Secure Access Manager (SAM)

Administrator Guide

September 2017

Secure Access Manager (SAM) Overview

Exostar's Secure Access Manager (SAM) 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.

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

Key Functions of SAM include:

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

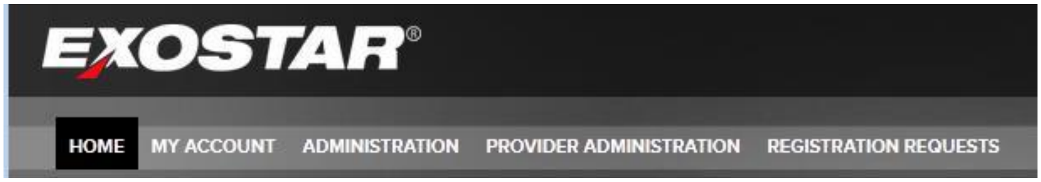
Administrative Roles Overview

There are several user roles within SAM, and each account is assigned a role upon creation. By default, each account is provisioned with the "User" role. In addition to the User role, administrative roles can be assigned, which provide additional access and management capabilities within the system.

- **Organization Administrator** (Org Admin): is an organization level administrator who can process new SAM user registration requests and manage the organization. Org Admins verify the user is an employee and provides the approvals for SAM enrollment. Org Admins are also responsible for accepting the online Terms and Conditions Agreement.
- **Service Provider Administrator** (SP Admin): is a system level administrator who can grant final approvals to users and organizations for application access, and set organizational approval setting. The SP Admin role is a system level administrator assigned by Exostar and is often referred to as the application owner.

SAM Navigational Overview

Several functional tabs are available within the SAM Portal. The *Home* and *My Account* tabs are available to all users, while the *Administration*, *Provider Administration* and *Registration Requests* tabs are available only to designated administrators.



- **Home** tab is available to all *users* and provides access to your applications. It contains several containers 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)* and provides user management capabilities. 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* (*Org Admins*) and used to grant approval for users who self-register for SAM accounts, and to approve OTP Token requests.
- **Provider Administration** tab is available to *Service Provider Administrators (SP Admin)* and is used to manage Organization and User account subscriptions and access. The SP Admin role is not an org level administrator, but rather a system level administrator assigned by Exostar.

Access the SAM Portal

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

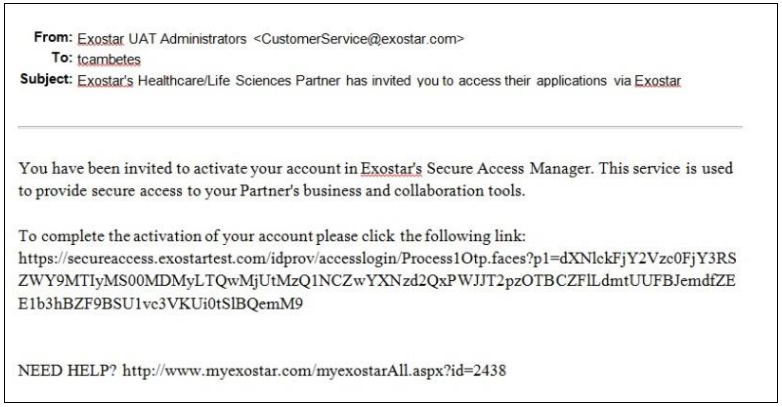
How to Activate my Account

Upon creation of a SAM account, you will receive an email notification containing the link to activate your SAM account. The account activation process will include creation of a password and selection of security questions. The system will send the account activation email two times every 30 days, and new activation notifications will supersede activation links sent in previous emails. You must complete your account activation within 180 days or the system will deactivate (delete) your account.

Once you have completed the first time login and are actively using the applications, the system requires you to change your password every 90 days.

Below are steps to complete your account activation:

1. Upon receipt of the activation notice, click the **Activation Link** provided in the email.



From: Exostar UAT Administrators <CustomerService@exostar.com>
To: tcambetes
Subject: Exostar's Healthcare/Life Sciences Partner has invited you to access their applications via Exostar

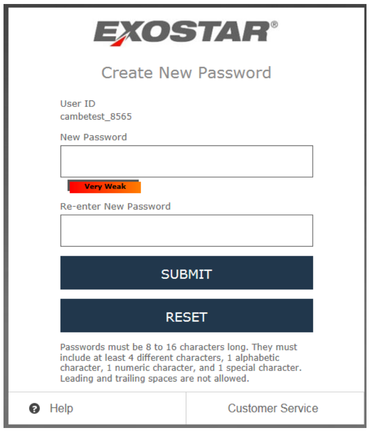
You have been invited to activate your account in Exostar's Secure Access Manager. This service is used to provide secure access to your Partner's business and collaboration tools.

