DATIM Primary User Administrator Guide & FAQ

Primary user Administrators Determine Access to DATIM

Due to the global scope of PEPFAR, DATIM accounts are managed in a decentralized way through user administrators. Primary User Administrators (PUAs) are identified by the DATIM Systems Team, by contacting already existing DATIM PUAs and/or an Organization Units PEPFAR Program Manager (PPM), to receive new account requests. Requests are made via email and either come from automatically generated account requests or from the DATIM Support Team if a user submits a help desk ticket for a new account.

Responsibilities:

The main responsibilities for DATIM PUAs are to:

- Actively review new DATIM account requests that are routed from register.datim.org or DATIM Support and complete the account setup process in the DATIM User Administration App.
- Edit user accounts to add and/or remove access (i.e. to data streams) using the user Administration App. Please note, user accounts are not able to be edited, converted, or transferred to a different OU, Agency, or Partner. A separate account would have to be created via the User Administration App.
- Reenable user accounts
- Disable user accounts that are no longer valid.

NOTE: If PUA does not have access to the DATIM User Administration App, they should contact another PUA or User Administrator to edit their account by checking the "User Administrator" box. If that does not resolve the issue, please contact DATIM support.

- Inform the DATIM Support Team if they or another PUA is no longer able to administrate DATIM users and help identify a replacement.

New Account Request Process:

There are two ways a new account can be requested in DATIM, either a user-initiated via register.datim.org, or where the PUA enters all the user's information manually from an ad-hoc request.

User Initiated Process
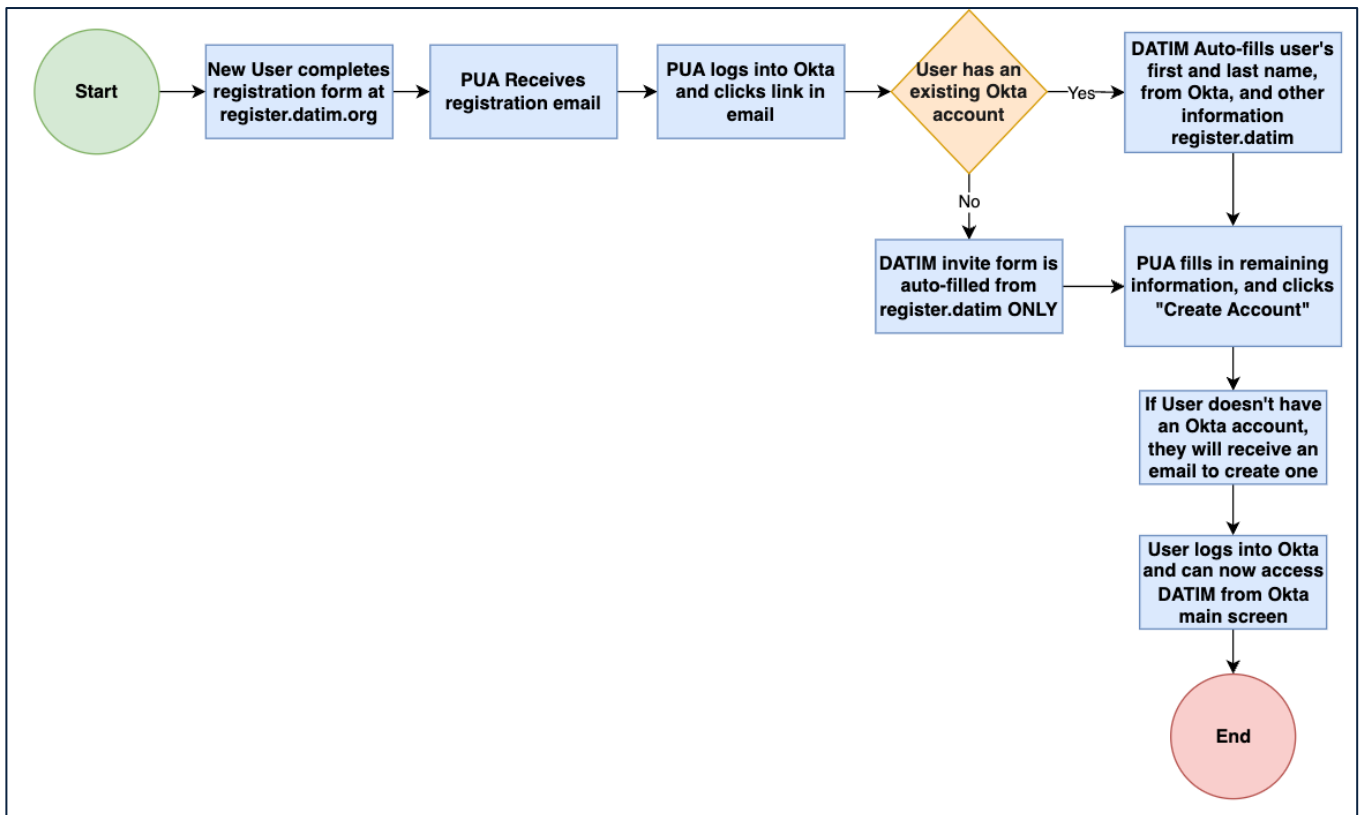
A user-initiated process follows these steps:

