<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Introduction and Overview</td>
</tr>
<tr>
<td>5</td>
<td>How to Use this Guide</td>
</tr>
<tr>
<td>6</td>
<td>What is an Entity?</td>
</tr>
<tr>
<td>7</td>
<td>Entity Management Overview</td>
</tr>
<tr>
<td>8</td>
<td>Entity Management Key Points</td>
</tr>
<tr>
<td>9</td>
<td>Systems Used for Entity Management: SAM.gov, DIAMD, and JustGrants</td>
</tr>
<tr>
<td>10</td>
<td>JustGrants Roles</td>
</tr>
<tr>
<td>11</td>
<td>Equal Employment Opportunity Program (EEOP) Roles</td>
</tr>
<tr>
<td>12</td>
<td>Initial Onboarding: Bringing an Entity into JustGrants During Application Submission</td>
</tr>
<tr>
<td>16</td>
<td>Entity User Management Overview</td>
</tr>
<tr>
<td>20</td>
<td>Entity User Management in Digital Identity and Access Management Directory (DIAMD)</td>
</tr>
<tr>
<td>22</td>
<td>View Entity</td>
</tr>
<tr>
<td>25</td>
<td>Change Entity Administrator</td>
</tr>
<tr>
<td>32</td>
<td>Invite Entity Users</td>
</tr>
<tr>
<td>41</td>
<td>Re-invite Entity Users</td>
</tr>
<tr>
<td>46</td>
<td>Add/Remove Roles from Entity Users</td>
</tr>
<tr>
<td>52</td>
<td>Remove Users from Entity</td>
</tr>
<tr>
<td>Page</td>
<td>Section</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>62</td>
<td><strong>Entity User Management in JustGrants</strong></td>
</tr>
<tr>
<td>63</td>
<td>Assign/Re-assign Entity Users to Applications</td>
</tr>
<tr>
<td>72</td>
<td>Remove Additional Application Submitter Roles</td>
</tr>
<tr>
<td>77</td>
<td>Assign/Re-assign Entity Users to Awards</td>
</tr>
<tr>
<td>88</td>
<td><strong>Entity Profile</strong></td>
</tr>
<tr>
<td>93</td>
<td><strong>Maintain Entity Documents</strong></td>
</tr>
</tbody>
</table>
Introduction and Overview
This Job Aid Reference Guide (JARG) helps the Entity Administrator (EA) fulfill their entity management-related duties. This JARG is part of a larger training and resource package that is accessible on the JustGrants Entity Management Training website.

Linked Content

This JARG uses a chapter-linked table of contents to help users navigate to specific content. A link has been included on each page to help the user navigate within this JARG.

Select the Home icon located at the bottom left corner of the page to return to the table of contents.
What is an Entity?

The term entity refers to applicants and award recipients. An entity has unique identifiers such as: legal name, doing business as (DBA) name, and one or more numeric or alphanumeric identifiers. In JustGrants, there are two distinct types of entities: Organizations and Individuals.

Most entities in JustGrants are considered organizational entities. There are many types of organizational entities, including but not limited to: nonprofits, American Indian tribes, state or local governments, and institutions of higher education.

Organizational entities must register and maintain an active registration status in SAM.gov in order to access federal funding. The SAM.gov Unique Entity Identifier (UEI) is considered the primary alphanumeric identifier for organizational entities in JustGrants.

An individual entity is a person, not an organization, applying for grant funding. Typically, an individual entity applies for a fellowship grant program.

Individual entities do not need to register in SAM.gov. Instead, individual entities should use their Internal Revenue Service (IRS) Federal Tax ID Employee Identification Number (EIN)/Tax Identifier Number (TIN) as their unique alphanumeric identifier.

