EXOSTAR®

EXOSTAR® UNIVERSITY

Managed Access Gateway (MAG)

Organization Administrator

September 2022

CONTENTS

DOCUMENT VERSIONS

Version	Impacts	Date	Owner
MAG 6.9	• View Complete Email Address • Employee Reference included in Search • Role Management • All Details report available to Organization Administrators provides all user details • Application Status Report available to Organization And Application Administrators provides status of application for all users • Application Status Report available to Organization And Application Administrators provides status of application for all users	July 2018	S. Puthanveetil
MAG 6.9	• Updated hyperlinks to training documents	September 2018	S. Puthanveetil
MAG 6.10	• Updated screenshots to include last Exostar IAM Platform (MAG) Access Date	November 2018	S. Puthanveetil
MAG 6.11	• Changed the product name from IAM to MAG • Wrote the section on reports available to Organization Administrators and Organization Stewards	April 2019	S. Puthanveetil
MAG 6.14	• Remove One-Time Password from First-Time Login Process • Update Password Policy	June 2020	B. Nair
MAG 7.0	• Self-Registration • New Organization Adoption Invitation registration process • Dashboard • Purchasing • Credentialing • Activation • Authentication	February 2021	B. Nair

Introduction

This role-based guide covers the primary actions performed specifically by users with the Organization Administrator role. For a more comprehensive guide, please reference the Exostar Managed Access Gateway Platform (MAG) User Guide from the MAG Training Resources page.

Organization Administrator

The Organization Administrator (Org Admin) is responsible for performing administrative activities on behalf of their organization. An organization can have a single or multiple Organization Administrators.

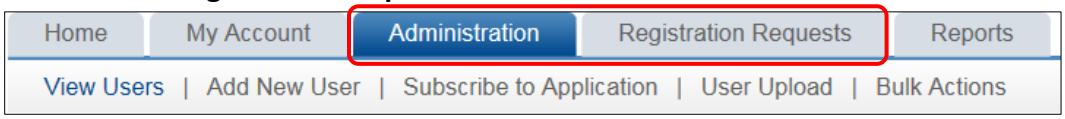
Organization Administrator responsibilities include:

- Accept Terms and Conditions for applications the organization is subscribed.
- Create, suspend, unsuspend, delete user accounts individually or using the Bulk Upload function.
- Request, suspend, unsuspend, and delete applications for users individually or in bulk.
- Approve user accounts for users who completed self-registration.
- Request access to application on a user's behalf.
- Subscribe the organization to public applications (e.g. Federated Identity Service [FIS])
- Reset user passwords.
- For organizations subscribed to Exostar's Enterprise Access Gateway (EAG) service, subscribe users to EAG using Bulk Uploads or Bulk Actions upload functionality.
- Update user roles.
- Run reports.

Exostar's Training Team provides bi-monthly Organization and Application Administrator webinars. For registration information and a list of upcoming training events, please see the MAG Webinars page.

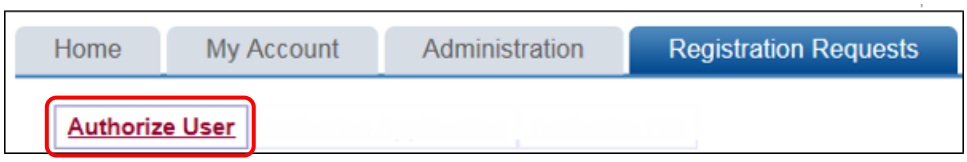
Administration and Registration Requests Tabs

Organization Administrators complete organization management functions from the **Administration** and **Registration Requests** tabs.



Registration Requests

Users with administrative privileges for an organization have access to the **Registration Requests** tab. Organization Administrators can approve users who self-register.

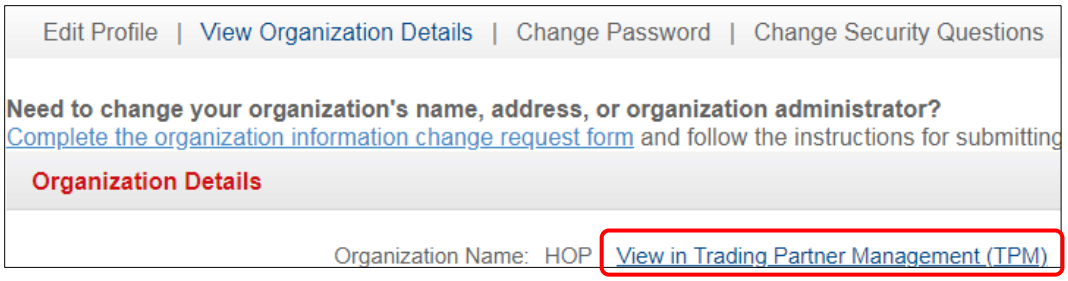


Restrict Credentials or Information from Search Results

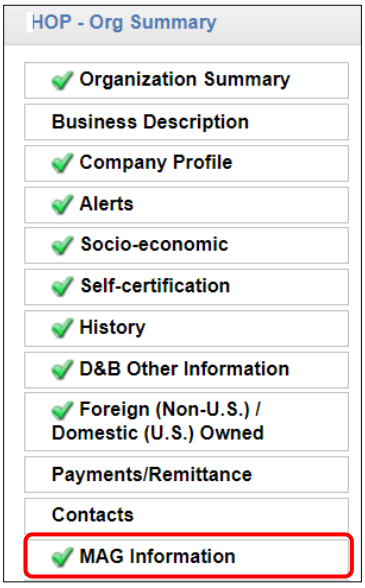
Organization Administrators can restrict users within their organization from using OTP Hardware and Phone OTP credentials. They can also restrict visibility of the organization and associated users from displaying in application invitation search results completed by customer companies (buyers).

To restrict:

1. For Organization Administrators, navigate to the **My Account** tab, then **View Organizations Details.**
2. Select **View in Trading Partner Management (TPM)** in the **Organization Name** section.

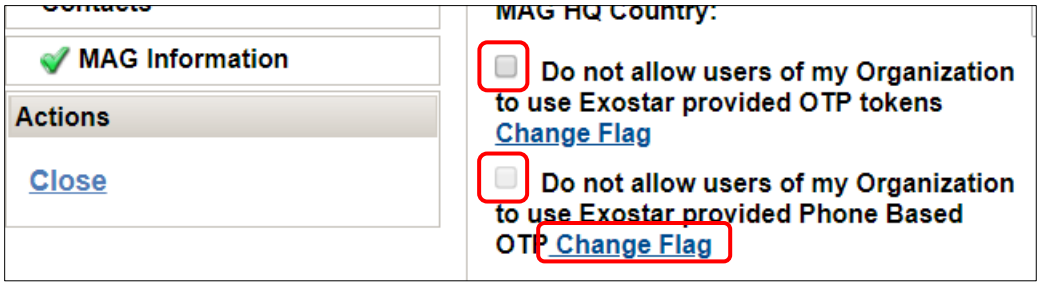


3. TPM displays. Click **MAG Information**.

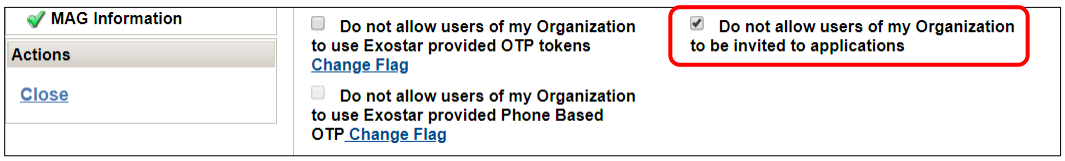


4. To restrict credentials, check the box for **Do not allow users of my Organization to use Exostar provided OTP Tokens** or **Do not allow users of my Organization to use Exostar**

