EXOSTAR®

Exostar
Secure Access Manager
(SAM) Administrator Guide

March 2024

EXOSTAR®

EXOSTAR®

DOCUMENT VERSIONS

Version	Impacts	Date
SAM 3.9	• 500-limit user account export has been removed. There is no maximum limit for export results.	September 2018
SAM 4.0	• Changed the product name from IAM to SAM • Updated the text and screenshots for the new login and authentication flow (all sections in "Login to your Exostar SAM Platform Account").	July 2019
SAM 4.1	• Activation workflow	March 2020
SAM 4.3	• Product Platform Upgrade – Phase 1 • Profile Management – Service Provider Administrator Role Improvement • Bugs, Defects, and Others	November 2020
SAM 6.2	• Admin Insights dashboard with widgets for Users & Application activity • BETA Bulk Upload process for Admins • Improved Service Provider Admin application and consolidation requests	March 2024

EXOSTAR®

THE OVERVIEW OF SECURE ACCESS MANAGER (SAM) PLATFORM FOR LIFE SCIENCES

Exostar's Secure Access Manager (SAM) Platform for Life Sciences is a consolidated portal used for account registration, authentication, and management. The authentication gateway supports secure authentication and provides access to applications and services hosted by Exostar and those managed by external entities.

The objective of Exostar's SAM Platform is to consolidate registration processes for connecting partners and applications in a secure environment, while providing flexible management and invitation capabilities to application owners.

Key Functions include:
- Extend the basic concept of Web based Single-Sign-On (SSO) to support single sign on and access to multiple applications.
- Support authentication credentials of varying assurance levels.
- Facilitate an organizational approach to registration, account management and application access.
- Provide organizational control over new user approval and access requests.

ADMINISTRATIVE ROLES

All new SAM accounts are created as *general user accounts*. Later, these accounts can be updated to include Administrative roles. There are six (6) types of administrative roles within SAM: Organization Administrator, Service Provider Administrator, Adoption Administrator, Credential Administrator, Management & Portal Administrator, and Exostar Portal Administrator. Below we explain the unique duties and responsibilities of each admin type.

Organization Administrator

The **Organization Administrator** (Org Admin) is an organization-level administrator who can create new accounts, process registration requests, manage existing accounts, resend activation emails, reset permanent passwords, and manage the organization details. Org Admins are also responsible for accepting the online Terms and Conditions Agreement.

Service Provider Administrator

The **Service Provider Administrator** (SP Admin) is an application-level administrator who can grant approvals to users and organizations for application access, view users, resend activation emails, reset permanent passwords and application subscriptions, and view organizations and set organizational approval setting. The SP Admin is also often referred to as the application owner.

Adoption Administrator

The **Adoption Administrator** (Adoption Admin) is an application and system-level administrator who can access the Adoption Module, create new user accounts and new organizations, subscribe users to applications, and track invitations.

Credential Administrator

The Credential Administrator is an organization level administrator who can approve, deny, or cancel a user's request for an OTP product (e.g. OTP Hardware Token).

Management & Portal Administrator

The Management & Portal Administrator (MPA) role is similar to the Org Admin that provides the ability to manage users within multiple organizations that fall under an Onboarding Sponsor or tenant.

- Ability to reset a user's permanent password
- Ability to view organization details
- Ability to modify user details
- Ability to suspend/restore account/application access

NOTE: MPAs cannot manage Shared User profiles.

Exostar Portal Administrator

The Exostar Portal Administrator (EPA) role is an Exostar role with full administrative privileges. The EPA role has the following capabilities:

- Ability to reset a user's permanent password
- Ability to view organization details
- Ability to modify user details
- Ability to suspend/restore account/application access

There is also the **EPA Lite** role. This role contains most of the same functionality as the **EPA**, except for the following:

- Ability to assign an R-IDP for an Organization
- Ability to suspend or restore account application access
- Ability to deactivate or activate an Org application subscription

THE TYPES OF USERS AND ORGANIZATIONS

The Exostar SAM Platform manages the following types of organizations: Organization-Managed Organizations, Exostar-Managed Organizations, and Sponsor-Managed Organizations. Users from Sponsor-Managed Organizations can transform into "Shared Users," if they begin to access applications that do not belong to their sponsor. Read below to understand the difference between these types of organizations.

Organization-Managed Organization

An **Organization-Managed Organization** in SAM refers to an organization that is responsible for managing itself. The Org Admin accepts the Terms and Conditions on behalf of the organization members. The organization manages and administers their own users. Org-managed organization is the only model that will permit establishing SSO / Federated access for their users. To sum up, an Organization-Managed Organization will have these features:

- It is self-managed
- Organization is responsible for all users in the organization
- Org Admin accepts T & Cs
- Typically larger organizations with established IT expertise
- Pre-requisite for establishing SSO / Federated connection

Exostar-Managed Organization

An **Exostar-Managed Organization** in SAM is an organization that is managed by Exostar. Users within Exostar-Managed organizations accept user-level Terms and Conditions, but they only need to be accepted once. Adding additional applications will not require users to accept additional terms and conditions again. This type of organization is intended for independent users of the system, who may not belong to a particular organization, and who may need access to multiple sponsor applications. For example, clinical investigators would belong to this type of organization. To sum up, an Exostar-Managed Organization will have all the features below:

- It will be registered and managed by Exostar
- Users will accept T & Cs only once, after subscribing to their first application
- Typically, it includes independent users who don't belong to a particular organization
- These users need access to multiple sponsor applications
- Users need to be added to an organization by Exostar, the Sponsor Inviter API, or Adoption Module Administrator.

Sponsor-Managed Organization

A **Sponsor-Managed Organization** is an organization registered in Exostar's SAM Platform and managed by the Sponsor. Members of this organization are the responsibility of the Sponsor.

The Organization Administrator will accept the Terms and Conditions on behalf of the users within this organization. As long as users access sponsor applications exclusively, the Sponsor's Admin will have full control over these users. However, once a user subscribes to a non-sponsor app, the sponsor's admin will stop having full admin control over the user but will continue administering their organization-specific applications. Shared Users will need to accept Terms and Conditions only once, after subscribing to their first non-sponsor application.

A Sponsor-Managed Organization will have these features:

- This organization is registered & managed by the Sponsor
- The Sponsor is responsible for all non-sponsor users in the organization
- Sponsor Org Admin/MPA accepts T&Cs for applications that belong to the Sponsor-Managed Organization
- Users become shared once subscribed to a non-sponsor application

Shared Users

Users who are under a Sponsor-Managed Organization (SMO) have the ability to become Shared Users. Shared Users can access applications outside of their sponsored organization. Once users become shared, they will need to accept Terms and Conditions for the first application belonging to a different sponsor. If any additional non-sponsored applications are added, Terms and Conditions will not be required again.

Once a user subscribes to a non-sponsor application, Organization Administrators and MPAs from the SMO will have only limited control over this user. For instance, they can no longer execute the following functions:

- Make profile updates for Shared Users
- Suspend/Enable Shared Users' SAM accounts
- Deactivate Shared Users' SAM accounts
- Suspend/Enable Organizations with any Shared Users (Applicable to MPAs only)
- Delete Organizations with any Shared Users (Applicable to MPAs only)

NAVIGATIONAL OVERVIEW

Several functional tabs are available within the Exostar SAM Platform Portal. The **Home** and **My Account** tabs are available to all users, while the **Administration**, **Provider Administration**, and **Registration Requests** tabs are available only to designated administrators.
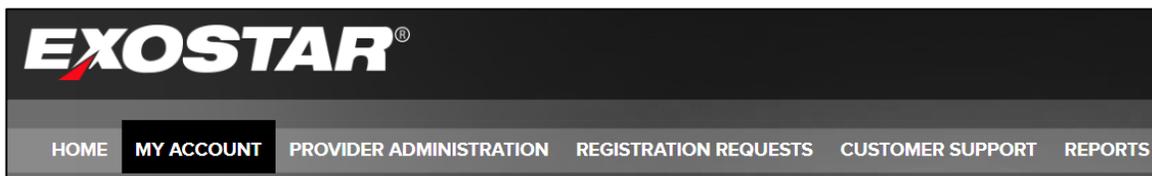
- **Home** tab is available to all users. Applications can be launched from this tab. It also contains several sub-tabs of information, including **My Applications**, **My Organization**, **My Tasks**, and **Account Summary**.

- **My Account** tab allows users to edit their account profile, view organizational details, manage email address, change password and security questions, and manage OTP tokens (if applicable).

- **Administration** tab is available to *Organization Administrators (Org Admins).* You can add new users within this tab and update existing user profiles. In addition, you may subscribe users to applications, and manage your organization information and subscriptions.

- **Registration Requests** tab is available to *Organization Administrators.* From this tab, admins can approve organizations and user application requests.

- **Provider Administration** tab is available to *Service Provider Administrators (SP Admins).* This tab allows SP Admins to manage Organization and User account subscriptions and access. The SP Admin role is a system-level admin role assigned by Exostar.

- **Adoption** tab is available to *Adoption Administrators (Adoption Admins).* It allows Adoption Admins to invite external or internal users to SAM and to bulk-subscribe users to applications or services. The Adoption Admin role is a system-level administrator role assigned by Exostar.

- **Credential Administration** tab is available to *Credential Administrators.* It allows Credential admins to accept, deny, or cancel users' requests for OTP Hardware tokens.

Access the Exostar SAM Platform Portal

Whether logging in to Exostar SAM Platform for the first time, returning to the portal, or logging in via EAG, you can access the portal at https://secureaccess.exostar.com.

How to Activate my Account

Upon creation of an Exostar SAM Platform account, you will receive an email notification with an activation link for your new SAM Platform account. During the account activation process, you will be required to create a permanent password and answer security questions. The system will send the account activation email two times every 30 days, and new activation notifications will supersede activation links sent in previous emails.

Please note that, in some cases, you must complete the account activation within 180 days, or the system will deactivate your account. *This does not apply to EAG users*. The SAM account password expires every 90 days.

Below are steps to complete your account activation:

1. You will receive an email invitation to active your account, click the **Activation My Account** button:
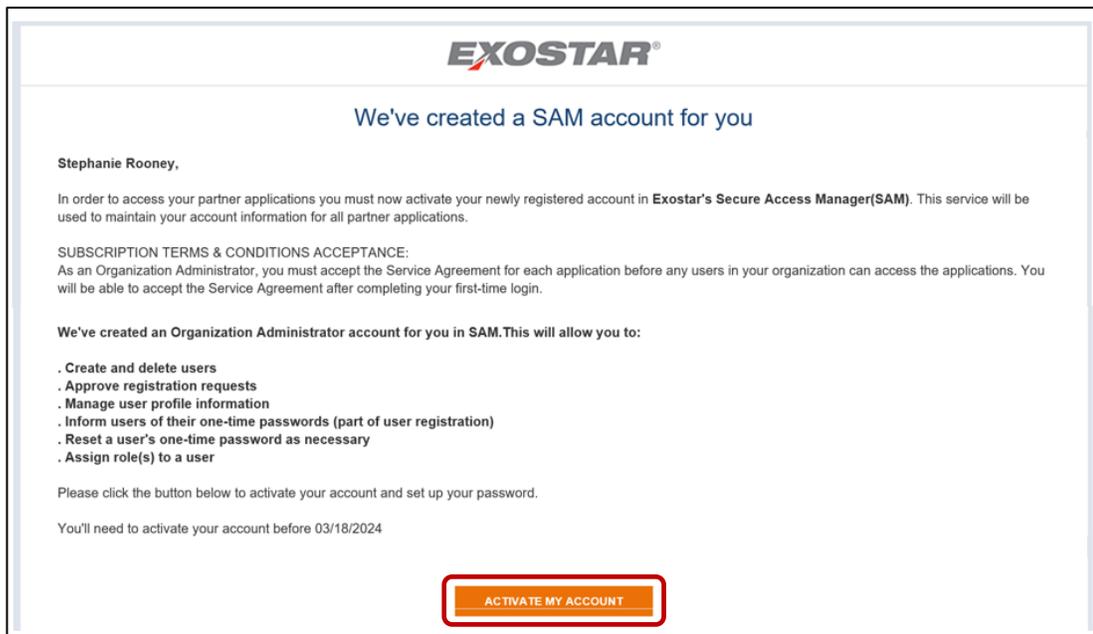
NOTE: You must activate your account by the date in the email, if you do not the link will expire and Exostar will have to resend the activation email.

2. You will be redirected to the Welcome screen, from here click **Let's Get started** button.
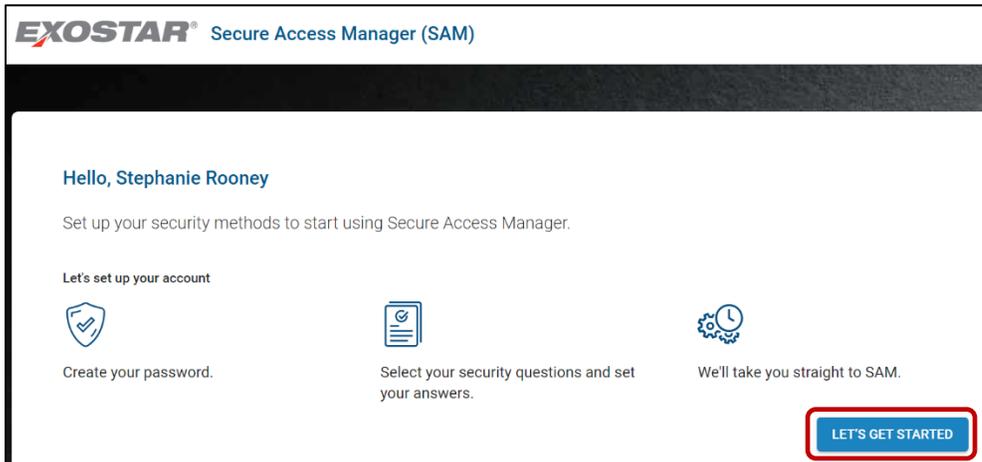
3. Create your password and re-enter the new password again in the fields provided. Please make sure you meet all the password requirements. Then click **Next.**

NOTE: Select the eye icon to view password input. Passwords expire after 90 days.

