Overview

This guide will provide information to:

• Explain the concept of “Entity” as it relates to doing business with the Department of Justice (DOJ)
• Explain the crucial role the website SAM.gov plays in maintaining Entity-level data
• Define what is meant by Entity Profile
• Define the concept of Entity User(s)
• Describe the six foundational Entity User roles and their respective duties in JustGrants
• Describe the unique abilities of the external Entity Administrator role

As an introduction to the information in this guide, let’s first define several terms used throughout and break down the JustGrants relationship to SAM.gov.

IMPORTANT

During the initial role-out of JustGrants, please be aware that:

• The system does not “auto save” your work.
• You will see a warning message after 10 minutes of inactivity (per security requirements).
• You will be automatically logged out if you are inactive for 15 minutes (per security requirements).
• Unsaved work will not be saved at logout.
Entity Management Basics

One term of note is “Entity”. We use this in place of “Organization”. When you first open JustGrants, you will find your navigation options labeled “Entity Profile”, “Entity Users”, and “Entity Documents”.

These all are sections that contain information specific to your entity. In the user hierarchy, one “Entity Administrator” (EA) is assigned to each entity—if you are reading this guide, it likely is you. The specific abilities and authorities of this role are detailed on Page 7.

Entities have several identifiers: Legal name, “Doing Business As” (DBA) name, and one or multiple numeric or alphanumeric identifiers.

Most entities in JustGrants will be organizational entities, composed of multiple individuals. Organizational entities must register in SAM.gov in order to apply for funding in Grants.gov.

- **An Individual Entity** (i.e. a fellow) is when the applicant is an individual person, not an organization, applying for grant funding. Individual entities do not need to register in SAM.gov. The Tax Identifier Number/Employee Identifier Number (TIN/EIN) is used for individual entities.

- **Currently, SAM.gov considers the Data Universal Numbering System (DUNS) number to be the government-wide definition of a unique entity identifier for organizations, which are captured through SAM.gov. Each Entity should possess one DUNS number. If an organization has more than one DUNS number, each DUNS number will require separate SAM.gov registration and will be registered as a different entity in JustGrants.**

- **Note:** COPS Office grantees and awards will need to retain the Originating Agency Identification (ORI) number as a reference field.
SAM.gov is considered the Federal Government’s “source of truth” or “authoritative source” of information regarding entities.

Entities register in SAM.gov in order to apply for funding on Grants.gov and must maintain active registration throughout the life of their federal award(s). Information added or updated in SAM.gov will generally appear in JustGrants the following day. Note: The DIAMD system is not connected to SAM.gov.

1. All Entity-level data is managed in SAM.gov. JustGrants pulls its Entity information directly from SAM.gov to ensure consistency and integrity.

2. Updates to Entity information occur in SAM.gov. JustGrants performs daily automated SAM.gov checks to collect current Entity information.

3. All Entity information is registered in SAM.gov and needs to be updated there by the EA rather than through a grant modification.

4. If an Entity’s SAM.gov registration is not active or has expired, their award can be delayed/suspended until registration is active in SAM.gov.
Roles & Authority
There are six foundational roles created to ensure Entity Users have the authority and ability to carry out specific requirements and tasks.

**Entity Administrator**
- Confirms information contained in the Entity Profile is current.
- Manages entity users, including user role assignments in DIAMD, and specific application and award-level assignments in JustGrants.

**Application Submitter**
- Completes and submits applications on behalf of an entity, including Entity Assurances and Certifications.

**Authorized Representative**
- Must possess legal authority within an entity to accept awards. This action binds the entity to the award terms and conditions.

**Grant Award Administrator**
- Submits programmatic-related award requirements, including Performance Reports, certain GAMs, and portions of the Closeout.
- Alternate
- Provides support to the Grant Award Administrator. Can initiate, but not submit, programmatic-related award requirements including GAMs.

**Financial Manager**
- Certifies and submits financial information and all Federal Financial Reports on behalf of an entity.

Multiple roles can be assigned to a single user.
Entity Administrator

Key Takeaways

• The Entity Administrator (EA) is the key role within an entity.
• The EA bears responsibility for managing entity information in JustGrants.
• The EA is the gatekeeper and manages the entity users.
• The EA ensures the accuracy of the Entity Profile in JustGrants and makes changes, when necessary, in SAM.gov.
Entity Users Management
Entity Users Management: Steps 1 - 2

JustGrants navigation menu is on the left side.

1) Open the **JustGrants** Landing Page.

2) Select **Entity Users** from the menu on the left side of the screen.
3) Navigate to the *Doing Business As* section of the Entity User page and select the **Manage Users** button to open the My Apps screen for access to the Secure User Management System called DIAMD.
Entity Users Management: Step 4

4) Select the tile for Digital Identity and Access Management Directory, commonly called DIAMD, to launch your Entity Management services.
Entity Users Management: Step 5

**Invite Member**

The Entity Admin can manage users or the Entity.

5) Select the **Invite Member** tile to open the details screen.
6) Complete the email and name fields in the Member Profile section.

7) Assign roles appropriate for the member.

8) Select the Submit button to save the information.

**Note:** Fields that are marked with a red asterisk are mandatory. You will not be able to submit if these fields are left blank.

Organization data will auto-populate the Entity Profile.
Entity Users Management: Step 9

Re-Invite Member

Entity management choices are in the DIAMD menu.

9) To re-invite a member, select the **Re-Invite Member** tile to search for and send a member a DIAMD invitation.
Most data are auto-populated in the Member Profile.

10) Begin typing a name to search for the member or click the dropdown menu to select the member you wish to re-invite.