For security purposes, JustGrants recommends not using a Social Security number (SSN) as the unique identifier.
Entity Management Overview

This Entity Management JARG:

• describes the roles and responsibilities of the Entity Administrator (EA).
• clarifies how JustGrants uses data from other federal systems.
• reviews the six (6) JustGrants user roles and their respective duties.
• introduces the four (4) Equal Employment Opportunity Program (EEOP) user roles.
• explains the process of managing entity users, roles, and assignments.
• provides instruction around planned or unplanned changes to the EA.
• illustrates the process to maintain and update entity-level information and documents.
Entity Management Key Points

The Entity Administrator (EA):

- is a critical user in JustGrants. Every entity must always have one user designated as the EA.
- acts as the entity's gatekeeper and bears responsibility for managing entity users, roles, and assignments in JustGrants.
- ensures the accuracy of the entity profile in JustGrants and coordinates applicable changes in SAM.gov.
- maintains entity documents within JustGrants.

**NOTE:** While working in JustGrants, be aware that:

- the system does not **auto save** any work. Unsaved work is not automatically saved at logout.
- JustGrants posts a warning message after ten (10) minutes of inactivity.
- all users are automatically logged out if inactive for fifteen (15) minutes.
Systems Used for Entity Management: SAM.gov, DIAMD, and JustGrants

- **SAM.gov**
  - SAM.gov is the federal government's source of truth for entity identifiers.
  - Organizational entities must maintain an active registration and ensure entity information is current.
  - Other federal systems use entity data from SAM.gov.

- **DIAMD**
  - The Digital Identity and Access Management Directory (DIAMD) is the Department of Justice’s (DOJ) secure user management system.
  - The Entity Administrator (EA) determines who should have access to their entity data and then invites those individuals to be entity users.
  - The EA keeps entity users and their roles up to date and re-assigns the EA role as needed.

- **JustGrants**
  - JustGrants is DOJ's grants management system.
  - The EA assigns and re-assigns entity users to specific applications and awards.
  - The EA uploads entity-level documents into the system.
## JustGrants Roles

There are six (6) roles in JustGrants, each with unique duties and abilities. An entity user can be assigned multiple JustGrants roles.

<table>
<thead>
<tr>
<th>Role</th>
<th>Count</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entity Administrator</strong></td>
<td>1 per entity</td>
<td>Confirms entity profile information is current. Manages users and assignments. Confirms the Authorized Representative has legal authority to accept or decline an award.</td>
</tr>
<tr>
<td><strong>Grant Award Administrator</strong></td>
<td>1 per award</td>
<td>Submits programmatic award requirements, including Performance Reports (PRs), Grant Award Modifications (GAMs), and portions of the Closeout.</td>
</tr>
<tr>
<td><strong>Authorized Representative</strong></td>
<td>1 – 2 per application &amp; award</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Alternate Grant Award Administrator</strong></td>
<td>1 per award (optional)</td>
<td>Supports the Grant Award Administrator in completing programmatic award requirements, including submitting GAMs, deliverables, and assigned PRs.</td>
</tr>
<tr>
<td><strong>Application Submitter</strong></td>
<td>1 – 3 per application</td>
<td>Completes and submits applications on behalf of an entity, including Entity Disclosures, Assurances, and Certifications requirements.</td>
</tr>
<tr>
<td><strong>Financial Manager</strong></td>
<td>1 per award</td>
<td>Certifies and submits the Federal Financial Report (FFR) on an entity's behalf.</td>
</tr>
</tbody>
</table>
Certain entities that receive DOJ funding are required to submit an Equal Employment Opportunity (EEO) plan. The purpose of the EEO plan is to ensure entities receiving DOJ financial assistance are providing full and equal employment opportunities to prospective employees.

There are four (4) EEOP roles, each with unique duties. Users can only possess one role.

**Entity Administrator**
- Manages entity users’ role assignments.

**User**
- Assists in completing EEOP reports. However, an EEOP user cannot sign and submit EEOP reports.

**Read-Only User**
- Views entity reports.

**Implementation Authority**
- Signs and submits reports within the EEOP system; may also prepare reports. Must have authority to implement entity’s EEOP per 28 CFR 42.304.

For additional information about EEOP, visit:
- [Civil Rights | Equal Employment Opportunity Program (EEOP) FAQs](https://ojp.gov)
- [Office of Justice Programs (ojp.gov)](https://ojp.gov)
Initial Onboarding: Bringing an Entity into JustGrants During Application Submission
Initial Entity Onboarding: Key Points

For entities that are new to JustGrants, the initial entity onboarding process occurs during application submission and relies on the following two federal systems for critical onboarding data: **SAM.gov** and **Grants.gov**.

