



SAM Administrator Guide

March 2026



Table of Contents

Introduction.....	3
Application Overview.....	3
Administrator Roles	3
Organization Administrator.....	4
Service Provider Administrator.....	4
Adoption Administrator	4
Credential Administrator	4
Management & Portal Administrator	4
Exostar Portal Administrator	5
Types of Organizations	5
Organization-Managed Organization	5
Exostar-Managed Organization	6
Sponsor-Managed Organization	6
Shared Users	7
SAM Portal Navigation.....	7
Login to SAM Portal.....	8
Administration Tabs.....	10
Credential Administration Tab	10
Approve Token Request.....	10
Cancel Token Request	12
Deny Token Request	13
SOTP Client Administrators	15
Administration Tab – Organization Administrators.....	15
View Users.....	16
Add New Users.....	18
Add Users Bulk Upload.....	19
Update Organization.....	21
Resend Activation Email.....	22
Modify Application Access	22
Reset Permanent Password	23
Reset Security Questions.....	24

Suspend or Delete User	25
Subscribe to Application	25
Update Organization Allowed Emails	27
Batch Subscription – Bulk User Upload.....	28
Bulk Actions.....	28
Service Provider Admins: Provider Administration tab.....	31
Approve Users.....	32
Approve User Requests	33
Suspend User Subscription	34
Reactivate User’s Subscription	35
Resend Activation Email	35
Resend User Provisioning Record	36
View Organizations.....	37
Suspend Organization’s Access.....	38
Reactivate Organization’s Access.....	39
Approval Settings.....	39
Remove Organization Approved List.....	40
Application Settings.....	41
Email Verification Settings	41
Email Restrictions.....	42
Registration Requests.....	43
Adoption Administrators	45
Invitation Process	45
Invite the User.....	46
Add User to Existing Organization	47
Add New User and Organization	49
Adoption Admin – User Upload	52
Track Invitations	55
Appendix A: CSV Requirements – User Upload.....	57
Appendix B: CSV File Requirements: User Uploads – Adoption Administrators.....	58

Introduction

This role-based guide covers the primary actions performed specifically by users with the SAM Organization Administrator role. For a more comprehensive guide, please reference *Exostar's Secure Access Manager (SAM) User Guide* from the [SAM Training Resources](#) page.

Application Overview

Exostar's [Secure Access Manager \(SAM\)](#) Platform 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 the 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 Platform Features:

- Our platform extends the basic concept of web-based Single-Sign-On (SSO) to support the single sign-on location to multiple applications.
- It supports authentication credentials of varying assurance levels.
- It facilitates an organizational approach to registration, account management, and application access.
- It provides organizations with tools to add new users and grant access to applications.

Administrator Roles

All new SAM accounts are created as *general user accounts*. Later, these accounts can be updated to be Administrator 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 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, which 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

Types of 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 (OMO)** 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 (EMO)** 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

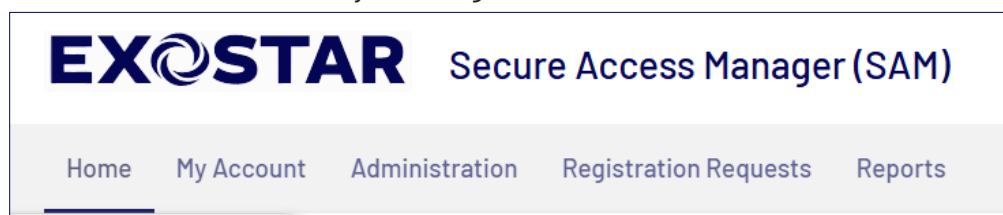
Users who are under a Sponsor-Managed Organization (SMO) have the ability to become Shared Users. Shared Users can access applications outside of their sponsored organization. Once users become shared, they will need to accept Terms and Conditions for the first application belonging to a different sponsor. 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)

SAM Portal Navigation

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**, **Registration Requests**, and **Reports** 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.

Login to SAM 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 SAM portal by following the steps below.

1. Login to SAM - <https://secureaccess.exostar.com>
2. Enter your **Email/User ID**. Click **Next**.
3. Then enter your **Password** and click **Next**.

EXOSTAR Secure Access Manager (SAM)

Step 1/2: Email Address / User ID

Login

Enter your Email Address or User ID

Email Address or User ID

Use the Email or User ID registered with your Exostar account

[Need help?](#) NEXT

Unauthorized access to this system may constitute a criminal offense.

EXOSTAR Secure Access Manager (SAM)

Step 2/2: Password

Password

training@exostar.com

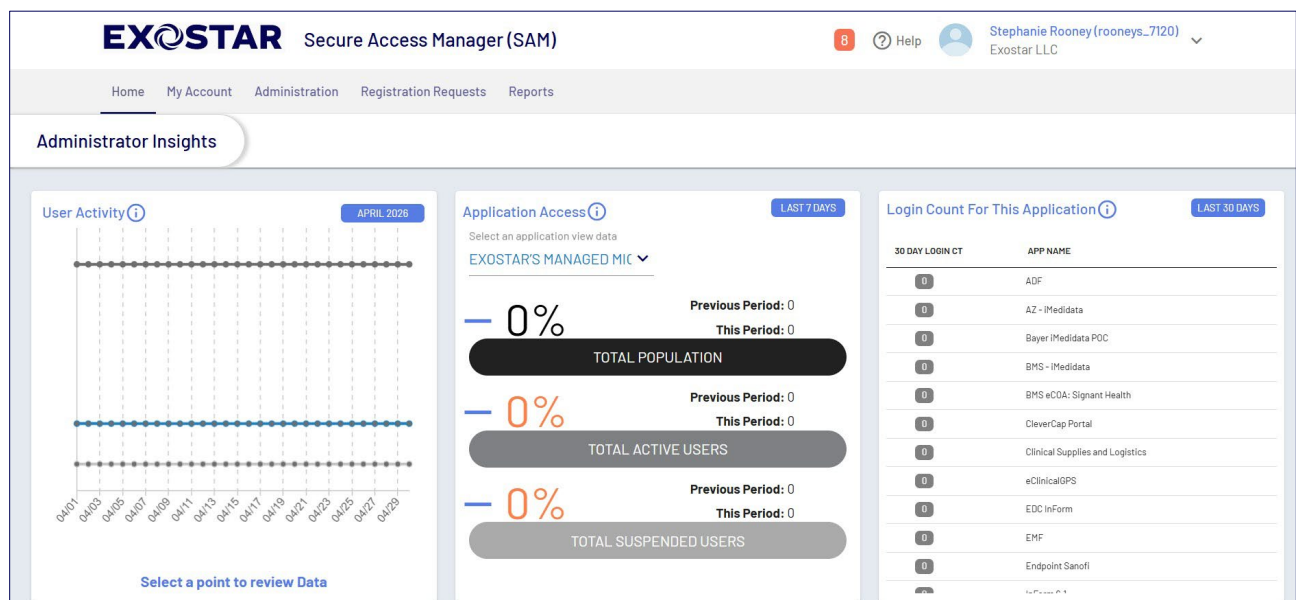
Enter your Password

Password

[Use a different Email or User ID](#) [Forgot Password?](#) NEXT

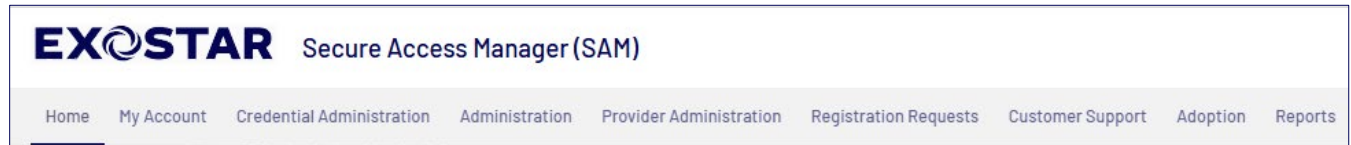
4. Once you successfully logged in, the Home Dashboard will display.

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.



Administration Tabs

Once you 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: Administration, Credential Administration, Provider Administration, Registration Requests, Adoption, and Report.



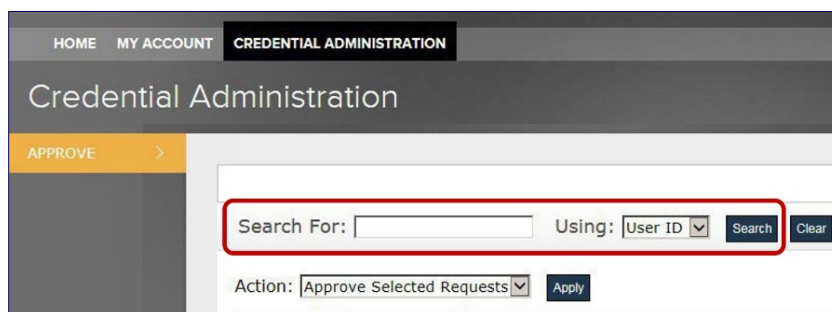
Credential Administration Tab

The **Credential Administration** tab is for Credential and SOTP Client Administrators. This is 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.

When you first select the **Credential Administration** tab, you will be prompted to submit a request for a for a Multi-Factor Authentication token.