To complete the activation of your account please click the following link:
https://secureaccess.exostartest.com/idprov/accesslogin/Process1Otp.faces?p1=dXNlckFjY2Vzc0FjY3RSZWY9MTIyMS00MDMyLTQwMjUtMzQ1NCZwYXNzd2QxPWJJT2pzOTBCZFlLdmtUUFBJemdfZEE1b3hBZF9BSU1vc3VKUi0tSlBQemM9

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

Note: If you do not use the link in email to initiate the process, but instead choose to enter your email address on the SAM login screen, the system prompts you to enter captcha in order to resend **Activation** email.

2. Enter a password and then reenter to confirm. Click **Submit** to continue.



Create New Password

User ID
cambetest_8565

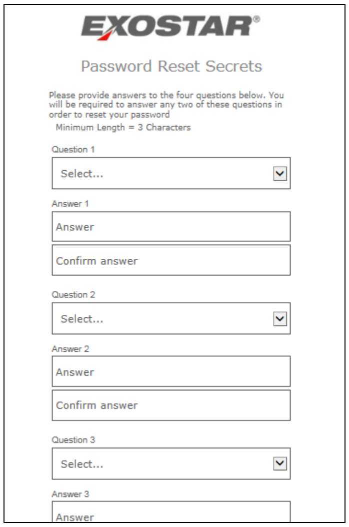
New Password

Re-enter New Password

Passwords must be 8 to 16 characters long. They must include at least 4 different characters, 1 alphabetic character, 1 numeric character, and 1 special character. Leading and trailing spaces are not allowed.

Note: Passwords must be 8 to 16 characters long. They must include at least 4 different characters, 1 alphabetic character, 1 numeric character, and 1 special character. Leading and trailing spaces are not allowed. Passwords will expire after 90 days.

3. Create your *password reset secrets* by selecting and responding to four security questions.



Password Reset Secrets

Please provide answers to the four questions below. You will be required to answer any two of these questions in order to reset your password

Minimum Length = 3 Characters

Question 1

Select...

Answer 1

Answer

Confirm answer

Question 2

Select...

Answer 2

Answer

Confirm answer

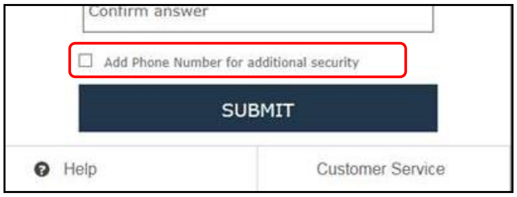
Question 3

Select...

Answer 3

Answer

Users may have the option to add a phone number for additional security. If selected, you can choose to register a phone number in order to receive a one-time password, instead of answering security questions, during account recovery.



Confirm answer

□ Add Phone Number for additional security

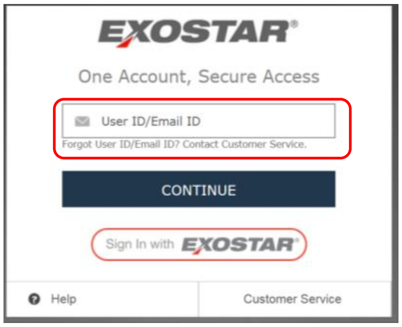
4. Upon successful entry of authentication information (password and security questions), you are redirected to the SAM portal, and your account authentication is complete.

How to Login to SAM

Once you have completed the account authentication login process, and have established your password and security questions, all subsequent **Logins to SAM** are as follows:

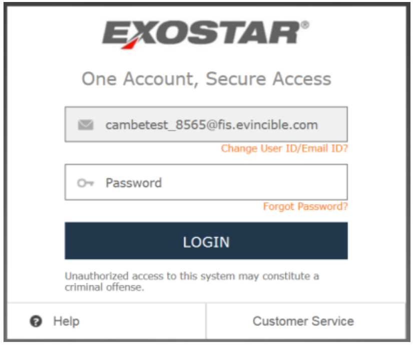
1. Go to the SAM login portal: *https://secureaccess.exostar.com*.