1) A DATIM account request is made via the "New User Request form" on register.datim.org.

2) After the user completes the webform, an email is generated and routed to the designated Primary user Administrators (PUAs) based on the selections made by the user. The link in the purple box leads directly to the DATIM user Administration application, and the information in the green box is auto-populated into the DATIM User Administration App for ease of account creation.

The following user has requested access to DATIM.

Please review their details below and set up an account using the link to the DATIM User Administration app if the user should be authorized to access DATIM.

If there are questions or clarifications needed from the user, please reply to this email to contact them directly.

You may also ask any questions through the DATIM Help Desk. To access the DATIM Help Desk, log into DATIM, click on Apps, and then select DATIM Support.

Thanks and regards,

DATIM Support

User Invite Link: https://www.datim.org/api/apps/User-Administration/index.html#/invite?&userType=Agency&email=ben%40dhis2.org&agency=State%2FGHSD%2FPEPFAR&language=English&country=XOivy2uDpMF&esop=view&viewUnapprovedData

----

First Name: ▮▮▮▮
Last Name: ▮▮▮▮
Email: ▮▮▮▮▮▮
User Type: Agency
Operating Unit: Angola
Agency: State/GHSD/PEPFAR
Data Streams: esop
Access Types: viewUnapprovedData
Language: English
Justification for Request: This is a test account—please ignore.

3) After the PUA clicks the link from the email, they are brought to the user invite screen with relevant information from the register.datim.org form auto-populated in the form.

As of June 17, 2024, all DATIM users will access DATIM via the single-sign on provider Okta. The user Administration application has been updated to check on the DATIM user's Okta status in order to streamline this process.

a. If the user has an existing Okta account, the user Administration application will check against the user's self-reported email address to verify whether the user has an Okta account associated with that same email. If so, the user Administration application will then bring over the user's first and last name from Okta with the message "The Name above has been retrieved from the user's Okta account"

> Name above has been retrieved from the user's Okta account   ✕

      b. If no Okta account exists, the user Administration App will prompt "Please enter a first name and last name to create an Okta account for this user

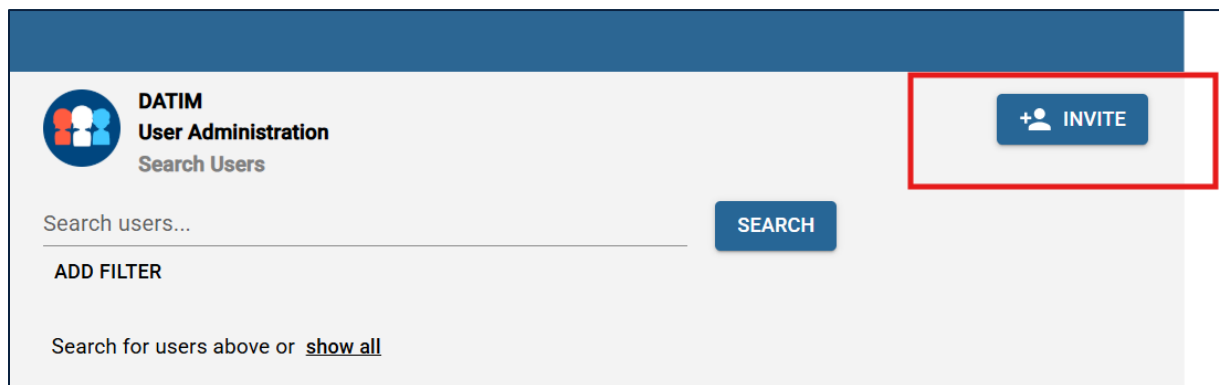> Please enter a first name and last name to create an Okta account for this user   ✕

