Managed Access Gateway (MAG)

Service Provider Administrator Guide

April 2025

CONTENTS

Document Version

Version	Impacts	Date
MAG 6.10	• Credential information displays for users during SP Administrator approval process • Last MAG Access Date column added to View Users sub-tab	November 2018
MAG 6.11	• Changed the product name from IAM to MAG	April 2019
MAG 6.12	• Resend provisioning records	August 2019
MAG 6.14	• Remove OTP from FTL process • Update Password Policy	June 2020
MAG 7.0	• Self-Registration • New Organization Adoption Invitation registration process • Dashboard • Purchasing • Credentialing • Activation • Authentication	February 2021
MAG 7.8	• New Admin Dashboard • Authorize users for application	October 2024
MAG 7.9	• Request batches 25, 50, 100 • No Search results message • Lockout 100 failed attempts	April 2025

INTRODUCTION

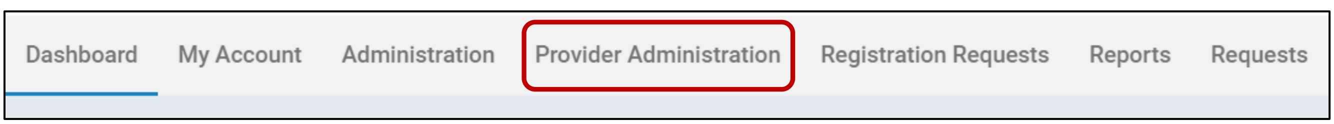
This role-based guide covers the primary actions performed specifically by users with the Service Provider (SP) Administrator role. For a more comprehensive guide, please reference the Exostar Managed Access Gateway (MAG) User Guide on the MAG Training Resources page.

ABOUT THE SERVICE PROVIDER ADMINISTRATOR

There are two types of SP Administrators: administrative and view only. The SP Administrator role with administrative permissions allows users to approve or deny access for specified partner company applications. The SP Administrator role has view only permissions. Additionally, SP Administrators can run reports. The SP Administrator role is only available to partner companies.

PROVIDER ADMINISTRATION TAB

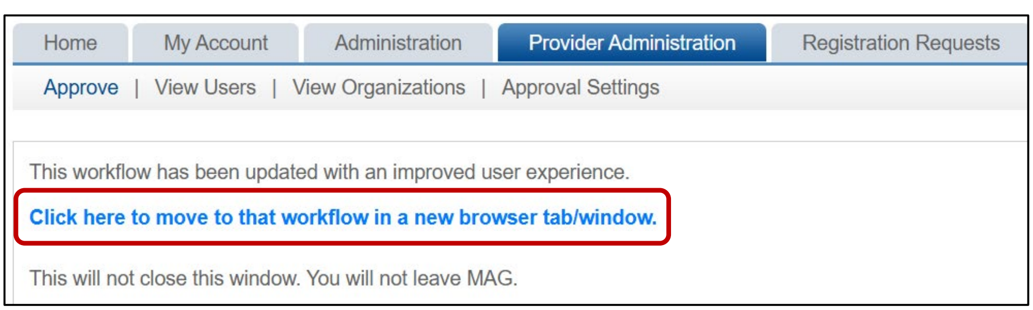
Partner companies with the Service Provider (SP) Administrator role can complete application approvals for applications that require SP Administrator approval, view users, and organization information. From the **Provider Administration** tab, SP Administrators can also set criteria for application requests from specified organizations to skip the SP Administrator approval step.



