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](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.
3. If you selected “Reset via Email” you will see the below screen.
4. Here is a sample email that you will receive:

Hi Naman Bhansali,

You are receiving this email because you have requested to reset password for your online Department of Justice (DOJ) account.

Click this link below to reset your password:

[Reset Password]

This link expires in 68 days. If that does not work, please contact DOJ Support at OJPITServiceDesk@usdoj.gov or 202-307-0627.

Don't recognize this activity?

The security of your account is important to us. If you don't recognize this activity, please contact DOJ Support at OJPITServiceDesk@usdoj.gov or 202-307-0627 immediately.

The purpose of this email is to ensure that we update you when important account actions are taken.

This is an automatically generated message. Please do not reply to this email.

Department of Justice (DOJ)
How do I receive a code via SMS during login?

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

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 reasons 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.

<table>
<thead>
<tr>
<th>Extra Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra verification increases your account security when signing in to Okta and other applications you use</td>
</tr>
<tr>
<td>Okta Verify</td>
</tr>
<tr>
<td>Security Key or Biometric Authenticator</td>
</tr>
<tr>
<td>Google Authenticator</td>
</tr>
<tr>
<td>SMS Authentication</td>
</tr>
<tr>
<td>Voice Call Authentication</td>
</tr>
</tbody>
</table>
How do I setup Biometric or Security Key Authenticator?

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

![Image of settings page with options for Extra Verification and Change Password]

**Step 2 – Setup Enrollment**

![Image of enrollment page with notices for users]

**NOTICE TO USERS**

You are accessing a U.S. Government information system, which includes (1) this computer, (2) all computers connected to this network, and (3) all devices and storage media attached to this network or 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, civil or criminal penalties, or both. By logging in to this information system, you are acknowledging that you understand and consent to the following:

- You bear or assume the responsibility of privacy regarding any communication transmitted through or data stored in this information system. At any time, the government may review, intercept, search, or seize data transiting or stored on this information system.
- Any communications transmitted through or data stored on this information system may be the direct or indirect result of any U.S. Government authorized purpose.

For further information see the Department of the Navy’s Use and Monitoring of Department Computers and Computer Systems.

**Privacy Act Statement**

![Image of prompts for multifactor authentication]

**Set up multifactor authentication**

Your company requires multifactor authentication to add an additional layer of security when signing in to your account.

1. **Security Key or Biometric Authenticator**
   - Use a security key (USB or Bluetooth) or a biometric authenticator (fingerprint, facial recognition, etc.).
   - **Setup**
Step 3 – Begin Authenticator Enrollment

NOTICE TO USERS

You are accessing a U.S. Government information system, which includes (1) this computer, (2) the computer network, (3) all computers connected to this network, and (4) all other devices and peripheral media attached to the network or a computer on the network. This information system is provided for U.S. Government authorized use only. Unauthorized access is a criminal offense under Federal Law. 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 create, intercept, search, seize, read, or use 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

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
Step 5 – Insert security Key

Use your security key with auth.usdoj.gov
Insert your security key and touch it

Choose another option  
Cancel

Step 6 – Allow system permissions to access security key

Allow this site to see your security key?
auth.usdoj.gov wants to see the make and model of your security key

Block  
Allow
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) its computer network; (3) all computer connected to this network; and (4) all devices and storage media attached to this network or 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, civil and criminal penalties.

By logging into 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, among other actions, your data transmission or search of 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 of the Navy and Monitoring of Department Computers and Computer Systems.

Privacy Act Statement

Step 8 – Insert security key and allow entry into the system.
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?”
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”
Step 2 - On the Manage Entity screen, select a new entity administrator, click “Save”
How do I invite new members to an entity?

Step 1 - From the DIAMD home page, select “Invite Member”
Step 2 - Fill in the member’s data, select one or more roles to grant them, click submit

<table>
<thead>
<tr>
<th>Invite Member</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Member Profile</strong></td>
</tr>
<tr>
<td>Email Address *</td>
</tr>
<tr>
<td>Confirm Email Address *</td>
</tr>
<tr>
<td>First Name *</td>
</tr>
<tr>
<td>Last Name *</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Entity Profile</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity ID *</td>
</tr>
<tr>
<td>DUNS:000000000</td>
</tr>
<tr>
<td>Entity Name *</td>
</tr>
<tr>
<td>Test Entity</td>
</tr>
<tr>
<td>Entity DBA</td>
</tr>
<tr>
<td>Test DBA</td>
</tr>
<tr>
<td>Select Roles to Add *</td>
</tr>
</tbody>
</table>

At least one role must be selected

[Cancel] [Submit]
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.**
### 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**

**Submit**
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.
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.
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.