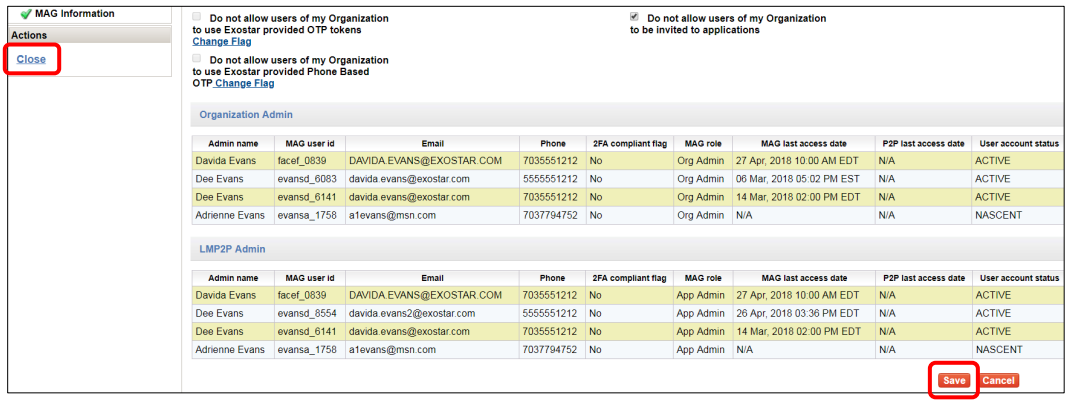
provided Phone Based OTP. If the box is greyed out, click **Change Flag**, then check the box.



5. To restrict visibility of the organization and associated users from displaying in application invitation searches completed by customer organizations (buyers), check the **Do not allow users of my Organization to be invited to applications** box.



6. To complete, click **Save** at the bottom of the page. To close the window, click **Close**.



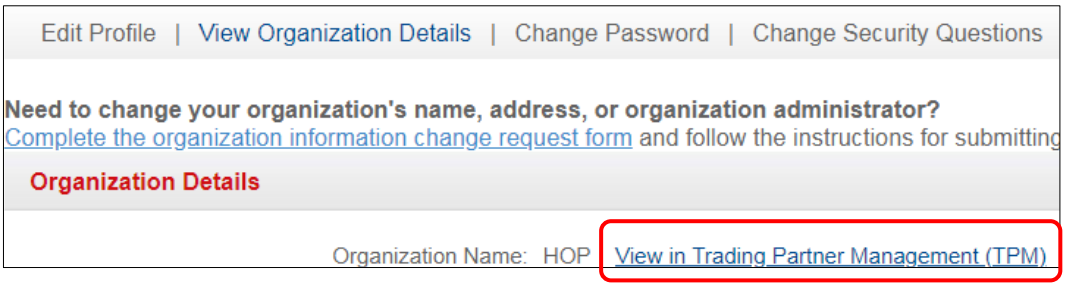
Identify Small Disadvantaged Business Status

If your organization is a small disadvantaged business (SDB), Organization Administrators can alert customer organizations (buyers) of the organization's SDB status.

To set the SDB flag:

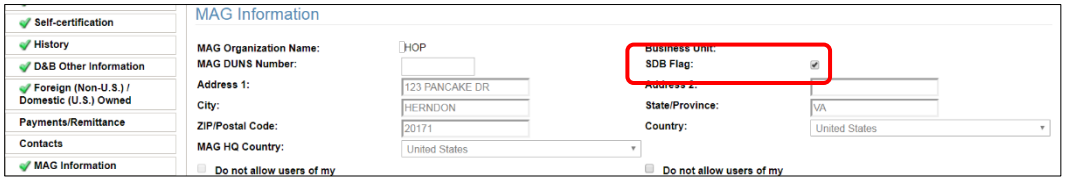
1. For Organization Administrators, navigate to the **My Account** tab, then click **View Organization Details.**

2. From **View Organization Details** or **View Organizations**, click **View in Trading Partner Management (TPM)** in the **Organization Name** section.



3. TPM displays. Click **MAG Information**.

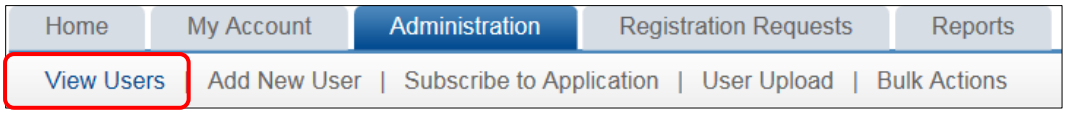
4. Check the box for **SDB Flag**. Scroll down and click **Save**.



VIEW USERS

The View Users sub-tab allows Organization Administrators to search and complete administrative functions. Administrators can complete user management activities such as request and suspend application access for users. If suspending application access, comments are required. Additionally, they can manage user activities such as assign user roles, suspend, reset passwords, and delete users.

Organization Administrators access **View Users** from the **Administration** tab of their Exostar MAG account.



Employee Reference

Organization Administrators can include employee reference information in the **Employee Reference** field for new or existing users. Employee reference can be added for new users using the User Upload function. To add employee reference for existing users:

1. Enter information in the **Employee Reference** field.
2. Scroll to the bottom of the page and click **Submit**.
3. Click **OK** to complete.

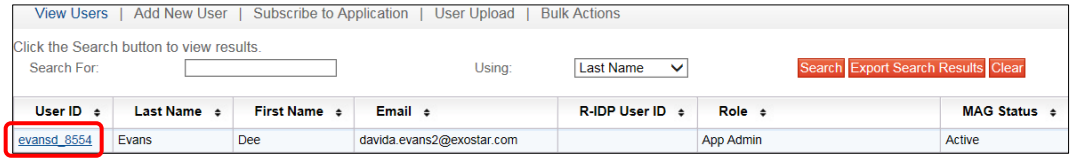
Change Role

Organization Administrators can update user roles. It is important to note if you are the only Organization Administrator for your organization's account and you change your role, there will be no Organization Administrators for the account.