Approve Token Request

1. Login to SAM Portal at: <https://secureaccess.exostar.com>
2. Then select the **Credential Administration** tab.
3. Use the search filters (*search by User ID or Email Address*) to locate a specific request. Click **Search**.



- Place a **checkmark** next to the *Request ID* you would like to make a change to.

OTP Requests				
Select	Request ID	User ID	Last Name	First Name
☐	HWOTPRQ_1238159036_1490986785256	bhanuril_4548@securepass.exostartest.com	bhanuri	laxmi
☒	HWOTPRQ_1170408125_1496420273361	bhanuril_7627@securepass.exostartest.com	bhanuri	laxmi

NOTE: You can only select or make changes to *Pending* requests.

- Select **Approve Selected Requests** from the **Action** menu. Then click **Apply**.

Search For: Using: User ID Search Clear

Action: Select Action
Approve Selected Requests
Deny Selected Requests
Cancel Selected Requests
Apply

- You will receive confirmation that the action has been completed.

HOME MY ACCOUNT **CREDENTIAL ADMINISTRATION**

Credential Administration

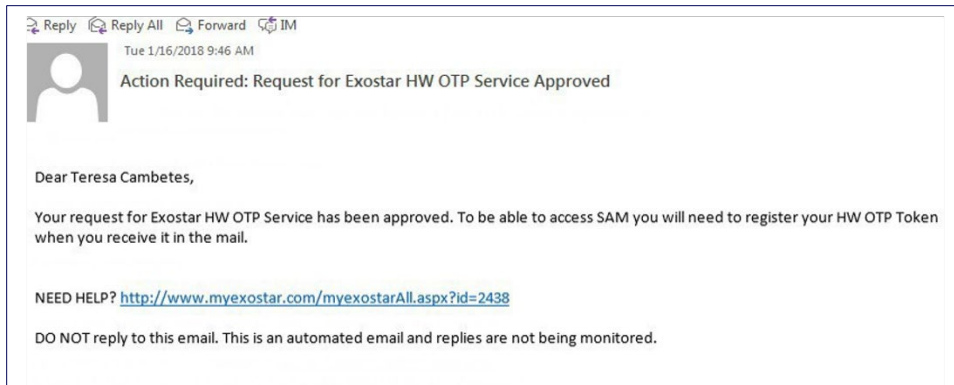
APPROVE >

1 requests have been approved.

Search For: Using: User ID Search Clear

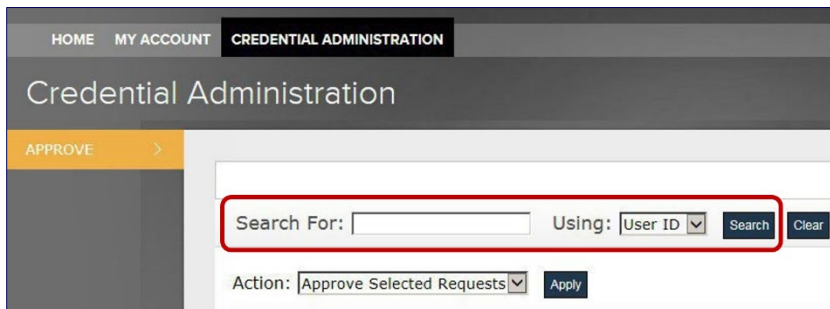
Action: Approve Selected Requests Apply

- The system will also generate an email to the user informing them that their OTP request was approved.



Cancel Token Request

1. Login to SAM Portal at: <https://secureaccess.exostar.com>
2. Then select the **Credential Administration** tab.
3. Use the search filters (*search by User ID or Email Address*) to locate a specific request. Click **Search**.

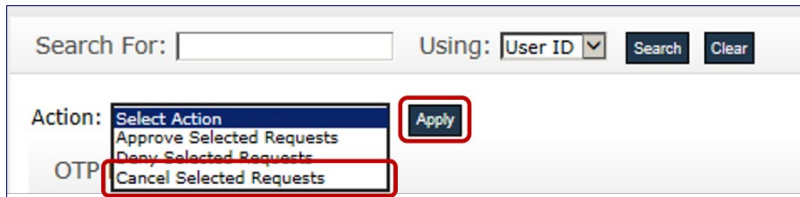


4. Place a **checkmark** next to the *Request ID* you would like to make a change to.

OTP Requests					
Select	Request ID	User ID	Last Name	First Name	
☐	HWOTPRQ_1238159036_1490986785256	bhanuril_4548@securepass.exostartest.com	bhanuri	laxmi	
☒	HWOTPRQ_1170408125_1496420273361	bhanuril_7627@securepass.exostartest.com	bhanuri	laxmi	

NOTE: You can only select or make changes to *Pending* requests.

5. Select **Cancel Selected Requests** from the **Action** menu. Then click **Apply**.

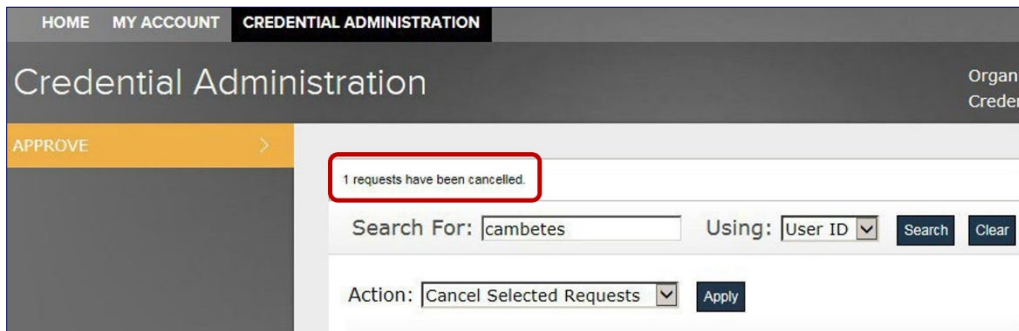


Search For: Using: User ID Search Clear

Action: Select Action
Approve Selected Requests
Deny Selected Requests
Cancel Selected Requests

OTP Apply

- You will receive confirmation that the action has been canceled.



HOME MY ACCOUNT **CREDENTIAL ADMINISTRATION**

Credential Administration

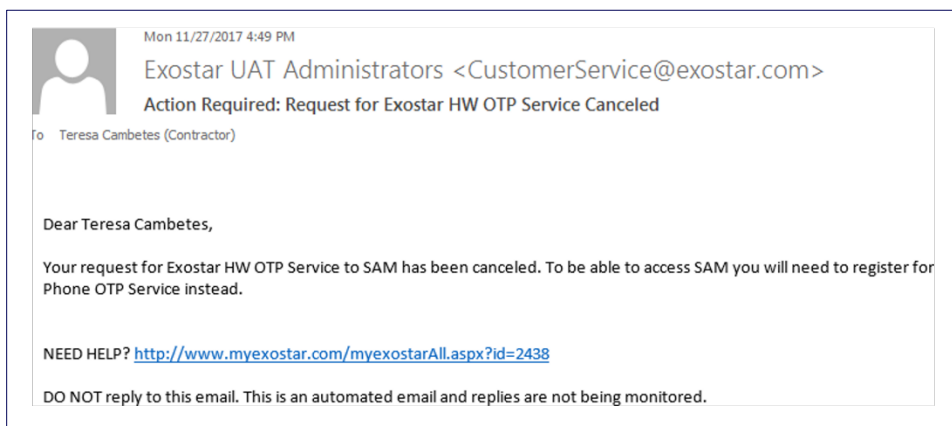
APPROVE >

1 requests have been cancelled.

Search For: cambetes Using: User ID Search Clear

Action: Cancel Selected Requests Apply

- The system will also generate an email to the user informing them that their OTP request was canceled.



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.

Deny Token Request

- Login to SAM Portal at: <https://secureaccess.exostar.com>
- Then select the **Credential Administration** tab.
- Use the search filters (search by User ID or Email Address) to locate a specific request. Click **Search**.

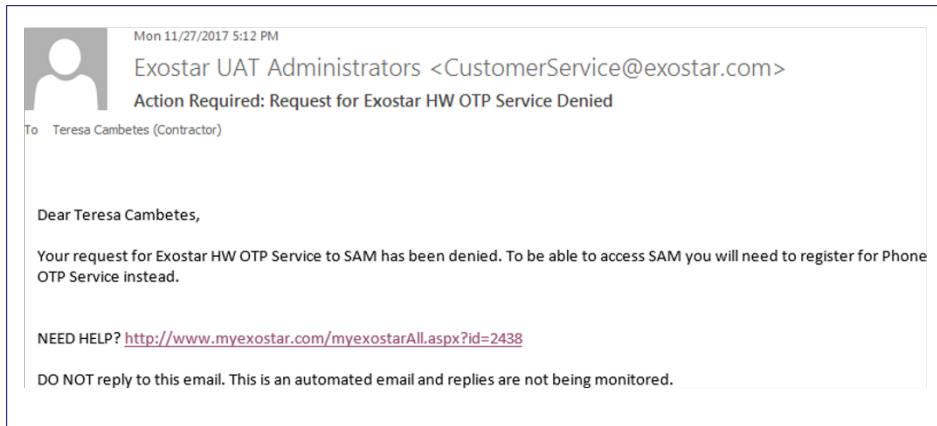
- Place a **checkmark** next to the *Request ID* you would like to make a change to.