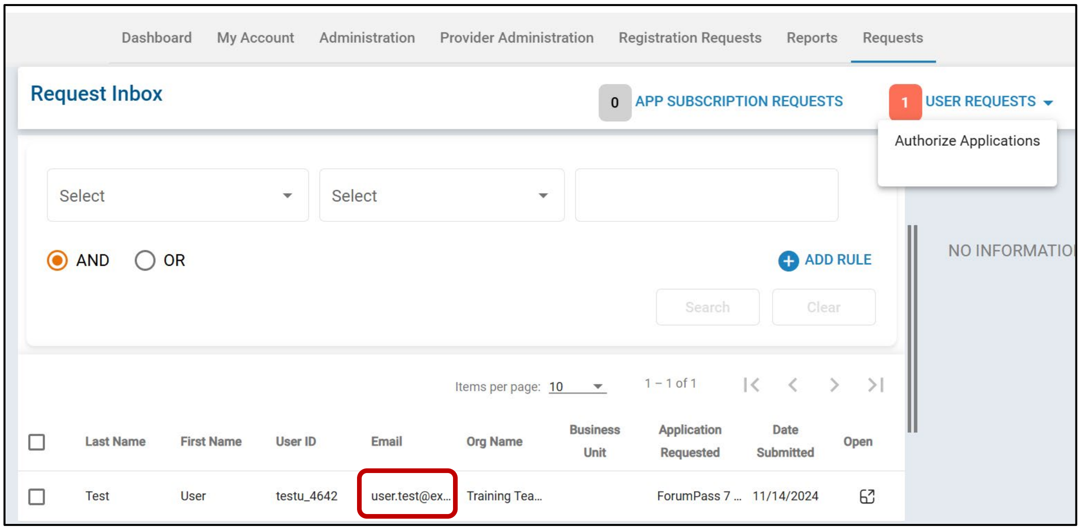
Approve

Approve allows SP Administrators to approve or deny requests for application access. To authorize or deny requests individually:

1. Select the **Provider Administration** tab**.**
2. Then select the option to click the link to view workflow in a new browser/window.
3. You will be redirected to the **Requests** tab. Any pending requests will display.

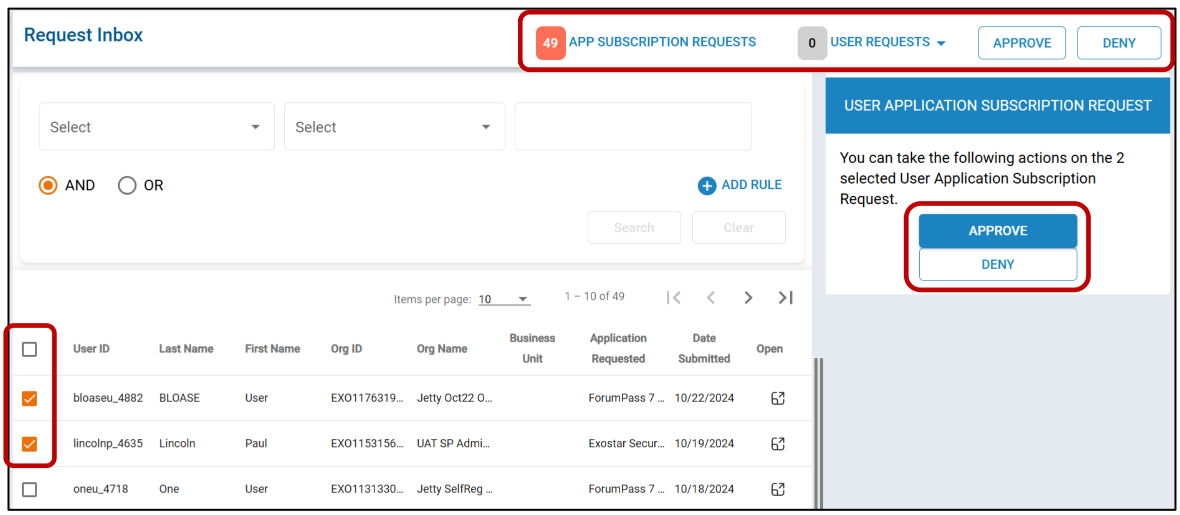


4. On the **Requests** page you can view any pending *Application and User Requests*.



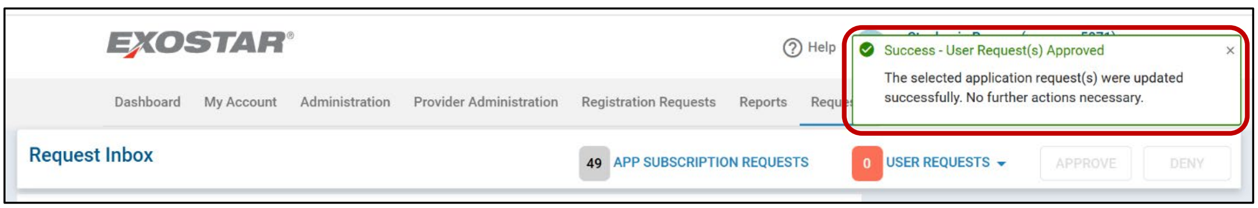
NOTE: To display full email address, hover your mouse over the email address field.