Change Role (Org Admin)

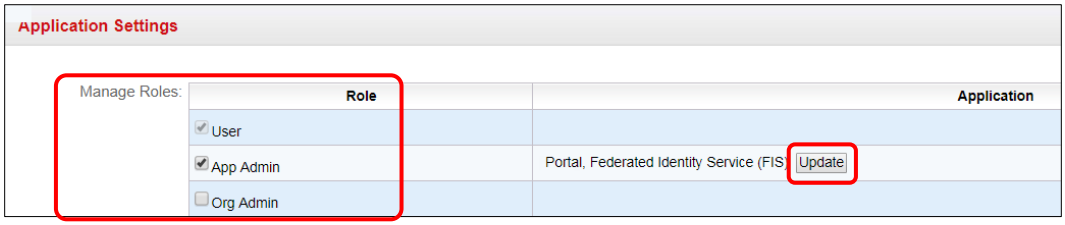
To change role(s) as an Organization Administrator:

1. Select **View Users** from the Administration tab.
2. Enter search criteria. Click **Search**.
3. Select the **User ID** to access user details.

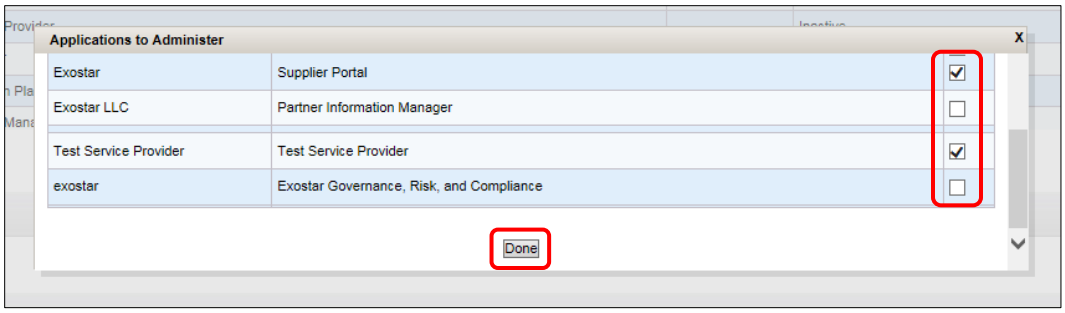


4. Scroll to the **Application Settings** section. Select role from the **Role** column.

NOTE: If assigning the Application Administrator role or updating applications for a user to administer, you must select the application you want the user to administer by selecting **Update**.



5. Check the **Select** column for the applications you want the user to administer. Click **Done**.

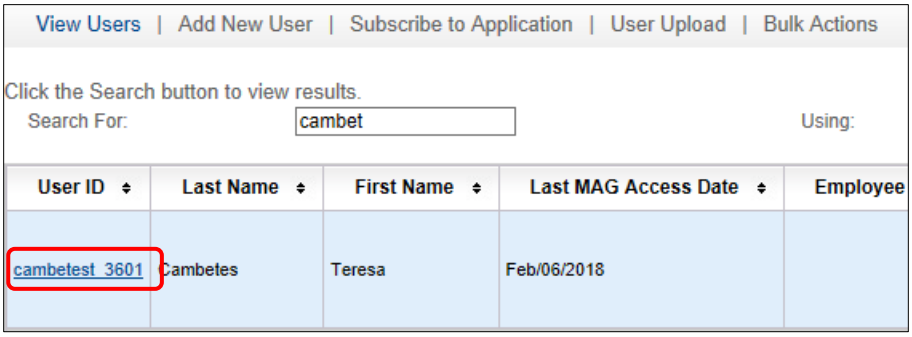


6. To complete role and/or application administration, scroll to the bottom of the page and click **Submit**.

Request or Suspend Application Access

Organization Administrators can request or suspend application access for users. Once suspended, users are unable to access the application. To modify application access:

1. Click **View Users**.
2. Use the search filter menu or select **Exact Match** to narrow results. Click **Search**. Click the hyperlinked **User ID.**



3. Scroll to **Application Settings**. Locate the application and click the appropriate action (i.e. Suspend). You are required to enter a suspension reason. Click **Activate** to unsuspend. **Delete** removes the ability for you to modify the application. Additionally, application access is deactivated for the user. However, the user can request access to the application again from their Home tab.

NOTE: Comments are viewable by the Application Administrator, Organization Steward, or SP Administrator. If requesting access, sponsor code is not required.

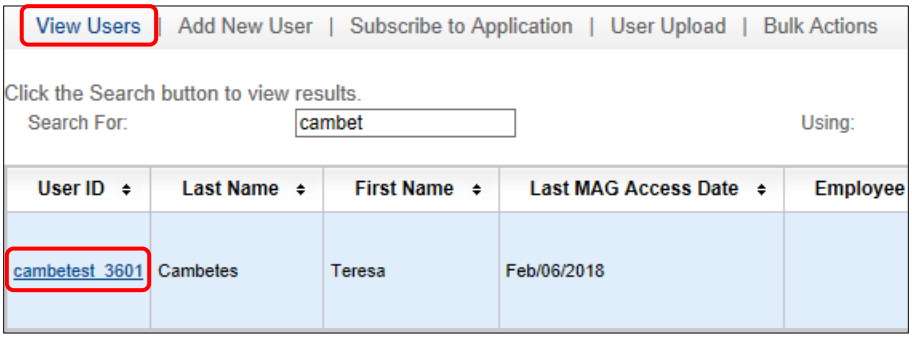
Restrict Profile Access Attribute

Organization Administrators can restrict access to ForumPass sites. ForumPass restricted profiles require users to have a user ID, password, Medium Level of Assurance (MLOA) certificate,

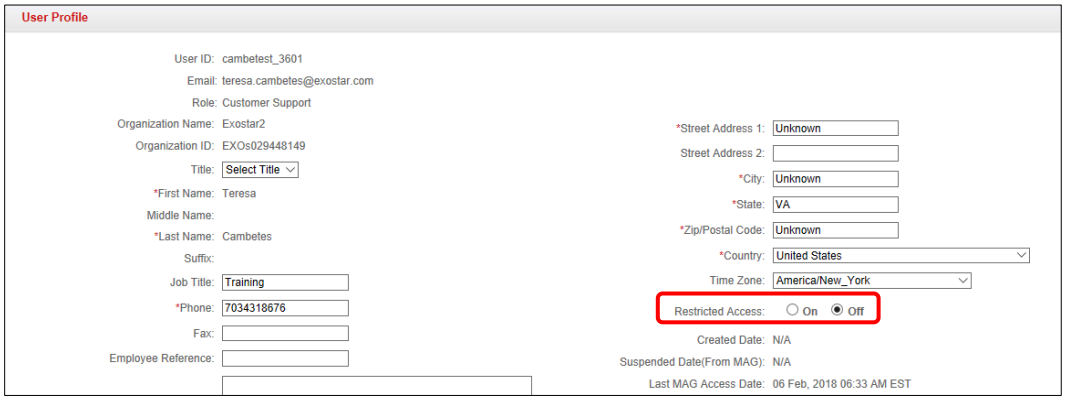
restricted attribute enabled in the MAG platform, and the TLS 1.0 setting. The **ON/OFF** setting is one of the factors that determines whether users can access restricted profile sites in ForumPass.

