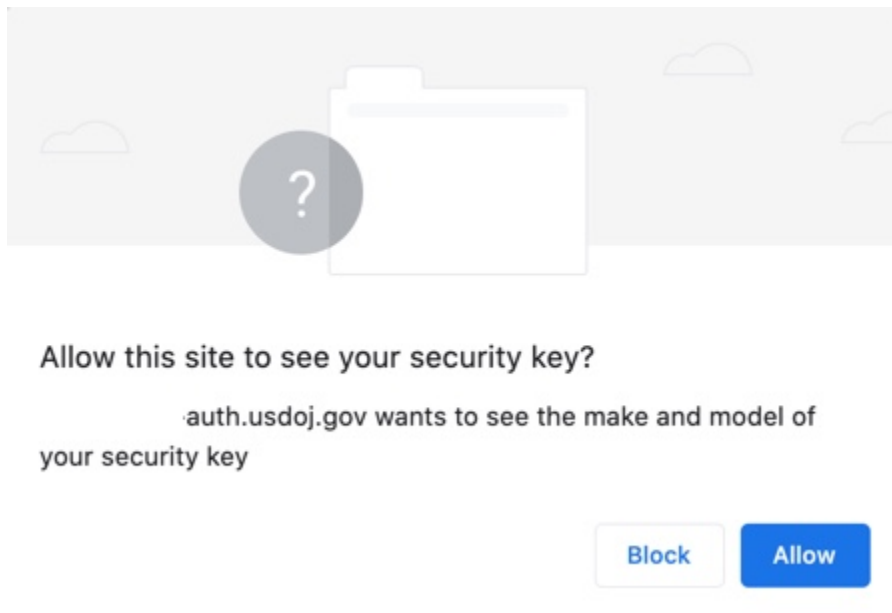
-  USB security key ▶
-  Built-in sensor ▶

[Cancel](#)

Step 5 – Insert security Key



Step 6 – Allow system permissions to access security key



Step 7 – You will be logged out and need to log back in with your username and password.

NOTICE TO USERS

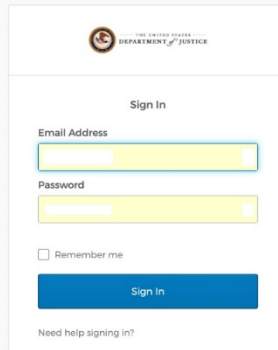
You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties.

By logging in to this information system you are acknowledging that you understand and consent to the following:

- You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transmitted or stored on this information system.
- Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

For further information see the Department order on Use and Monitoring of Department Computers and Computer Systems.

[Privacy Act Statement](#)



The screenshot shows the DOJ Sign In page. At the top is the Department of Justice logo. Below it is the heading "Sign In". There are two input fields: "Email Address" and "Password". Below the password field is a checkbox labeled "Remember me". A blue "Sign In" button is at the bottom. Below the button is the text "Need help signing in?" and a link to "DOJ Privacy Policy".

Step 8 – Insert security key and allow entry into the system.

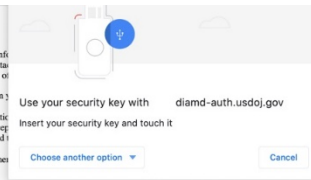
You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties.

By logging in to this information system you are acknowledging that you understand and consent to the following:

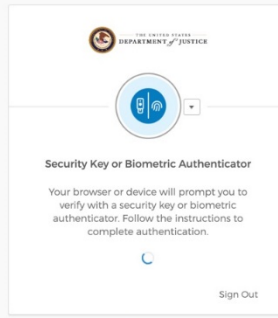
- You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transmitted or stored on this information system.
- Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

For further information see the Department order on Use and Monitoring of Department Computers and Computer Systems.

[Privacy Act Statement](#)



The screenshot shows a dialog box titled "Use your security key with diamd-auth.usdoj.gov". It contains the text "Insert your security key and touch it". Below the text are two buttons: "Choose another option" and "Cancel".



The screenshot shows the "Security Key or Biometric Authenticator" page. It features the DOJ logo at the top. Below it is a circular icon with a security key and a biometric symbol. The text reads: "Security Key or Biometric Authenticator. Your browser or device will prompt you to verify with a security key or biometric authenticator. Follow the instructions to complete authentication." At the bottom right is a "Sign Out" button. Below the page is a link to "DOJ Privacy Policy".