OTP Requests					
Select	Request ID	User ID	Last Name	First Name	
☐	HWOTPRQ_1238159036_1490986785256	bhanuril_4548@securepass.exostartest.com	bhanuri	laxmi	
☒	HWOTPRQ_1170408125_1496420273361	bhanuril_7627@securepass.exostartest.com	bhanuri	laxmi	

NOTE: You can only select or make changes to *Pending* requests.

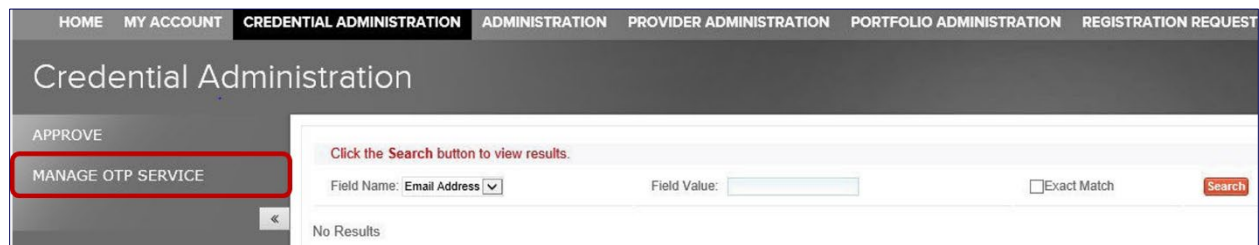
- Select **Deny Selected Requests** from the **Action** menu. Then click **Apply**.

- You will receive confirmation that the action has been denied.
- The system will also generate an email to the user informing them that their OTP request was denied.



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.

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.

Administration

Organization: Exostar LLC
Credential Strength: Userna

VIEW USERS

ADD NEW USER

SUBSCRIBE TO APPLICATION

USER UPLOAD

UPDATE ORGANIZATION

BATCH SUBSCRIPTION

BATCH ACTIVATION EMAIL

BULK ACTIONS

Click the Search button to view results.

Last Name Search term... Search Clear

Set Columns Results Per Page

User ID	Last Name	First Name	Email Address	Organization ID
zhou3l_9062	Zhou3	Lisa3	lisa.qaTest@	exostar
zhou1030l_5574	Zhou1030	Lisa1030	lisa.zhou+_1030	exostar
zhou1l_2982	Zhou1	Lisa1	lisa.zhou1@	exostar
zhou0720l_7157	Zhou0720	Lisa0720	lisa.zhou+	exostar

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

The **View Users** sub-tab allows you to view users associated with your organization's account. To View Users:

1. Select the **Administration** tab, you will be prompted to **Authenticate** your account.
2. Enter the **Verification Code** you received via email, then click **Next**.
3. Once you are authenticated, then select the **View Users** sub-tab.
4. You can search for a specific user or click **Search** to view all users.
5. The search results will display. Click the **hyperlink User ID** to view the user's details.

Administration

Organization: Exostar LLC
Credential Strength: Username and Password

Click the Search button to view results.

Last Name: test Search Clear

Set Columns Results Per Page: 25

User ID	Last Name	First Name	Email Address	Organization ID	Organization Name
testerj_6120	Tester	Joe	ryan.wick+_11819@exostar.com	exostar	Exostar LLC
testa_9066	test	a	saleha.ali+_01@exostar.com	exostar	Exostar LLC
test7u_0494	Test7	User7	user7@partner.qa1multi1.com	exostar	Exostar LLC
testt_2342	Test	Training	training@exostar.com	exostar	Exostar LLC
testt_7796	Test	Thanigai	venu.movva_786673@exostar.com	exostar	Exostar LLC

6. You can make edits to the user's profile, including the following options:

- Request Access to applications
- Change the Role
- Reset Permanent Password or Security Questions
- Suspend or Delete User

User Profile

User ID: testt_2342 Phone: 703-123-0500

E-mail: training@exostar.com Fax:

Modify E-mail

Role: User Street Address 1: 2325 Dulles Corner Boulevard

Organization: Exostar LLC Street Address 2: Ste 600

Name: City: Herndon

Organization ID: exostar Country: UNITED STATES

Onboarding Sponsor: General State: Virginia

Title: Select... Zip/Postal Code: 20171-4065

First Name: Training Time Zone: GMT

Middle Name: Restricted Access: On Off

Last Name: Test Created Date: 03/11/2026 19:14 PM GMT

Suffix: Suspended Date: N/A

Job Title: From SAM: Last Access Date: 06/03/2026 16:11 PM GMT

Application Settings

Role: User

Application Access:	Provider	Application	Expiration Date	Last Access Date	Status	Action
	Exostar	SAM Service Access Manager			Pending Approval by the Application Owner	
	Exostar	Exostar's Managed Microsoft 365			Inactive	Request Access
	Referral Management	BMS Trial Bee - Honey			Inactive	Request Access

Status: Active

[Suspend User Access](#) [Reset Permanent Password](#) [Reset Security Question](#) [Delete User](#)

[Continue](#)

- If you make any changes to the user's profile, click **Continue** at the bottom of the page and then **Submit** to save your changes.

Add New Users

Organization Admins and MPAs can add new users in SAM by adding user's one at a time or bulk user upload. User's can also user 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 (Individual)

Organization Administrators can add new users one at a time by filling out the user profile and application information. To add a new user:

- In the SAM portal click on the **Administration** tab, you will be prompted to **Authenticate** your account.
- Enter the **Verification Code** you received via email, then click **Next**.
- Once you are authenticated, then select **Add New User** sub-tab.
- Enter the user's information in the **required fields** (marked with an asterisk *).

5. Then scroll down and select the user's **role** (user or admin).
6. Next place a **checkmark** next to the application(s) they will need access to and make sure to enter a subscription period (a minimum of 60 days).
7. Then click **Continue**. Review and verify the information is correct, then click **Submit**. (If you need to make any changes to the user's information, click *Modify*).

Application Access	Select	Subscription Period
Org Admin	☐	Years Months Days <i>i</i>
Application Admin	☐	Years Months Days <i>i</i>
Org Admin & Application Admin	☐	Years Months Days <i>i</i>
Merck	☐	Years Months Days <i>i</i>
Merck Veeva Vault	☐	Years Months Days <i>i</i>
Exostar LLC	☐	Years Months Days <i>i</i>
SecureShare	☐	Years Months Days <i>i</i>

An email will be sent to the new user to activate their account. Administrators will also receive an email confirming a new user was added to the organization.

Add Users Bulk 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 A** 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** sub-tab.
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**.

The screenshot shows the Exostar Administration interface. The top navigation bar includes 'HOME', 'MY ACCOUNT', 'ADMINISTRATION' (highlighted with a red box), 'REGISTRATION REQUESTS', and 'REPORTS'. The 'ADMINISTRATION' section has a sidebar with options: 'VIEW USERS', 'ADD NEW USER', 'SUBSCRIBE TO APPLICATION', 'USER UPLOAD' (highlighted with a red box), 'UPDATE ORGANIZATION', 'BATCH SUBSCRIPTION', 'BATCH ACTIVATION EMAIL', and 'BULK ACTIONS'. The main content area is titled 'Load Users' and contains instructions: 'To upload new users to this organization, select the CSV file to be loaded and click the **Validate** button *Required below.' Below the instructions are two buttons: 'Pick a file' (highlighted with a red box) and 'Upload' (highlighted with a red box). The 'File Selected' status shows 'No file selected'. There is a dropdown menu for 'Onboarding Sponsor' set to 'General' and a checkbox for 'Defer E-mails'. At the bottom right, there are 'Validate' and 'Clear Uploaded File' buttons.

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.
6. Click **Commit** to upload the users.

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 from allowing them 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 restricted domain(s), follow the steps below:

1. Click the **Administration** tab, then select click **Update Organization** sub-tab.
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.

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**.

Application Settings						
Role: User						
Application Access:						
Provider	Application	Expiration Date	Last Access Date	Status	Action	
Test Service Provider	Test Service Provider			Active	Edit	Suspend
EngageZone	EngageZone.msd.com			Inactive	Request Access	
Exostar LLC	SecureShare			Inactive	Request Access	
Exostar LLC	SecureShare - MD Anderson			Inactive	Request Access	

Status: User Inactive [Resend Activation Email](#) [Delete User](#)

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

Modify Application Access

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
- 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.

1. Locate the user's profile and click on their name to edit their details.
2. The Org Admin can **Suspend**, **Edit**, and **Reactivate** a user's access to an application.
3. Click **Suspend** next to the application to suspend access to it.
4. Click **Edit** to modify the subscription period for the application.
5. Click **Delete** to remove a user's access to the application.

- Click **Continue**. A confirmation page will be displayed. The user's status will change to **Inactive**.

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

- 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

- A confirmation page will be displayed.

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.

Reset Permanent Password

Organization Admins can reset a user's permanent password and reset security questions.

To reset a user's permanent password:

- Locate the user's profile and click on their name to edit their details.
- Scroll down to the Application Settings and click **Reset Permanent Password** button.