Organizational entities seeking federal funding are required to register and maintain an **active** status in **SAM.gov**. For this reason, SAM.gov is considered the federal government's **source of truth** for organizational entity identifiers.

If an organizational entity is new to JustGrants, the **SAM.gov E-Biz point of contact (POC)** is onboarded as the **Entity Administrator (EA)** in **JustGrants**.

Once onboarded into JustGrants, the SAM.gov E-Biz POC can transfer the EA role to another entity user.

For entities that are new to JustGrants, the **initial** entity onboarding process is triggered when an entity submits an application for Department of Justice (DOJ) funding in **Grants.gov**, where entities first apply as part of the two-step grant application process.

Once JustGrants receives the Grants.gov application, the **EA** will receive an e-mail with onboarding instructions.

**NOTE:** For individual entities, initial entity onboarding bypasses SAM.gov and relies solely upon information provided in the Grants.gov application. Individuals must use one alphanumeric identifier consistently in JustGrants.
Initial Entity Onboarding

Application Submission

Organizational entities must register with SAM.gov to apply for federal assistance. Registration details cascade through to Grants.gov and JustGrants.

<table>
<thead>
<tr>
<th><strong>Steps</strong></th>
<th><strong>Steps</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Register, renew, or confirm with SAM.gov</td>
<td>✓ Obtain or confirm the Unique Entity Identifier (UEI) number in SAM.gov</td>
</tr>
</tbody>
</table>

**NOTE:** Individual entities will bypass SAM.gov Step 1 and go directly to Grants.gov Step 2.

Grants.gov is the central place to locate federal funding opportunities.

<table>
<thead>
<tr>
<th><strong>Steps</strong></th>
<th><strong>Steps</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Search Grants.gov</td>
<td>✓ Submit SF-424 and SF-LLL forms in Grants.gov</td>
</tr>
<tr>
<td>✓ Select correct Competition ID</td>
<td></td>
</tr>
</tbody>
</table>

DIAMD and JustGrants are the two DOJ systems that enable entities to manage users and work.

<table>
<thead>
<tr>
<th><strong>Steps</strong></th>
<th><strong>Steps</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Manage entity users and their roles</td>
<td>✓ Assign users to awards and applications</td>
</tr>
</tbody>
</table>

Entity users log into JustGrants and complete assigned work.
Troubleshooting: Initial Entity Onboarding

Entities may experience the following issues preventing immediate onboarding into JustGrants:

**Entity's SAM.gov registration status is expired or newly activated**

JustGrants only receives information from SAM.gov when an entity's registration has an **active** status. Visit SAM.gov and use the **Check Entity Status** function to confirm this status. Once activated, JustGrants typically receives the information within one to five (1 – 5) days.

**SAM E-Biz POC did not receive a DOJ/DIAMD e-mail invitation**

Check the POC's spam folder and look for an e-mail from DIAMD-NoReply@usdoj.gov. Users may also receive e-mails from do-not-reply@ojp.usdoj.gov or ojp@servicenowservices.com.

**SAM.gov E-Biz POC already associated with an existing entity in JustGrants**

An individual user's e-mail address can only be associated with one entity in JustGrants. For entities that are managed by the same individual, that user will need to establish and use a unique e-mail address for each entity in JustGrants or be removed as a user in the existing entity.

**Entity wants to use the SAM.gov Alternate E-Biz POC for onboarding**

SAM.gov allows entities to identify an **Alternate E-Biz POC**. In the event of a JustGrants conflict with the primary SAM.gov E-Biz POC. Entities may elect to use this alternate POC for initial onboarding. The Alternate E-Biz POC should contact JustGrants User Support for onboarding assistance.
Entity User Management Overview
Entity User Management Key Points

Entity user management is performed in two intersecting Department of Justice (DOJ) systems — **Digital Identity and Access Management Directory (DIAMD)** and **JustGrants**.