4. Next setup your security questions and answers. Then click **Next**.

![Exostar®]

NOTE: To view your answers, check the **Show all Answers** box.

5. After you setup your password and security questions, your account is now **Active**. Click **Continue** to access the SAM portal.

How to Login to Exostar's SAM Platform

After the account authentication login, follow these steps to login to your **Exostar SAM Platform** account:

1. Go to the Exostar SAM Platform login portal: https://secureaccess.exostar.com.
2. Enter your Email address and click **Next**.
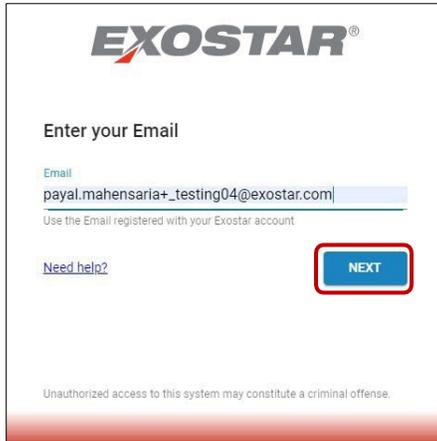
NOTE: SSO/EAG users will have a cookie installed redirecting them to their organization's R-IDP. If the user deletes the cookie or uses another browser, entering the email address will direct the user to authenticate with R-IDP or company credential once again.

3. Enter your password. Click **Next**.
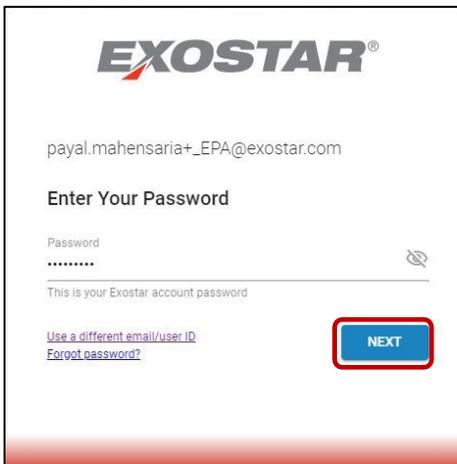
NOTE: If the system recognizes your account has not been activated yet, you will be prompted to resend the activation email.

4. Upon successful login, the Exostar SAM Platform **Home** tab displays. The **Home** tab includes access to your active applications and organization information. Click an application in the My Applications section to launch it.
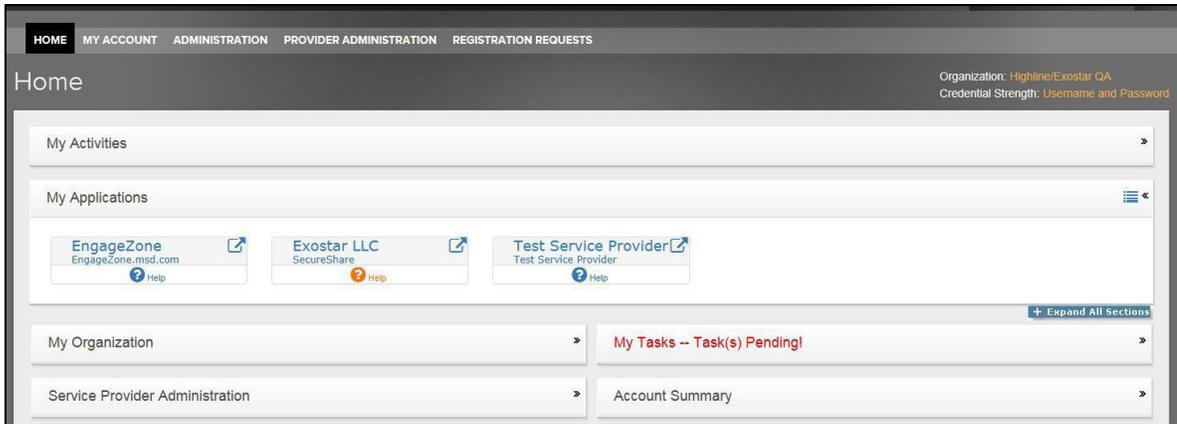
NOTE: In some cases, the *Terms and Conditions* may display the first time you access an application. Please contact Exostar Customer Service for more information.

GENERAL ADMINISTRATIVE FUNCTIONALITY

Upon login to the Exostar SAM Platform portal, the landing pages consist of several tabs. The **Home** tab and the **My Account** tab are available to all users. Only Administrators will have access to the following tabs: Credential Administration, Administration, Provider Administration, Registration Requests, and Adoption.
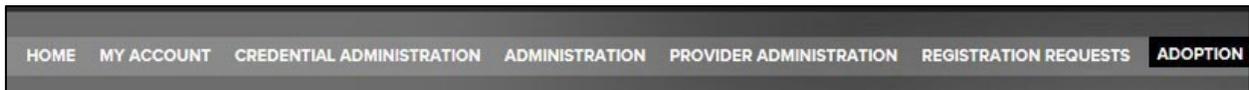
The Credential Administration Tab – Credential and SOTP Client Administrators

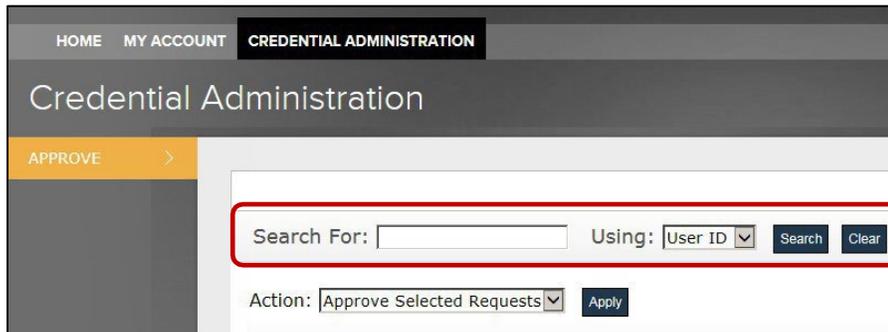**The Credential Administration** tab is the location where Credential Administrators can process user requests for OTP hardware tokens. These tokens provide additional security for applications secured in SAM, and Credential Admins are responsible for granting authorization to users requesting these tokens.
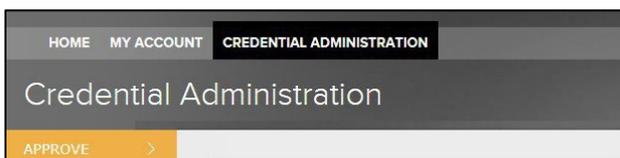
During the first attempt to launch an application, the user will be prompted to submit a request for a for a Multi-Factor Authentication token.
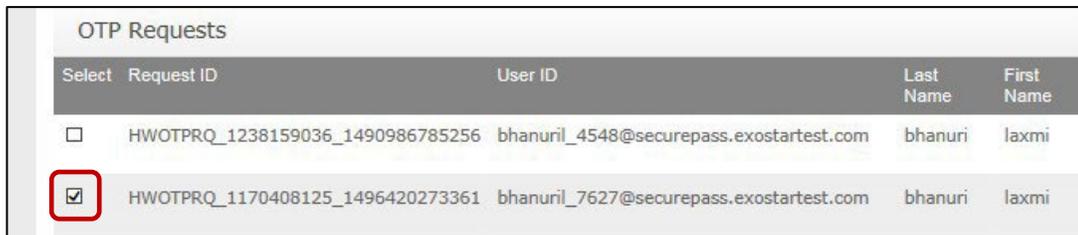
How to Approve a User's Request for a Token

1. Go to https://secureaccess.exostar.com and login to the Exostar SAM Platform with a Credential Administrator account. Access the **Credential Administration** tab.

2. Use search filters (search by *User Id* or *Email Address*) to locate a specific request. Click **Search**.

3. Place a checkmark next to the request you would like to action.

   NOTE: You can only action requests with a status of Pending.

4. Select **Approve Selected Requests** from the **Action** menu.
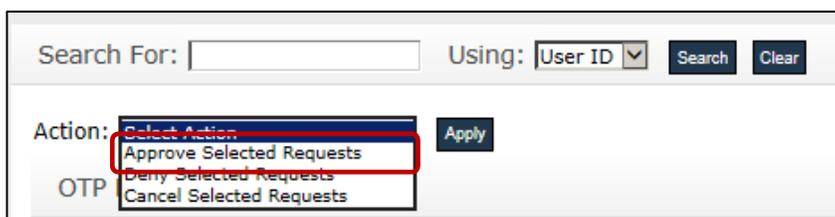
5. Click **Apply** to proceed with the action.

6. The requested action is completed, and the system reflects confirmation of the action.
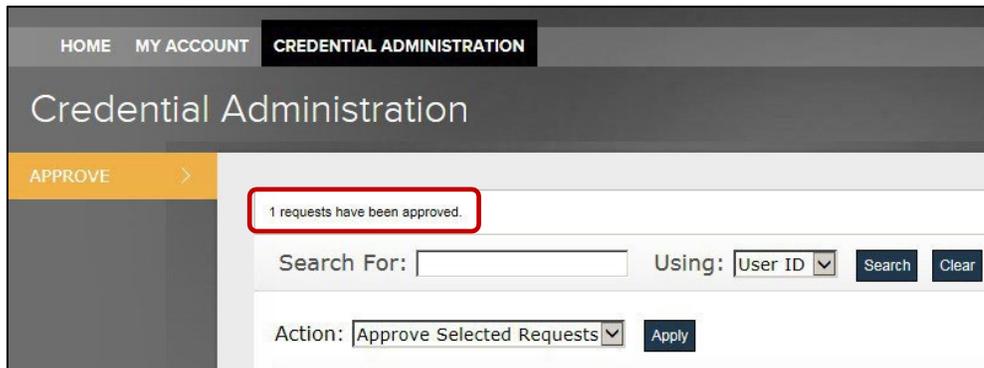
7. The system generates an email to the user informing them that their OTP request was approved.

How to Cancel a User's Request for a Token

1. Go to https://secureaccess.exostar.com and login to Exostar's SAM Platform with a Credential Administrator account. Access the **Credential Administration** tab.

2. Use search filters (search by *User Id* or *Email Address*) to locate a specific request. Click **Search**.

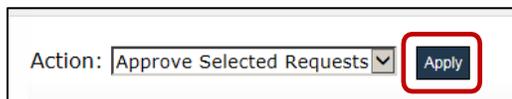3. Place a checkmark next to the request you would like to action.

   NOTE: You can only action requests with a status of **Pending**.

4. Select **Cancel Selected Requests** from the **Action** menu.

5. Click **Apply** to proceed with the action.

6. The requested action is completed, and the system reflects confirmation of the action.

HOME   MY ACCOUNT   CREDENTIAL ADMINISTRATION

Credential Administration

APPROVE

1 requests have been cancelled.

Search For: cambetes   Using: User ID ▼   Search   Clear

Action: Cancel Selected Requests ▼   Apply

7. The system generates an email to the user informing them their OTP request was cancelled.

Mon 11/27/2017 4:49 PM

Exostar UAT Administrators <CustomerService@exostar.com>

Action Required: Request for Exostar HW OTP Service Canceled

To   Teresa Cambetes (Contractor)

Dear Teresa Cambetes,

Your request for Exostar HW OTP Service to SAM has been canceled. To be able to access SAM you will need to register for Phone OTP Service instead.

NEED HELP? http://www.myexostar.com/myexostarAll.aspx?id=2438

DO NOT reply to this email. This is an automated email and replies are not being monitored.

How to Deny a User's Request for a Token

1. Go to https://secureaccess.exostar.com and login to Exostar's SAM Platform with a Credential Administrator account. Access the **Credential Administration** tab.
2. Use search filters (search by *User Id* or *Email Address*) to locate a specific request. Click **Search**.

HOME   MY ACCOUNT   CREDENTIAL ADMINISTRATION

Credential Administration

APPROVE

Search For: [   ]   Using: User ID ▼   Search   Clear

Action: Approve Selected Requests ▼   Apply

3. Place a checkmark next to the request you would like to action.

NOTE: You can only action requests with a status of Pending.

4. Select **Deny Selected Requests** from the **Action** menu.

5. Click **Apply** to proceed with the action.

6. The request is denied, and the system reflects confirmation of the action.

7. The system generates an email to the user informing them that their OTP request was denied.

Mon 11/27/2017 5:12 PM

Exostar UAT Administrators <CustomerService@exostar.com>

Action Required: Request for Exostar HW OTP Service Denied

To   Teresa Cambetes (Contractor)

Dear Teresa Cambetes,

Your request for Exostar HW OTP Service to SAM has been denied. To be able to access SAM you will need to register for Phone OTP Service instead.

NEED HELP? http://www.myexostar.com/myexostarAll.aspx?id=2438

DO NOT reply to this email. This is an automated email and replies are not being monitored.