I lost my welcome email. How do I get another copy sent to me?

Step 1 – Contact DIAMD Service Desk and they will Re-Invite you.

1. In order to receive another welcome email, please contact the DIAMD Service Desk by calling (202) 307-0627 or via email at OJP.ITServiceDesk@usdoj.gov and ask to be re-invited to your entity.

My legal name has changed, how do I update it in DIAMD?

Step 1 – Contact DIAMD Service Desk and they will initiate a name change.

1. In order to have your name updated, please contact the DIAMD Service Desk by calling (202) 307-0627 or via email at OJP.ITServiceDesk@usdoj.gov

My email has changed, how do I update it in DIAMD?

Step 1 – Contact DIAMD Service Desk and they will initiate an email change.

1. In order to have your email updated, please contact the DIAMD Service Desk by calling (202) 307-0627 or via email at OJP.ITServiceDesk@usdoj.gov

How do I terminate my DIAMD account?

Step 1 – Contact DIAMD Service Desk and they will terminate your account.

1. In order to have your DIAMD account terminated, please contact the DIAMD Service Desk by calling (202) 307-0627 or via email at OJP.ITServiceDesk@usdoj.gov

How do I reset my password recovery questions?

Step 1 – Contact DIAMD Service Desk and they will reset your password recovery questions.

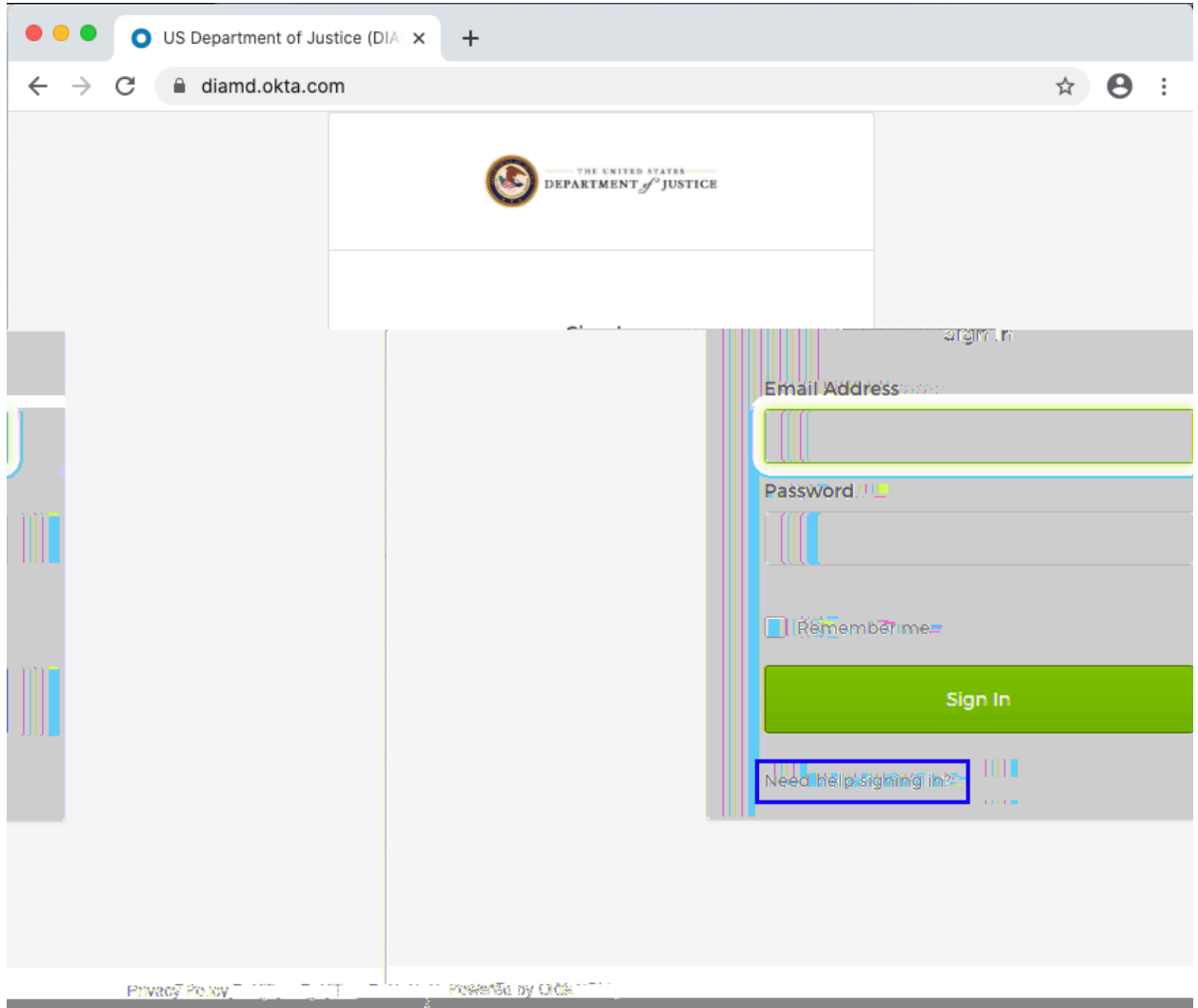
1. In order to have your DIAMD account recovery questions reset, please contact the DIAMD Service Desk by calling (202) 307-0627 or via email at OJP.ITServiceDesk@usdoj.gov.