5. To approve pending requests, click the drop-down menu for either *App Subscription* or *User* requests.]



6. Then place a checkmark next to the user or select all to **Approve** or **Deny** the request.
   If you **Deny** a request, you must provide a reason to reject the request. Then click **Continue.**

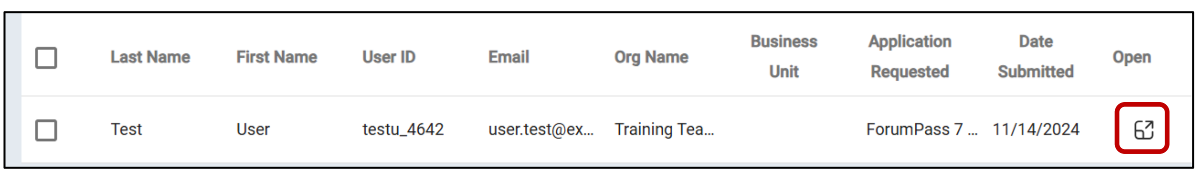
Once **Approved**, the action is complete. The request is either approved (providing user access to the application), denied, or routes to the Application Owner for final approval. An application's administrative approval workflow depends on what is set for the application. Additionally, users receive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



View Request Details

To view the details of the application or user request:

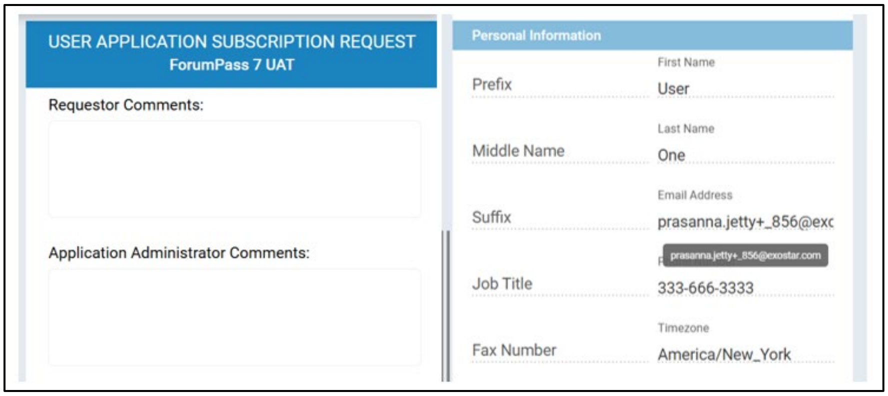
1. Next to the request, click the **Open** icon to view the details.

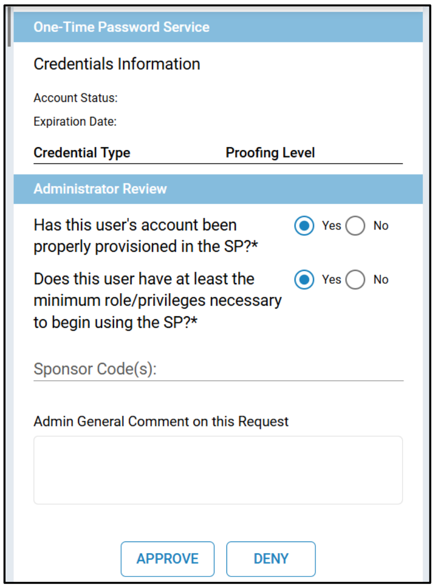


☐	Last Name	First Name	User ID	Email	Org Name	Business Unit	Application Requested	Date Submitted	Open
☐	Test	User	testu_4642	user.test@ex...	Training Tea...		ForumPass 7 ...	11/14/2024	

2. The user request details will display with any comments, personal information and administrator review. You can also Approve or Deny the request.