4) The PUA verifies all information in the form, enters any missing information, then clicks Create account
5) If the user does not have an Okta account, an Okta activation email will be generated and sent to the user.
      a. The user must activate their Okta account before they will be able to access DATIM
      b. If the user already has an Okta account, then no Okta email will be generated

Ad-Hoc Process
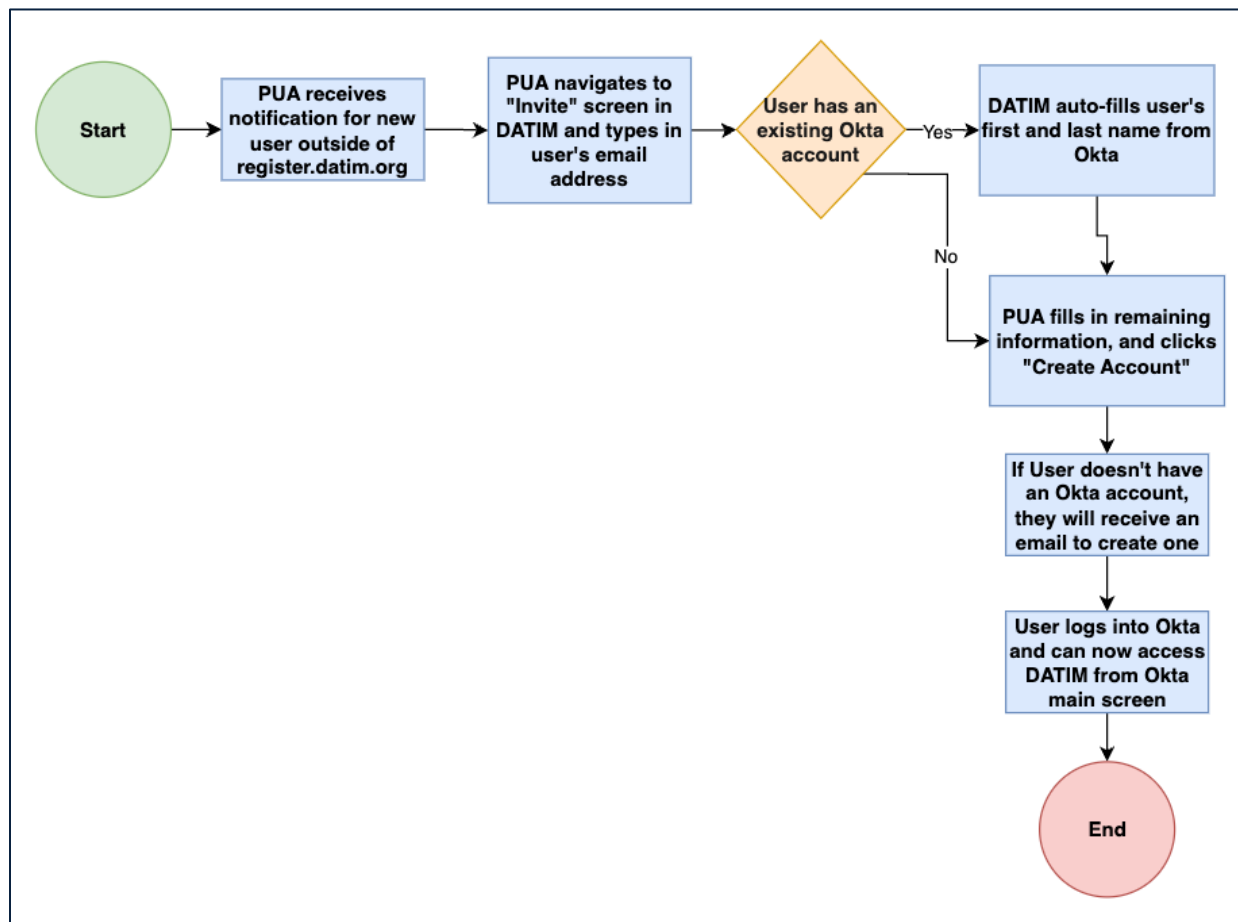
For an ad-hoc request, the PUA can use the following steps