Application Settings

Role: User

Application Access:

Provider	Application	Expiration Date	Last Access Date	Status	Action
Exostar	SAM Service Access Manager			Pending Approval by the Application Owner	

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

- The user will receive an email with instructions on how to reset the permanent password.

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 a user's permanent password or resend the activation email.

Reset Security Questions

- Locate the user's profile and click on their name to edit their details.
- Scroll down to the Application Settings and click **Reset Security Questions** button.

Application Settings

Role: User

Application Access:

Provider	Application	Expiration Date	Last Access Date	Status	Action
Exostar	SAM Service Access Manager			Pending Approval by the Application Owner	

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

- The user will receive an email with instructions on how to reset their security questions.

Suspend or Delete User

Organization Admins can suspend or delete a user from the SAM platform. To suspend or delete a user:

1. Locate the user's profile and click on their name to edit their details.
2. Scroll down to the Application Settings and click **Suspend User Access** to suspend a user's access. To delete a user's account, click **Delete User** to permanently remove a user from SAM.

The screenshot shows the 'Application Settings' interface. At the top, there is a 'Role:' dropdown menu set to 'User'. Below this, a table lists application access details. The table has columns for 'Provider', 'Application', 'Expiration Date', 'Last Access Date', 'Status', and 'Action'. One entry is visible for 'Exostar' with the application 'SAM Service Access Manager' and a status of 'Pending Approval by the Application Owner'. At the bottom, the 'Status' is 'Active', and there are four buttons: 'Suspend User Access', 'Reset Permanent Password', 'Reset Security Question', and 'Delete User'. The 'Suspend User Access' and 'Delete User' buttons are highlighted with red rectangles.

Application Access:	Provider	Application	Expiration Date	Last Access Date	Status	Action
	Exostar	SAM Service Access Manager			Pending Approval by the Application Owner	

Status: Active

Suspend User Access **Reset Permanent Password** **Reset Security Question** **Delete User**

3. A confirmation page will be displayed.

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

Subscribe to Application

Organization Admins can subscribe their organizations to an application in the SAM portal. Please note, most applications are *invitation-only* and *require* the Exostar EPA to complete the subscription.

To subscribe your organization to an application:

1. Select the **Administration** tab. Then select **Subscribe to Application** sub-tab.
2. Find the application you want to subscribe to, then click the **Subscribe to Application** button.

The screenshot shows the 'Administration' section of the Exostar web application. The navigation bar includes 'HOME', 'MY ACCOUNT', 'ADMINISTRATION' (selected), 'REGISTRATION REQUESTS', and 'REPORTS'. On the right, it displays 'Organization: Exostar LLC' and 'Credential Strength: Username and Password'. The left sidebar contains links: 'VIEW USERS', 'ADD NEW USER', 'SUBSCRIBE TO APPLICATION' (highlighted with a red box), 'USER UPLOAD', and 'UPDATE ORGANIZATION'. The main content area is titled 'Subscribe to Application' and contains a table with the following data:

Company	Application	Action
Greenphire Inc	ClinCard	Subscribe to Application (highlighted with a red box)

- Next complete the Administrator information page. You can choose an *existing administrator* from the drop-down list or add a *new administrator*. Then click **Next**.

The screenshot shows the 'Administrator' information page. It includes a section titled 'Roles and Responsibilities' explaining the role of an Application Administrator. Below this, there is a form to select an administrator from a dropdown menu (currently set to 'Other'). The form also contains various input fields for personal and contact information, including Title, First Name, Middle Name, Last Name, Suffix, Sponsor E-mail Address, Job Title, Timezone, Phone, Fax, E-mail, Confirm E-mail Address, Address 1, Address 2, City, Country, State/Province, and Zip/Postal Code. At the bottom right, there are 'Cancel' and 'Next >>' buttons, with the 'Next >>' button highlighted by a red box.

- Confirm you have the correct administrator selected, then click **Next**.
- You will receive a reference number confirming your submission.

The screenshot shows the 'Submission Confirmation' page. It contains a thank you message: 'Thank you for submitting your registration. Once your registration has been processed, you will be contacted by the Customer Support within the next 24-72 hours, after which you can access products and services that you may have selected.' It also states: 'You may close your browser at any time.' At the bottom, it provides a reference number: 'Please use reference number **SIG_1428506146296** if you need to contact support with questions. Refer to the help or customer service options at the top of this page for additional support.'

Update Organization Allowed Emails

Organization Admins can update the **Allowed Email Domains** for user's email addresses in the SAM Portal. If an administrator chooses to define "allowed domains", all existing users with need to conform to this standard.

To update allowed email domains:

1. Select the **Administration** tab. Then choose the **Update Organization** sub-tab.
2. In the **Allowed Email Domains** field, enter email domains permitted for automatic provisioning (for example: exostar.org). Then click **Submit**.

The screenshot shows the 'Administration' tab selected in the top left. The 'UPDATE ORGANIZATION' sub-tab is highlighted in the left sidebar. The main content area displays 'Organization Details' for 'Exostar LLC'. The 'Allowed Email Domains' field is highlighted with a red box, and the 'Submit' button is also highlighted with a red box. The 'Allowed Email Domains' field contains the text 'Allowed Email Domains:'. Below the field, there is a note: 'Enter list of domains allowed in user email address. For example: exostar.com, myexostar.com'.

3. If any existing users do not comply with the allowed email domains, you will see the following error message:

Error
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.

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

Batch Subscription – Bulk User Upload

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. Select the **Administration** tab, then select **Batch Subscription** sub-tab.
2. Click **Pick a file** to locate the correct file (see **Appendices A through D** for file formatting requirements). Then click **Upload**.
3. Next select the **Application** from the drop-down list. Click **Validate** to proceed.

The screenshot shows the 'Administration' tab selected in the top navigation bar. On the left sidebar, the 'BATCH SUBSCRIPTION' option is highlighted. The main content area is titled 'Batch Subscription' and contains the following elements:

- A message: 'To batch subscribe users in this organization to applications, select the CSV file to be loaded and click the **Validate** button -Required below'
- Buttons: 'Pick a file' and 'Upload' (both highlighted with red boxes)
- Text: 'File Selected: SAM-User-Upload-Template_Training.csv'
- Dropdown menu: '-Application: SAM Service Access Manager' (highlighted with a red box)
- Form fields: 'Subscription Period: Years [] Months [] Days []' with an information icon.
- Buttons at the bottom right: 'Validate' and 'Clear Uploaded File' (both highlighted with red boxes).

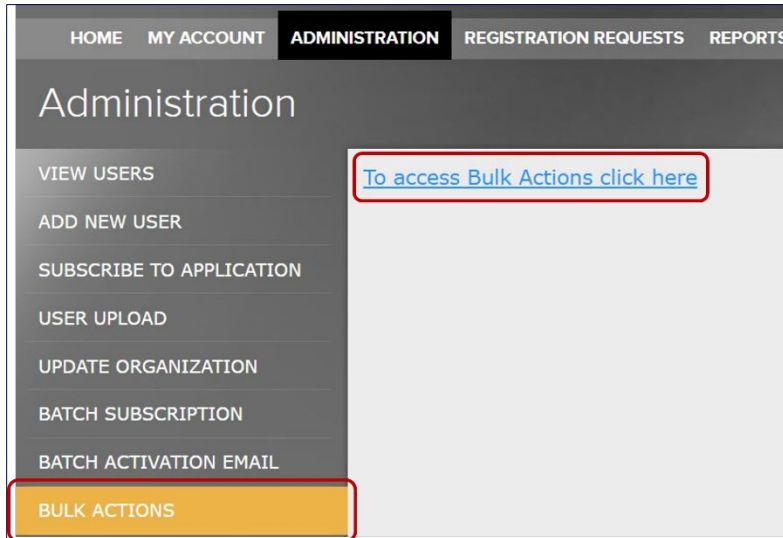
4. A confirmation message will display. Click **Commit** to load user subscriptions.

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.

Bulk Actions

Organization Admins can complete Bulk Actions using the BETA Bulk Jobs Board to upload new users in bulk or suspend, unsuspend and delete multiple users at once. To complete a bulk actions job:

1. Select the **Administration** tab. Then click **Bulk Actions** sub-tab.
2. Click the hyperlink **"To access Bulk Actions click here"** to open the Bulk Jobs Board.



3. A new window opens with the BETA **Bulk Jobs Board**. From here you can begin a new bulk job.

EXOSTAR Secure Access Manager (SAM)

Bulk Jobs Board (Exostar LLC)

STATUS Row #: 30 - SAM-Bulk-Upload-Template-XLS(4).xlsx - Action Taken: Upload Users

100.0% Completed

Success 1
Fail 0

1

TOTAL USERS SELECTED

1

SUCCESSFUL ACTIONS

[Download](#)

—

ISSUES FOUND

BEGIN A BULK JOB

- Upload Users
- Suspend Users
- Unsuspend Users
- Delete Users

PREVIOUS JOBS

ROW #	USER LIST NAME	ACTION TAKEN	JOB START	JOB END	STATUS	TOTAL	SUCCESS	FAIL
30	SAM-Bulk-Upload-Template-XLS(4).xlsx	Upload Users	05/09/2026 03:36 AM	05/09/2026 03:36 AM	complete	1	1	0
29	020926.xlsx	Upload Users	02/09/2026 09:50 PM	02/09/2026 09:50 PM	complete	3	3	0

4. Click **BEGIN A BULK JOB**. Then select the action you wish to complete: Upload Users, Suspend Users, Unsuspend (re-activate) Users, or Delete Users.