To restrict or remove the restriction attribute:

1. Organization Administrators go to the **Administration** tab, then click **View Users**.
2. Enter search criteria. Click **Search**. Select the required **User ID**.



3. From the **User Profile** section, select the required radio button for **Restricted Access**.



4. Scroll to the bottom of the page and click **Submit**. The setting is saved. To learn more about the additional settings for restricted access, please reference the ForumPass User Guide.

Password Reset

Organization Administrators can reset a user's MAG account password.

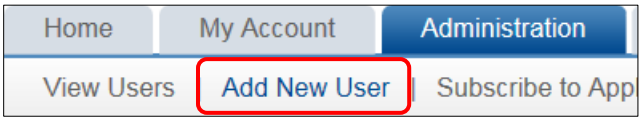
To reset a user's permanent password:

1. Organization Administrators, access **View Users** from the **Administration** tab.
2. Enter search criteria. Click **Search**.
3. Select the required **User ID**.
4. Scroll to the **Application Settings** section of the page. Click **Reset Permanent Password**.

The user's password is reset. The user receives an email with a system generated password.

ADD NEW USERS

The **Add New User** sub-tab allows Organization Administrators to create new user accounts for their organization.



To add a new user:

1. From the **Administration** tab, click **Add New User** and enter user details.
2. Select the user's role and select the applications to which you want to subscribe the user.
3. Click **Continue**.
4. Click **Submit**.
5. The user will receive an email notification to activate their account.

Organization Administrators can send users a self-registration invitation.

To send the self-registration invitation:

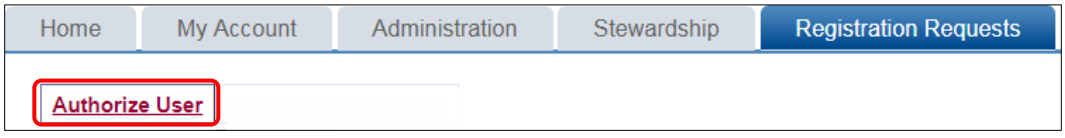
1. Send the user the self-registration URL: https://portal.exostar.com and your company's Exostar Organization ID.
2. Once the user completes the invitation, you are required to approve the request from your MAG account. For assistance with authorization, see the section below, Approve/Deny User Requests.

Approve or Deny User Requests

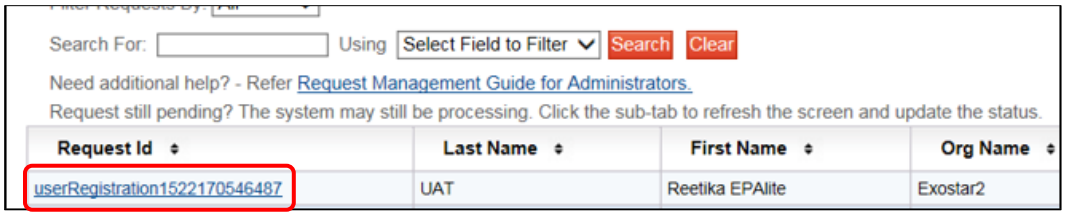
Organization Administrators can approve or deny new user requests. When a user completes a self-registration invitation, the request requires approval before the user's account is created.

To approve:

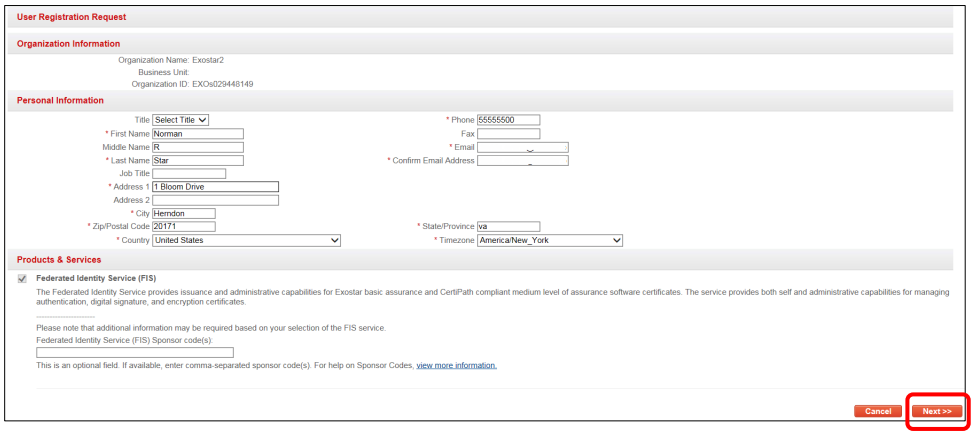
1. Organization Administrators can access **Registration Requests** tab, and click **Authorize User.**



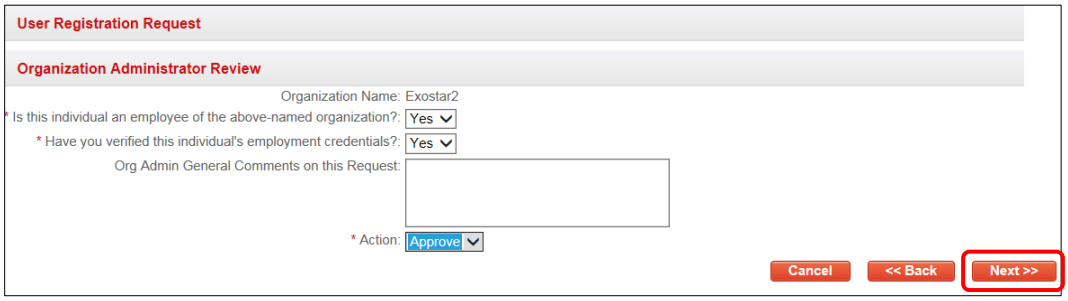
2. Click the hyperlinked **User ID** in the **Request ID** field.



3. View the request and modify personal information if necessary. Click **Next**.



4. Answer questions by selecting responses from the drop-down menus. If approving, select **YES** for both questions. If denying, enter denial comments (required). Click **Next** to complete.



Once approved, a user ID is created, and the user receives instructions on how to complete account activation. If denied, the user receives a denial notification.

User Upload

User Upload allows Organization Administrators to add multiple users to an organization in a single instance using a .CSV file upload. The file upload can also be used to subscribe existing users to new applications.