1) A PUA receives a new account request from somewhere outside of the register.datim form.
2) In DATIM, the PUA navigates to the DATIM User Administration App and clicks on the "Invite" button.

As of June 17, 2024, all DATIM users will access DATIM via the single-sign on provider Okta. The User Administration application has been updated to check on the DATIM user's Okta status in order to streamline this process.

a. If the user has an existing Okta account, the user Administration application will check against the user's self-reported email address to verify whether the user has an Okta account associated with that same email. If so, the user Administration application will then bring over the user's first and last name from Okta with the message "The Name above has been retrieved from the user's Okta account"

b. If no Okta account exists, the user Administration App will prompt "Please enter a first name and last name to create an Okta account for this user"

Please enter a first name and last name to create an Okta account for this user ✕

3) The PUA verifies all information in the form, enters any missing information, then clicks Create account

Name above has been retrieved from the user's Okta account ✕

Note to help user identify this DATIM account

Language
English ▾

Country
Global ▾

User Type
Global ▾

☐ User Administrator

Data Streams

CXAE	●—○—○	No Access
DHI	●—○—○	No Access
ER	○—●—○	View Data
ESOP	○—●—○	View Data
HRH	●—○—○	No Access
MCAE	●—○—○	No Access
MER	○—●—○	View Data
MOH	○—●—○	View Data
SaSR	○—●—○	View Data
SIMS	○—●—○	View Data

CREATE ACCOUNT ➤

4) "Note to help user identify this DATIM account" field is optional but may be important to PUA and User Admin to give users details about their newly created account.

5) If the user does not have an Okta account, an Okta email will be generated and sent to the user. The user must activate their Okta account before they will be able to access their DATIM account

a. If the user already has an Okta account, then no Okta email will be generated

6) After the user creates their Okta account (if needed), they can then access DATIM via the Okta landing screen.

Administration for Existing Accounts: Primary User Admins should have access to DATIM's User Administration application which allows them to re-enable existing user accounts, edit user data streams, and disable users that no longer require access to DATIM.

A PUA's ability to edit other DATIM user accounts depends on their own type of DATIM account

- You are also not able to edit and/or create an account that has a role you do not (e.g., a standard InterAgency level user Admin will not be able to edit an InterAgency level account that has the Site Admin role).
- If a user Admin sees the "unable to edit" button they can scroll over the button, and it will display a message as to why that user Admin cannot edit that account.

Inter-Agency user Administrators can only create:

►Inter-Agency UAs & Inter-Agency users

Partner user Administrators only create:

► Partner UAs & Partner users (*Only from the same partner organization*)

MOH user Administrators only create:

► MOH UAs & MOH users

Global user Administrators only create:

► Global UAs & Global users

Global Agency user Administrators only create:

► Global Agency UAs & Global Agency users (*Only from the same agency*)

Agency user Administrators can only reate:

► Agency UAs & Agency users (*Only from the same agency*)

Partner user Administrators only create:

► Partner UAs & Partner users (*Only from the same partner organization*)

Global Partner user Administrators only create:

► Global Partner UAs & Global Partner users (*Only from the same partner*) *organization*)

Examples of PUA user administration actions from the above table:

- Global PUAs are only able to create/edit other Global user accounts.
- PUA Agency level accounts are only able to create and/or edit other Agency accounts or Partner (IP) accounts associated with their agency.
- InterAgency level PUAs are not able to edit Global, Global Agency, Global Partner, or Agency level accounts. So, if an InterAgency PUA is blocked from editing a different account type, they should delegate to an Agency level DATIM user Administrator.