SOTP Client Administrators

SOTP Client Administrators have access to the managed OTP service area in Exostar's SAM Platform. Click the **Credential Administration** tab, and navigate to the **Manage OTP Service** sub-tab:
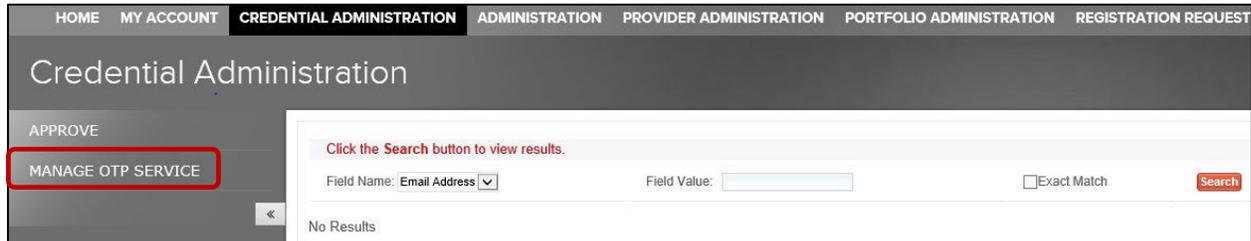
You can search records by e-mail address, user's first and last name, and user reference. To view the full list of records, click **Search** without selecting the search value. Click the hyperlinked User ID to access individual accounts. Client Administrators can perform the following activities: revoke accounts, manage One-Time Password Service for clients, and manage tokens, phones, and credentials.

The Administration Tab – Organization Administrators

The **Administration** tab is available to Organization Administrators. Within this tab, you can create new users and update existing user profiles. In addition, the administrator may subscribe their organization to additional publicly available applications.
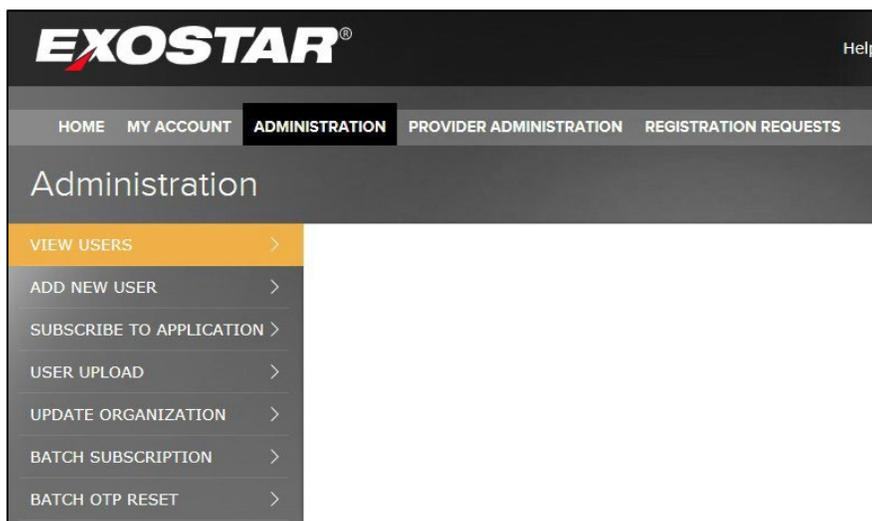
The **Administration** tab contains the functionality that allows Organization Administrators to:

- View and manage existing users
- Manually add new users
- Subscribe the organization to new public ally available applications

- Upload/Add users in bulk
- Update organization
- Subscribe users to a resource in bulk
- Resend activation email using Batch OTP Reset

View Users

View Users allows you to view users associated with your organization's account.

To View Users:

1. Click **View Users**.
2. Enter user criteria and click **Search**. If you have no search criteria, click **Search**.
3. The list of users will display.
4. Click the **User ID** to view details.

Column Customization

Columns that display are customizable. You can set columns to view the data that you want displayed.

To Customize Columns:

1. Click **Set Columns**.

2. Column options will display. Select the columns you want to set for your display. User ID is an unchangeable column, and it displays with any customization.

Set Columns   ✕

☐ Select All   Restore Defaults

Required Columns

   User ID

Selected Columns

☑ Last Name
☑ First Name
☑ Email Address
☑ Organization ID
☑ Organization Name
☐ RIDP User ID
☐ User Status

Available Columns

☐ Middle Name
☐ RIDP Name
☑ Active Applications
☐ Pending Applications
☐ User Level Sponsor
☐ System Role(s)
☐ User Unique Identifier
☐ Shared User (Y/N)
☐ Account Creation Date
☑ Last Access Date
☐ Country of Residence
☐ Phone Number
☐ Fax Number
☐ Job Title
☐ Account Suspended Date

[**Save**] [Cancel]

3. After completing selection, click **Save**. Going forward, this is your defaulted view. You can revert to the original display by clicking **Restore Default.** Search results can be exported to *.xls* format. Additionally, there is no account maximum for returned and exported results.

How to Add a New User

You can add new users to the Exostar SAM Platform in several ways. Org Admins and MPAs can add new users to SAM using the **Add New User** or the **User Upload** links. In addition, you can direct users to a self-registration link, where they can submit their organization requests.

- **Add New User** link allows Org Admins and MPAs to create new SAM user
- **User Upload** link allows Org Admins and MPAs to upload users to their organizations in bulk, using a .csv file.
- **Self-Registration** allows a user to initiate the registration process. Requests are approved by Org Admins and MPAs.

Add New User Link

The *Add New User* link allows Org Admins to add new users manually, by filling out their user profile and application subscription information. To add an individual user:

1. Login to the Exostar SAM Platform. Access the **Administration** tab and select **Add New User**. Even though password message displays, password is <u>not</u> required.

2. In the **Add New User** section of the page, complete all required fields.

3. In the **Application Settings** section of the page, select a **Role** for the new user. Roles include User, Organization Admin, Application Admin, and both Organization Admin and Application Admin.

4. Select the applications users should have access to. Click **Continue**. The list of applications will include all applications the organization is subscribed to.

**NOTE**: If the **Application Administrator** or **Organization Administrator & Application Administrator** role is assigned, you must also designate the applications this user will be authorized to administer. By default, the Application Administrator role is disabled for most applications.

5. Review and verify the information you have entered. You may click **Modify** to make any changes or **Cancel** to cancel this transaction. Click **Submit** to complete.
6. The confirmation page will display. The user will receive an email containing the account activation link.
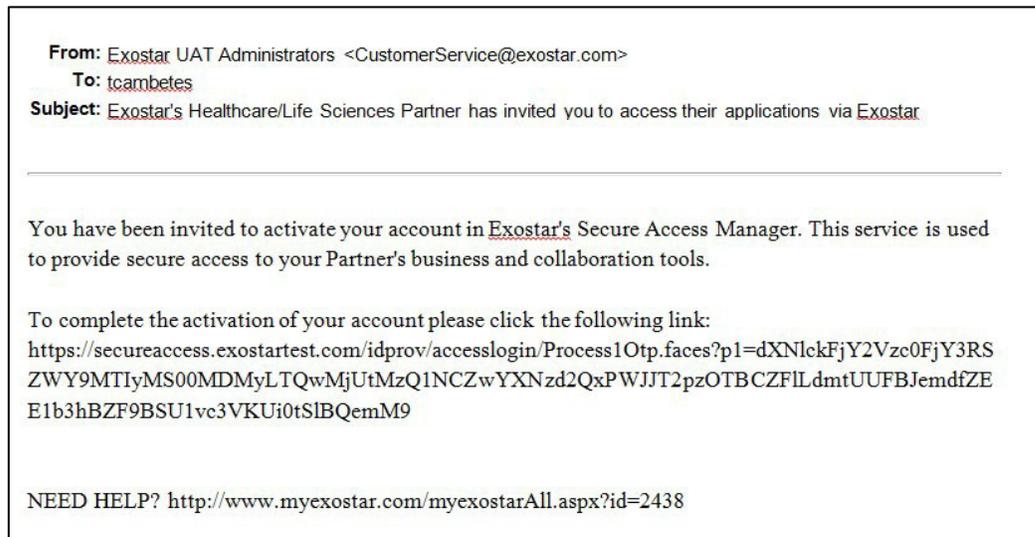
User Upload

Uploading users into Exostar SAM Platform with the **User Upload** feature is the most common use case for adding new users. This option allows administrators to add individual users or users in bulk, while importing their user and organization information directly and seamlessly.

To begin, prepare a CSV file containing user and organization information. See Appendix for samples and templates of acceptable .csv file formats. When preparing the file, include the R-IDP User ID, when applicable. R-IDP will provision enterprise users directly using enterprise credentials.

1. Access the **Administration** tab. Click **User Upload** link.
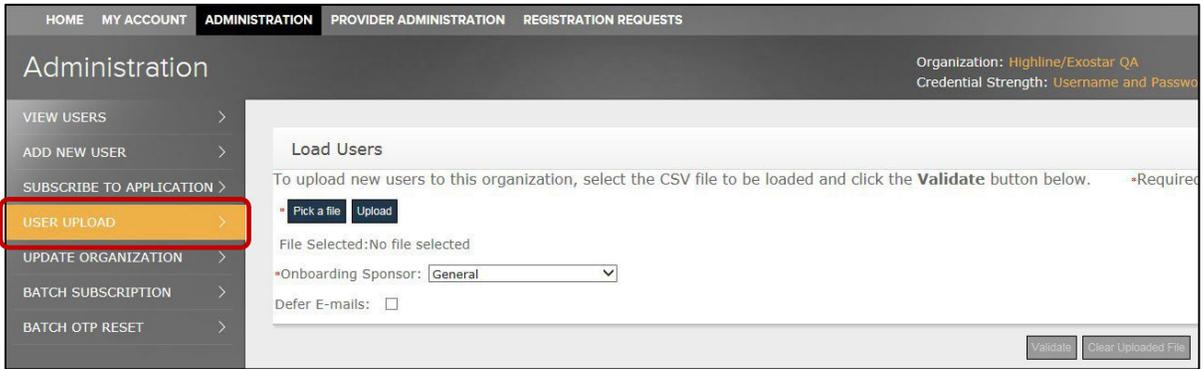
2. To upload new users to your organization, create a .csv file that contains user information. See **Appendices A through D** for file format and field requirement information.

3. Once you create the file, click **Pick a file.** Navigate and select the desired file. Click **Upload**.
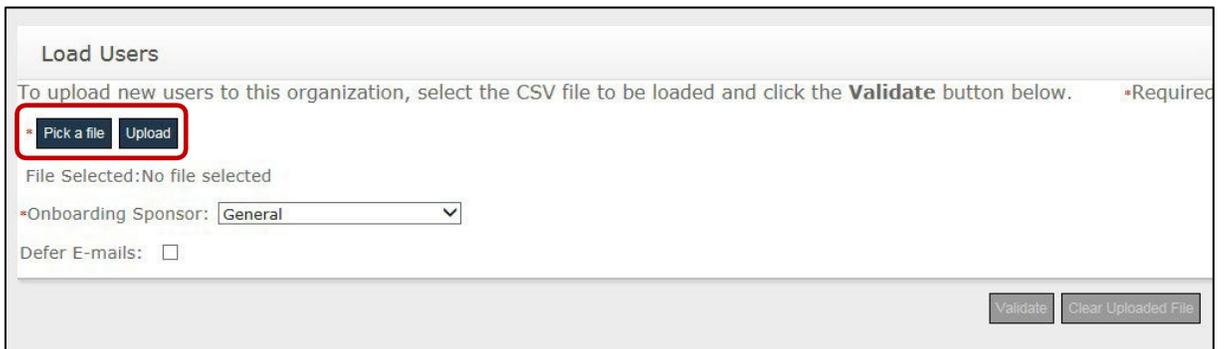
4. Using the drop-down menu, select the **Onboarding Sponsor**.

   NOTE: The **Onboarding Sponsor** selection will affect the branding, help links, and content specific to that sponsor.

5. After selecting the file and onboarding sponsor, click **Validate**. The system will examine the file. If the system detects errors, they will display on the screen, marked with a red X. User information with errors will not be processed. Please correct the errors, and re-upload the file.

![Exostar logo]

6. Click **Commit** to upload the users.
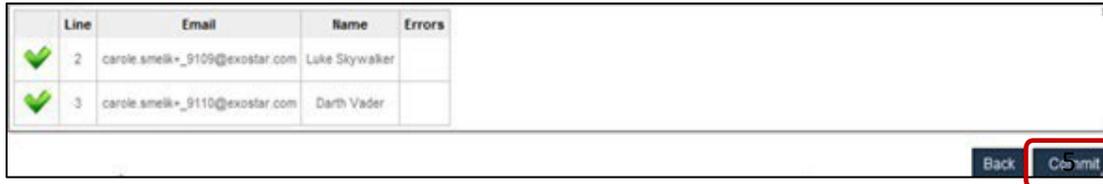
	Line	Email	Name	Errors
✔	2	carole.smelk+_9109@exostar.com	Luke Skywalker	
✔	3	carole.smelk+_9110@exostar.com	Darth Vader	

Back   Commit

7. The system will create new accounts and send emails to users informing them about their new SAM accounts.

NOTES:

- If users are created with the *Defer E-emails* option enabled, **no first-time login emails will be sent to these users**. Depending on what type of user is created in the .csv file (username/password vs. SSO user), there are two options to enable the users:

 1. **Username/Password users**: Use the **Resend Activation Email** link from within the user profile or use the **Batch OTP Reset** option to resend the activation email to multiple users.

  2. **SSO/Federated/EAG users**: There is no option to retrigger login emails for SSO users. Instead, instruct the users to go to the Exostar SAM Platform Login Page (https://secureaccess.exostar.com), and to enter their email address or User ID. Exostar SAM Platform will then link the user to the proper R-IDP.

- If the R-IDP User ID is specified for the user, the system shall link that user to the organization's R-IDP using the specified R-IDP User ID. Instruct the user to go to the Exostar SAM Platform Login page and enter their email address or user ID.

- User not uploaded with an R-IDP ID will receive the **Account Activation** email.

Update Organization

Organization Administrators can restrict email domains allowed to register for a SAM Platform account. When domains are added (e.g., "@xyz.com"), only users with the specified email domains are allowed to register.