Bulk Actions

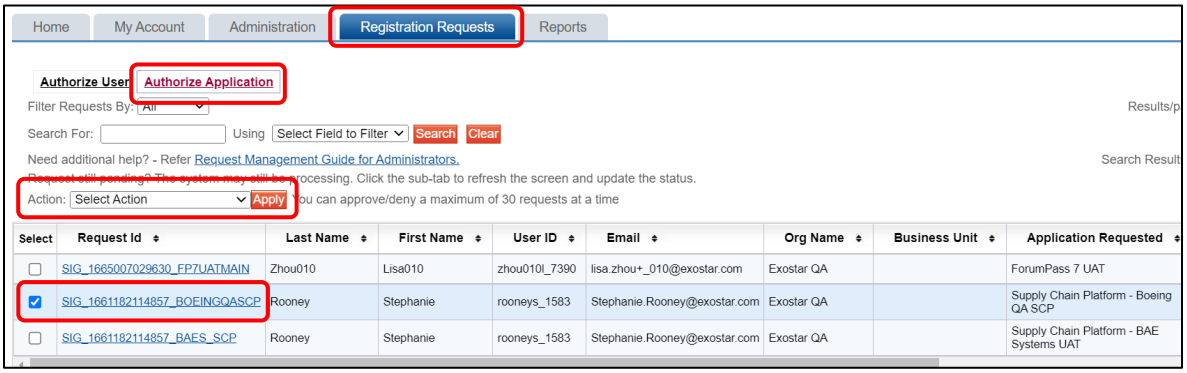
Bulk Actions allows Organization Administrators to delete, suspend, and/or unsuspend multiple

user accounts and/or applications in a single instance using a .CSV file upload.

Approve or Deny Application Access

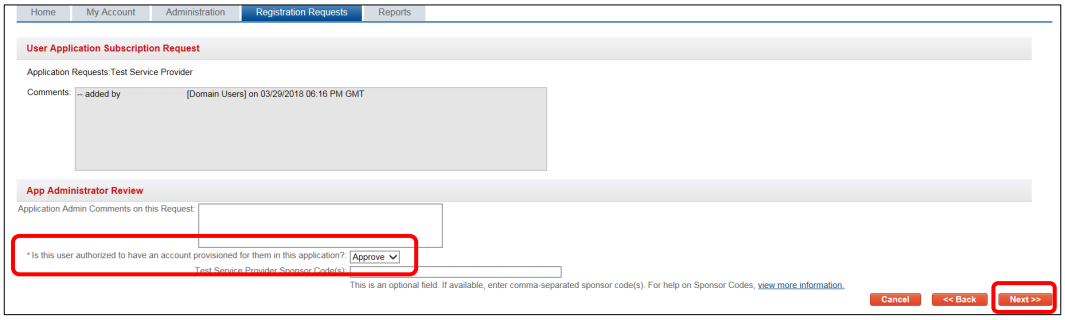
To authorize or deny requests individually:

1. Click **Registration Requests** tab.
2. Then select **Authorize Application** sub-tab.
3. Find the user and check the **Select** box next to the hyperlinked **Request ID.**



NOTE: If the user requests reactivation of a suspended application, comments display in the **User Application Subscription Request** section if the user entered them. Review the information and click **Next**.

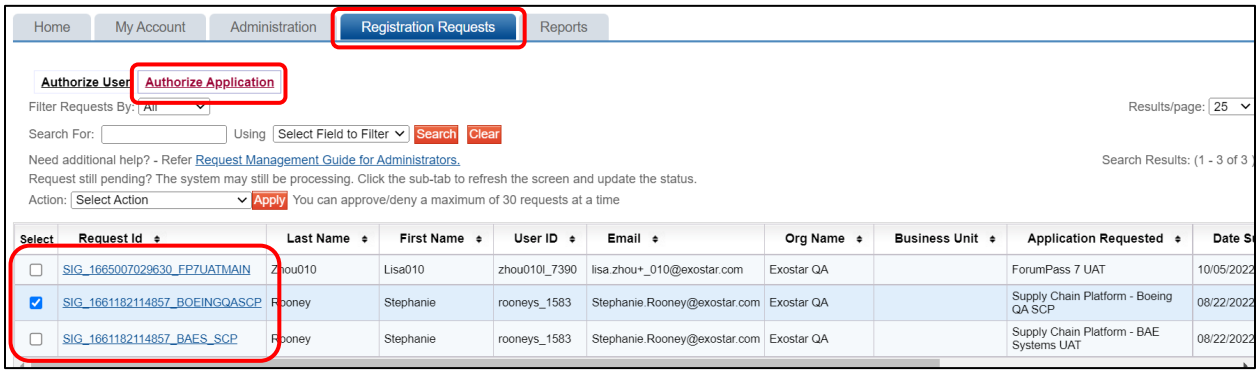
4. From the *Action* drop-down menu choose to **Approve** or **Deny** application access then hit **Apply**. If denying, you must enter a denial comment. Sponsor code is optional. Click **Next**.



Once approved, the action is complete. The request is either approved (providing user access to the application), denied, or routes to the Application Owner for final approval. An application's administrative approval workflow depends on what is set for the application. Additionally, users receive an email notification of the approval or denial.

To administer requests in multiples**:**

1. Under the **Registration Requests** tab, select the **Authorize Application** sub-tab.
2. Check and select the users you are approving or denying. From the **Action** menu, select **Approve** or **Deny Selected Requests,** click **Apply**. If denying, denial comments are required.

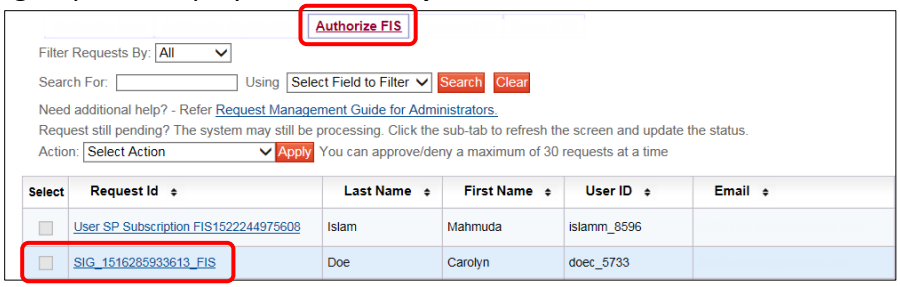


3. Click **YES** to complete the action. Regardless of how the request for application was administered, the request is either approved (providing user access to the application), denied, or routes to the Application Owner for approval. An application's administrative approval workflow depends on what is set for the application. Users receive an email notification of the approval or denial.