What do I do if my account is locked?

Step 1 – Navigate to DIAMD login page

1. Navigate your browser to the DIAMD home page: <https://diamd-auth.usdoj.gov>


2. Click "Need help signing in?"



3. Select "Unlock Account?"

Office of Justice Programs DIA x +

← → ↻ 🔒 diamd.oktapreview.com

 THE UNITED STATES
DEPARTMENT of JUSTICE

Sign In

Email Address

! Please enter a username

Password

Remember me

[Sign In](#)

[Need help signing in?](#)

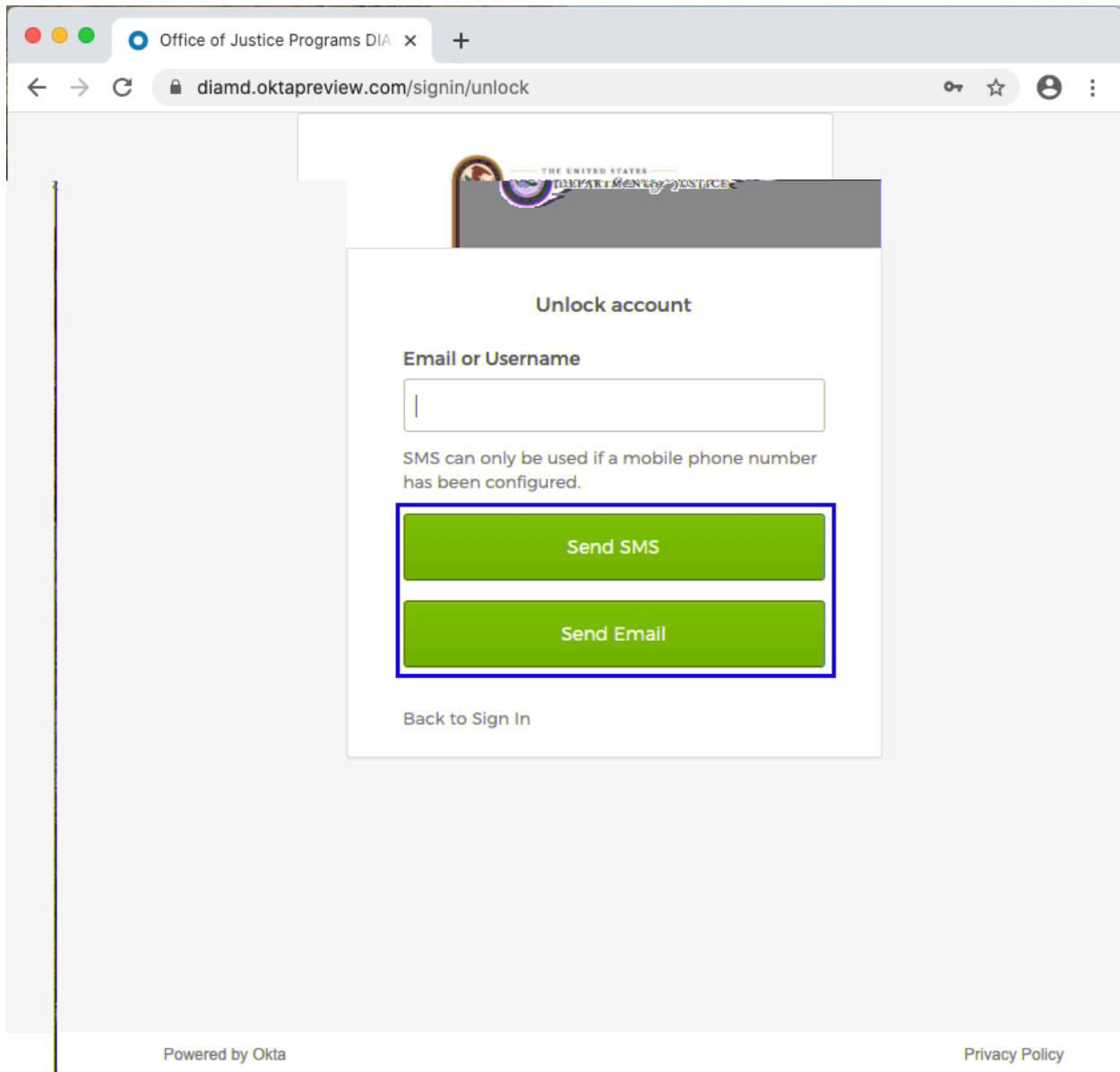
[Forgot Password/](#)

