Table of Contents

Page 6
Roles & Authority
Foundational roles in JustGrants and details of the authority and abilities of each role

Page 9
DIAMD
Setup instructions for SMS (text) or Voice secondary authentication required to access JustGrants

Page 21
DIAMD - Biometric Security Key Access
Setup instructions for biometric and secondary authentication required to access JustGrants

Page 30
User View
The navigation bar and various tabs that allow the user to access the award particulars

Page 41
Role Reassignment
Step-by-step instructions for the Entity Administrator to reassign tasks based upon roles
Overview

This guide will provide information to:

• Identify the six foundational external roles and their respective capabilities in JustGrants

• Navigate the JustGrants Entity Landing Page to access Entity-level information and act on assigned work

• Explain the use of the JustGrants navigational tab structure

As an introduction to the information in this guide, some of the terms, processes, and features of JustGrants will be covered.

IMPORTANT

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

• The system does not “auto save” the user’s work

• A warning message will appear after 10 minutes of inactivity (per security requirements).

• The user will be automatically logged out after 15 minutes of inactivity (per security requirements).

• Unsaved work will not be saved at logout
With the release of JustGrants, applicants and grantees have a system that provides access and transparency throughout the grant process. There are terms and processes that align DOJ with the larger Federal Government to streamline the grants process for all users.

The first term of note is “Entity”, which is used in place of “Organization”. Upon opening JustGrants, users find navigation options on the left. They are labeled “Entity Profile”, “Entity Users”, and “Entity Documents”.

**Entity-level data is now managed in SAM.gov** which is considered the Federal Government’s “source of truth” or “authoritative source” of information regarding Entities. Information changes and updates are made in SAM.gov. JustGrants communicates with SAM.gov daily, ensuring data consistency and integrity between the systems.

JustGrants provides users with **two notifications sections**. One displays system-wide alerts across banners on the “Home” page; the other provides “bell notifications” specific to the user.

The **customized “Home” page is prepopulated** with information relevant to the specific user. The “Home” page features “My Worklist”, which displays tasks based on all of the user's designated roles, application, and award assignments.

**A new, intuitive navigation system** is featured with a user-friendly visual design that clearly differentiates workspaces, distinguishes sections by font size, and improves data management using different colors to separate table sections.
JustGrants User: *Highlights*

---

**Key Takeaways**

• In addition to the introduction of six foundational roles, JustGrants introduces increased visibility among users within the Entity, the Entity User, and their Entity Profile allowing more efficient user management.

• **One Email Address = One User = One Entity.** Users register an email address as the username for JustGrants access. Users accessing multiple JustGrants accounts cannot use the same email address to access different accounts.

• **One Email Address = One User = Multiple Roles = One User Experience.** All the work and permissions associated with a username are dynamically displayed on the home page.

• **Entity-level information (name, unique identifiers, etc.) is managed within SAM.gov,** eliminating the need for grant modifications to change this information.
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 Entity profile information is current. Manages users and user assignments. Confirms Authorized Representative has proper legal authority to accept or decline an award.

**Grant Award Administrator**
Submits programmatic-related award requirements, including Performance Reports, Grant Award Modifications (GAMs), and Closeouts.

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

**Grant Award Administrator** (ALTERNATE)
Supports the Grant Award Administrator. Can initiate and submit programmatic-related award requirements, including Performance Reports and GAMs.

**Authorized Representative 1**
Accepts or declines awards on behalf of an Entity. Must have legal authority to enter into contracts, grants and cooperative agreements with the federal government on behalf of the Entity.

**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 user management role within an Entity.

• The EA bears responsibility for managing Entity information in JustGrants.

• The EA is the gatekeeper for access to JustGrants and manages the Entity Users.

• The EA ensures the accuracy of the Entity Profile in JustGrants and makes changes in SAM.gov, when necessary.
DIAMD

Digital Identity and Access Management Directory
To access JustGrants, users must register in DIAMD.

After receipt of the JustGrants Welcome email, register the user’s account in the system.

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

**Note:** Users have limited time after receiving the invitation email to complete this process. After the time has elapsed, the Entity Administrator will need to re-invite the user to restart the process.
DIAMD: Steps 2 – 3

Selecting the link from the email will open the web browser to DIAMD, where the user will provide login information details for the system.

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

3) Type the answer into the Answer box.

Select a question that only the user can answer.
4) Users can create an optional question of their own.

5) To choose their own question, type the question into the Custom question box.

6) Type the answer in the Answer box.

7) When done, select the Create My Account button.

Optional: Create a personalized question and answer.
8) To reset a password, follow the directions for password security and create a password in the **Enter new password** box.

9) Enter the new password again in the box below.

10) Select the **Reset Password** button.

---

The six previously used passwords cannot be reused.
Set up multifactor authentication for the account using either Secure Key, Biometrics, Google Authenticator, SMS (text), Voice Call, or Email Authentication.

The following instructions will focus on SMS and then Voice.

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

Note: Users with biometric key abilities are encouraged to use biometrics for secondary authentication, reference page 22.

Use either SMS or a standard voice call for authentication.
12) When selecting SMS (text), a new selection box opens. Select the appropriate country from the dropdown menu.

13) Enter the user’s phone number in the **Phone number** box, then select the **Send code** button to receive an SMS (text) message.

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

14) The system will send an SMS (text) message to the phone number entered. Once received, enter the code in the Enter Code box.

15) Select the Verify button to submit the code for second-level authentication.

Enter the code sent via SMS (text) to the user’s phone.
16) The system will return to the multifactor authentication screen and note SMS Authentication completion with a green check mark.