- DIAMD ensures that only authorized users — those designated by the Entity Administrator (EA) — can access entity information in JustGrants.
- Each entity can have only one EA.
- Only the EA can make changes in DIAMD.
- The EA uses DIAMD to invite new entity users and add and remove roles as needed.
- Once the EA invites new entity users, DIAMD sends an e-mail to users with instructions to register and log in to JustGrants.

- JustGrants is where entity users complete DOJ grant-related activities.
- EAs will assign entity users to specific applications and awards within JustGrants.
- Once an entity user is assigned to an application or award, they will receive assignments and take actions associated with their role.
Inviting New Entity Users to JustGrants

Successful entity user management depends on sequential actions taken by both the Entity Administrator (EA) and entity users.

The EA takes these actions in DIAMD:
- Invites each entity user;
- Assigns roles to each entity user.

Each entity user receives an instructional e-mail from DIAMD and completes these actions within 72 hours:
- Logs into DIAMD to set a password and multi-factor authentication;
- Logs into JustGrants.

The EA makes user assignments in JustGrants:
- Applications — assigns Application Submitter(s) and Authorized Representative(s);
- Awards — assigns Authorized Representative(s), Grant Award Administrator, and Financial Manager.

The entity user logs into JustGrants and acts on assigned applications and awards.
Troubleshooting: Entity User Management

Entity Administrators commonly encounter the following issues:

I invited a new entity user in DIAMD, but I don't see them listed in the Entity Users section in JustGrants.

After the EA invites a user in DIAMD, an e-mail is sent to that user from DIAMD-NoReply@usdoj.gov. The user must follow the instructions outlined in this e-mail to create a password and log in to JustGrants within 72 hours.

Check with the entity user to confirm they have taken these actions. If the user cannot locate the e-mail, or if the link contained in the e-mail has expired, re-invite the user in DIAMD. Once the user successfully logs into JustGrants, their name will appear on the Entity Users section.

I added or removed roles from an existing entity user in DIAMD, but those changes are not reflected in JustGrants.

Refresh the JustGrants screen. The changes should synchronize immediately.
Entity User Management in Digital Identity and Access Management Directory (DIAMD)
**DIAMD Navigation**

When the Entity Administrator (EA) logs into DIAMD, the screen displays options related to the actions listed on this page.

![DIAMD Navigation Interface](image)

**View Entity** - View information such as the current EA and entity users and their roles.

**Manage Entity** - Replace the current EA with another active entity user or remove user(s).

**View User** - View information about entity users, including their role(s) and last invitation date.

**Invite Entity User** - Invite new entity users. If the user does not have an existing DIAMD account, a new account is created, and the user will receive an instructional e-mail.

**Re-Invite Entity User** - Send a new DIAMD invitation e-mail to reset the user’s password and multi-factor authentications. The user must follow the instructions contained in the e-mail. Upon completion, the user's account will be re-enabled.

**Manage Entity User** - Add or remove roles from an entity user or remove the user from the entity.
The Entity Administrator (EA) can view the following entity-wide information using View Entity:

- Entity Profile (Entity ID, Entity Name, and Entity Doing Business as (DBA) Name);
- Current EA;
- Entity Users (Names, E-mail Address, Roles, and Account status).

1) To view entity information, select **View Entity**.
2) To view all entity users, use the scroll feature at the bottom right of the page. Entity accounts will be shown as enabled or disabled.

NOTE: Select Cancel to exit View Entity.
Change Entity Administrator
Change Entity Administrator
Overview

The Entity Administrator (EA) is a critical entity role; every entity must have one user assigned as the EA. Entities should also be prepared to have a **back-up** EA so the role can easily be reassigned. The following points should be considered for a change in EAs — both planned and unplanned.

---

**Planned EA Changes**

- ✓ Identify which entity users can fulfill the EA responsibilities.
- ✓ Ensure those users have access to training and critical entity information.
- ✓ Current EA logs into Digital Identity and Access Management Directory (DIAMD) and selects a user to assign as the new EA.
- ✓ Newly assigned EA logs in and assumes EA-related duties.