NOTE: If domain restriction is added, existing users within an organization must meet the domain restriction criteria. To add domain restriction, follow the steps below:

1. From the **Administration** tab, click **Update Organization**.
2. Enter allowed domains in the **Allowed Email Domains** field (e.g. exostar.com, xyz.com, etc.). Click **Submit**.
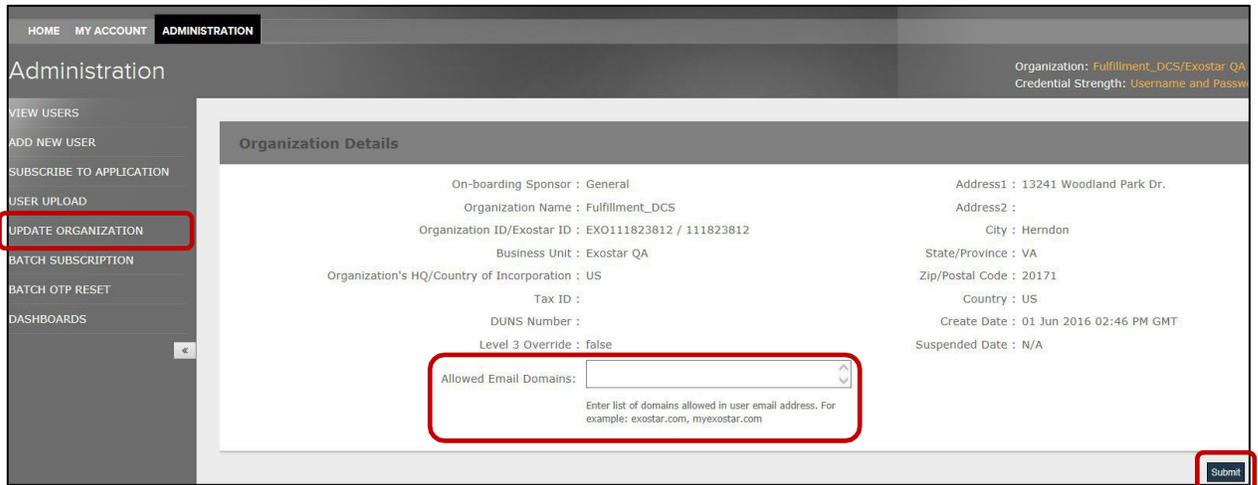
3. Domains that are entered can register for a user account. Unlisted domains will be unable to complete registration.

User Self-Registration

Admins may direct users to the **Self-Registration** portal to initiate their Exostar SAM Platform account registration.

The **Self-Registration** website is: https://secureaccess.exostar.com/userRegistration.

NOTE: The Admin must provide the Org ID to the user in order for the user to proceed through Self-Registration.

How to Locate and Modify Users

Org Admins can use the **View Users** link to locate existing users and modify user profiles.

You can use the search filters to help narrow your search. Once a user is found, you may view and update their user profile, role, and the applications to which they have access. Do so from the user's **Details** page. This page contains two sections:

- **User Profile**: here you can view and update the details of the individual's profile.
- **Application Settings**: here you can view and update a user's role, access to applications, and access to SAM. You can also reset the user's one-time password.

To locate and update a user's account:

1. Access the **Administration** tab on the Exostar SAM Platform portal. Click **View Users**.
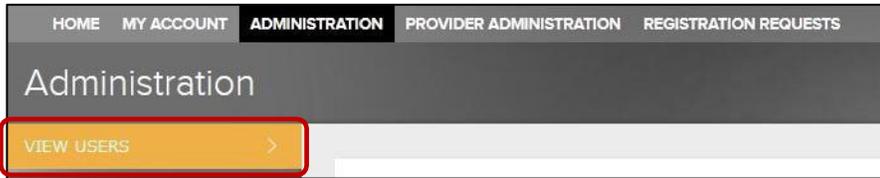
2. Use filters to narrow your search or view the complete list of users in your Organization by clicking only **Search**.

3. All search results will display. Click the **User ID** to access the user's profile information.

4. In the **User Profile** section, you can update any field, excluding the User ID, Role, Org Name, and Org Id. Make changes, and click **Continue**.

The **Modify Email** option allows you to update a user's email address. After an Org Admin modifies the email address, the user will receive an email with the activation code and steps for activating their new email address. The new email address will not be reflected in Exostar SAM Platform until the user completes the activation process.

NOTE: This feature will not work with SSO/EAG users. SSO/EAG users who need to update their email must contact their Corporate Helpdesk.

5. Verify the changes. You can click **Modify** to go back and make further changes, or **Cancel** to go back to the **Search** page. Click **Submit**.

6. A confirmation page will display, and the changes will be saved in the system.

NOTE: Admins of a Sponsor-Managed Org will not be able to update user profiles once a user becomes "Shared," or subscribed to at least one non-sponsor application.

How to Resend Activation Email

Organization or Service Provider Administrators can resend the **Activation Email** for inactive users from the **Application Settings** section of the **User Details** page. Locate the user and access their profile page by following the steps above. Then complete these steps:

1. If a user account has an **Inactive** status, Org Admins can click **Resend Activation Email**.

2. A confirmation page will display. Click **Submit** to resend the email.

Click submit to re-generate first time login activation link. The user will receive a new email with the new activation link.

Resend Activation Email

User ID: pattersonp_4932

Submit

How to Suspend, Reactivate, and Delete User Accounts

There are several options for account access management available on the User Details page in the **Application Settings** section:

- Suspend, Edit and Reactivate access to an application
- Suspend access to Exostar's SAM Platform
- Permanently delete access to Exostar's SAM Platform

The system will notify users by email of a suspension or deletion action.

NOTE: Please note that Sponsor Managed Organization Administrators and MPAs cannot suspend, reactivate, or delete **Shared User** accounts. However, Service Provider Administrators can suspend, reactivate, or edit access.

How to Suspend, Edit, and Reactivate Application Access

1. Locate the user and access their profile page (as detailed above).
2. The Org Admin can **Suspend, Edit, and Reactivate** a user's access to an application.
3. Click **Suspend** next to the appropriate application to suspend access to it.
4. Click **Edit** to modify the subscription period for the application.

Role:	User					
Application Access:	Provider	Application	Expiration Date	Last Access Date	Status	Action
	Test Service Provider	Test Service Provider			Active	Edit Suspend Delete
Status: Active	Suspend User Access	Reset Permanent Password	Reset Security Question	Delete User		

Continue

5. Click **Continue**. A confirmation page will display. The user status will change to **Inactive**.

Edit User

User ID: cambetest_5561
Full Name: Teresa Cambetes
New Status: Disabled

Return to User Profile

6. Return to the user's profile page. The **Application Settings** section shows the user's status as **Suspended**. To reinstate access to the application, click **Activate**.

Application Settings

Role: User

Application Access:	Provider	Application	Expiration Date	Last Access Date	Status	Action
	EngageZone	EngageZone.msd.com			Suspended	Activate

Status: Active Reset Permanent Password Reset Security Question

7. A confirmation page will display.

NOTE: Sponsor Managed Organization Administrators and MPAs cannot suspend, edit, or reactivate non-sponsored applications on Shared Users Exostar SAM Platform accounts. However, Service Provider Administrators can suspend, reactivate, or edit access.

How to Reset User's Permanent Password and Security Questions

1. Locate the user and access the profile page (as detailed above).

2. The Org Admin can **Reset Permanent Password** and **Reset Security Question**. To reset the user's permanent password, click **Reset Permanent Password**. Click **Reset Security Question** to reset the user's security question.

Status: Active Suspend User Access Reset Permanent Password Reset Security Question Delete User

3. The user will receive an email with instructions on how to reset the permanent password and security questions.

NOTE: Please be advised that once a user becomes a **Shared User**, Sponsor Managed Org Admins and MPAs will be unable to reset their password. SP Administrators can reset permanent password or resend the activation email.

How to Delete a User Account in Exostar's SAM Platform

1. Locate the user and access the profile page (as detailed above).

2. The Org Admin can **Suspend** or **Delete** a user's access to Exostar's SAM Platform. To suspend access, click **Suspend User Access**. Click **Delete User** to permanently delete a user account in SAM.

3. A confirmation page will display.

NOTE: Sponsor Managed Organization Administrators and MPAs cannot permanently delete Shared Users Exostar SAM Platform accounts.

How to Subscribe your Organization to an Application

The **Subscribe to Application** link allows an Org Admin to initiate an application subscription for their organization.

NOTE: Most applications are invitation-only and require the Exostar EPA to complete the subscription.

To subscribe your organization to an application:

1. Access the **Administration** tab. Locate the desired application and click **Subscribe to Application**.
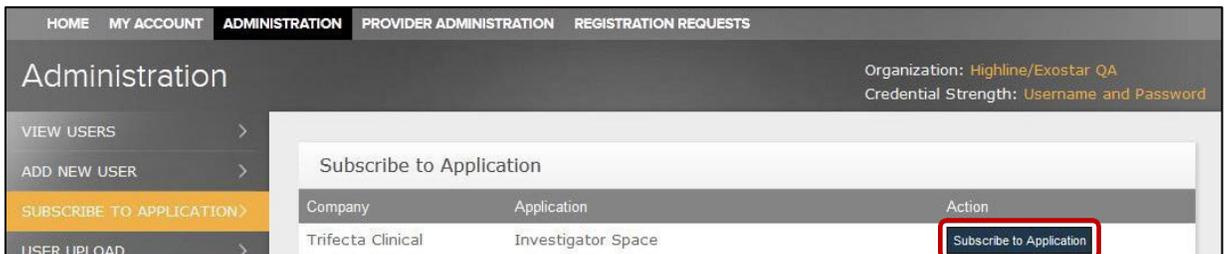
2. Complete the Administrator information page.

3. You may choose to select an existing administrator from the drop-down list or enter information for a new administrator. Click **Next**.

4. Confirm the administrator selection and information. Click **Next**.

5. The submission confirmation will display. It will contain a reference number.

## How to Update Organization's Allowed Email Domains

Within the **Update Organization** page, Org Admins may choose to identify **Allowed Email Domains** for user email addresses allowed to access Exostar's SAM Platform. If an administrator chooses to define "allowed domains," all existing users will need to conform to this standard.

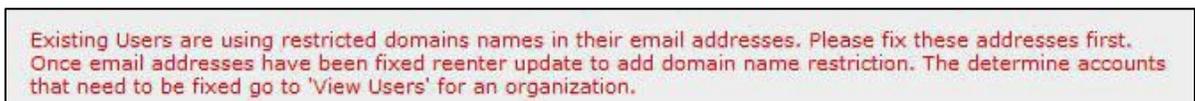To define **allowed domains** for an organization:

1. Access the **Administration** tab. Click the **Update Organization** link.

2. Enter email domains permitted for automatic provisioning (for example, exostar.org). Click **Submit**.
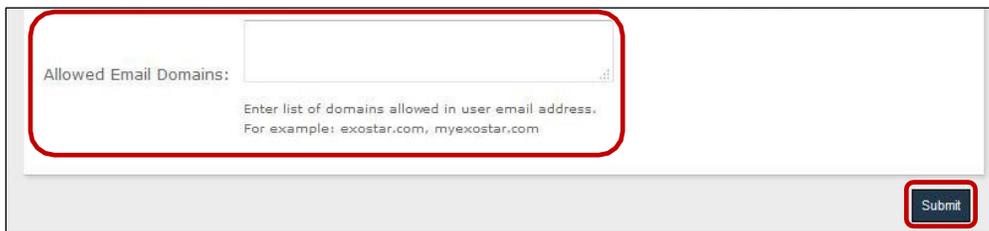
3. If any existing users do not comply with the allowed email domains, you will see the following error message:

> Existing Users are using restricted domains names in their email addresses. Please fix these addresses first. Once email addresses have been fixed reenter update to add domain name restriction. The determine accounts that need to be fixed go to 'View Users' for an organization.

Correct the list of domains to include all current user domains or modify user emails to comply with the new restriction.

4. Click **Submit**.

NOTE: Please be advised once a user becomes a **Shared User**, Sponsor Managed Organization Administrators and MPAs are unable to make any modifications on their Exostar SAM Platform accounts.

How to Add Multiple Users to an Application - Batch Subscription

Org Admins may choose to provision existing user accounts to a specific application in bulk, using the **Batch Subscription** function. To do so, simply upload a .csv file containing user IDs and the subscription period (optional). Follow the steps below to complete this batch operation:
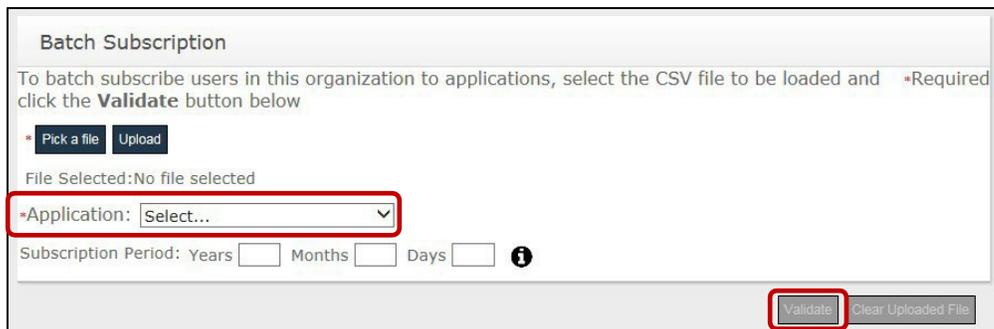
1. Access the **Administration** tab. Click **the Batch Subscription** link.
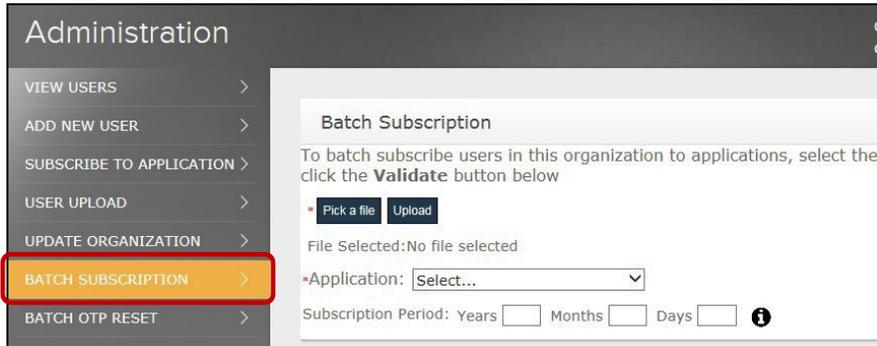
2. Click **Pick a file** to locate the correct file (see **Appendices A through D** for file formatting requirements). Click **Upload** to upload the file.
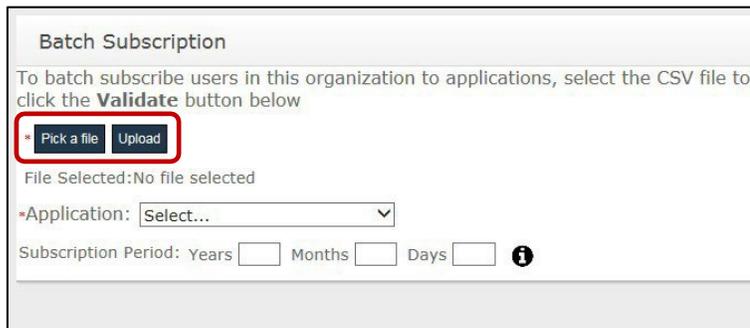
3. Select the application. Click **Validate** to proceed.