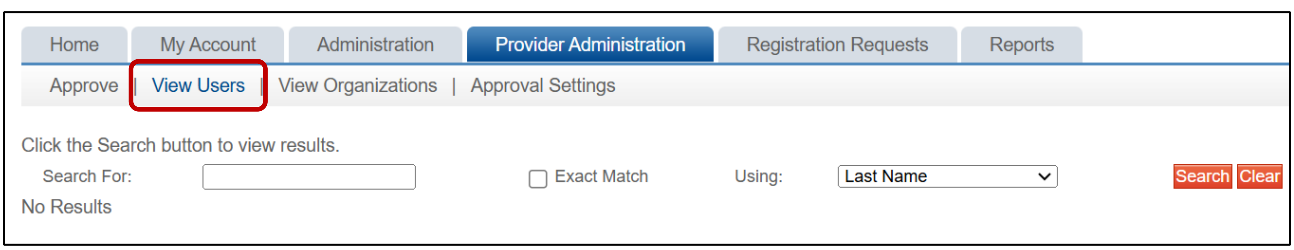
   NOTE: To view the user's full email address, hover your mouse cursor over the email field.





View Users

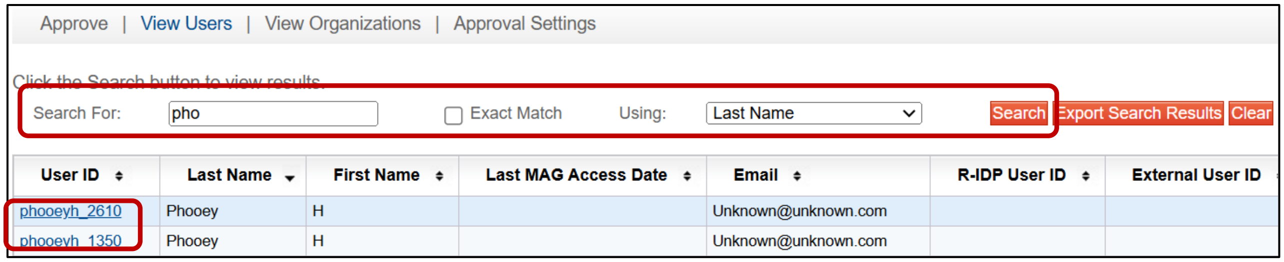
The **View Users** sub-tab allows SP Administrators to search for users subscribed to their application. From **View Users**, you can modify application access such as request and suspend application access for users. If suspending access, comments are required.



Determine User Role

SP Administrators can determine a user's role by following the steps below.

1. Click **View Users**.
2. Enter search criteria. Click **Search**.
3. Click the **User ID** hyperlink to view the user's details.



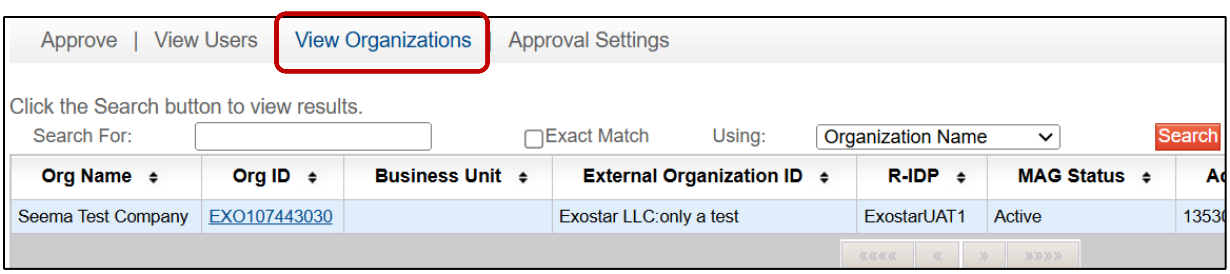
4. Scroll to the **Application Settings** section to view the **Manage Roles** section. You can modify the user's access or make them an Administrator. Then select which Applications they will have access to.

Determine User Credentials

If a user registered multi-factor credential (such as a One Time Password product or FIS Digital Certificates), credential information displays in **Certificates** or **One-Time Password Service** sections.

View Organization

View Organization allows SP Administrators to search for organizations subscribed to their application.