**Unplanned EA Changes**

- ✓ Requires JustGrants User Support assistance.
- ✓ Entity must onboard a new EA into JustGrants.
- ✓ Upon request, JustGrants User Support confirms entity’s current SAM.gov E-Biz point of contact (POC) and onboards that POC as the new EA.
- ✓ The SAM.gov E-Biz POC receives instructional e-mail from DIAMD.
- ✓ Newly onboarded EA logs in and assumes EA-related duties.
1) To reassign the EA role to another user, the current EA will select **Manage Entity**.
2) To replace the EA, either enter the replacement EA name in the **Entity Administrator Management** dropdown list or open the dropdown to choose the replacement EA from a list.

3) Select **Next**.
4) Ensure the correct entity user is selected as the replacement EA.
5) Select **Next**.
6) After selecting **Next**, DIAMD asks for confirmation of the new EA.
7) Select **Back** to make corrections or **Confirm** to proceed.

**Entity Profile**
- **Entity ID**: UE1.RK2VTM8MF03
- **Entity Name**: JGII Test Org26 Doing Business As
- **Entity DBA**: JGII Test Org26

**Current Entity Administrator**
- **First Name**: John
- **Last Name**: Doe
- **Email Address**: justgrand226@gmail.com

**Entity Administrator Management**
- Select an Entity User to replace the current Entity Administrator
- **Jane Doe**
- The selected user will be assigned as the new Entity Administrator

**Entity User Management**
- Select Entity Users to remove
- The selected users will be removed from this Entity

Steps take place in DIAMD
When the EA is no longer available to transfer the EA role to another user, the entity must take the following steps to onboard a new EA:

**SAM.gov:**
- Confirm the entity's SAM.gov E-Biz POC and update the POC in SAM.gov, if needed.
- Alert the E-Biz POC that they will be onboarded as the new EA and should prepare for action.

**JustGrants:**
- Contact JustGrants support at JustGrants.Support@usdoj.gov or 833-872-5175. Advise that the entity EA is no longer available, and request to onboard the current E-Biz POC as the new EA.

**DIAMD:**
- E-Biz POC receives an instructional e-mail from DIAMD and successfully logs in within 72 hours.

**JustGrants:**
- New EA logs in and assumes all EA-related duties.
Invite Entity Users
To invite entity users, the Entity Administrator (EA) must log in to JustGrants.

1) View the Home page.
2) Select the Entity Users link on the left to view current users.

NOTE: The EA can access Digital Identity and Access Management Directory (DIAMD) via JustGrants. DIAMD is where the EA invites, re-invites, and manages entity users.
3) Select Manage Users to open the My Apps screen for access to DIAMD.

NOTE: Only the EA can access DIAMD and make changes to entity users. If an entity user does not know who their EA is, look for the EA icon in the Entity Users section. Each entity has only one EA.
4) Select **Invite Entity User** to open the details screen.
5) Enter the entity user’s e-mail address, first name, and last name into the designated fields in the **Entity User Profile** section.

6) Expand the **Select Roles to Add** dropdown menu.

**NOTE:** Fields that are marked with a red asterisk are mandatory. It is not possible to **Submit** if these fields are blank. The data populating the Entity Profile section is pulled from the entity information entered in **SAM.gov**.
7) Select a role(s) from the dropdown menu.
8) After completing the Entity User Profile and the Select Roles to Add, select Next.
9) After selecting **Next**, DIAMD asks for confirmation of the e-mail address, first name, and last name fields in the Entity User Profile section as well as assigned role(s).

10) Select **Back** to make corrections or **Confirm** to proceed.
11) After the EA confirms the Entity User Profile information, an e-mail is sent to the entity user from **DIAMD-NoReply@usdoj.gov**.

**NOTE:** The links in the e-mail expire after 72 hours. If the entity user does not take the two outlined steps within 72 hours, the EA will have to re-invite the user in DIAMD.
Re-invite Entity Users
Re-invite Entity Users

Step 1

The Entity Administrator (EA) can re-invite an entity user when:

- An entity user's account is disabled;
- A user forgot their password and needs a reset;
- The links in their instructional Digital Identity and Access Management Directory (DIAMD) e-mail have expired (after 72 hours);
- The user gets a new phone number and needs to update their access.

1) To re-invite a user, select Re-Invite Entity User to search for a specific entity user and re-send a DIAMD invitation.