2. Enter your **User ID** or **Email Address**. Click **Continue**.


EXOSTAR®
One Account, Secure Access
User ID/Email ID
Forgot User ID/Email ID? Contact Customer Service.
CONTINUE
Sign In with EXOSTAR®
Help
Customer Service

Note: SSO/EAG users will have a cookie installed which redirects to their organization R-IdP. If the user deletes the cookie or uses another browser, entering the email address will redirect the user to the proper R-IdP.

3. Enter your password. Click **Login**.

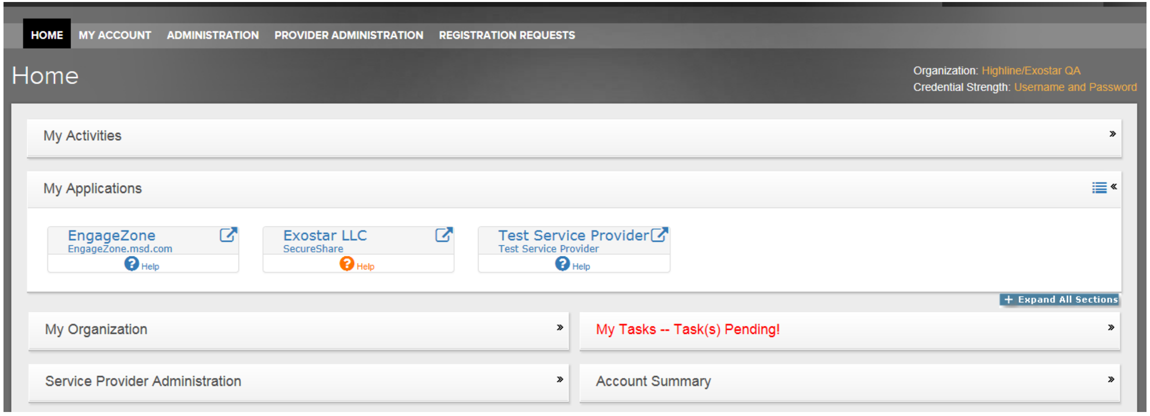


cambetest_8565@fis.evincible.com

Unauthorized access to this system may constitute a criminal offense.

Note: If the system recognizes your credential has not been activated, you will be prompted to resend the activation email.

4. Upon successful login, the SAM Home tab displays. The **Home** tab includes access to your active applications and organization information. Click an application in the My Applications section to launch the solution.

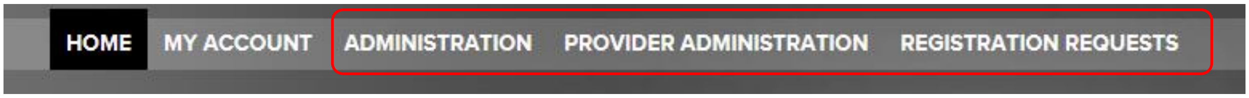


Organization: Highline/Exostar QA
Credential Strength: Username and Password

Note: In some cases, you may be presented with the *Terms and Conditions* the first time you access and application. Please contact Exostar Customer Service for more information.