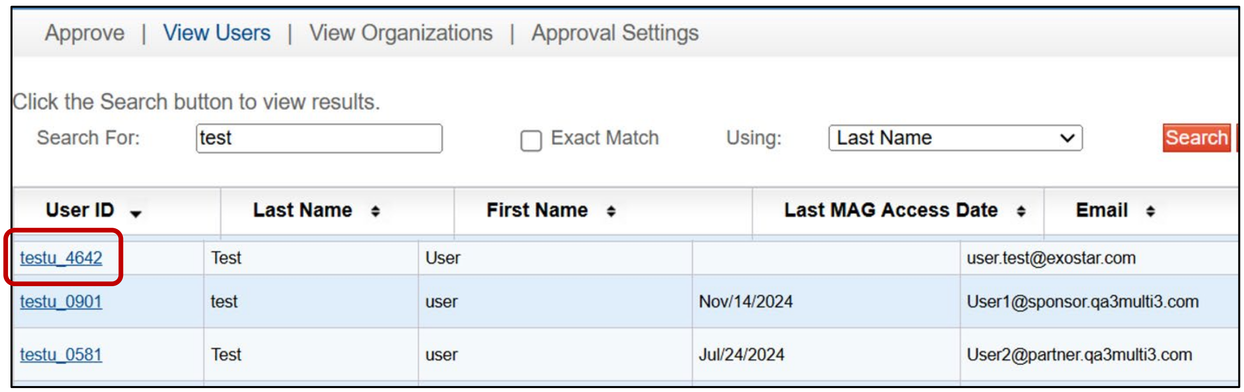
Modify Application Access

The SP Administrator can modify applications for users or organizations for applications they administer. If suspending, users will be unable to access the application.

Users

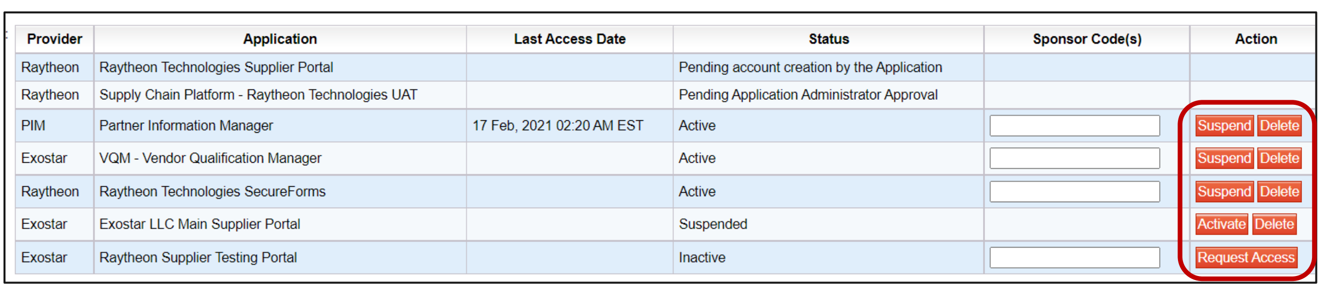
You can modify access to your application for users. Once suspended, users are unable to access the application. To modify a user's application access:

1. Click **View Users**.
2. Enter search criteria. Click **Search**.



3. From results, click the hyperlinked **User ID**.
4. To modify application access, scroll to **Application Settings**. Locate the application and click the appropriate action**.** If you suspend access, 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.

   NOTE: The user can request access to the application again from their dashboard.