11) Select the **Submit** button to re-invite the member.
Select the Manage Member tile to access member attributes and add or remove the roles assigned to the member.
Entity Users Management: Steps 13 – 15

Add/Remove Roles

Most data are auto-populated in the Member Profile.

13) To add a role, select a role to add from the **Select Roles to Add** drop-down.

14) To remove a role, select a role to remove from the **Select Roles to Remove** drop-down.

15) Select the **Submit** button to complete the action.
Entity Management
Entity Management: Step 1

Manage Entity

To manage the Entity, select the Manage Entity tile.

1) Select the Manage Entity tile to remove a member or replace the Entity Administrator.
2) To remove a member, type to begin a search or select the dropdown to choose the member from a list.

3) Select the **Submit** button to complete the information.
Replace Entity Administrator

4) To replace the Entity Administrator, type to begin a search for the entity or select the dropdown to choose the member from a list.

5) To find the administrator's name, type to begin a search or select the dropdown to choose the administrator from a list.

6) Select the **Submit** button to finalize.
Entity Profile
Entity Profile: Steps 1 – 2

JustGrants Landing Page

1) To confirm any changes made in the DIAMD were successful, open the JustGrants Landing Page.
2) Select Entity Profile from the menu on the left side of the screen.

Note: If any information is incorrect, the Entity Administrator must make the correction in SAM.gov. It can take 24 hours for the updated SAM.gov information to update in JustGrants.
3) The **Details** button next to an individual user allows you to view user details. Confirm any changes you have made.

4) The following fields can be edited directly in JustGrants (only by the Entity Administrator): **Law Enforcement**, **Faith-Based**, **Legal Address Designation**.
Entity Profile: Step 5

Submit Changes

Any selections need to be submitted to be completed.

5) Select the **Submit** button to complete any changes made in JustGrants to the profile.
DIAMD
Digital Identity and Access Management Directory
To access JustGrants, you must register in DIAMD.

After receipt of your JustGrants Welcome email, you will need to register your account in the system.

1) Select the “here” link in the email to begin the registration process.

Note: You will have a period from receipt to complete this process. After that, the Entity Administrator will need to restart the process with a re-invite.
DIAMD: Steps 2 – 3

Selecting the link from the email will open your web browser to DIAMD, where you will complete your login information details for the system.

2) Select a “forgot password question” from the dropdown menu.

3) Type your answer into the Answer box.
4) Optionally, create a question of your own.

5) If you choose your own question, type your question into the Custom question box.

6) Type your answer into the Answer box.

7) When done, select the Create My Account button.
8) Next, you will reset your password by following the directions for password security and creating your password in the Enter new password box.

9) Repeat the new password in the box below.

10) Select the Reset Password button.
Next, you will set up multifactor authentication for your account using either Secure Key or Biometrics, Google Authenticator, SMS (text), Voice Call, or Email Authentication. Here we will focus on SMS first, then Voice.

11) For SMS (text), select the Setup button under the SMS Authentication directions.

**Note:** Users with a biometric key are encouraged to use it for secondary authentication, as shown on page 23.
12) When you select SMS (text), a new selection box will open. Select your country from the dropdown menu.

13) Enter a phone number where you can receive an SMS (text) message in the Phone number box, then select the Send code button.
14) The system will send an SMS (text) message to the number you have entered. Once you receive it, enter the code in the Enter Code box.

15) Select the Verify button to submit the code for system second-level authentication.
16) The system will return to the multifactor authentication screen and acknowledge completion of **SMS Authentication** with a green check mark.

At this point, you can select the **Finish** button, or you can add an additional optional authentication factor.
17) For Voice Call Authentication, select the **Setup** button under the **Voice Call Authentication** directions.

*This process going forward mirrors the process for SMS (text) steps 12 and 16 and will conclude with an additional green check mark for Voice Call Authentication. Once completed, select the **Finish** button to complete multifactor authentication.*
18) After clicking the Finish button, you will arrive at the My Apps screen. Select the JustGrants tile to access the system.
The email confirms your enrollment details.

After completing this process, you should receive an email confirming your enrollment.
DIAMD

Biometric Security Key Access
Note: Users with a biometric key are encouraged to use this method for secondary authentication. It is the DOJ preferred method.

You can also use a biometric security key as a secondary authentication method if phone or internet service are not available.

1) Select **Settings** to open the available choices.
2) Select **Setup** to begin the configuration of this method of multifactor authentication.
DIAMD Biometric Key: Step 3

3) Select **Enroll**.
You have two biometric choices.

4) Select the **USB security key** from the list.
5) Insert your security key and touch the biometric reader window on the key.
The system will pop up a window requesting permission.

6) Click **Allow** to grant your computer system permission to let DIAMD access the security key.
The system will log you out.

7) After you have been logged out, enter your login information again and click the Sign In button.
DIAMD Biometric Key: Step 8

A dialog box will open with a prompt.

8) Insert your security key and touch the biometric window to provide secondary authentication for the system.

You will see the progress of the authentication and then the system will open the DIAMD access page.
Entity Documents
Entity Documents: Step 1

JustGrants Landing Page

Add a document to the Entity Document Library.

Open the JustGrants Landing Page.

1) Select the **Entity Document** tab from the menu on the left side of the screen.
Entity Documents: Step 2

Upload Document

Any files previously uploaded will be displayed here.

2) Select the **Add New Document** button.
3) Select the **Select File** button, browse your workstation or shared drive to locate the file you want to upload to the Entity Document Library, then select the file.

**Recommended file formats are PDF, Word, and Excel.**
4) After the file is brought into the system, the dialog box will expand to allow entry of additional information. Complete these fields as needed.

5) Select the **Submit** button to complete the file upload into JustGrants Entity Documents.