AUTHORIZE FIS

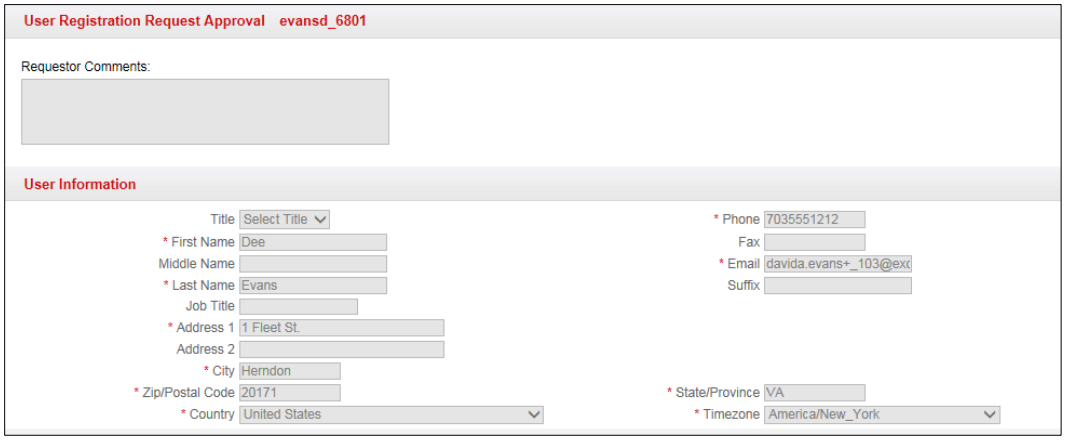
To Authorize FIS Organization Administrators, need to work with their organization's FIS Administrator to authorize requests. FIS Administrators access the **Authorize FIS** sub-tab to approve or deny requests for FIS.

1. Click **Authorize FIS**.
2. Pending requests display. Click the **Request ID**.



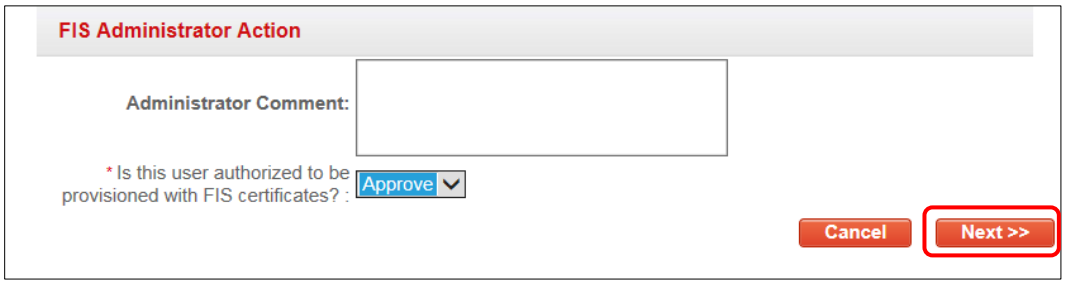
3. Review the information in the **User Information** section. Please ensure the user is using a valid email address (public email addresses such as Hotmail, Gmail, etc. are not allowed). You must verify the user's user ID, first and last name matches their legal name.

NOTE: For example, Dee Evans is a match for evansd_6801. If the request displays a first and last name of Dee Evans, but the user ID is smithj_1234, the request must be denied.



NOTE: If the user requested Medium Level of Assurance (MLOA) Digital Certificates, it is important their first and last name match their identity documents. Please ensure the address information is accurate. This is the address where a trusted agent will be dispatched to complete in-person proofing. Please ensure the user does not have a PO Box listed.

4. You can modify the following fields if the user entered incorrect information:
   - **Partner/Application** that requires the digital certificates.
   - **Certificate Assurance Level**: Basic (BLOA), Medium (MLOA), or Unknown.
   - **Certificate Usage**: Only displays if user selects Basic
   - **Certificate Type**: Software, Hardware, or Unknown.
   - **Certificate Validity Period**: 1 or 3 years. Basic only offers 1 year.
   - **Request Reason**: Reason why user requires certificates.
5. From **FIS Administrator Action**, select **Approve** or **Deny.** If denying, you are required to enter comments. Click **Next**.



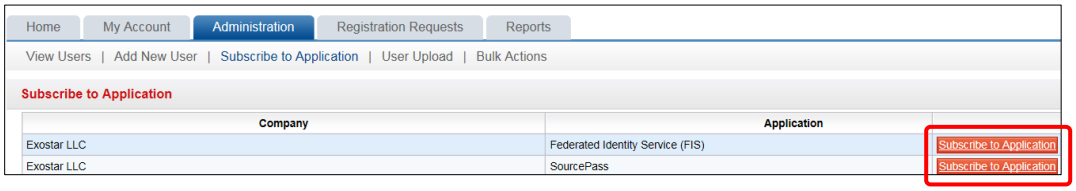
6. If approving a BLOA certificate request, the user receives an email with installation instructions. If approving MLOA certificates, the request is routed to Exostar for purchase review and proofing dispatch. If you are denied the request, the user receives a notification along with denial comments.

SUBSCRIBE TO APPLICATION

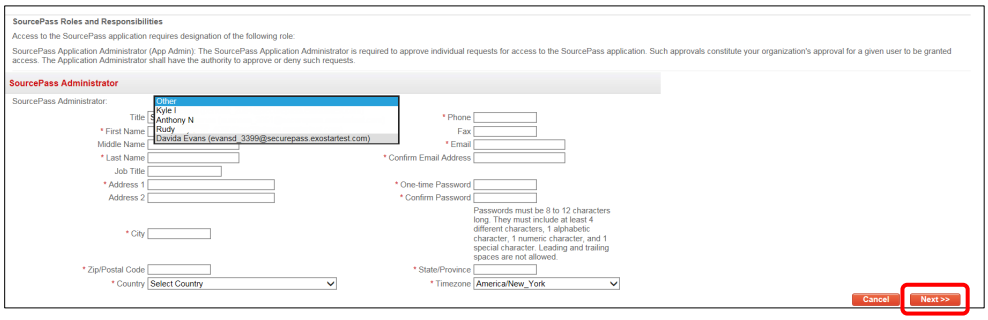
The Subscribe to Application sub-tab allows Organization Administrators to subscribe their organization to public applications. If the organization is subscribed to all available public applications, application subscription information is unavailable.

To subscribe your organization or group of organizations to public applications:

1. Click the **Subscribe to Application** button next to the desired application.



2. Assign an existing Application Administrator from the drop-down menu or create a new Application Administrator. Click **Next**.



NOTE: If creating a new Application Administrator, a new user account is created.

The request routes to Exostar for approval. It can take up to 48 business hours to process. If approved, Organization Administrator or Application Administrator for the application must accept Terms and Conditions before users can request access to the application.

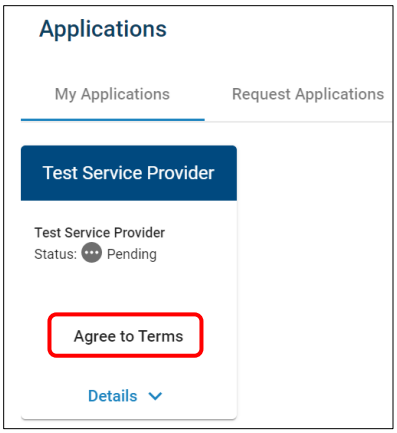
ACCEPT TERMS AND CONDITIONS

Organization Administrators can accept Terms and Conditions (T&C) for applications to which their organization is subscribed. Once Terms and Conditions are accepted, users from the organization can request access to these applications.