5. Next fill out the Excel template with the user's information for the selected action.
Save the file. (You can find the Bulk Actions template on the [SAM Training Resources](#) page).
6. Then in the SAM Bulk Actions Job Board, drag & drop or **Browse** for the file.

Bulk Actions Upload Users 0 Apps Selected CANCEL APPLY BULK ACTION

UPLOAD A LIST OF USERS

Drag and drop a file or click 'Browse' to upload users.

Once uploaded select applications from a newly populated list (below). Activated selections are check marked-highlighted.

The "APPLY BULK ACTION" button (above, right) will initiate the job and return you to the Bulk Jobs dashboard.

Drag and drop file here to upload
OR
BROWSE

Follow the guide and download the template CSV/Excel file, [click here to visit MyExostar](#).

SELECT APPLICATIONS FOR BULK ACTION(OPTIONAL)

SELECT	PROVIDER	APPLICATION	SPONSOR CODES
--------	----------	-------------	---------------

7. Next place a **checkmark** next to the application(s) you want to complete the bulk action for. Then click **Apply Bulk Action** button.
8. If the upload is successful, it will show as complete and success.

Bulk Jobs Board (Exostar LLC) BEGIN A BULK JOB

STATUS Row #: 29 - 020926.xlsx - Action Taken: Upload Users

100.0% Completed

Success 3
Fail 0

3

TOTAL USERS SELECTED

3

SUCCESSFUL ACTIONS

[Download](#)

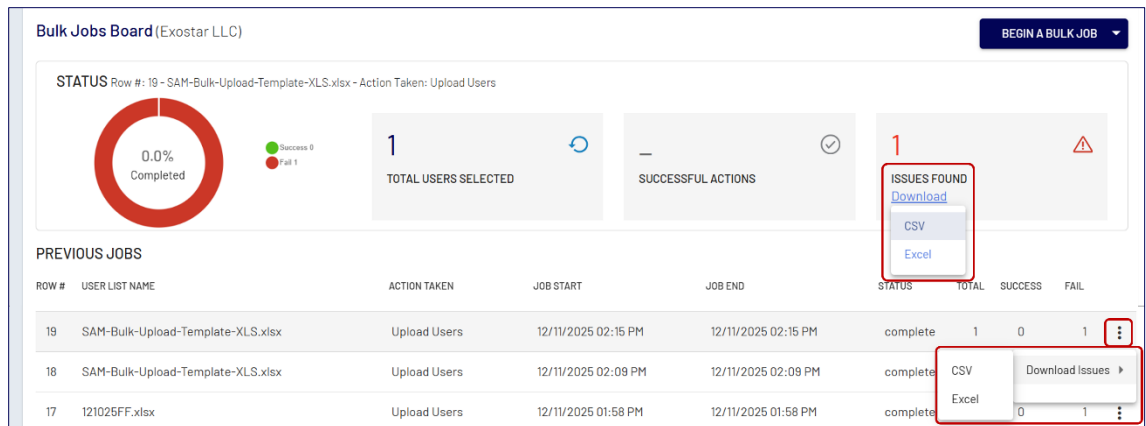
—

ISSUES FOUND

PREVIOUS JOBS

ROW #	USER LIST NAME	ACTION TAKEN	JOB START	JOB END	STATUS	TOTAL	SUCCESS	FAIL
30	SAM-Bulk-Upload-Template-XLS (4).xlsx	Upload Users	05/09/2026 03:36 AM	05/09/2026 03:36 AM	complete	1	1	0
29	020926.xlsx	Upload Users	02/09/2026 09:50 PM	02/09/2026 09:50 PM	complete	3	3	0

- a. If it fails, click the [Download](#) hyperlink or select the 3-ellipsis dots and download the Excel file. Then correct the errors and re-upload the file again.



Common Failure Errors

When a bulk action fails for one or more users, the failure record will include a reason code. The table below describes the possible failure reasons:

Failure Reason	Explanation
State_mismatch	The user is already in the status that the action would produce, or is in a status that prevents the action from being applied. Examples: attempting to subscribe a user whose access is suspended, or suspending a user whose access is already suspended.
Forbidden	The SP Admin does not have permission to perform the action for the affected user. This is typically an edge case and may indicate that the user does not fall within the SP Admin's scope of administration.

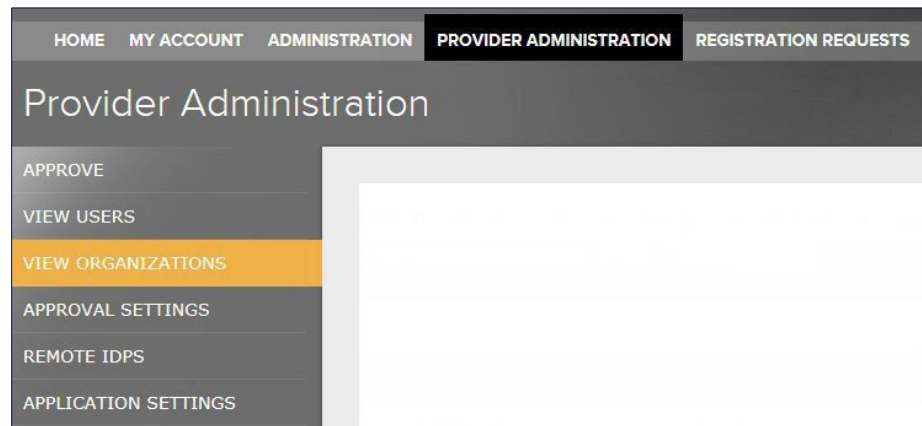
Service Provider Admins: Provider Administration tab

Service Provider Administrators (SP Admins) can access the **Provider Administration** tab 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 Users

SP Administrators can search and approve users in the Approve section under the Provider Administration. The **Approve** sub-tab allows you to:

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

Search Users

1. In the SAM platform, select the **Provider Administration** tab. Then select the **Approve** sub-tab.
2. Use the search filters and fields to locate a specific approval request. The following search filter fields are available:
 - a. **Filter Request By:** allows you to filter by All, New, and Pending requests.
 - b. **Search For:** allows you to enter search criteria, such as username, user ID, or organization information.

The screenshot shows the 'Provider Administration' tab selected in the top navigation bar. On the left, the 'APPROVE' button is highlighted. The main area contains a 'Filter Requests By: All' dropdown, a 'Search For:' input field, and a 'Search' button. Below these is an 'Action: Select Action' dropdown and an 'Apply' button. A message states: 'You can approve/deny a maximum of 30 requests at a time'.

3. Enter search criteria and click **Search**. The search results will display. Click the **Request ID** link to access the desired request.

Approve User Requests

SP Admins can process user access requests individually (one by one), or multiple requests simultaneously. To process user access requests:

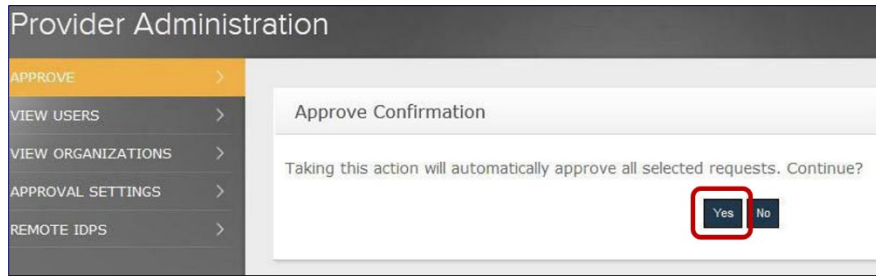
1. Login to the Exostar SAM Platform and access the **Provider Administration** tab.
2. To **approve** or **deny** an individual access request, select the desired request by clicking the **Request ID** link. Then select the **Action** from the drop-down list.

The screenshot shows the 'Provider Administration' tab with search results displayed. The 'Filter Requests By:' dropdown is set to 'New'. The 'Search For:' field is empty. The 'Action:' dropdown is set to 'Select Action'. The 'Apply' button is highlighted. A message states: 'You can approve/deny a maximum of 30 requests at a time'. Below the message is a table with the following data:

Select	Request ID	User ID	Last Name	First Name	Org ID	Org Name
☒	SIG_1428415491432_MPF	t_5182	Merck	test	EX0115826757	Exostar21
☒	SIG_1428415169198_MPF	agrawal2s_5621	agrawal2	shishinka	EX0115826757	Exostar21

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.