4. A confirmation message will display. Click **Commit** to load user subscriptions.

NOTE: Users with the green checkmark next to their name are granted access. If any users are listed with the red X mark, it means they were not processed due to errors. Review the list of errors and correct them to complete the upload.

How to Reset Inactive Accounts – Batch Reset

If there are multiple users who are inactive and activation emails need to be resent to them, Org Admins can reset their OTP accounts by using the **Batch OTP Reset** function. Admins simply have to upload a .csv file with user IDs to reset the inactive accounts in bulk. Follow the steps below to complete this action:

1. Access the **Administration** Tab. Click **the Batch OTP Resets** link.
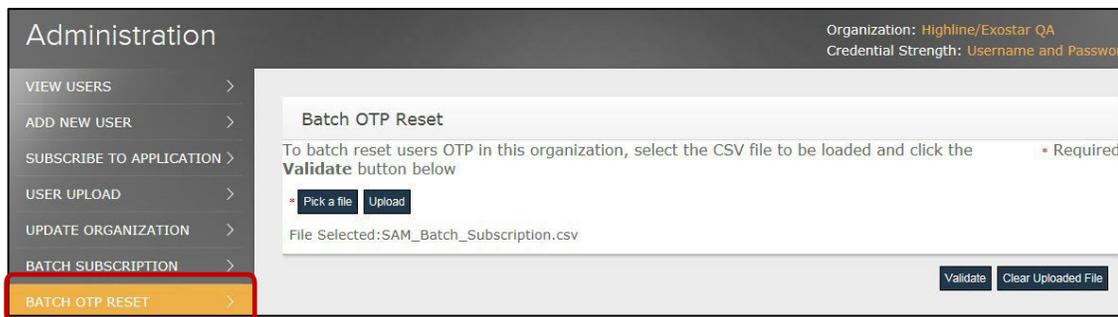
2. Click **Pick a file** to locate the file containing user information (see **Appendices A through D** for the file formatting information). Click **Upload** to upload the file.
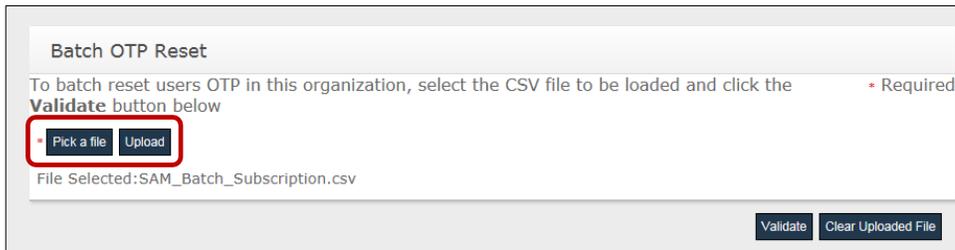

NOTE: The *CSV* file for **Batch OTP Reset** contains two columns: "userID" and "subscriptionPeriod" (optional). The "userID" field can contain either email address or Exostar SAM Platform User ID.

3. Click **Validate** to proceed.
4. A confirmation message will display. Click **Commit** to complete the reset.

The Provider Administration Tab - Service Provider Administrators

Service Provider Administrators (SP Admins) can access the **Provider Administration** tab in order to approve and provision users and organizations with specific applications. Often referred to as application owners, the SP Admins manage access to the applications that they administer.
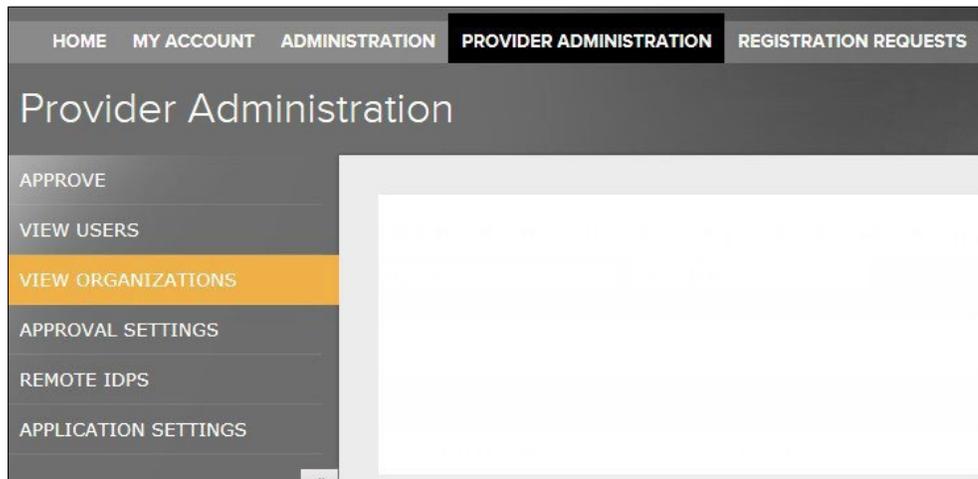
The **Provider Administration** tab contains the following options:

- **Approve:** displays the list of all users awaiting approval for access to the application.
- **View Users**: allows the SP Admin to search for users subscribed to the application.
- **View Organizations**: allows the SP Admin to search for organizations subscribed to the application.
- **Approval Settings**: allows the SP Admin to add to the list of organizations whose users do not require your approval for access to the application.
- **Application Settings:** allows the SP Admin to view applications, view application settings, and enter allowable email addresses and domains for application access.
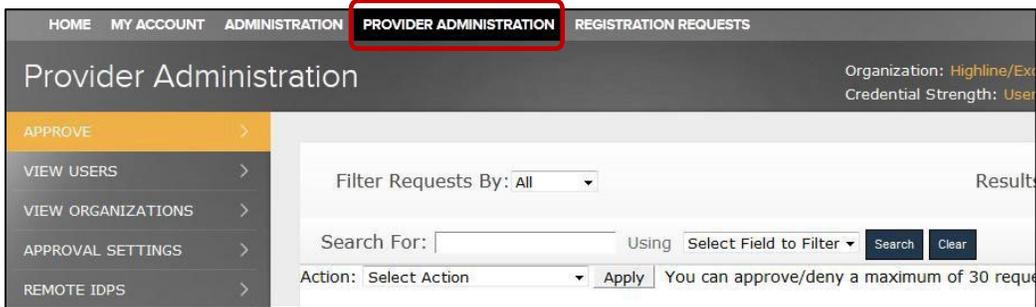
Approve: Approving User Access Requests

Working in the **Approve** page, SP Admins may perform the following functions:

- Filter and search for users
- Approve or deny individual requests
- Approve or deny requests in multiples

How to Filter and Search for Users

1. Login to the Exostar SAM Platform and access the **Provider Administration** tab.

2. Use the search filters and fields to locate a specific approval request.
   The following search filter fields are available:
   - **Filter Request By:** allows you to filter by All, New, and Pending requests.
   - **Search For:** allows you to enter search criteria, such as username, user ID, or organization information.
3. Enter search criteria and click **Search**. The search results will display. Click the **Request ID** link to access the desired request.

How to Process User Access Requests

SP Admins can process user access requests individually (one by one), or multiple requests simultaneously. To process user access requests:
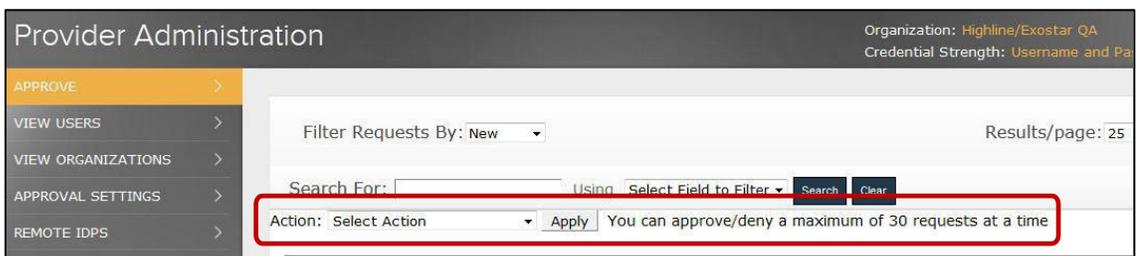
1. Login to the Exostar SAM Platform and access the **Provider Administration** tab.

2. To approve or deny an individual access request, select the desired request by clicking the **Request Id** link.
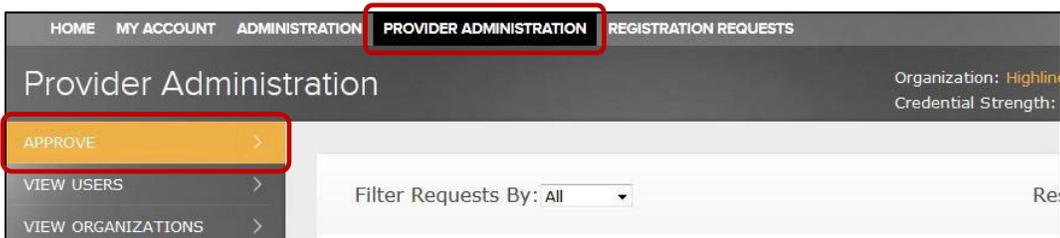
To approve or deny multiple requests, select the desired requests by placing a checkmark in the box next to the **Request ID** link.
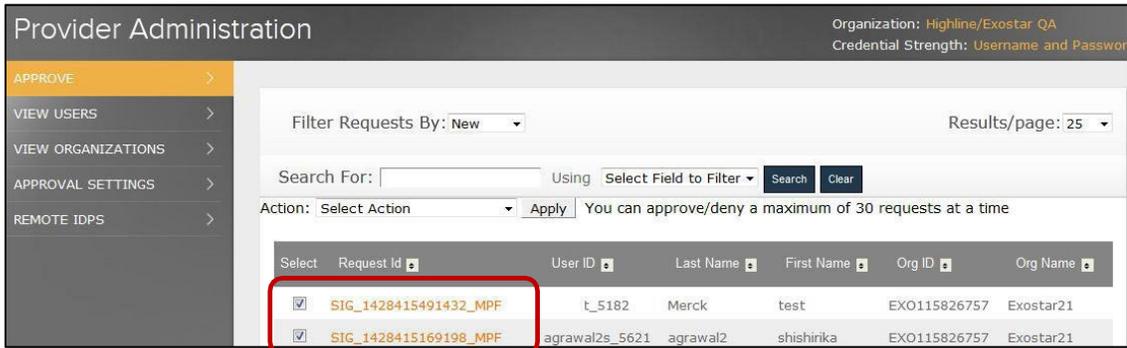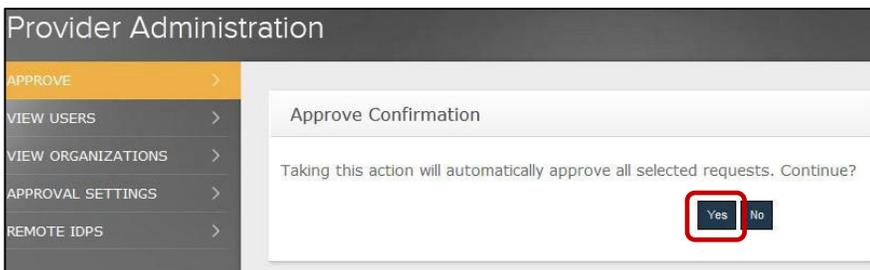

3. Select the desired **Action**.

NOTE: In order to **Approve** a user request, the user's account must be properly provisioned, and the user must have the minimum required role/privileges.

4. Then click **Yes** to approve your changes. Next, a confirmation message will display, and the user(s) will receive an email advising of approval.

`

View Users: Locate and Update User Accounts

Using the **View Users** page, SP Admin may perform the following functions:

- Search for user accounts.
- View user account details, including Exostar SAM status and active and pending applications.
- Suspend and restore a user's application access.

The SP Admin can search for a user subscribed to an application on the **View Users** page. This page lists all Active, Inactive, or Pending users.

Column Customization

Columns that display are customizable. You can set your preferences for visible columns. Please see the [Column Customization](#) section for instructions.