NOTE: If the entity user does not receive an e-mail invitation from DIAMD to register their account, the EA will need to re-invite the entity user.
2) Search for the entity user to re-invite. The search can be conducted by first and last name or e-mail address.

3) Select **Next**.

**NOTE:** Use the displayed form to send a new registration link to an entity user’s e-mail address or to reset the entity user’s password and multi-factor authentication (MFA) selections. The entity user will need to update their existing password and MFA selections using the link provided. If the entity user is currently disabled, then the entity user will be re-enabled prior to sending the new registration link.
4) Type the desired entity user’s name or use the dropdown menu to select the entity user to be re-invited.

5) Select **Next**.
6) After selecting **Next**, DIAMD asks for confirmation.

7) Select **Back** to make changes or **Confirm** to proceed.
Add/Remove Roles from Entity Users
Add/Remove Roles from Entity Users

Overview

One of the primary duties of an Entity Administrator (EA) is to continually manage entity users in Digital Identity and Access Management Directory (DIAMD). This includes adding and removing roles as entity user responsibilities change.

Individual users can be assigned multiple roles in DIAMD. When adding and removing roles for users in DIAMD, the EA should consider the following:

- Who should have access to view the entity’s information — applications and awards — in JustGrants? Generally, all entity users can view all entity information (except a user who only possesses the Application Submitter (AS) role).

- Who needs to take actions on specific applications and awards?

- What roles would enable those users to take those actions?

- Having multiple users with multiple roles who can quickly receive reassignments in JustGrants during staff absences and changes.
1) To add or remove roles from entity users, the EA will select **Manage Entity User**.
2) Either enter the desired entity user’s name or use the dropdown menu to select the entity user to be added or removed.

**NOTE:** After selecting the entity user’s name, the Entity User Profile auto-populates.
3) Use the **Select Roles to Add** or **Select Roles to Remove** dropdown menus to add or remove the relevant role(s) pertaining to the identified entity user. Both dropdown menus can be used at the same time.

4) Select **Next**.
5) After selecting **Next**, DIAMD requires confirmation of the entity user’s name and role(s) being added/removed.

6) Select **Back** to make corrections or **Confirm** to proceed.

---

### Add/Remove Roles from Entity Users

Steps 5 – 6

<table>
<thead>
<tr>
<th>Manage Entity User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please review and confirm your values. Click 'Back' to make changes or 'Confirm' to proceed.</td>
</tr>
</tbody>
</table>

1. **Search by First Name, Last Name or Email Address**:
   - Jane Doe
   - Filtered to Users within your Entity

2. **Entity User Profile**
   - **First Name**: Jane
   - **Last Name**: Doe
   - **Email Address**: jude@spicomt.com@gmail.com

3. **Entity ID**
   - JD-R121/M08/03

4. **Entity Name**
   - JD-N Test Org/2 Doing Business As

5. **Entity EDA**
   - JD-N Test Org/28

6. **Current Roles**
   - Role: GLM Authorized/Representative
   - Role: GLM-Financial/Manager

7. **Select Roles to Add**
   - Role: GLM-Financial/Manager

8. **Select Roles to Remove**
   - Role: GLM-Financial/Manager

9. **Last Invited Date**

10. **Account Status**
    - Enabled

---

**Steps take place in DIAMD**
Remove Users from Entity
Part of the ongoing maintenance duties of the Entity Administrator (EA) includes keeping users and roles current in Digital Identity and Access Management Directory (DIAMD). This involves adding as well as removing entity users from DIAMD.

When an EA needs to remove an entity user (e.g., when a user is seeking to become a user with a different entity or when a user is leaving an entity), the EA must remove the user from DIAMD.

The EA has two options to remove entity users from DIAMD:

- Manage Entity
- Manage Entity User

Steps take place in DIAMD
Remove User from Entity (Manage Entity)

Step 1

The first option the EA can use to remove an entity user from DIAMD is **Manage Entity**.

1) Select **Manage Entity**.
2) In the **Entity User Management** section, enter the entity user’s name in the **Select Entity Users to remove** dropdown list, or open the dropdown to choose the entity user from a list.