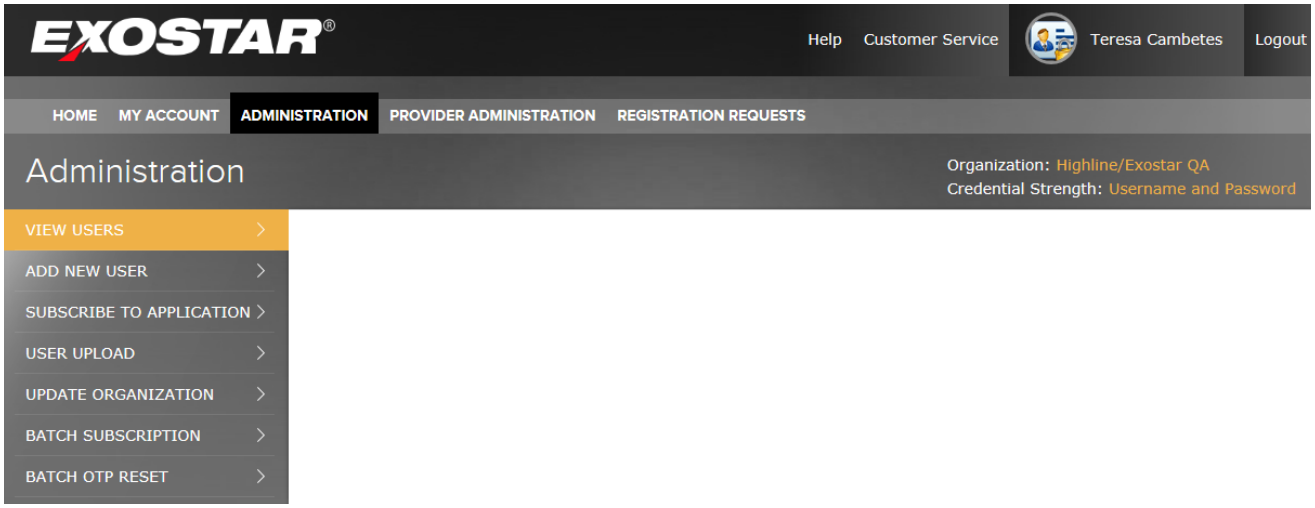
General Administrative Functionality

Upon login to the SAM portal, the landing pages consist of several tabs. The **Home** tab and the **My Account** tab are available to all users. The **Administration** tab, **Provider Administration** tab, and **Registration Requests** tab are administrative tabs with role-based provisioning.



The Administration Tab – Organization Administrators

The **Administration** tab is available to Org Admins and provides user management features. Within this tab, you can create new users and update existing user profiles. In addition, the administrator may subscribe their organization to additional Applications.



Administration

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

The **Administration** tab contains the functionality that allows Org Admins to:

- View and manage existing users
- Manually add new users
- Subscribe the organization to new applications
- Upload/Add users in bulk
- Update organization
- Subscribe users to a resource in bulk
- Reset OTP in bulk

How to Add a New User

You can add new users to SAM in several ways. Organization Administrators can add new users to SAM using the **Add New User** or the **User Upload** links. In addition, you can direct users to a self-registration link, which allows them to submit a registration request for approval.

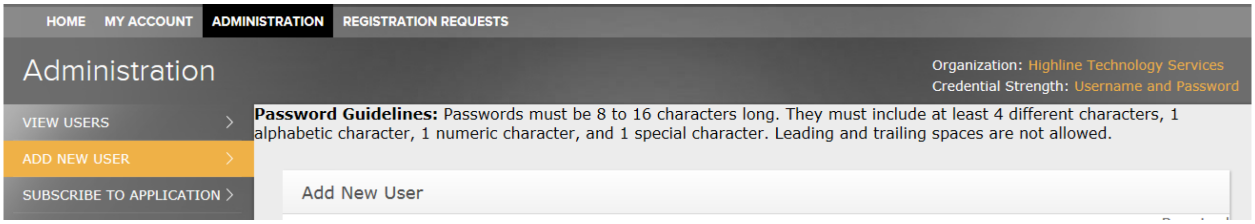
- **Add New User** link allows Org Admins to create a user account in SAM on behalf of the user.
- **User Upload** link allows Org Admins to load users into their organization from a batch upload via .csv file.
- **Self-Registration** allows a user to initiate the registration process. Requests are then approved by the Org Admin.

Add New User link

The *Add New User* link allows Organization Admins to add a new user by manually entering the user profile and application subscription information.

To add an individual user:

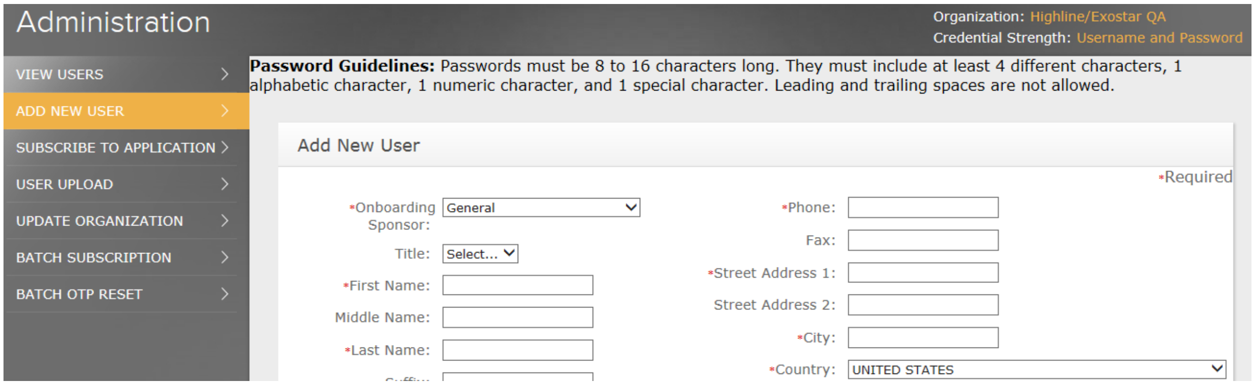
1. Login to SAM with an Org Admin account. Access the **Administration** tab and select **Add New User**.