How to Locate a User Account

You can perform searches by using search criteria and filters. Once you locate a user, you may view and update their user profile, their user role, and the applications they have access to via the **User Details** page. A user's details page contains two sections:

- **User Profile**: you can view the details of the individual's profile.
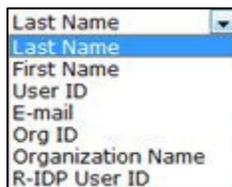- **Application Settings**: you can view a user role and update application access.

To locate a user:

1. Login to the Exostar SAM Platform, and access the **Provider Administration** tab.
2. Click the **View Users** link.
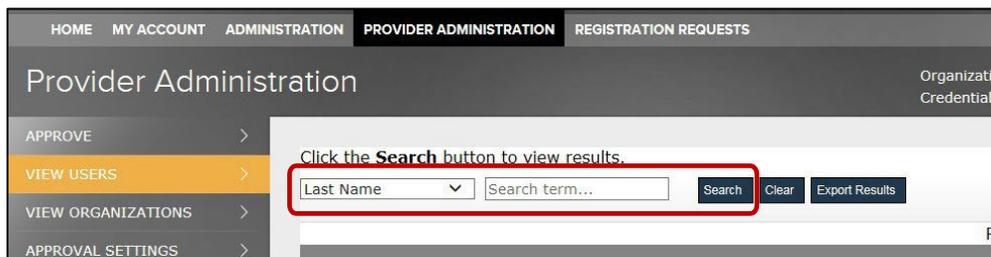
3. Enter search criteria.

   NOTE: You may search for a user based on the following filter criteria:

4. To access the User Profile, **click on the User ID** link. The **User Profile** section contains all user information, including account and contact information.

   NOTE: There are two active links contained within each search result entry:
   1. Click the **USER ID** link to view the profile for this particular user.
   2. Click the **ORG ID** link to view the Organizational Details for this user.

How to Reset User's Permanent Password and Security Questions

1. Locate the user and access the profile page (as detailed above).

2. The Provider Admin can **Reset Permanent Password** and **Reset Security Question**.

   - To reset the user's permanent password, click **Reset Permanent Password**.

   - Click **Reset Security Question** to reset the user's security question.

3. The user will receive an email with instructions on how to reset the permanent password and security questions.

   NOTE: Please be advised that once a user becomes a **Shared User**, Sponsor Managed Org admins and MPAs will be unable to reset their permanent password or security questions.

How to Suspend a User Subscription

There are times when a user may no longer need access to an application or resource, perhaps temporarily. However, the user will still need to maintain an active account within SAM. The SP Admins may modify the user status in order to suspend access to a specific resource.

To suspend a user account subscription:

1. Login to Exostar SAM Platform, and access the **Provider Administration** tab.

2. Locate the desired user. Click the **User ID** link.

3. The user's profile will display. Scroll to the bottom to locate the **Application Settings** section. Click **Suspend** next to the desired application.

4. A confirmation message will display. Click **OK** to suspend the user's access.

5. The user's account updates and their access to this application is now suspended. An updated status for the user will display.

   NOTE: Please be advised that once a user becomes a **Shared User**, Sponsor Managed Org admins and MPAs will be unable to suspend non-sponsored applications
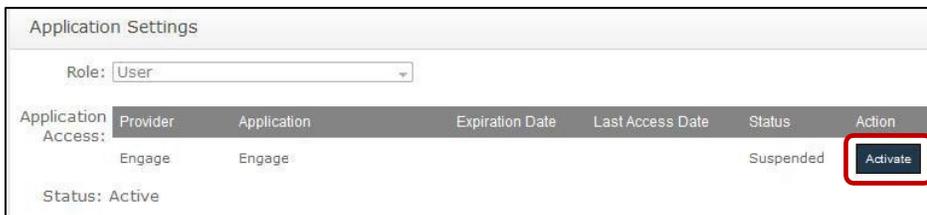
How to Reactivate a User's Subscription

SP Admins can reactivate a user's access to an application. To reactivate a user account subscription:

1. Login to Exostar SAM Platform and access the **Provider Administration** tab.
2. Locate the desired user. Click the **User ID** link.

3. The user's profile will display. Scroll to the bottom to locate the **Application Settings** section. Click **Activate** next to the desired application.

4. A confirmation message will display. Click **OK**.

   NOTE: Once a user becomes a **Shared User**, Sponsor Managed Org Admins and MPAs will be unable to reactivate subscriptions to non-sponsored applications. However, SP Administrators can suspend, un-suspend or edit application access.

How to Reset User's Permanent Password

SP Admins can reset an active user's permanent password. To reset a user's permanent password:

1. Login to Exostar SAM Platform and access the **Provider Administration** tab.
2. Locate the desired user and click the **User ID** link**.**

User ID ▾	Last Name ▾	First Name ▾	Email ▾	R-IDP ID ▾	Org ID ▾	Organization Name ▾	
testert_2281	Tester	Tracy	tracytester@exostar.com		EXO114766233	Highline/Exostar QA	U
testers_9179	Tester	Susie	stester@exostar.com		EXO114766233	Highline/Exostar QA	Us

3. The user's profile will display. Scroll to the bottom to locate in the **Application Settings** section. Click **Reset Permanent Password**.

Application Access:	Provider	Application	Expiration Date	Last Access Date	Status
	EngageZone	EngageZone.msd.com			Active

Status: Active [Reset Permanent Password] [Reset Security Question]

4. A confirmation message will display, and an email will be sent to the user's email address. The email will contain a system-generated password.

NOTE: Once a user becomes a **Shared User**, Sponsor Managed Org admins and MPAs will be unable to reset their permanent password. However, SP Administrators can reset permanent passwords or resend activation email.

How to Resend Activation Email

SP Admins can resend the activation email to an inactive user. To resend the activation email:

1. Login to Exostar SAM Platform and access the **Provider Administration** tab.
2. Locate the desired user and click **User ID** link**.**

User ID ▾	Last Name ▾	First Name ▾	Email ▾	R-IDP ID ▾	Org ID ▾	Organization Name ▾	
testert_2281	Tester	Tracy	tracytester@exostar.com		EXO114766233	Highline/Exostar QA	U
testers_9179	Tester	Susie	stester@exostar.com		EXO114766233	Highline/Exostar QA	Us

3. The user's profile will display. Scroll to the bottom to locate in the **Application Settings** section. Click **Resend Activation Email**.

4. A confirmation message will display.

How to Resend User's Provisioning Record

SP Admins can reset an active user's provisioning record. To reset a user's provisioning record:

1. Login to Exostar SAM Platform and access the **Provider Administration** tab.
2. Locate the desired user and click the **User ID** link**.**

3. The user's profile will display. Scroll to the bottom of the page to locate the **Provisioning Settings** section. Select the Application from the drop-down menu. Then click **Resend or Force Resend** provisioning record.

Once you have resent the provisioning record, it will display the time and date it was resent.

View Organizations

The View Organizations page provides SP Admins with the ability to view and action organizations subscribed to their application. Administrators can also suspend and reactive organizational access to the resource. SP Admins can perform the following actions:
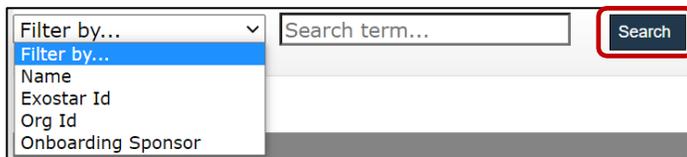
- Search for an Organization
- View Organization details, including Active Applications
- Suspend and Restore an Organization's application access

How to Locate an Organization

1. Login to the Exostar SAM Platform and access the **Provider Administration** tab.
2. Click the **View Organizatio**ns link.
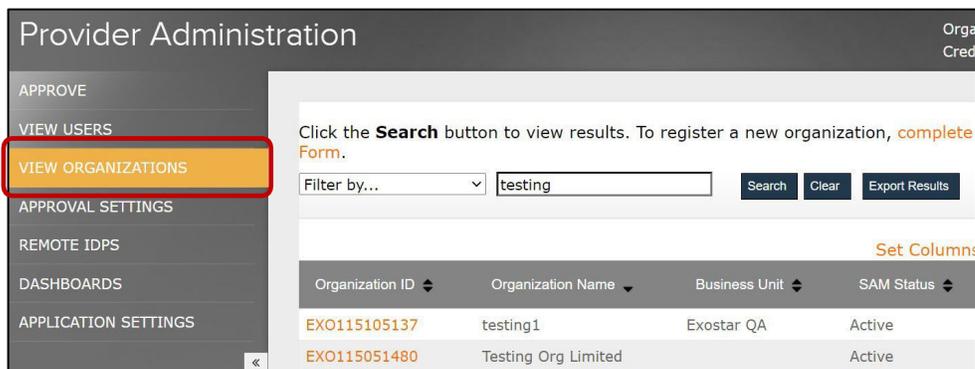
3. From the drop-down list, select the **Filer by** option. Or enter a **Search Term** in the dedicated field. Then click **Search**.

NOTE: If you leave the search criteria field blank, the full list of organizations will display.

4. The list of search results will display. Click the **Organization ID** to view all organizational information, contacts, and administrators.
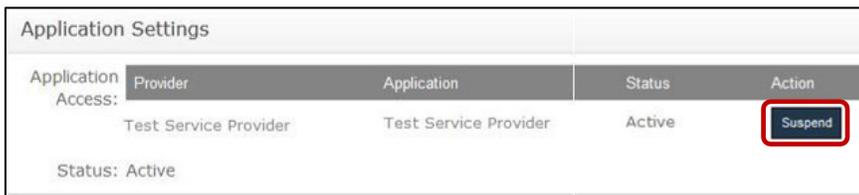
Suspend an Organization's Access

SP Admins can suspend an organization's access to the application. If an organization's access to a specific resource is suspended, the users from that organization will no longer have access to the resource.

1. Locate the organization for which you would like to suspend access. Click the **Org ID** for this organization.
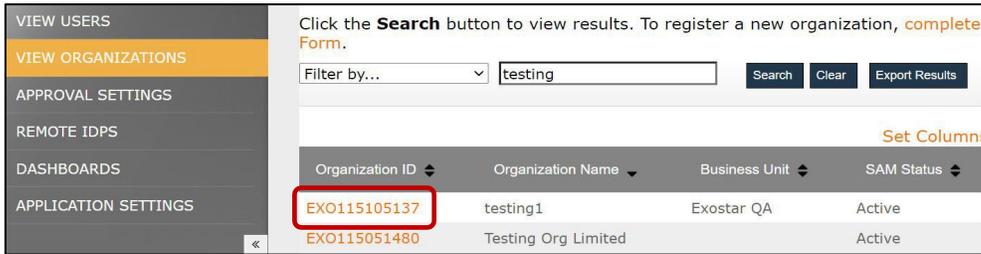
2. Scroll to the bottom of the Organization's profile page. Click **Suspend**.

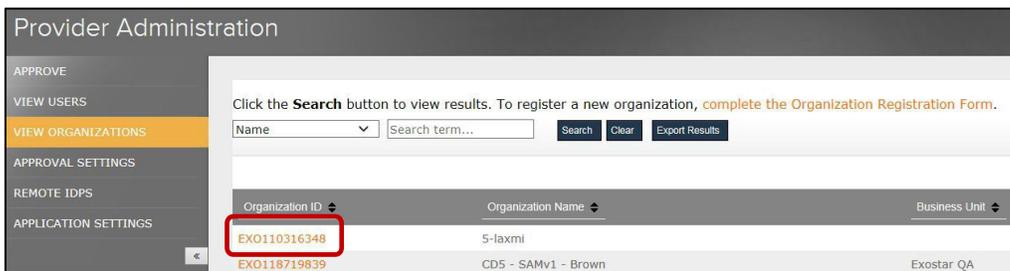3. You will be prompted to confirm the **Suspension**. Then click **OK**.

4. The confirmation message will display.

Reactivate an Organization's Access

SP Admins can reactivate an organization's access to the application. To reactive access:

1. Search for and find the organization you want to reactive access. Click the **Org ID** for the applicable organization.

2. Scroll to the bottom of the profile to the **Application Settings** section and click **Activate**.

3. You are prompted to confirm the **Activation**. Click **OK**.

4. The confirmation message will display.

Approval Settings

The Approval Settings page allows SP Admins to set automatic approvals for all users from a given organization. For example, if an organization is included in the 'approved list,' the users will not need to be approved by an SP Admin.

How to Add an Organization to the Approved List

1. Login to Exostar SAM Platform, and access the **Provider Administration** tab.

2. Click the **Approval Setting** link.
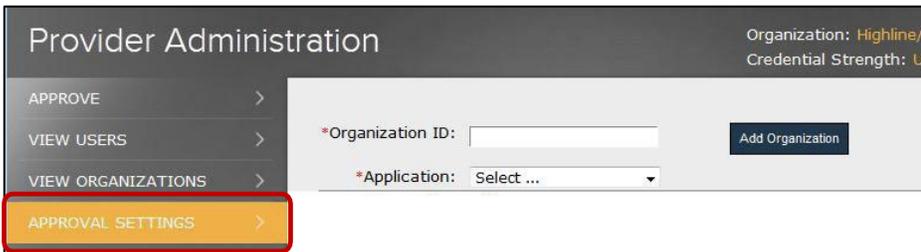
3. To add an organization to the approved list, enter the Organization ID. Select the application you would like to add the Organization to the approved list. Click **Add Organization**.

4. The page will refresh, now showing the organization on the approved list.

   Note: *You may add as many organizations as you wish to the approval list for each application.*

How to Remove an Organization from the Approved List

SP Admins can also remove an organization from the approved list.

1. Login to the Exostar SAM Platform and access the **Provider Administration** tab.
2. Click the **Approval Setting** link.
3. Use the search fields to locate the desired organization.
4. Click the **Remove** link to remove of an organization from the approved list.