From the DATIM user Administration App (pictured above), Primary user Admins can:

- Edit data access rights and permissions for existing users as needed.
    - The DATIM Systems Team will send notifications if/when a new data stream is added so PUAs can administer them as appropriate.
- Enable accounts for existing users
- Disable a user's account if:
    - A user is no longer supporting the PEPFAR program or is now supporting another country or agency.
    - The user has been found in violation of DATIM policies and system access should be terminated.

*For more information on the DATIM user Admin App, please reference the **User Administration Application Reference Guide** on the DATIM Support Site [here](#).

**Frequently Asked Questions (FAQ)**

Who are PUAs?

- Ideally 1-3 PUAs, per Organization Unit or HQ Agency that are identified by PEPFAR Program Managers (PPM) and/or other PUAs
- They receive the register.datim.org DATIM account request emails from people seeking access to DATIM and can invite users to create new accounts if the request was initiated outside of register.datim.org
- They are considered the DATIM User Administrator Points of Contact for their OUs, Implementing Partners, or U.S. Agency by the DATIM Systems support team.

Why are PUAs Important?

- Primary user Admins are one of the most important roles a DATIM user can have. The DATIM user community is so large that the DATIM Team is unable to actively maintain or manage users – especially since different users may or may not need access to a variety of PEPFAR data streams
- PUAs help administer new data streams to their users if/when needed

A user replied that they are unable to access their DATIM account after I created it for them. What should I do?

- Ask the user if they have received and completed the Okta account activation email, as ALL users must have an active Okta account before they can access DATIM.
- In DATIM, navigate to the User Administration App choose to search by the user's email
    - If the user already exists in DATIM, and their account is listed as "Inactive", use the toggle in the edit screen to, change their account status to "Active"
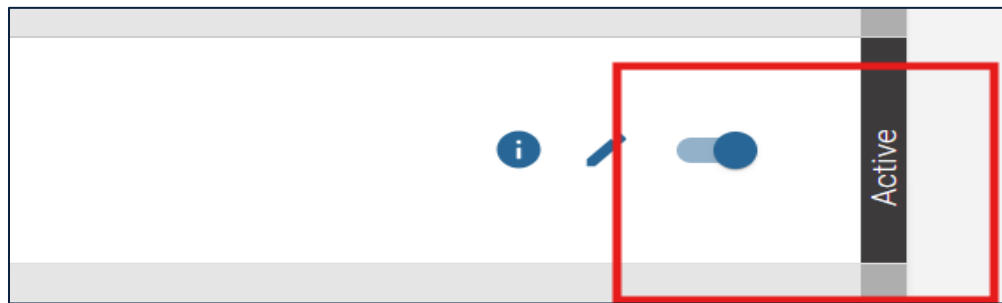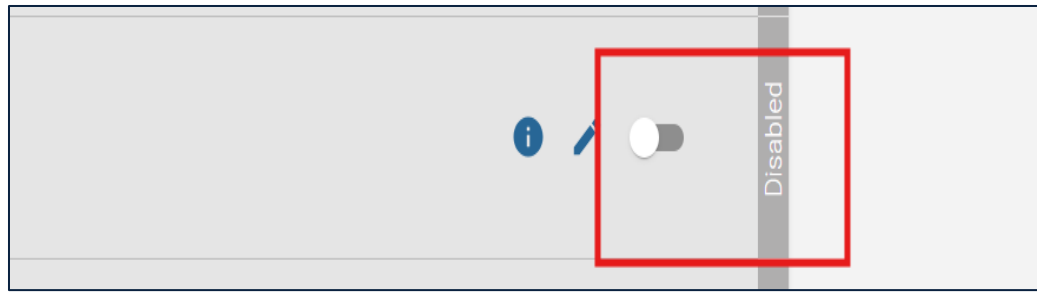
- o If the user still can't access DATIM, advise them to submit a help desk ticket