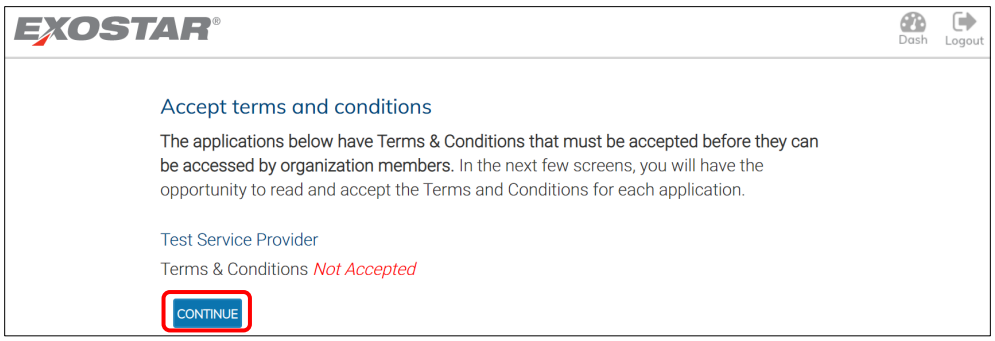
Accept Terms and Conditions (Org Admin)

To accept Terms and Conditions as an Organization Administrator:

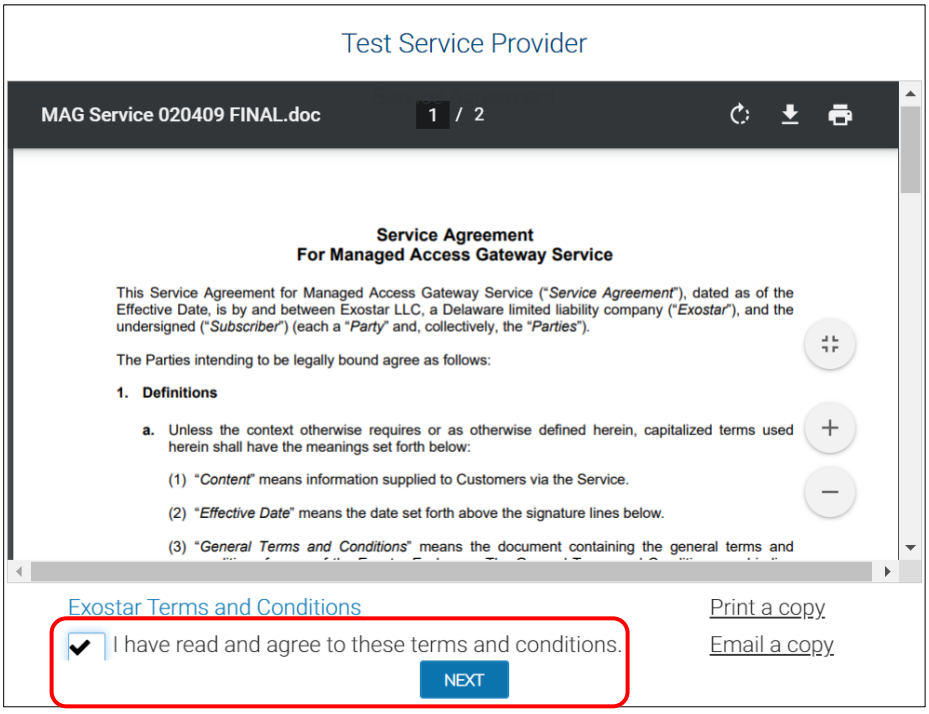
1. Organization Administrators **accept Terms and Conditions** during the organization registration process or from the Home dashboard.



2. Review the information. Click **Continue**.



3. Review the **Terms and Conditions**, and check the box for **I have read and agree to these terms and conditions.** Click **Next**.



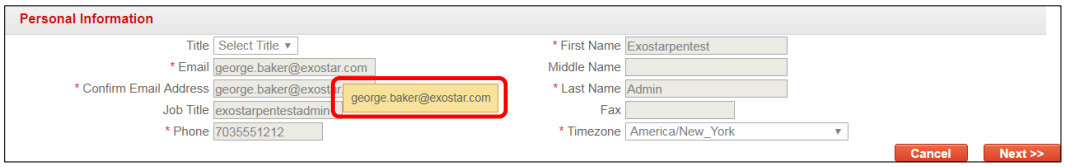
Your organization is now successfully subscribed to the application. Organization and Application Administrators for the application can start subscribing users within their organization to the application. Users can start requesting access to the application.

What happens if you do not accept the Service Agreement?

- If you do not accept Terms and Conditions by skipping the agreement, Terms and Conditions will remain in **Pending Acceptance of Terms & Conditions** status.
- Until acceptance occurs, Organization and Application Administrators for the application cannot start subscribing users within their organization the application.
- Users cannot start requesting access to the application.

View Complete Email Address

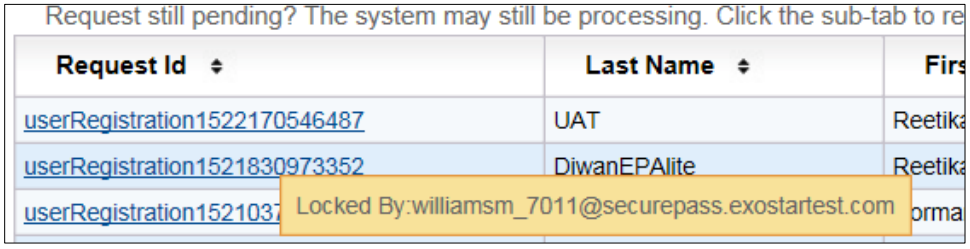
If you have the Organization Administrator role and need to view a user's complete email address when approving or denying a request, please hover over the email address to display the full address.



Unable to Approve or Authorize

If the status of a request is **Pending**, you are unable to action the request because another administrator has locked the request. Place your cursor over the request ID to determine who locked the request.

To unlock the request, contact the individual whose name displays.



If you are unfamiliar with the user ID of the locked request, follow these steps to determine whom to contact:

1. Organization Administration need to go to the **Administration** tab and click **View Users**.
2. Enter user ID in the **Search For** field. Select **User ID** from the search criteria drop-down menu. Click **Search**.