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

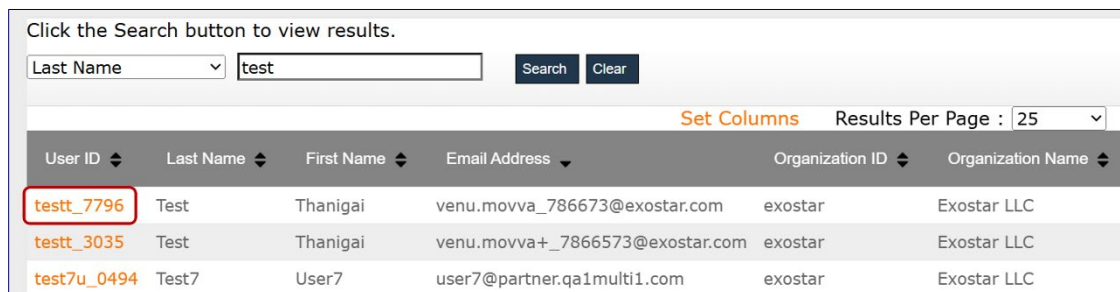


Suspend User Subscription

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. Select **View Users** sub-tab and **search** for the user. Then click the **User ID hyperlink**.



3. The user's profile will display. Scroll to 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.

Reactivate User's Subscription

SP Admins can reactivate a user's access to an application. Similar to the process above, to reactivate a user account subscription:

1. Select the **Provider Administration** tab. Then click **View Users** sub-tab.
2. Search for the user and click the **User ID** hyperlink.
3. The user's profile will display. Scroll to the **Application Settings** section. Click **Activate** next to the desired application.

NN	RTSM	Suspended	Activate	Delete
----	------	-----------	-----------------	--------

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.

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 select the **Provider Administration** tab.
2. Find the desired user and click **User ID** hyperlink.

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
testers_9179	Tester	Susie	stester@exostar.com		EXO114766233	Highline/Exostar QA

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

Application Access:	Provider	Application	Expiration Date	Last Access Date	Status	Action
	EngageZone	EngageZone.msdc.com			Active	Edit Suspend
	Exostar LLC	Secure Share			Pending Acceptance of Terms & Conditions	

Status: User Inactive [Resend Activation E-mail](#)

- A confirmation message will display.

Resend User Provisioning Record

SP Admins can resend an active user's **Provisioning Record**. To resend a user's provisioning record:

- Login to Exostar SAM Platform and access the **Provider Administration** tab.
- Locate the desired user and click the **User ID** hyperlink.

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
testers_9179	Tester	Susie	stester@exostar.com	EXO114766233		Highline/Exostar QA

- 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.

Provisioning									
Provisioning Records:	Service Provider	In Queue	Queued Time	Last Completed Time	Fail Count	Retry After	On Hold	Last Error Code	Last Error Detail
	EngageZone.msdc.com	No	NA	03 Nov 2020 03:23 PM EST		NA	No		

Select an application: [Please Select](#) [Resend](#) [Force Resend](#)

- After you resend the provisioning record, it will display the time and date it was completed.

Provisioning									
Provisioning Records:	Service Provider	In Queue	Queued Time	Last Completed Time	Fail Count	Retry After	On Hold	Last Error Code	Last Error Detail
	EngageZone.msd.com	No	NA	03 Nov 2020 03:23 PM EST		NA	No		

View Organizations

The **View Organizations** tab 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

To view an organization:

1. In the SAM portal, select the **Provider Administration** tab.
2. Next select the **View Organizations** sub-tab.

Provider Administration

APPROVE
VIEW USERS
VIEW ORGANIZATIONS
APPROVAL SETTINGS
REMOTE IDPS
DASHBOARDS
APPLICATION SETTINGS

Click the **Search** button to view results. To register a new organization, **complete Form**.

Filter by... **Search** **Clear** **Export Results**

Set Columns

Organization ID	Organization Name	Business Unit	SAM Status
EXO115105137	testing1	Exostar QA	Active
EXO115051480	Testing Org Limited		Active

3. From the drop-down list, select the **Filter by** option, then enter a **Search Term** in the dedicated field. Next click **Search**.

Filter by... **Search**

- Filter by...
- Name
- Exostar Id
- Org Id
- Onboarding Sponsor

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

- The search results will display. Click the **Organization ID** to view all organizational information, contacts, and administrators.

Suspend 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.

To Suspend an Organization's Access:

- Locate the organization for which you would like to suspend access. Click the **Org ID** for this organization.

Click the **Search** button to view results. To register a new organization, [complete Form](#).

Filter by... Search Clear Export Results

[Set Columns](#)

Organization ID	Organization Name	Business Unit	SAM Status
EXO115105137	testing1	Exostar QA	Active
EXO115051480	Testing Org Limited		Active

- Scroll to the bottom of the Organization's profile page. Click **Suspend**.

Application Settings

Application Access	Provider	Application	Status	Action
	Exostar LLC	Secure Share	Active	Suspend

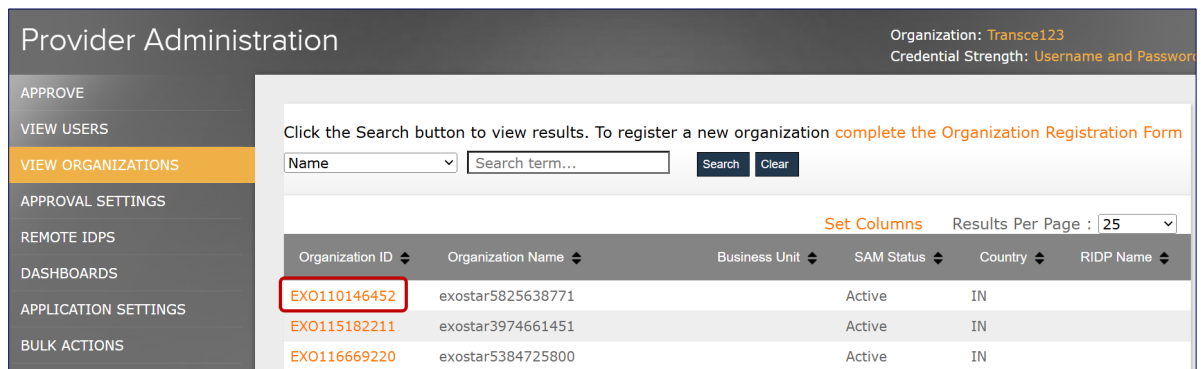
Status: Active

- You will be prompted to confirm the **Suspension**. Then click **OK**.
- A confirmation message will display.

Reactivate Organization's Access

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

1. Search for the organization you want to reactivate access. Then click the **Org ID** to access the organization's profile.



Provider Administration

Organization: Transce123
Credential Strength: Username and Password

APPROVE
VIEW USERS
VIEW ORGANIZATIONS
APPROVAL SETTINGS
REMOTE IDPS
DASHBOARDS
APPLICATION SETTINGS
BULK ACTIONS

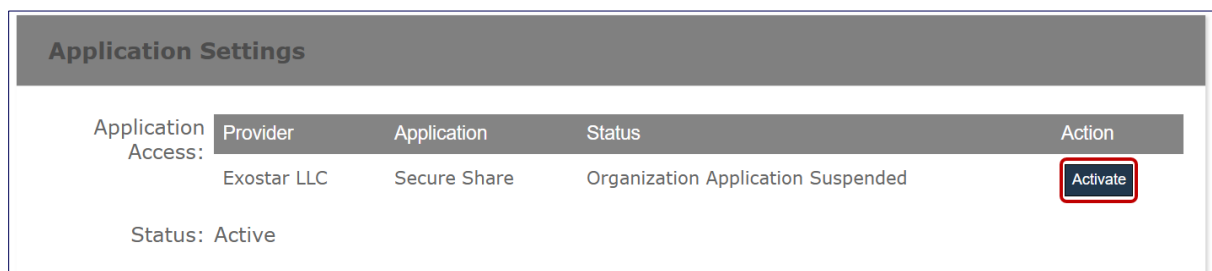
Click the Search button to view results. To register a new organization complete the Organization Registration Form

Name Search term... Search Clear

Set Columns Results Per Page : 25

Organization ID	Organization Name	Business Unit	SAM Status	Country	RIDP Name
EXO110146452	exostar5825638771		Active	IN	
EXO115182211	exostar3974661451		Active	IN	
EXO116669220	exostar5384725800		Active	IN	

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



Application Settings

Application Access:	Provider	Application	Status	Action
	Exostar LLC	Secure Share	Organization Application Suspended	Activate

Status: Active

3. You are prompted to confirm the **Activation**. Click **OK**.
4. A confirmation message will display.

Approval Settings

The **Approval Settings** tab 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.

To add an Organization to the Approved List:

1. Select the **Provider Administrator** tab. Then click **Approval Settings** sub-tab.

- 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**.

The screenshot shows the 'Provider Administration' interface. On the left is a sidebar with navigation options: APPROVE, VIEW USERS, VIEW ORGANIZATIONS, APPROVAL SETTINGS (highlighted with a red box), REMOTE IDPS, DASHBOARDS, APPLICATION SETTINGS, and BULK ACTIONS. The main content area is titled 'Add Setting' and contains a form with two required fields: '*Organization ID:' (with an empty text input) and '*Application:' (with a dropdown menu set to 'Secure Share'). Below these fields is an 'Add Organization' button. To the right of the form is a table listing approved organizations. The table has columns: Organization ID, Organization Name, SP, Added By, Added On, and a 'Remove' button. The first row contains the data: EXO111025461, SAM_QAtest/Exostar QA, Secure Share, Jogesh Rout, 08-14-2025, and a 'Remove' button.