[Unlock Account?](#)

[Help](#)

Powered by Okta [Privacy Policy](#)

4. Enter your email address and select “Send SMS” or “Send Email.” Follow the instructions provided.



How do I replace myself as an entity administrator?

Step 1 - From the DIAMD home page, select “Manage Entity”



Home My Work ▾

Home

Notifications >

0

Entity Management

Manage Entity >

Invite Member >

Manage Member >

Re-Invite Member >

Step 2 - On the Manage Entity screen, select a new entity administrator, click "Save"



< Form

Manage Entity

Entity Profile

Entity ID
DUNS.000000000

Entity Name *
Test Entity

Entity DBA
Test DBA

Current Entity Administrator

First Name: Testadmin Last Name: TestAdmin

Email Address: test@test.com

Entity Administrator Management

Select a member to replace the current Entity Administrator
[Dropdown menu]
The selected member will be assigned as the new Entity Administrator

Member Management

Select members to remove
[Dropdown menu]
The selected members will be removed from this Entity

Cancel Submit

How do I invite new members to an entity?

Step 1 - From the DIAMD home page, select “Invite Member”



A screenshot of the DIAMD home page. At the top, there is a dark blue navigation bar with a hamburger menu icon, the text "Home", and a dropdown arrow next to "My Work". Below the navigation bar, the page content is on a light gray background. It starts with a "Home" header and a home icon. Underneath is a "Notifications" widget showing "0" notifications. Below that is the "Entity Management" section, which contains four buttons: "Manage Entity", "Invite Member", "Manage Member", and "Re-Invite Member". The "Invite Member" button is highlighted with a red rectangular border. Each button has a right-pointing chevron icon.

Step 2 - Fill in the member's data, select one or more roles to grant them, click submit