Either select the Finish button or add an additional authentication factor (optional).
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 concludes with an additional green check mark for Voice Call Authentication. Once completed, select the **Finish** button to complete multifactor authentication.*
18) Select the **Finish** button to open the **My Apps** screen. Select the **JustGrants** tile to access the system.

**Note:** Until a user logs into JustGrants by selecting this tile, the account is not active.
DIAMD: Confirmation

After completing this process, the user will receive an email confirming enrollment.

The email confirms enrollment details.
DIAMD

Biometric Security Key Access
DIAMD: Biometric Key: Step 1

**Note:** Users with a biometric key are encouraged to use this method for secondary authentication. It is the preferred method of DOJ.

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.

To follow this path, select **Settings**.
2) Select **Setup** to begin configuring this method of multifactor authentication.
3) Select Enroll.

Enroll to set up the user’s biometric key.
There are two biometric choices.

4) Select the **USB security key** from the list.
DIAMD: Biometric Key: Step 5

5) Insert the security key and touch the biometric reader window on the key.

After inserting, touch the biometric window.
DIAMD opens a pop-up window requesting permission.

6) Select **Allow** to grant permission for DIAMD access the security key.
The user is automatically logged out of DIAMD.

7) After logging out, enter the login information again and select the Sign In button.

The user must sign in again.
8) Insert the security key and touch the biometric window to provide secondary authentication for the system.

Users can view the progress of the authentication; the system will open the DIAMD access page.

The user’s security key provides secondary authentication.
User View
Landing Page: Step 1

When viewing the Landing Page, note that the content of the top heading and left navigation bar do not change.
Landing Page: Step 2

The top heading contains the Logo, Bell Notifications, Help Icon, and User Logoff.

Click on the Help Icon for links to JustGrants User Support contact information and JustGrants Resources.
When viewing the Home Page, the following tabs are available to users: a tab labeled **Alerts**, which displays system-wide notifications; and **My Worklist**, which displays the user's current assigned tasks. A **Load More** option may appear at the bottom of the alerts if more notifications exist than those that are currently displayed.

The alerts are color coded: **Information** (blue); **Notifications** (green); and **Warnings** (orange). The alert designations are managed internally by DOJ.

**NOTE:** User-assigned work resides in **My Worklist** on the Home Page. All Entity work is located under the respective award and applications navigation tabs.
For Entity profiles, Entity-level information is displayed on the Entity Profile; all Entity Users and DOJ Users can access this information. SAM.gov will populate Legal Name, Doing Business As Name (if applicable), DUNS, UEI, TIN, Business URL, Year Established, Fiscal Year (end), and SAM Registration Status (Expiration Date and Last Updated date) information. SAM.gov data will populate the mailing address, as appropriate. ROID is populated by DOJ once the Entity has completed registration with ASAP.

Entity Administrators can change: Law Enforcement, Faith-Based Entity, and Designation of Entity’s Legal Address.

NOTE: If the SAM profile is marked as Not Public, only a mailing address will populate in the Entity Profile.
All Entity Users are displayed on this tab once the Entity Administrator has added that user in DIAMD and the user has successfully logged into JustGrants.

Entity Users can select **View Details** to access information about each user, including their assigned roles. **Users can update their own User Profile information.**

In addition, Entity Administrators will have access to the **Manage Users** button.
Entity Administrators can upload documents to this location so that other Entity Users (and DOJ Users) can view and download those documents for use on specific applications, awards, and monitoring activities.

The forms located in this section are applicable to the Entity as a whole, or relate to multiple applications and awards (e.g., indirect cost agreements, financial capability questionnaires).
Applications

Users can access the applications that have been submitted by the Entity as well as the status of each application. The list will consist of all DOJ applications, both active and closed.

All Entity Users can access all the Entity’s applications; however, only users assigned to specific applications will be able to take actions within those applications.

**NOTE:** User-assigned work is located on the **Home** screen under the **Task List.** All Entity work is found under the **Award** and **Applications** navigation tabs.
The **Awards** tab includes a list of all DOJ awards, both active and closed; older Awards are being migrated into JustGrants. All Entity Users will be able to access all the funded awards; however, only users assigned to specific awards will be able to take actions within those awards.

Also, users assigned to an award can request a **Grant Award Modification (GAM)** by clicking on the Award Number; this takes the User to the “Funded Award Case”, where all activities associated with a specific funded award can be accessed.

**NOTE:** All Entity work is located under the **Award** navigation tabs.
All DOJ Entity monitoring activities are listed on the Monitoring tab, as well as the award status and contact information.
The Federal Forms tab contains a list of forms generally used in the administration of federal funds.

**NOTE:** Federal Forms are created, edited, and deleted by DOJ personnel. Entity Users can download and populate data in Federal Forms, but cannot add, edit, or delete the forms.
Role Reassignment
Role Reassignment

Individual user management.

The Entity Administrator can perform role assignment and management on an application-by-application and award-by-award basis; this enables the more effectively management of users across an Entity in one location.

1) Open the **JustGrants** Landing Page.
2) Select **Awards** from the navigation bar on the left side of the screen. Use the **Applications** menu option to access roles. The page is slightly different, but the following process is the same.
Select Award, Role, Assignee

3) Select the checkboxes next to the awards to be reassigned.

4) Select the **Choose Role** dropdown menu to select the role to reassign. This filters the user view to display only those with that role available for assignment.

5) Select the **Assign to** dropdown menu to select the user to reassign.
Role Reassignment: Reassign

Users can only be assigned to roles assigned in DIAMD.

6) Select Assign to complete the action.