Application Settings

The Application Settings page allows SP Admins to view listed applications and determine if **Email Verification (Email OTP)** and **Email Restriction** is turned ON or OFF. Email Verification (Email OTP) and Email Restriction can only be set by Exostar. When the setting displays **True**, the setting is turned ON. When the setting displays **False**, the setting is turned OFF.

Email Verification for Applications

When **Email Verification (Email One Time Password [OTP]** is turned on for an application, users are required to enter a One-Time Password (OTP) code to access an application. Users will receive an email with an OTP code that is required to access the application.

Without the code, users will be unable to access the application. Email OTP is a multi-factor authentication, separate from other security credentials such as Phone OTP, Hardware OTP, or Exostar Mobile ID. Email OTP is used in addition to these security credentials. If using a security credential, you will be asked to enter the additional OTP code for applications that require Email OTP.

Turn On Email Verification for an Application:

1. Contact SAM Support to submit the request.
2. Once Email OTP is turned ON, users will be required to enter an OTP code to access their application.

Turn Off or Turn On Email Verification for an Application:

1. Contact SAM Support to submit your request.
2. Once Email OTP is turned OFF, users will no longer be required to enter an OTP code to access their application.

For instructions on how to access applications when Email Verification is turned ON, please review the Exostar SAM Platform User Guide.

Email Restriction for Applications

If **Email Restriction** is turned ON for an application, SP Administrators can add specific emails (for existing SAM users) and specific domains (for instance, company.com) to allow these users access specific applications. Users, whose email addresses, and domains are not listed here, will not be able to access applications. To add approved email domains and addresses:

1. Open an Exostar online support case requesting to turn on **Email Restriction** for the application. You are notified once the request is completed.
2. From the **Provider Administration** tab, click **Application Settings**.
3. Click the **Application Name** you are adding email restriction to.

4. Enter allowed email domains and/or address in the **Allowed Email Domains and Address field** (for instance, yahoo.com or firstname.lastname@domain.com). You can enter both domain and email address simultaneously. Please use commas to separate information.

NOTE: You will be unable to edit an existing email address for an active user. You will need to enter the modified email addresses or domains as new.

5. Scroll to the bottom of the page and click **Submit**. You will receive a success message.

6. Email addresses or domains that are included in the list will be able to access the application. Allowable email addresses and domains will display in the **Allowable Email Domains** column. You can also view the complete list by clicking the **Application Name**.

7. Email addresses or domains that have not been included will receive an error message when trying to access the application.

The Registration Requests Tab – Organization and Application Administrators

The **Registration Requests** tab lists all pending user requests, including registration requests from new users or requests for access to applications.

1. The **Verify** link will display the list of all self-registered users who are pending Exostar's approval for access to SAM. The Org Admin is responsible for handling these requests.
2. The **Authorize** link will display the list of users who were approved to access SAM but are still waiting for the approval to access their applications. The Application Administrator is responsible for approving these requests. By default, the Application Administrator role is disabled for most applications.

NOTE: The links available may depend upon your admin role. For example, the Org Admin role will not show the Authorize link.

User Access Approvals (Verify Link)

An Organization Administrator will receive email notifications for pending user requests. After verifying user's registration and employment status, follow the steps below to approve self-registered users:

1. Login to Exostar SAM Platform as an Org Admin and navigate to the **Registration Requests** tab. Access the **Verify** link to view the list of pending requests.
2. Click the **Request Id** link for the request you would like to approve.
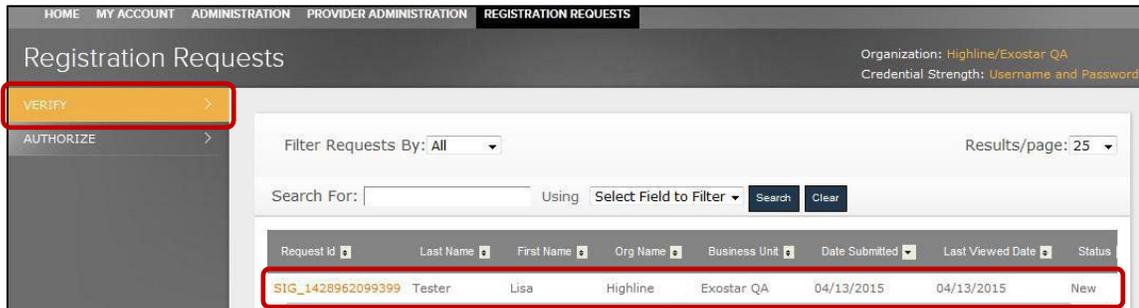
3. Review the **User Registration Request** information, including the **Products & Services** access request. Click **Next.**

4. Complete all required fields and click **Next**.

NOTE: If you select **Deny**, you will be required to enter **Comments** to explain your reasons for denial.

5. The **Confirmation** page will display, confirming the user's active SAM status.

The Adoption Tab – Adoption Administrators

The Adoption Module allows you to invite external companies and external or internal users to use Exostar's Secure Access Manager (SAM). In addition, the Adoption Module allows you to subscribe companies or users to applications or services.

NOTE: You MUST have the Adoption Administrator role to gain access to the adoption module, and this role is granted by Exostar. If during the invitation process you do not see the application or service you are inviting the user or company to, reach out to your Exostar Contact to modify the settings for your account.
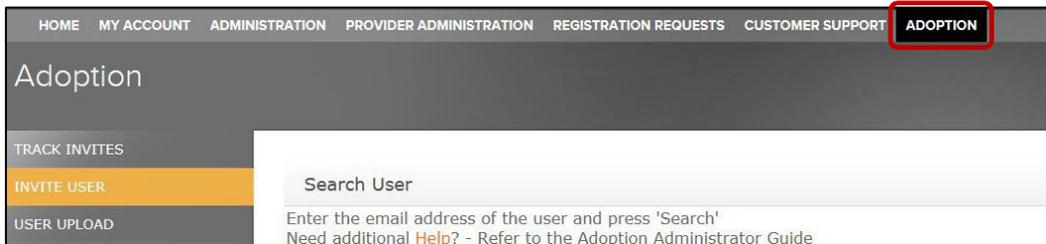
From the Adoption Module, select one of the following workflow options:

- **Track Invites:** allows you to search existing invitations or continue to save invitations.
- **Invite User:** allows you to begin a new invitation for a user or new company.

Invitation Process Overview:

- **Step 1:** Search for the user you would like to invite. If the user exists in the systems, invite the user to the application.
- **Step 2:** If the user is not found, search for the User's organization name and other information, such as address and Exostar ID.
- **Step 3:** If you locate the organization, proceed with inviting the user. If you cannot locate the organization, invite the organization and user.

Search for a User

To begin the invitation process, you <u>MUST</u> first search for the user to ensure the user was not already invited to the applications. To search for a user, you need the user's RFC822 compliant email address. To search for a user:

1. Login to Exostar SAM Platform and access the **Adoption** tab.
2. Click the **Invite User** link.
3. Enter the user's email address and click **Search**.

4. Once the user search is complete, proceed as follows:

   - If the user is found in our system, proceed with [inviting the user to the application](#).
   - If the user is not found in our system, continue with [searching for the organization](#). If the organization is found in the system, add the user to the organization.
   - If the user and the organization are not found in the system, proceed [with adding both the organization and the user](#).

Invite an Existing User

1. Always begin by [searching for the user](#) in the system.
2. Once you searched for and located the user, the search results will show the user's name, Organization information, Exostar SAM Platform account status, and active and pending applications.

3. Select the user account by clicking on the **Last Name** link.

4. The user's profile page will display. Place a check next to the applications you would like to subscribe the user to. Click **Subscribe to Application(s).**

5. The invitation information will display. You can designate a **Subscription Period**, if desired, which enforces a duration period for the account. Click **Submit**.

6. The users will receive a confirmation email.

Add User to an Existing Organization

1. Always begin by [searching for the user](#) in the system.
   If you conducted a search but were unable to locate the user, you should then search for the organization.
2. On the search results pages, click **Search Organization**.

3. Enter the organization information. You can enter the name, Exostar ID, address, etc. Click **Search**.

4. The search results may include one or more organization accounts. If multiple organizations display, select the organization by clicking the **Organization Name**.

5. Select **Add User to Organization.**

6. Enter the user details and select the applications the user should subscribe to.

   Optional: You can enter a subscription period (optional), and a message to include in the email confirmation. Click **Submit Request**.

7. Confirm the invitation information and click **Submit**.

8. A confirmation page displays, and the user will receive an email containing their registration information.

Add a New Organization and User

1. Always begin by searching for the user in the system.
2. If you conducted a search but were unable to locate the user, you then search for the organization.
3. If no organization matches are found, click **Add User to New Organization** to start the invitation process for both the Organization and the User.

4. Verify that no duplicate organizations exist by entering the Organization information and clicking **Check for Duplicates**.

Organization Details

Fill out organization details to first check for duplicate organizations, then if not a duplicate add user to new organization
All field marked with * are required
Need Additional Help?-Refer to the Adoption Administrator Guide

*On-boarding Sponsor : [Select Tenant... ▼]
*Organization Name: [ryan demo]
*Address1 : [ ]
Address2 : [ ]

[Check for Duplicates] [Clear] [Cancel]

5. If no duplicates are found, the page below will display. Verify the organization information.

Organization Details

Review Organization details, Add users, and click 'Submit Request' to complete
Select 'Back' button to edit organization details
Need Additional Help?-Refer to the Adoption Administrator Guide

On-boarding Sponsor : General   Address1 : 123 street
Organization Name: Ryan Demo   Address2 :
DUNS Number :   City : herndon
                                                Country : US
                                                State/Province : US-VA
                                                Zip/Postal code : 20171

6. Select the applications you would like to subscribe the organization to.

Select Application

Select the checkbox next to the applications the user should be subscribed to
At least one application must be selected

Select	Application Name
☐	SecureShare

7. Click **Add User**.

Add User

Click the email address to edit user's information
At least one user with one application must be entered

Email Address	Last Name	First Name	Application

[Add User]

[Back] [Submit Request] [Cancel]

8. Enter the user details. Click **Submit Request**.

9. Enter an optional message to include with the email notification to the user. Click **Submit Request**.

Upon successfully submitting the request, the "Invitation Success" message will display. The user will receive an email invitation containing a registration link.

User Upload

Adoption Administrators can subscribe multiple users from a single organization to one or more applications via a .csv file upload. If an Adoption Administrator subscribes users to applications that their organization is *not* subscribed to, the organization will be automatically subscribed to these applications after the fact of the upload. Before the users of an OMO (Organization Managed Organization) can access these applications, their Org Admin must accept Terms and Conditions for the applications. This requirement does not apply to SMOs (Sponsor-Managed Organizations).

Bulk Upload allows Adoption Administrators to add:

- New users to a new organization
- New users to an existing organization
- Existing users to a new organization
- Existing users to an existing organization

To Complete Upload:

1. From the Adoption tab, click **User Upload**.
2. Complete the template. Please see [Appendix B – CSV File Requirements – User Uploads for Adoption Administrators](#) for template requirements.
3. Once the template is complete, save it as a .CSV file.
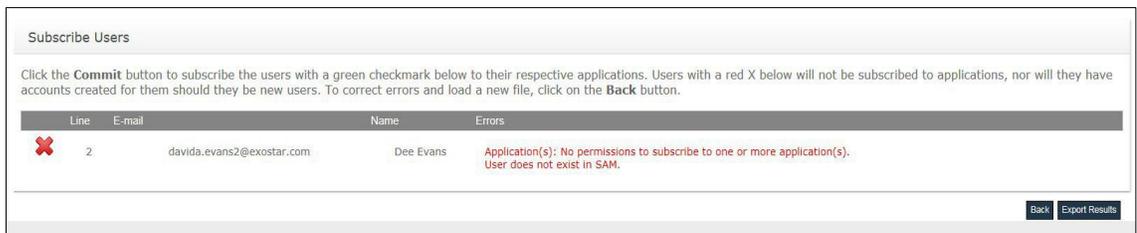4. Click **Pick a file**, and then click **Upload**. The uploaded file name will display.
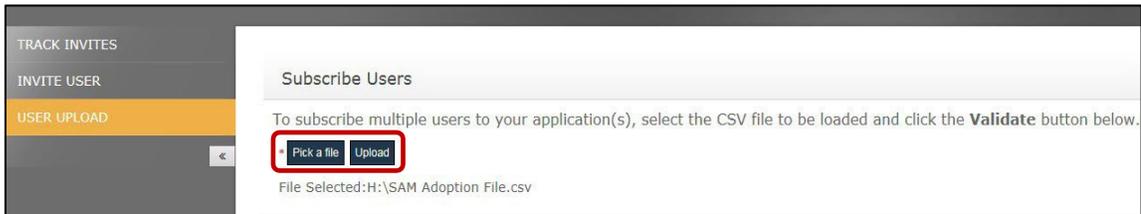
5. Click **Validate**. If the file contains errors, errors will display. You will need to correct the errors, and to re-upload the file.

NOTE: You can only subscribe users for applications that you are a SP Administrator for. If you attempt to subscribe them for an application that your organization is not subscribed to, you will receive an error message.

6. If there are no issues, you will receive a green check mark. Click **Search Organizations** to locate the organization that you are adding users to or create a new organization.
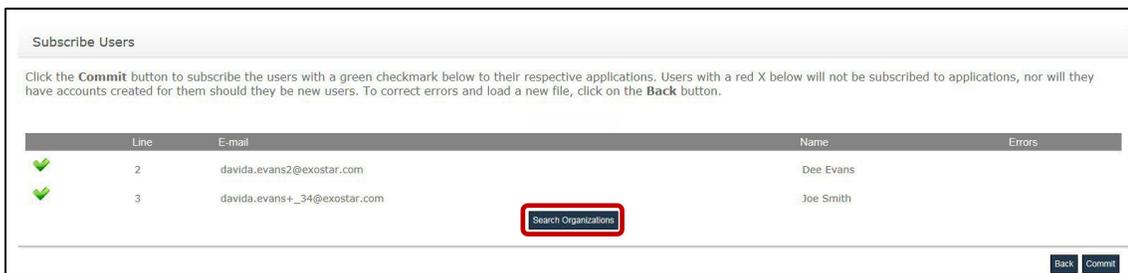
7. If you find the organization, click the **Organization Name** to add users to an existing organization. If the organization does not exist, click [Add User(s) to New Organization](#).