Home My Work

< Form

Invite Member

Member Profile

Email Address *

Confirm Email Address *

First Name *

Last Name *

Entity Profile

Entity ID *

Entity Name *

Entity DBA

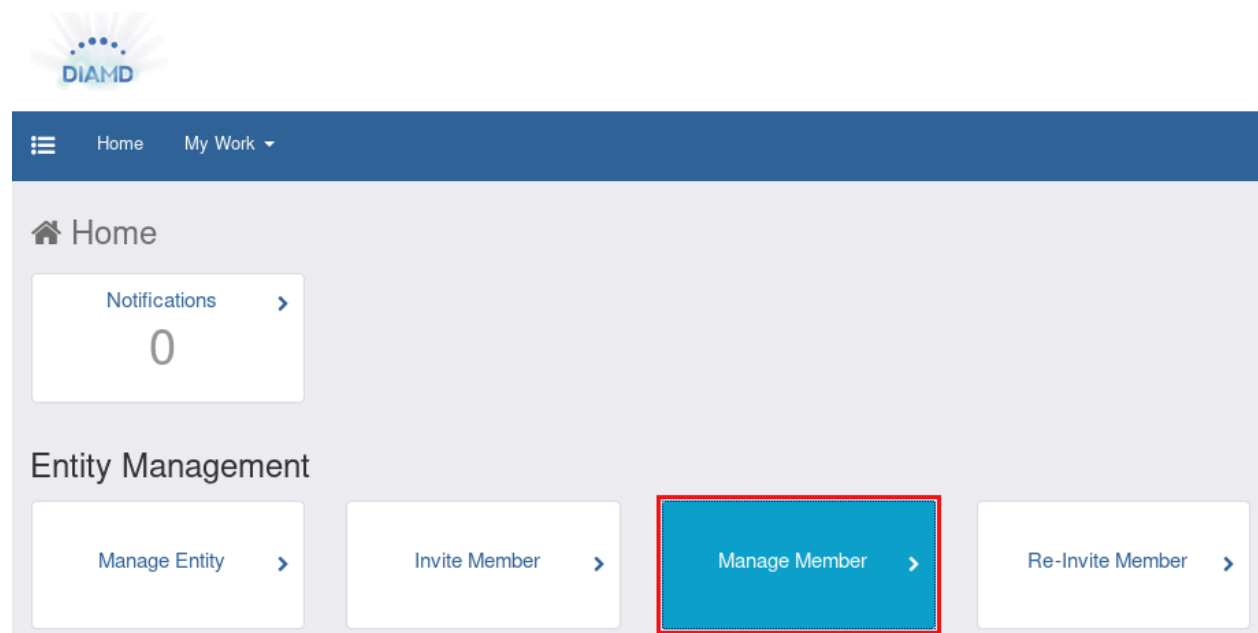
Select Roles to Add *

At least one role must be selected

Cancel

How do I add or remove roles from a member?

Step 1 - From the DIAMD home page, select “Manage Member”



Step 2 - From the “Manage Member” screen, select the roles you wish to add or remove from the member. Click Submit.



< Form

Manage Member

Search by First Name, Last Name or Email Address *

Filtered to Members within your Entity

Member Profile

First Name *

Last Name *

Email Address

Entity ID

Entity Name

Entity DBA

Current Roles +

Select Roles to Add ▼

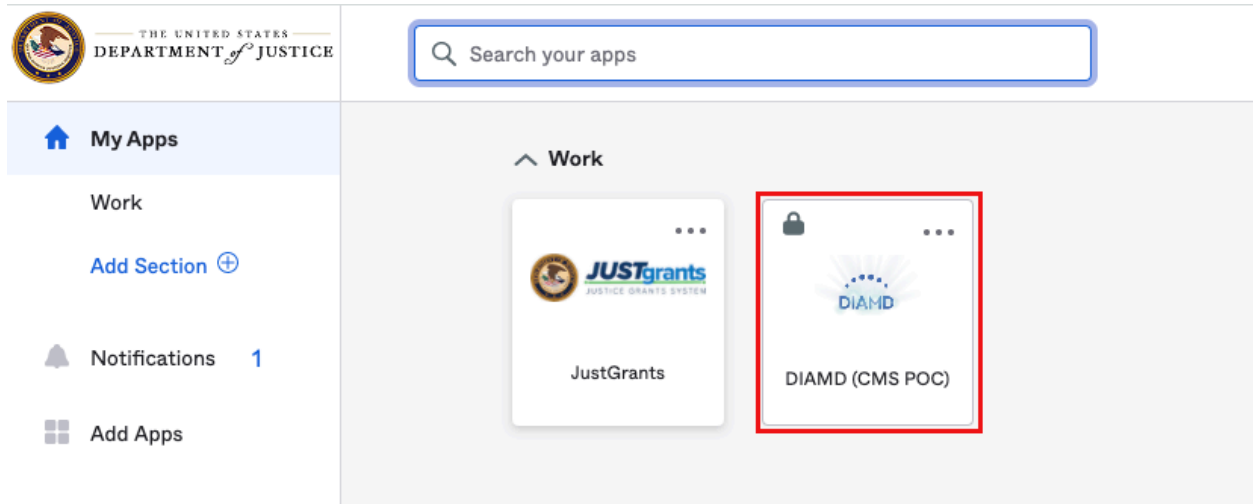
Select Roles to Remove ▼

Account Status ▼

CancelSubmit

What do I do if I don't see the DIAMD tile?