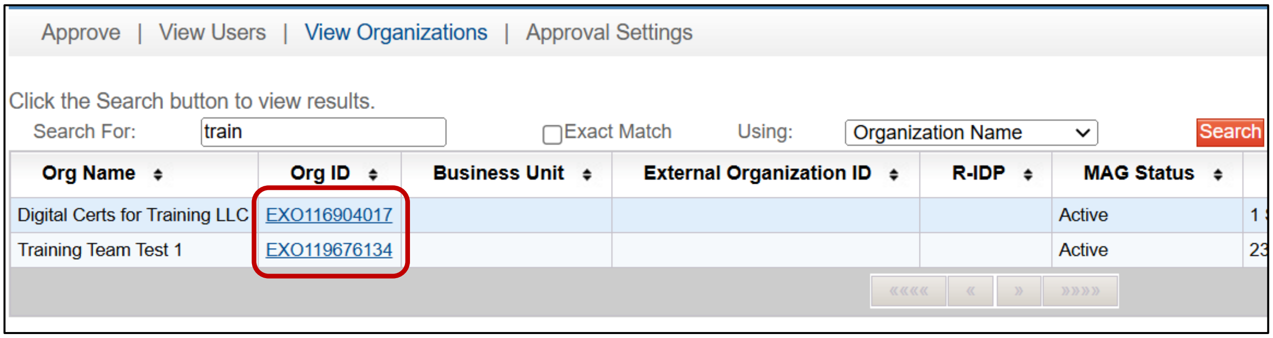


Provider	Application	Last Access Date	Status	Sponsor Code(s)	Action
Raytheon	Raytheon Technologies Supplier Portal		Pending account creation by the Application		
Raytheon	Supply Chain Platform - Raytheon Technologies UAT		Pending Application Administrator Approval		
PIM	Partner Information Manager	17 Feb, 2021 02:20 AM EST	Active		Suspend Delete
Exostar	VQM - Vendor Qualification Manager		Active		Suspend Delete
Raytheon	Raytheon Technologies SecureForms		Active		Suspend Delete
Exostar	Exostar LLC Main Supplier Portal		Suspended		Activate Delete
Exostar	Raytheon Supplier Testing Portal		Inactive		Request Access

Organizations

You can modify access to your application for an entire organization. Once suspended, users are unable to access the application. To modify an organization's application access:

1. Click **View Organizations**.
2. Enter search criteria. Use the search filter menu or select Exact Match to narrow results. Click **Search**.



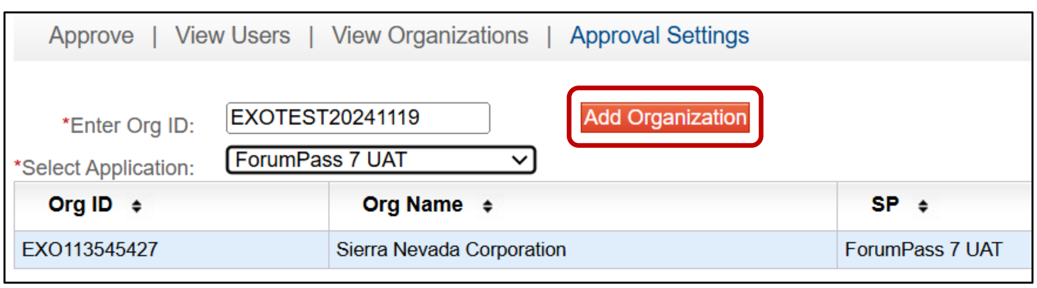
3. From results, click the hyperlinked **Org ID**.
4. To modify application access, scroll to **Application Settings**. Locate the application and click the appropriate action (i.e. Suspend). You are required to enter a suspension reason. Click **Activate** to unsuspend.

Approval Settings

Approval Settings allows SP Administrators to add organizations for automatic approval for application requests. When organizations are added, all users who request access to a SP Administrator's application do not require SP Administrator approval.

To manage approval settings:

1. Enter the organization's Exostar **Organization ID** in the **Enter Org ID** field and select the application you are adding for approval.



2. Click **Add Organization** to complete. To remove from approval list, click **Remove**. Once removed, application requests require SP Administrator approval.

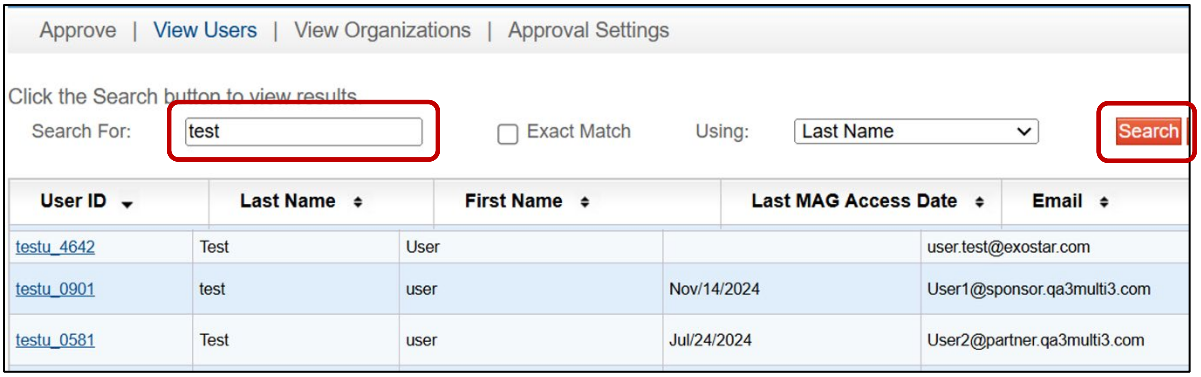
Search

Depending on role, search criteria and functionality varies for Administrators and Organization Stewards. To complete a search:

1. Select search type (e.g. View Users or View Organizations).

EXOSTAR®

2. Select search criteria from the drop-down menu and enter search criteria in “Search For” field. Then click **Search.**



3. Results display. Click the hyperlinked **User ID** or **Organization ID** to obtain details and complete necessary functions (i.e. suspend, reactivate, etc.).

Search Field Definitions

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

View User Results Fields

User ID	Unique identifier for the user
Last Name	Last name of user
First Name	First name of 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

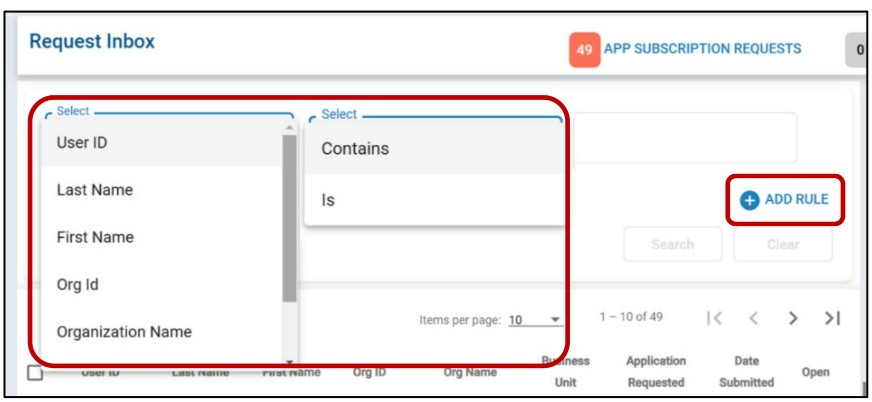
View Organization Search Criteria

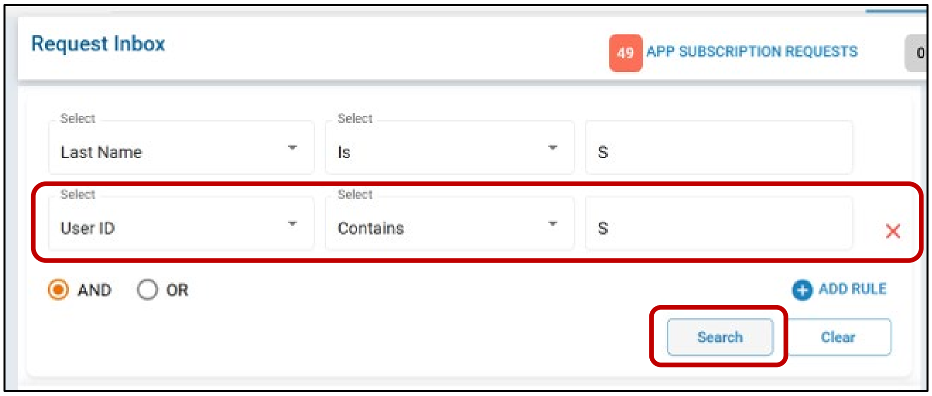
Org Name	Organization Name
Org ID	Organization ID for Exostar MAG account
External Organization ID	Organization ID that partner company uses

New Search Interface

The new search interface allows Administrators to apply more filters. As an Administrator you can filter by:

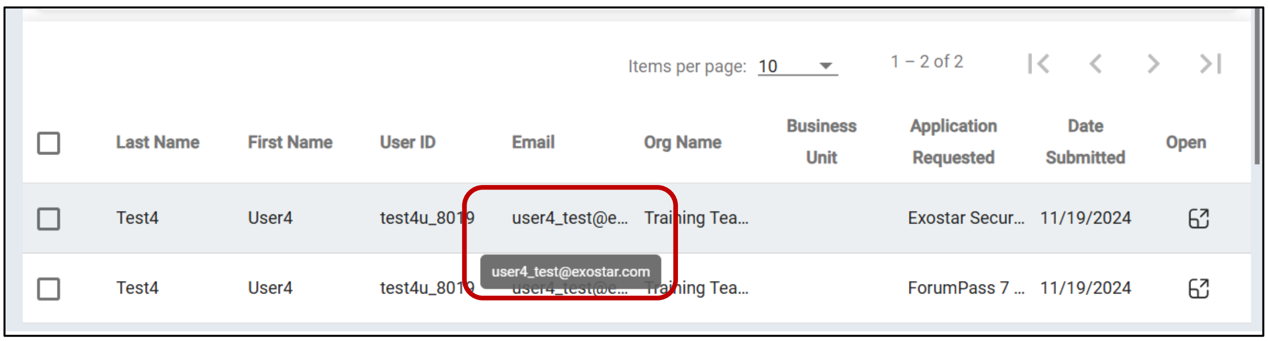
- User ID, Last Name, First Name, Org ID, Organization Name, Business Unit, and Application Name.
- You can apply a Rule/Condition to the available fields and type in a value to be matched.
  - The ''Is" condition matches field values to exactly what is typed.
  - The "Contains" condition expands the search to include any value that includes the typed text.
- To apply more rules, you can click **Add Rule** to add additional search criteria. (To remove the added rule, click the **X** option).
- You can view search results in batches of 25, 50, or 100.
- Click **Search** to display the results.
- If no search results are found, a message will display.





View Complete Email Address

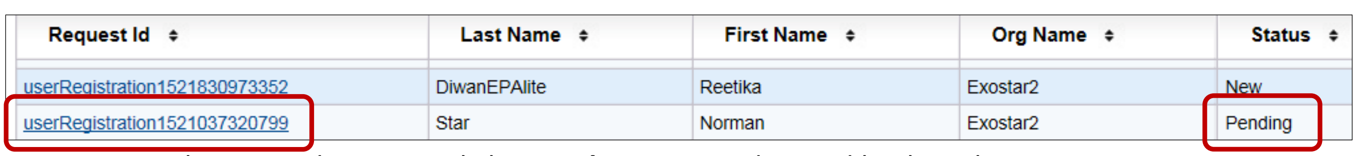
If you have the SP Administrator role and need to view a user's complete email address when approving or denying a request, please hover over the email address to display the full address.



Unlock Pending Requests

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

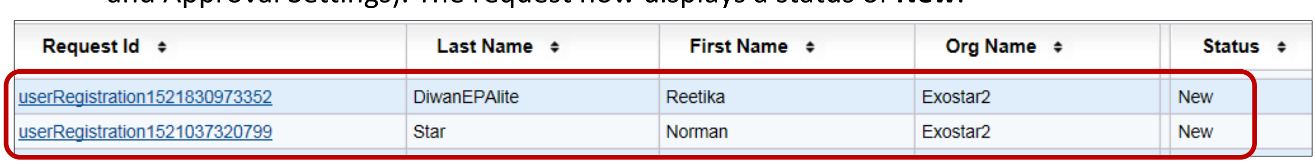
1. Click the **Registration Requests** tab.
2. Status of the request displays as **Pending**. Locate the request and click the hyperlinked **User ID**.



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

3. From the opened request, click **Cancel**. You are redirected back to the request queue.

4. Click the appropriate action sub-tab to refresh (Approve, View Users, View Organizations, and Approval Settings). The request now displays a status of **New**.



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

Resend Provisioning Records

To resend provisioning records:

1. Log into your MAG account.
2. Select the **Provider Administration** tab. Select one of the following:
    a. **View Users**: select a user and click the user ID.
    b. **View Organizations**: select an organization and click the org ID.
3. Locate the **Provisioning** section.

NOTE: The **Select an application** drop down lists all applications the selected user/org is subscribed to and the SP Admin has the administration permissions for.

4. Select an application and click the **Resend** button to resend the record.

NOTE: Resend only works if there was a change from the previous provisioning record to the new one and Force Resend resends the provisioning record to the selected service provider regardless of whether or not a change happened in the provisioning record.