8. In the new screen, click **Add Users to Organization**.

9. Review the list of users and click **Commit to complete**.

10. Existing users are now subscribed to the application(s). New users will receive the activation email to activate their account.

11. If no matches are found after completing an organization search and you are certain that there are no duplicates, click **Add User(s) to New Organization**.

12. Select required fields (marked with an *) and click **Check for Duplicates**.

13. If no duplicates are found, organization details will display. Click **Confirm**, and then click **Commit**. Existing users are now subscribed to the application(s). New users will receive the activation email to activate their account.

NOTE: If a match is found, click the organization name to add user to the organization. If this is not a duplicate, click **Ignore Duplicate and Request New Organization**. New users will receive the activation email to register their organization.

How to Track Invitations

You can search for the previously sent invitations by using the **Track Invites** option.

1. Log into the Exostar SAM Platform and access the **Adoption Module**.
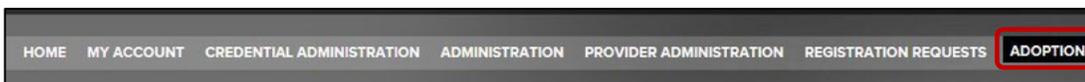
2. Click the **Track Invites** link.
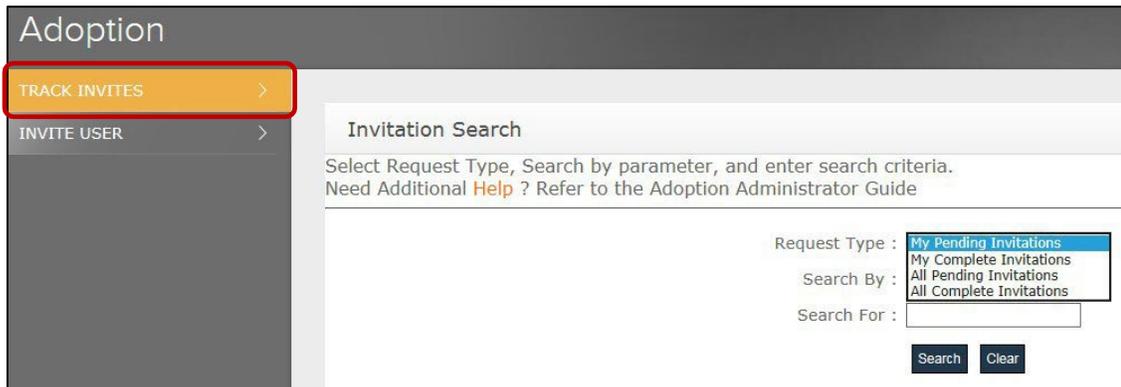
3. Select the desired **Request Type** from the dropdown menu. **Request Type** options include:
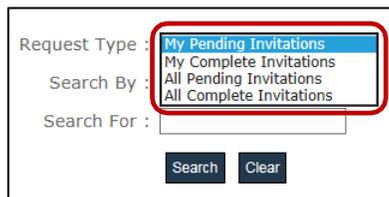
- **My Pending Invitations:** All unaccepted invitations issued by the Administrator.
- **My Complete Invitations:** All accepted invitations issued by the Administrator.
- **All Pending Invitations:** If there are multiple adoption administrators, then this will show all in-progress invitations.
- **All Complete invitations:** Accepted invitations by all adoption administrators.

4. Select the desired **Search By** criteria. Search criteria options include:

- Email Address of invitee
- First Name of Adoption Administrator
- Last Name of Adoption Administrator
- Date the request was issued
- Date the request was completed (not available for Pending requests)
- External Organization ID
- External User ID
- Exostar ID

NOTE: By default, only the invitations completed within the past 60 days will display. To search for older invitations, use the **Date Requested** or **Date Completed** search criteria.

5. Click **Search**.

6. The search results will display. Click the **Request ID** link to obtain information about the request, including username, user ID, email address, organization information, adoption administrator who invited the user, dates submitted and completed, and the status of the invitation.

ORGANIZATION REGISTRATION OVERVIEW

During the registration process, organizations provide their organization details and designate individuals to serve in administrative roles. Please note that these roles can be assigned to multiple or a single individual within your organization.

- **Organization Administrator**: is responsible for creating and managing users in your organization, approving user self-registrations, and maintaining the vendor profile information.
- **Company Contact**: can be the same person as your Organization Administrator or another person within the organization. The company contact is responsible for managing relations with Secure Access Manager (SAM) Platform partners.

New Organization Registration

The registration of a new organization in SAM consists of three stages:

- Entering the Organization Information
- Subscribing to Products and Services
- Providing the Administrator(s) Information

Organization Registration

STEP 1 — Organization Information → STEP 2 — Products & Services → STEP 3 — Administrator(s) Information

To begin, enter your organization information:

1. Open your Internet Explorer browser and access the organization registration page via the following link https://secureaccess.exostar.com/orgRegistration.

2. Fill out the required information in the Organization Information section.

Organization Information

* Individual-Level Organization? ☐
* Onboarding Sponsor: General
* Organization Name: testing
Business Unit:
* Organization's HQ/Country of Incorporation: UNITED STATES
TaxID (US Only):
DUNS #:
Is your organization certified as a Small Disadvantaged Business in the SB PRO-Net Database? (US Only): ○ Yes ○ No

* Address 1: 123 exostar
Address 2:
* City: herndon
* Country: UNITED STATES
* State/Province: Virginia
Zip/Postal Code:

3. Fill out the required information in the Organization Administrator section.

Organization Administrator

Title: Select...
* First Name:
Middle Name:
* Last Name:
Suffix:
Sponsor E-mail Address:
Job Title:
* Timezone: Select...

* Phone:
Fax:
* E-mail:
* Confirm E-mail Address:
* Address 1:
Address 2:
* City:
* Country: Select...
* State/Province:
Zip/Postal Code:

NOTE: User login instructions will be sent to the provided email address.

4. Complete the Company Contact information. Click **Next** to continue.

   NOTE: If the Organization Administrator will also act as the Company Contact, select **Same as Organization Administrator.**
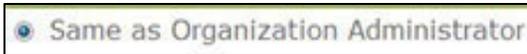
5. Select the desired product(s) from the list provided on the Products and Services page. Click **Next**.

NOTE: Publicly available applications will display. If you need to access applications available by invitation only, please contact Exostar SAM Support to have applications added.

6. Designate the Application Administrator for each selected product. The Application Administrator will be responsible for managing and approving user access to their applications. However, for most applications the Application Administrator role is disabled by default.

The Application Administrator can be the same as the Organization Administrator.

7. If "*Same as… (Organization Administrator)*" is selected, the user information will be pre-populated. Click **Next** to complete the new organization registration.

If "Other" is selected, complete the required fields to designate the Administrator. Click **Next** to complete the new organization registration.

8. You will receive a **Submission Confirmation** page, containing the reference number for your registration request.

Email Confirmations

Throughout the process of registration, you will be receiving email confirmations for the various steps of registration and approval. Depending on your administrative role, you will receive all or some of the below emails:

1. **Organization Registration – Submitted to Secure Access Manager:** You will receive this email immediately after submitting your registration request, along with the reference number for your record.
2. **Account Registration – Accepted in Secure Access Manager:** The Organization Administrator will receive this email when the organization's registration request is approved. This email will contain the important login information.
3. **Secure Access Manager Point of Contact – Organization Registration Approved:** The designated Point of Contact will receive this confirmation when the organization account is approved.

Accept Terms and Conditions

Organization and Management & Portal Administrators will complete the Acceptance of Terms and Conditions for all subscribed applications. Follow the steps below to accept Terms and Conditions:

1. Login to the Exostar SAM Platform at https://secureaccess.exostar.com.
2. Navigate to the Home page. The **View Service Agreement** link will display next to the application(s). Click **View Service Agreement**.
3. After reviewing the Agreement, click **I Agree** to accept it. You will receive the Service Confirmation message:

> You have successfully accepted the service agreement. You should receive an email shortly.

NEXT STEPS

Once the Organization Registration has been completed, the Organization Administrator will be responsible for managing the organization's SAM users. Below is the list of tasks that are the responsibility of an Org Admin:

- Viewing and managing user accounts
- Adding new users
- Authorizing user access
- Deleting/suspending users
- Viewing organization details

- Subscribing organization to new applications

For more information on SAM, go to https://www.myexostar.com/

APPENDIX A – CSV FILE REQUIREMENTS – USER UPLOADS

Field	Cardinality/ Values	Response/Comments
Subscription Period	*Optional*	Acceptable Options: #y#t#d#h#m#s e.g., 1y = 1 Year, 1y1t = 1 year + 1 month Leaving this value blank will default to the Application Maximum Subscription Duration (if provided)
Honorific	*Optional*	Acceptable options: Mr., Mrs., Ms., Dr.
Last Name	**Required** Max 50 characters	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Middle Name	*Optional* *Max 50 characters*	Accepts letters, numbers, and printable special characters except for '<' or '>'.
First Name	**Required** Max 50 characters	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Job Title	*Optional* *Max 75 characters*	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Email Address	**Required** RFC822 compliant	Must be unique
Phone	**Required** Min 4 characters /Max 40 characters	Accepts only the following characters: Numbers, '-', '+', '.', '(', ')', 'e', 't', 'x' and embedded white spaces
Fax	*Optional* *Min 4 characters / Max 40 characters*	Accepts only the following characters: Numbers, '-', '+', '.', '(', ')', 'e', 't', 'x' and embedded white spaces
Street Address 1	**Required** Max 200 characters	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Street Address 2	*Optional* *Max 100 characters*	Accepts letters, numbers, and printable special characters except for '<' or '>'.
City	**Required** Max 52 characters	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Zip/Postal Code	*Optional* *Max 30 characters*	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Region Code	**Required**	Accepts letters, numbers, and printable special characters except for '<' or '>'.

Country	**Required**	Must be in the form of ISO 3166-1 Alpha-2 Code (i.e., United States = US)
Applications	**Required**	Multiple applications must be separated by a semicolon ';' Organization must be subscribed to the listed application(s)
Application Admin	*Optional*	Multiple applications must be separated by a semicolon ';' User will be assigned the application administrator role for application(s) listed in the column Organization must be subscribed to the application(s) listed
Role	**Required**	User or Admin User will be assigned the organization administrator role if 'Admin' is listed in the column
R-IDP User ID	*Optional*	R-IDP User ID must be unique for the associated R-IDP Organization must be associated to an R-IDP Note: For Merck, the R-IDP User ID and the ISID are the same thing.
Suffix	*Optional*	4 Char Limit
Sponsor Email Address	*Optional* RFC822 compliant	75 Char Limit

EXOSTAR®

Field	Cardinality/ Values	Response/Comments
Last Name	**Required** Max 32 characters	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Middle Name	*Optional Max 32 characters*	Accepts letters, numbers, and printable special characters except for '<' or '>'.
First Name	**Required** Max 32 characters	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Job Title	*Optional Max 50 characters*	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Email Address	**Required** RFC822 compliant	Must be unique
Phone	**Required** Min 4 characters /Max 20 characters	Accepts only the following characters: Numbers, '-', '+', '.', '(', ')', 'e', 't', 'x' and embedded white spaces
Fax	*Optional Min 4 characters / Max 20 characters*	Accepts only the following characters: Numbers, '-', '+', '.', '(', ')', 'e', 't', 'x' and embedded white spaces
Street Address 1	**Required** Max 64 characters	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Street Address 2	*Optional Max 64 characters*	Accepts letters, numbers, and printable special characters except for '<' or '>'.
City	**Required** Max 52 characters	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Zip/Postal Code	**Required** Max 16 characters	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Region Code	**Required**	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Password	**Required**	
State / Province	*Optional*	
Country	**Required**	Must be in the form of ISO 3166-1 Alpha-2 Code (i.e., United States = US)
Applications	**Required**	Multiple applications must be separated by a semicolon ';' Organization must be subscribed to the listed application(s)

		Multiple applications must be separated by a semicolon ';' User will be assigned the application administrator role for application(s) listed in the column
Application Admin	*Optional*	Organization must be subscribed to the application(s) listed
Role	**Required**	User or Admin User will be assigned the organization administrator role if 'Admin' is listed in the column
R-IDP User ID	*Optional*	R-IDP User ID must be unique for the associated R-IDP Organization must be associated to an R-IDP *Note for Merck: the R-IDP User ID and the ISID are the same thing.*
Suffix	*Optional*	4 Character Limit
Sponsor	**Required**	
Honorific (Title such as Dr.)	*Optional*	Acceptable options: Mr., Mrs., Ms., Dr.
Subscription Period	*Optional*	Acceptable Options: #y#t#d#h#m#s e.g., 1y = 1 Year, 1y1t = 1 year + 1 month Leaving this value blank will default to the Application Maximum Subscription Duration (if provided)

APPENDIX C – CSV FILE REQUIREMENTS – BATCH SUBSCRIPTION/ OTP

Field	Cardinality/Values	Response/Comments
User ID	**Required**	Accepts approved users with valid User ID
Subscription Period	*Optional*	Acceptable Options: #y#t#d#h#m#s e.g., 1y = 1 Year, 1y1t = 1 year + 1 month Leaving this value blank will default to the Application Maximum Subscription Duration (if provided)