3) Ensure the correct entity user is selected for removal and select **Next**.
Remove User from Entity (Manage Entity)

Steps 4 – 5

4) After selecting **Next**, DIAMD asks for confirmation to remove the entity user.

5) Select **Back** to make corrections or **Confirm** to proceed.

<table>
<thead>
<tr>
<th>Entity Profile</th>
<th>Current Entity Administrator</th>
<th>Entity Administrator Management</th>
<th>Entity User Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity ID: UEJ9XZ9V7X6F093</td>
<td>First Name: John</td>
<td>Select an Entity User to replace the current Entity Administrator</td>
<td>Select Entity Users to remove</td>
</tr>
<tr>
<td>Entity Name: JUN Test Org26 Doing Business As</td>
<td>Last Name: Doe</td>
<td>The selected user will be assigned as the new Entity Administrator</td>
<td>The selected users will be removed from this Entity</td>
</tr>
<tr>
<td>Entity DBA: JUN Test Org26</td>
<td>Email Address: <a href="mailto:justgrants026@gmail.com">justgrants026@gmail.com</a></td>
<td></td>
<td>justgrants026.authenticatedrep (<a href="mailto:justgrants026.authenticatedrep@gmail.com">justgrants026.authenticatedrep@gmail.com</a>)</td>
</tr>
</tbody>
</table>

**Steps take place in DIAMD**
The second option the EA can use to remove an entity user from DIAMD is **Manage Entity User**.

1) Select **Manage Entity User**.
2) Either enter the desired entity user’s name or use the dropdown menu to select the entity user to be removed.

**NOTE:** After selecting the entity user’s name, the Entity User Profile auto-populates.
3) Select the **Remove User From Entity** option.
After selecting the **Remove User From Entity** option, a note will appear instructing the EA how to invite the entity user back into DIAMD after being removed.

4) Ensure the correct entity user is selected for removal and select **Next**.
5) After selecting **Next**, DIAMD asks for confirmation to remove the entity user.

6) Select **Back** to make corrections or **Confirm** to proceed.
Entity User Management in JustGrants
Assign/Re-assign Entity Users to Applications
User assignments to applications are managed by the Entity Administrator (EA) on an application-by-application basis, enabling entities to manage users and assign work across an entity in one location.

To assign and re-assign entity users to applications, the EA will log in to JustGrants:

1) View the Home page.
2) Select Applications.
3) Select the checkbox(es) next to the application(s) being assigned or reassigned.
4) Select the **Choose Role** dropdown menu to select the role to assign or reassign.

**NOTE:** Each application can be assigned to up to three (3) Application Submitters. Each Office of Justice Programs (OJP) and Office on Violence Against Women (OVW) application will be assigned one Authorized Representative (AR); the Office of Community Oriented Policing Services (COPS) applications will be assigned two (2) ARs.
5) A list of users with the selected role appears in the Assign to field. Select the Assign to dropdown menu to select the user to assign/re-assign.

NOTE: If a user does not appear in the Choose User menu, the EA needs to add that role to the user in DIAMD.
6) After choosing a role and the user assigned to that role, select Assign.
7) A confirmation page appears with the option to cancel or submit the assign/reassignment. Select **Submit** to assign the application. Select **Cancel** to end the process and return to the Application without changes.
8) The submission is confirmed by the following text appearing on the banner at the top of the page: “The following reassignment(s) have succeeded.”

9) Select the caret to the left of the checkbox to expand and review the application details.
10) The EA can review the application details. Any edits will be performed using the dropdown menus and buttons at the bottom of the page.
Remove Additional Application Submitter Roles
The Application Submitter (AS) is a required role and cannot be deleted, only re-assigned by the Entity Administrator (EA). The second and third AS are not required roles and can be reassigned or deleted by the EA.

1) From the Applications page, select a caret next to an application to open the Application Detail page.

**NOTE:** To learn more about how multiple Application Submitters access and work on applications, see JustGrants Application Submission training.
To remove the AS 2 or 3 roles from an application, select the trash can icon to the right of the AS 2 or 3 roles.
3) A confirmation page will appear. Select **Submit** to remove the additional AS role(s). Select **Cancel** to return to the Application Details without any changes.
4) Return to the **Application Details** to confirm that the selected AS 2 has been removed.

