Entity Management

Job Aid
Reference Guide

Aug 20, 2020
Page 6
Roles & Authority
Foundational roles of JustGrants, with specifics about their authority and abilities

Page 9
Secure User Management
Step-by-step instructions to complete multifactor authentication via DIAMD

Page 21
Entity Management
Step-by-step instructions for the Entity Administrator to manage entity: replacements; role additions/removals

Page 28
Entity Users Management
Step-by-step instructions for the Entity Administrator to manage users: invites; manage users; replacements

Page 38
Entity Profile
Step-by-step instructions for verifying information and accessing user profiles

Page 42
Entity Documents
Step-by-step instructions for uploading documents into the Entity Document Library

Table of Contents
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, including 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

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.

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.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity Administrator</td>
<td>Manages Entity Users and their roles, information about the organization, and assignments of users associated with different Applications and Awards</td>
</tr>
<tr>
<td>Application Submitter</td>
<td>Submits complete Applications on behalf of an organization, including Entity Assurances and Certifications</td>
</tr>
<tr>
<td>Authorized Representative</td>
<td>Enters into an agreement on behalf of the Entity and binds it to the Award terms and conditions</td>
</tr>
<tr>
<td>Grant Award Administrator</td>
<td>Manages and submits programmatic requirements of Awards, including submission of performance reports, on behalf of an Entity</td>
</tr>
<tr>
<td>Alternate Grant Award Administrator</td>
<td>Supports the Grant Award Administrator in carrying out many of the programmatic requirements of Awards</td>
</tr>
<tr>
<td>Financial Manager</td>
<td>Certifies and submits financial information and all federal financial reports on behalf of an Entity</td>
</tr>
</tbody>
</table>

Multiple roles can be assigned to a single user.
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.
Secure User Management
Secure User Management (SUM)

When you first access JustGrants, you must complete the multifactor authentication process.

You will receive a JustGrants “Welcome” email to authenticate your account.

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

**Note:** Users 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.
Selecting the link from the email will open your web browser to our Secure User Management (SUM) system known as DIAMD. Here you will complete your multifactor authentication.

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

3) Type your answer into the Answer box.
4) If you prefer, you can also choose to 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.
SUM: Steps 8 – 10

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.
SUM: Step 11

Next, you will set up multifactor authentication for your account using either SMS (text) or a voice call.

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

You can use either SMS or a standard voice call.
SUM: Steps 12 – 13

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.

“Send code” sends an SMS (text) with authentication.
SUM: Steps 14 – 15

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 mirrors the process for SMS (text) steps 16 and 17 and will conclude with an additional green check mark for Voice Call Authentication.*

18) Select the **Finish** button to complete multifactor authentication.

*This is an optional process.*
SUM: Step 19

19) After clicking the **Finish** button, you will arrive at the My Apps screen. Select the JustGrants tile to access the system.
After enrollment, you should receive an email confirming your enrollment.

Hi,

You have been enrolled in multi-factor authentication for your account.

**Enrollment Details**
Factor Type: SMS Authentication
Requested Date:
Requested Location:

**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 OJP.ITServiceDesk@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)
Entity Management
Login to JustGrants to access the JustGrants Landing Page.

1) Select **Entity Users** from the menu on the left side of the screen.

**Note:** Your login identity will always be an email address.
2) Select the **Manage Users** button in the *Doing Business As* section to open the My Apps screen for access to entity management in the Secure User Management system, DIAMD.
3) Select the DIAMD tile to launch the entity management services.

My Apps provides access to Secure User Management.
Entity Management: Step 4

4) Select the **Manage Entity** button to remove a member or replace the Entity Administrator.

To managed the Entity, select the Manage Entity tile
5) To remove a member, type to begin a search or select the dropdown to choose the member from a list.

6) Select the **Submit** button to process the request.

Most data are auto-populated in the Entity Profile.
Entity Management: Steps 7 – 9

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

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

9) Select the **Submit** button to process the request.
Entity Users Management
Login to JustGrants to access the JustGrants Landing Page.

1) Select **Entity Users** from the menu on the left side of the screen.

**Note:** Your login identity will always be an email address.
2) Select the Manage Users button in the Doing Business As section to open the My Apps screen for access to the Secure User Management System (SUMS) entity management tile.
3) Select the SUMS tile to launch SUMS entity management services.
4) Select the **Invite Member** tile to open the details screen.
5) Complete the email and name fields in the Member Profile section.

6) Assign roles appropriate for the member.

7) Select the Submit button to complete the information.

Note: Fields that are marked with a red asterisk are mandatory. You will not be able to submit if these fields are not completed.
8) To re-invite a member, select the **Re-Invite Member** tile to search for and re-send a member a SUMS invitation.
EUM: Steps 9 – 10

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

10) Select the Submit button to re-invite the member.
EUM: Step 11

Select Manage Member to begin.

11) Select the **Manage Member** tile to access member attributes and add or remove the roles assigned to the member.
EUM: Steps 12 – 14

Add/Remove Roles

Most data are auto-populated in the Member Profile.

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

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

14) Select the Submit button to complete the action.
The Entity Profile populates with SAM.gov data.

1) To confirm success of DIAMD entity updates, at the JustGrants Landing Page 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.**
Only the Entity Administrator can make changes.

2) The Details button next to an individual user allows you to view user details. Confirm any changes you have made.

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

Submit Changes

Any selections need to be submitted to be completed.

4) Select the Submit button to process any changes made in JustGrants to the profile.
Entity Documents
Add a document to the Entity Document Library.

Open the JustGrants Landing Page.

1) Select **Entity Documents** from the menu on the left side of the screen.

**NOTE:** Unlike Federal Forms, Entity Documents can be created, edited, and deleted by the Entity Administrator.
Entity Documents: Step 2

Upload Document

Any files previously uploaded display 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.
4) After the file is brought into the system, the dialog box will expand to allow entry of additional information, such as dates the file can be accessed via Start/End dates. Complete these fields as needed.

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