3. Results display. Click the hyperlinked **User ID** to access user details.

User ID	Last Name	First Name	Last MAG Access Date
williamsm_7011	Williams	Matthew	Oct/31/2018

4. You must contact the user to unlock the request.

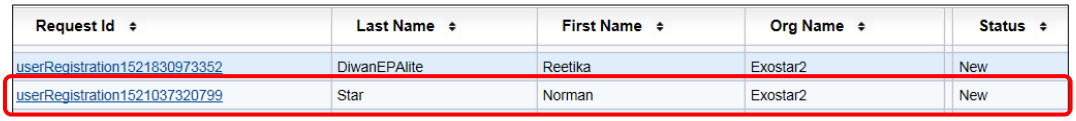
Unlock Pending Requests

Requests transition to a pending status when a request was opened, but not cancelled or processed. To unlock a pending request:

1. Locate the pending request, and click the hyperlinked User ID. The status of the request will show as **Pending**.

Request Id	Last Name	First Name	Org Name	Status
userRegistration1521830973352	DiwanEPAlite	Reetika	Exostar2	New
userRegistration1521037320799	Star	Norman	Exostar2	Pending

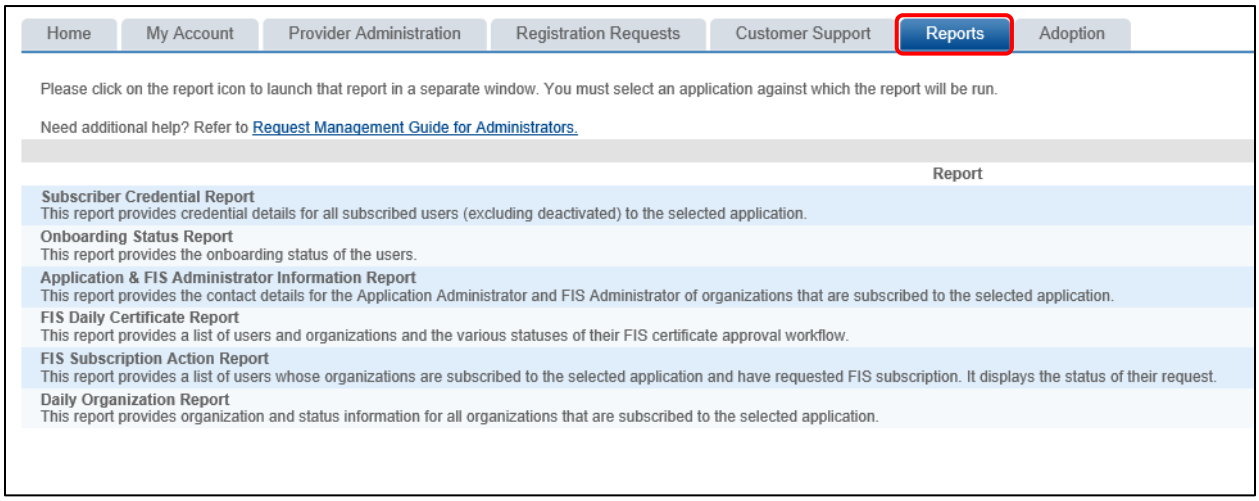
2. From the opened request, click **Cancel**. You are redirected to the request queue.
3. Click the appropriate action sub-tab to refresh. The status of the request switches to **New**.



Request Id	Last Name	First Name	Org Name	Status
userRegistration1521830973352	DiwanEPAlite	Reetika	Exostar2	New
userRegistration1521037320799	Star	Norman	Exostar2	New

Reports Tab

The reporting feature is available to Organization Administrators. Click the Reports tab to access the list of reports available to you. Follow the prompts to generate your reports.



We encourage you to spend some time exploring reporting options to see what type of user data might make your administrative duties easier. Organization Administrators have access to the following reports: All Details Report, Organization User Details Report, and Application Status Report.

All Details Report is one of the most comprehensive reports available in MAG. It conveniently packages all data across an organization into a single document: comprehensive user data, MAG statuses, access to applications, and dates of account creation and last access.

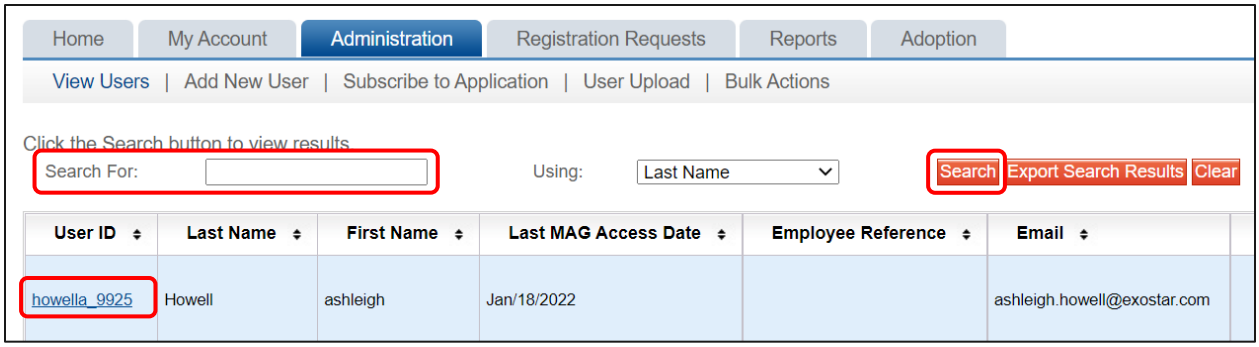
Organization User Details Report is the abbreviated version of All Details Report. Along with the User ID and name, you will get a quick overview of MAG statuses, dates of last MAG login, and access to partner applications.

Application Status Report provides Application Administrators with the overview of the team's MAG and partner application statuses. Do you need to check who on the team has active MAG accounts, and when they last accessed a specific partner application? This report is an excellent option for getting these details in a single document.

Search

Search options will be different for Organization Administrators.

1. Select the type of search (for instance, **View Users** or **View Organizations**).
2. Select the search criteria from the drop-down menu, and then type your query in the **Search For** field. Click **Search.**



3. From the list of results, click the hyperlinked **User ID** or **Organization ID** and complete necessary actions (i.e. suspend, reactivate, etc.).

View User Search Criteria

Last Name	Unique identifier for the user
First Name	Last name of user
User ID	Unique identifier for the user
Email	First name of user
R-IDP User ID	Email address of user
Employee Reference	Unique employee ID/reference for the user

View User Results Fields

User ID	Unique identifier for the user
Last Name	Last name of user
First Name	First name of user
Employee Reference	Unique employee id/reference for the user
Last MAG Access Date	Last date user logged into Exostar's MAG account
Email	Email address of user
R-IDP User ID	Remote Identity Provider User ID (information displays in the column if user has linked their account)
Role	Role(s) assigned to user.
MAG Status	Status of user's access. Active status means user has completed first time login. Inactive status means user has not completed first time login.
Active Applications	Applications active for the user
Pending Applications	Applications pending approval by an Administrator
External User ID	User ID that partner company uses
External Organization ID	Organization ID that partner company uses
Org ID	Organization ID for Exostar MAG account
Org Name	Name of organization

View Organization Search Criteria

Org Name	Organization Name
Org ID	Organization ID for Exostar MAG account
External Organization ID	Organization ID that partner company uses

Organization Results Fields

Org Name	Organization Name
Org ID	Organization ID for Exostar MAG account
Business Unit	Unit of an organization representing a specific business function
External Organization ID	Organization ID that partner company uses
R-IDP	Remote Identity Provider (information displays in column if organization is using EAG.)
MAG Status	Status of organization's account. Active status means the organization is active in Exostar's MAG Platform.
Address	Organization's Address
City	Organization's City
State	Organization's State
Country	Organization's Country
Active Applications	Applications active for the organization.
Suspended Application	Applications suspended for the organization