Organization ID	Organization Name	SP	Added By	Added On	
EXO111025461	SAM_QAtest/Exostar QA	Secure Share	Jogesh Rout	08-14-2025	Remove

- 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.

Remove Organization Approved List

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

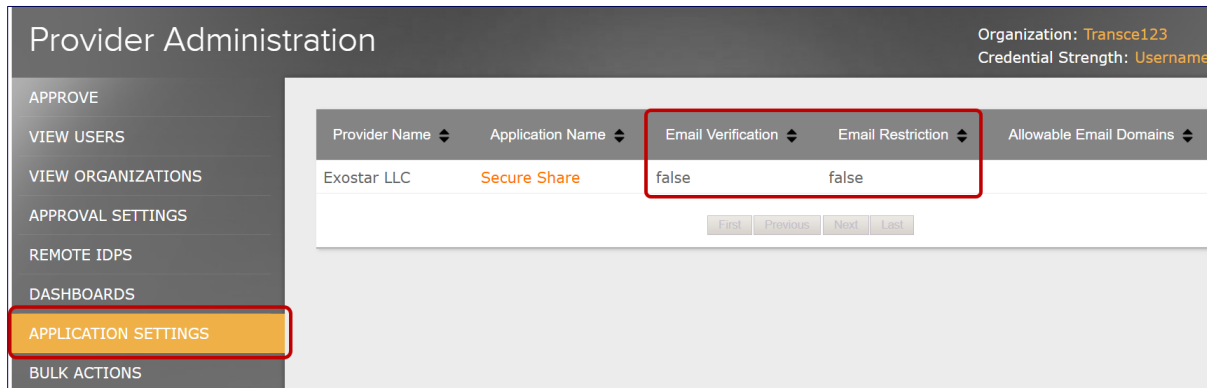
- Select the **Provider Administration** tab. Then choose the **Approval Setting** sub-tab.
- Use the search fields to locate the desired organization.
- Click the **Remove** button to delete an organization from the approved list.

This screenshot is similar to the previous one, showing the 'Provider Administration' interface with the 'APPROVAL SETTINGS' tab selected. The 'Add Setting' form is visible. The table below it shows the same organization as before. In this view, the 'Remove' button in the table row is highlighted with a red box, indicating the action to be taken.

Organization ID	Organization Name	SP	Added By	Added On	
EXO111025461	SAM_QAtest/Exostar QA	Secure Share	Jogesh Rout	08-14-2025	Remove

Application Settings

The **Application Settings** sub-tab 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 Settings

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 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 User Guide](#).

Email Restrictions

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** sub-tab.
3. Click the **Application Name** you are adding email restriction to.

Provider Name ▾	Application Name ▾	Email Verification ▾	Email Restriction ▾	Allowable Email Domains ▾	RBA ▾
Exostar LLC	Secure Share	false	false		false
First Previous Next Last					

4. Enter Allowed email domains and/or address in the **Allowed Email Domains** and Address field (e.g., 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.

Edit Service Provider

Application Name:	Secure Share		
Email Verification:	Off		If Email Verification is On, the user would be required to receive a One Time Password (OTP) in the email address registered with SAM and verify the same before being able to access this application.
Email Restriction:	Off		If Email Restriction is On, the system would be required to verify that the user's email address registered with SAM is included in the list of allowable email domains / email addresses for this application, before the user can navigate further
	RBA:	Off	
	Allowed Email Domains and Addresses		
Submit Back			

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**.
 - a. Email addresses or domains that have not been included will receive an ERROR message when trying to access the application.

Application Name ▾	Email Verification ▾	Email Restriction ▾	Allowable Email Domains ▾
File Based Test SP	true	true	yahoo.com,davida.evans@exostar.com

Registration Requests

The **Registration Requests** tab is available to Organization and Application Admins. 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.

Approve Users

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. Click the **Verify** sub-tab to view the list of pending requests.
2. Click the **Request ID** link for the request you would like to approve.

Registration Requests

Organization: Highline/Exostar QA
Credential Strength: Username and Password

VERIFY >

AUTHORIZE >

Filter Requests By: All

Results/page: 25

Search For: Using Select Field to Filter Search Clear

Request ID	Last Name	First Name	Org Name	Business Unit	Date Submitted	Last Viewed Date	Status
SIG_1428962099399	Tester	Lisa	Highline	Exostar QA	04/13/2015	04/13/2015	New

3. Review the User Registration Request information, including the Products & Services access request. Click **Next**.
4. Complete all required fields and click **Next**.

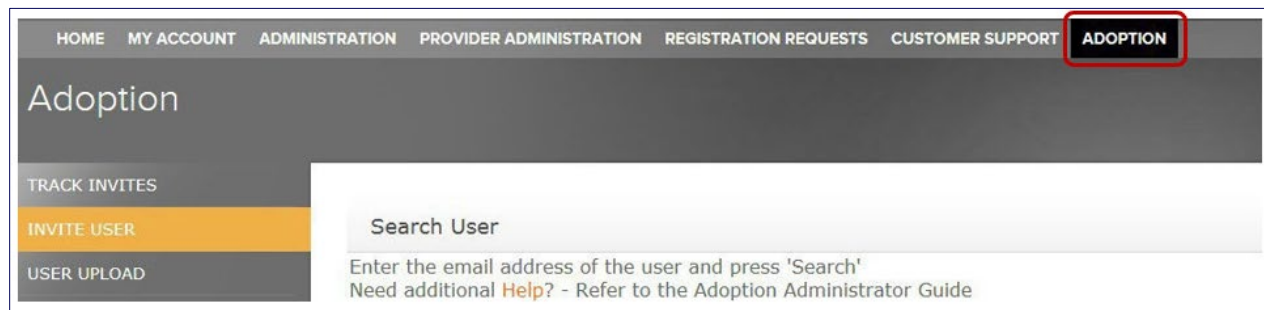
NOTE: If you select **Deny**, you will be required to enter **Comments** to explain your reasons for denial.

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

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.



The **Adoption** tab allows you to:

- 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

- **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.

To begin the invitation process, you **MUST** 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 select the **Adoption** tab.
2. Click the **Invite User** sub-tab.
3. Enter the user's email address and click **Search**.

TRACK INVITES >

INVITE USER >

Search User

Enter the email address of the user and press 'Search'
Need additional [Help?](#) - Refer to the Adoption Administrator Guide

* Email Address :

Last Name :

First Name :

4. Once the user search is complete, proceed with one of the scenarios outlined below:
 - 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 **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 the 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** hyperlink.
4. The user's profile page will display. Place a check next to the applications you want to subscribe the user to. Click **Subscribe to Application(s)**.

Application Information

Select the checkbox next to the applications the user should be subscribed to, then click on 'Subscribe to Application ' button.

Select	Application Name
☐	SecureShare

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

The screenshot shows a web form titled "Invitation Information". Below the title, it says "Click 'Submit' to issue the invitation for the application(s) listed and take the following additional action(s):". The form contains the following fields: "Full Name : Ryan Wick", "Email Address : ryan.wick2@exostar.com", "Organization Name: Ryan Test Org", "Organization ID: EX0118568832", and "Message to User :". Below these fields is a section titled "Application Information". It has a table with two columns: "Subscribe User to Application" and "Subscription Period". The first row shows "SecureShare" under the first column. Under the "Subscription Period" column, there are input fields for "Years", "Months", and "Days". At the bottom of the form, there are two buttons: "Submit" (highlighted with a red box) and "Cancel".

- The user will receive an email invitation.

Add User to Existing Organization

- Search for the user first. If you conducted a search but were unable to locate the user, you should then search for the organization.
- On the search results pages, click **Search Organization**.

The screenshot shows a web form titled "Search User". Below the title, it says "Enter the email address of the user and press 'Search'" and "Need additional [Help?](#) - Refer to the Adoption Administrator Guide". The form contains the following fields: "Email Address : ryan.wick5@exostar.co" (highlighted with a red box), "Last Name :", and "First Name :". There are "Search" and "Clear" buttons. Below these fields is a "Results per page:" dropdown menu set to "10". Below the search fields is a section titled "User Search Results". It contains the text "No matches found" and a button "Search Organizations" (highlighted with a red box).

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

Organization Search

In an effort to avoid duplication you should only proceed with creating a new organization if you are certain that the organization does not already exist. Use more than one search criterion to narrow down your results. Need additional [Help?](#) - Refer to the Adoption Administrator Guide

Organization Name :
Exostar ID :
DUNS Number :
US Federal Tax ID Number :
Address 1 :

Address 2 :
City :
Country :
State/Province :
Postal/Zip Code :

Results per page:

4. The search results may include one or more organization accounts. If multiple organizations display, select the organization by clicking the **Organization Name** hyperlink.
5. Select **Add User to New Organization**.

Organization Search Results

Please review the search results carefully. In an effort to avoid duplication you should only proceed with creating a new organization if you are certain that the organization does not already exist. To add user to existing organization click on organization name link.

Organization Name	Organization ID	Exostar ID	SAM Status
exostar-3	EXO117897139	117897139	ACTIVE

6. Enter the user details and select the applications the user should subscribe to.
 - a. **Optional:** You can enter a subscription period (optional), and a message to include in the email confirmation. Click **Submit Request**.