5) The **Grants Package Information** page also indicates AS 2 has been removed.
Assign/Re-assign Entity Users to Awards
User assignments to awards are managed by the Entity Administrator (EA) on an award-by-award basis, thereby enabling entities to effectively manage users and assign work across an entity in one location.

To assign/re-assign entity users to awards, the EA will:

1) View the Home page.
2) Select Awards.
3) Select **Show/Hide Roles** to display the roles dropdown menu.
Assign/Re-assign Entity Users to Awards

Step 4

4) Select as many role checkboxes, as necessary. The roles selected from this menu will then populate the Awards table to display current assignments. Select **Confirm**.

**NOTE:** Select **Cancel** to hide the dropdown menu without selection(s) being made.
5) Select the checkbox(es) next to the award(s) being assigned or re-assigned.
6) Use the **Choose Role** dropdown menu to select the role to assign or re-assign.
7) A list of users with the selected role appears in the **Assign to** field. Select the **Assign to** dropdown menu to select the user to assign/re-assign.
Assign/Re-assign Entity Users to Awards

Step 8

8) After choosing a role and the entity user assigned to that role, select Assign to complete the action.

NOTE: Users can only be assigned to roles they have been assigned in the Digital Identity and Access Management Directory (DIAMD).
9) A confirmation page appears with the option to cancel or submit. Select **Submit** to assign the user to the award. Select **Cancel** to end the process and return to the Award without changes.
10) A submission confirmation screen will be displayed: “The following reassignment(s) have succeeded” appears in the banner at the top of the page.

11) Select the carets to the left of the checkboxes to expand and review award details.
12) The EA can review the award details. Edits are made using the dropdown menus and buttons at the bottom of the page.
To access the Entity Profile, the Entity Administrator (EA) will:

1) View the Home page.
2) Select **Entity Profile**.

**NOTE:** If any Entity Profile information is incorrect, corrections must be made in SAM.gov. Allow one to five (1 – 5) days for the updated SAM.gov information to be reflected in JustGrants.
3) The EA can edit the following fields directly in JustGrants:

- Law Enforcement (defaults to **no**);
- Faith-Based (defaults to **no**);
- Legal Address Designation (options are **physical** or **mailing**).

**NOTE:** Information shown in the Entity Profile page is retrieved from the entity’s SAM.gov profile. The EA must designate whether the entity is Law Enforcement or Faith-Based and designate the entity’s legal address as the physical or mailing address.
4) Select **Submit** to complete any profile changes made in JustGrants.
5) An audit trail of entity profile changes is displayed in the History section located at the bottom of the Entity Profile page.

NOTE: Users can search the history by keyword, group, or field.
Maintain Entity Documents
Entity Administrators (EA) can upload documents to the **Entity Documents** section so that other entity and Department of Justice (DOJ) users can view and download selected documents for use on specific applications, awards, and monitoring activities. The documents located in this section apply to the entity as a whole or relate to multiple applications and awards (e.g., indirect cost agreements, financial capability questionnaires).

To view, add, or remove documents:

1) View the **Home** page.
2) Select **Entity Documents**.
Maintain Entity Documents

Step 3

3) To download and view an entity document, select the **File Name**.
4) To view the **Document Notes** for an entity document, select the **caret** to the left of the file name.
5) To add a new document to the repository, select **Add New Document**.
6) **Select the Select File option.** The types of documents that can be uploaded into the repository include:

- .doc, .docx;
- .pdf;
- .xlsm.
Step 7

7) Fill in the confirmation page text fields and select **Submit**.

**NOTE:** Select **Cancel** to stop the upload and return to the **Entity Documents** page.
8) Newly submitted entity documents appear in the document list.
9) To delete an entity document, select the \textbf{trash can} icon located to the left of the File Name columns.

\textbf{NOTE:} When the EA selects the trash can icon to delete a document, a confirmation screen appears asking to confirm the deletion. However, if the document is associated with any other application or award, a pop-up appears stating, \textit{“Unable to delete, file is associated with the following case(s)”}. A list showing the Case ID and Case Information appears below the notice. The EA will not be able to delete the document.