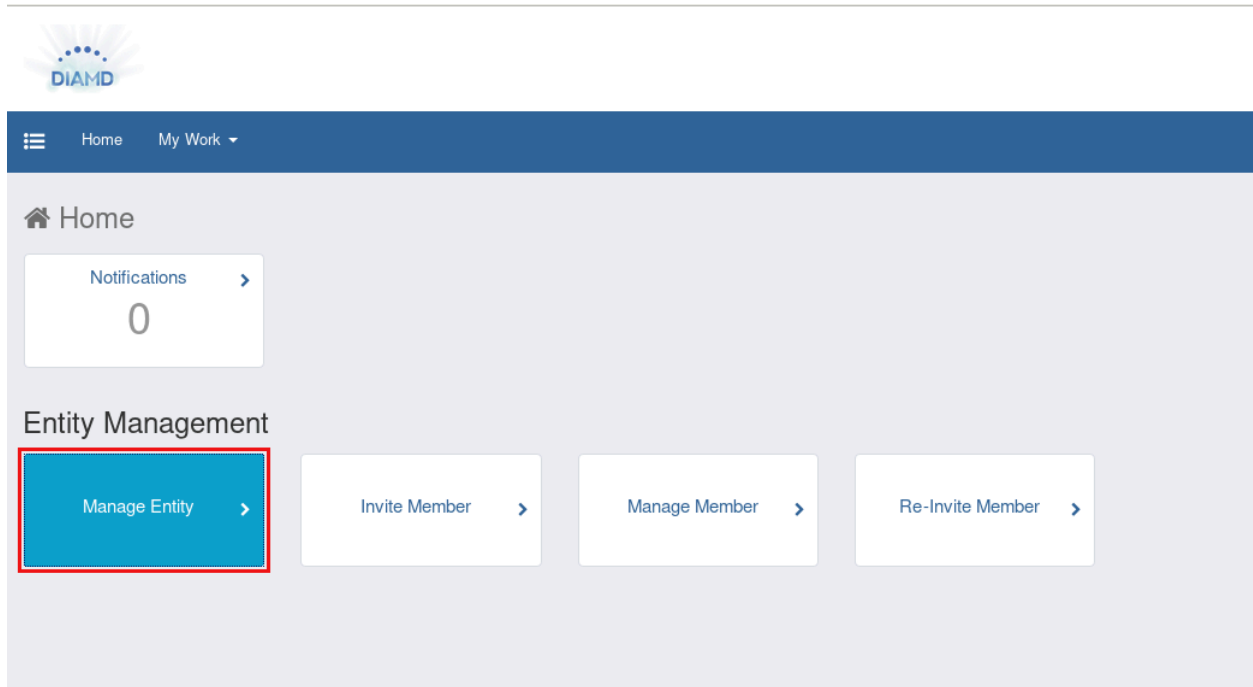
Step 1 – If the DIAMD tile is missing, please contact the service desk.



The screenshot displays the 'My Apps' section of a user interface. At the top left is the Department of Justice logo and the text 'THE UNITED STATES DEPARTMENT OF JUSTICE'. A search bar at the top right contains the text 'Search your apps'. The left sidebar includes a 'My Apps' header, a 'Work' section, an 'Add Section' button, a 'Notifications 1' indicator, and an 'Add Apps' button. The main content area shows a 'Work' section with two app tiles: 'JustGrants' and 'DIAMD (CMS POC)'. The 'DIAMD (CMS POC)' tile is highlighted with a red rectangular border. The 'DIAMD' tile features a lock icon in the top left corner and a sunburst icon with the text 'DIAMD' in the center.

How do I remove members from an entity?

Step 1 - From the DIAMD home page, select “Manage Entity”



Step 2 – Locate the “Member Management” section of the page and select the members to be removed from the entity.



Home My Work

< Form

Manage Entity

Entity Profile

Entity ID
DUNS.000000000

Entity Name *
Test Entity

Entity DBA
Test DBA

Current Entity Administrator

First Name: Testadmin Last Name: TestAdmin

Email Address: test@test.com

Entity Administrator Management

Select a member to replace the current Entity Administrator

The selected member will be assigned as the new Entity Administrator

Member Management

Select members to remove

The selected members will be removed from this Entity

Cancel Submit

What if the wrong person on my team was invited as entity administrator?

The Correct Admin needs to have the user from their entity who received the invite into DIAMD **perform** the following:

- Step 1 - Register & login
- Step 2 - Navigate to the DIAMD tile
- Step 3 - Click on Invite member
- Step 4 - Invite the Correct Admin to their entity
- Step 5 - Click on Manage Entity
- Step 6 - Replace entity administrator with the Correct Admin. Then once the correct Admin receives the invite and register/logs in they will be able to be the entity administrator.