*On-boarding Sponsor :
Title :

*First Name :
Middle Name :
*Last Name :
Suffix :
Job Title :

*Email Address :
*Confirm Email Address :

*Address1 :
Address2 :
*City :
*Country:
*State/Province:
*Postal/Zip Code:
*Phone :
Fax :
TimeZone :

Organization Name: Ryan Demo

Select	Application Name	Subscription Period
☐	SecureShare	Years Months Days

Message

Optionally, enter text to included in email notification to user

Message to New user:

Submit Request
Clear
Cancel

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

Invitation Information

Click 'Submit' to issue the invitation for the application(s) listed and take the following additional action(s):

Full Name : Ryan Tester

Email Address : ryan.wick3@exostar.com

Organization Name: exostar-3

Organization ID: EXO117897139

Message to User : I've added you to SecureShare

Application Information

Subscribe User to Application	Subscription Period
SecureShare	Years Months Days i

Submit
Cancel

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

Add New User and Organization

1. Search for the user first. If you conducted a search but were unable to locate the user, you then search for the organization.
2. If no organization matches are found, click **Add User to New Organization** to start the invitation process for both the Organization and the User.

Organization Search Results	
No matches found	Add User to New Organization

- 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

- 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

- Select the **Application(s)** you want 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

6. Next click **Add User**.

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

8. 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.

Adoption Admin - 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 automatically be subscribed to these applications after the fact of the upload.

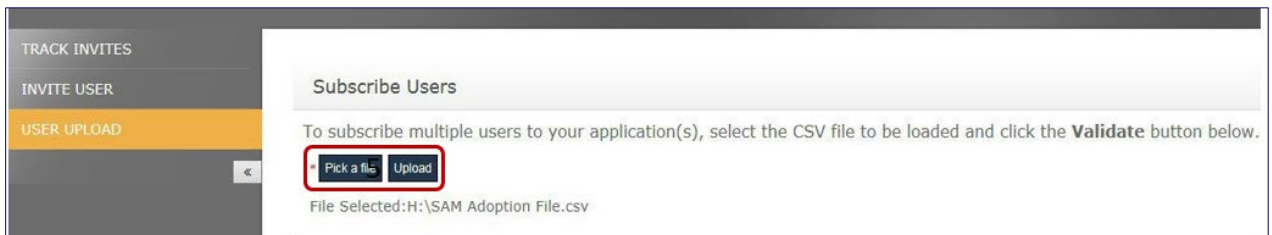
Before the users of an OMO (Organization Managed Organization) can access these applications, their Org Admin must accept Terms and Conditions for the applications. This requirement does not apply to SMOs (Sponsor-Managed Organizations).

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 bulk upload users:

1. From the **Adoption** tab, click **User Upload** sub-tab.
2. Fill out 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.

Subscribe Users

Click the **Commit** button to subscribe the users with a green checkmark below to their respective applications. Users with a red X below will not be subscribed to applications, nor will they have accounts created for them should they be new users. To correct errors and load a new file, click on the **Back** button.

Line	E-mail	Name	Errors
	2	davida.evans2@exostar.com	Dee Evans Application(s): No permissions to subscribe to one or more application(s). User does not exist in SAM.

[Back](#)
[Export Results](#)

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.

- 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.
- 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**.

Organization Search

In an effort to avoid duplication you should only proceed with creating a new organization if you are certain that the organization does not already exist.
Use more than one search criterion to narrow down your results.
Need additional [Help?](#) - Refer to the Adoption Administrator Guide

Organization Name :
Exostar ID :
DUNS Number :
US Federal Tax ID Number :
Address 1 :

Address 2 :
City :
Country :
State/Province :
Postal/Zip Code :

[Search](#)
[Clear](#)
[Cancel](#)

Results per page:

Organization Search Results

Please review the search results carefully.
In an effort to avoid duplication you should only proceed with creating a new organization if you are certain that the organization does not already exist.
To add user to existing organization click on organization name link.

Organization Name	Organization ID	Exostar ID	SAM Status	Active Applications	Pending Applications
Fulfillment_DCS	EXO111823812	111823812	ACTIVE	EngageZone.msdc.com,TEST Service Provider 1,Digital Certificate Service,EngageZone Qualification	

[Add User\(s\) to New Organization](#)

- On the new screen, click **Add Users to Organization**.

Organization Details

On-boarding Sponsor : General	Address 1 : 13241 Woodland Park Dr.
Organization Name: Fulfillment_DCS	Address 2 :
Organization ID: EXO111823812	City : Herndon
Exostar ID : 111823812	Country : US
Business Unit : Exostar QA	State/Province : VA
Organization's HQ/Country of Incorporation: US	Zip/Postal Code : 20171
DUNS Number :	R-IDP Status : Unlinked
SAM Status : ACTIVE	

Back
Add User(s) to Organization

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

Subscribe Users

Click the **Commit** button to subscribe the users with a green checkmark below to their respective applications. Users with a red X below will not be subscribed to applications, nor will they have accounts created for them should they be new users. To correct errors and load a new file, click on the **Back** button.

Search Organizations

Line	E-mail	Name	Errors
2	davida.evans2@exostar.com	Dee Evans	
3	davida.evans+_34@exostar.com	Joe Smith	

Search Organizations

Back
Commit

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**.

Organization Search

In an effort to avoid duplication you should only proceed with creating a new organization if you are certain that the organization does not already exist. Use more than one search criterion to narrow down your results. Need additional [Help?](#) - Refer to the Adoption Administrator Guide

Organization Name : ABC Training LLC	Address 2 :
Exostar ID :	City : Herndon
DUNS Number :	Country : UNITED STATES OF AMERICA
US Federal Tax ID Number :	State/Province : Virginia
Address 1 : 1 Fleet St.	Postal/Zip Code : 20171

Search Clear Cancel

Results per page: 10

Organization Search Results

No matches found

Add User(s) to New Organization

12. Select required fields (marked with an *****) and click **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 :

*Organization Name:

*Address 1 :

Address 2 :

*City :

*Country:

*State/Province:

Postal/Zip code:

DUNS Number :

13. If no duplicates are found, the 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.

Resolve Duplicates

The system has found up to 1 potential duplicates for the organization you wish to create
Please review the list of duplicates carefully, click on organization name to view details
In an effort to avoid duplication, you should only proceed with creating a new organization if you are certain that the organization does not already exist
Need Additional Help? Refer to the Adoption Administrator Guide

Organization Name	Organization ID	Exostar ID	SAM Status	Active Applications
Fulfillment_DCS	EXO111823812	111823812	ACTIVE	TEST Service Provider 1, Digital Certificate Service,

Track Invitations

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

- Click the **Track Invites** sub-tab.
- Log into the Exostar SAM Platform and access the **Adoption** tab.
- Select the desired **Request Type** from the dropdown menu.
- Then choose the desired **Search By** criteria. Next click **Search**.

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.

Adoption

TRACK INVITES >

INVITE USER >

Invitation Search

Select Request Type, Search by parameter, and enter search criteria.
Need Additional [Help](#) ? Refer to the Adoption Administrator Guide

Request Type :

Search By :

Search For :

My Pending Invitations

My Complete Invitations

All Pending Invitations

All Complete Invitations

Search

Clear

- 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.

Invitation Search

Select Request Type, Search by parameter, and enter search criteria.
Need Additional [Help](#) ? Refer to the Adoption Administrator Guide

Request Type : All Complete Invitations

Search By : Date Submitted

Start Date : 21 May, 2017

End Date : 30 May, 2017

Search

Clear

Results per page: 100

Existing Invitations

Request ID	Invitee	Invitee Ref	Adoption Admin First Name	Adoption Admin Last Name
fe2c8d64-237d-43a5-9898-rara9rR1a0d9	test test	test_1149@securepass.exostartest.com	Shared Investigator Platform	(SIP)

Appendix A: CSV Requirements – User Upload

Field	Cardinality/ Values	Response/Comments
Subscription Period	<i>Optional</i>	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	<i>Optional</i>	Acceptable options: Mr., Mrs., Ms., Dr.
Last Name	Required Max 50 characters	Accepts letters, numbers, and printable special characters except for '<' or '>'.
Middle Name	<i>Optional</i> 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	<i>Optional</i> 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	<i>Optional</i> 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	<i>Optional</i> 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	<i>Optional</i> 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 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 <i>Note: For Merck, the R-IDP User ID and the ISID are the same thing.</i>
Suffix	Optional	4 Char Limit
Sponsor Email Address	Optional RFC822 compliant	75 Char Limit

Appendix B: CSV File Requirements: User Uploads - Adoption Administrators

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	<i>Optional</i> 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	<i>Optional</i>	
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	<i>Optional</i>	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	<i>Optional</i>	R-IDP User ID must be unique for the associated R-IDP Organization must be associated to an R-IDP <i>Note for Merck: the R-IDP User ID and the ISID are the same thing.</i>
Suffix	<i>Optional</i>	4 Character Limit
Sponsor	Required	
Honorific (Title such as Dr.)	<i>Optional</i>	Acceptable options: Mr., Mrs., Ms., Dr.
Subscription Period	<i>Optional</i>	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)