Organization: Highline Technology Services
Credential Strength: Username and Password

Password Guidelines: Passwords must be 8 to 16 characters long. They must include at least 4 different characters, 1 alphabetic character, 1 numeric character, and 1 special character. Leading and trailing spaces are not allowed.

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

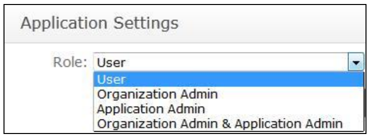


Organization: Highline/Exostar QA
Credential Strength: Username and Password

Password Guidelines: Passwords must be 8 to 16 characters long. They must include at least 4 different characters, 1 alphabetic character, 1 numeric character, and 1 special character. Leading and trailing spaces are not allowed.

*Onboarding Sponsor: General
Title: Select...
*First Name:
Middle Name:
*Last Name:
*Phone:
Fax:
*Street Address 1:
Street Address 2:
*City:
*Country: UNITED STATES

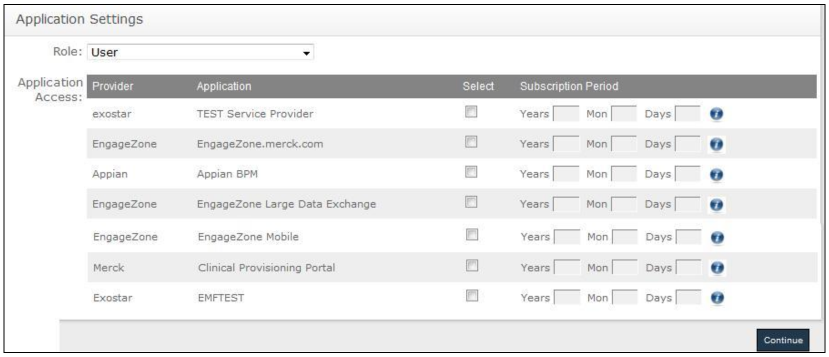
3. In the **Application Settings** section of the page, select a **Role** for the new user. Roles include User, Organization Admin, Application Admin and both Organization Admin and Application Admin.



Role: User
User
Organization Admin
Application Admin
Organization Admin & Application Admin

4. Select the applications the user should be provisioned to access. Click **Continue**.

   The list of application options will include all applications to which the organization is subscribed.



Application Settings

Role: User

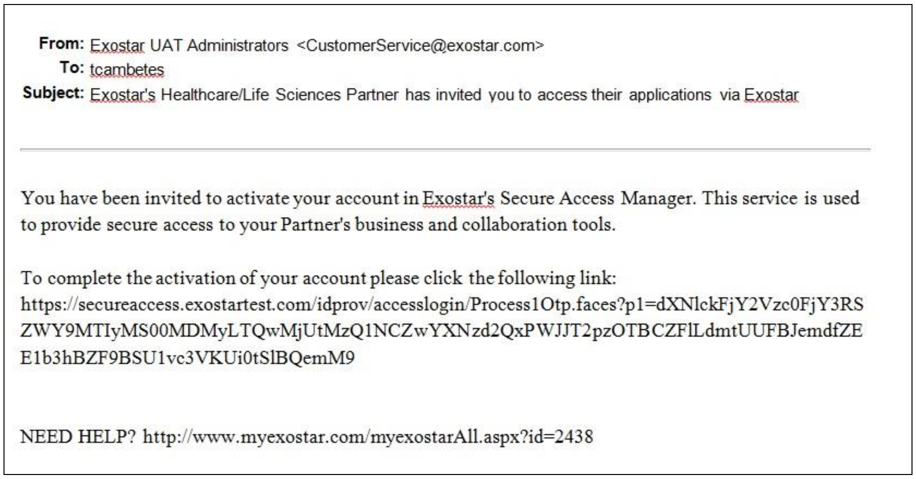
Application Access:

Provider	Application	Select	Subscription Period
exostar	TEST Service Provider	□	Years Mon Days
EngageZone	EngageZone.merck.com	□	Years Mon Days
Appian	Appian BPM	□	Years Mon Days
EngageZone	EngageZone Large Data Exchange	□	Years Mon Days
EngageZone	EngageZone Mobile	□	Years Mon Days
Merck	Clinical Provisioning Portal	□	Years Mon Days
Exostar	EMFTEST	□	Years Mon Days

   Note: If the **Application Admin,** or **Organization Admin & Application Admin** role is assigned, you must also designate the applications this user will be authorized to administer.

5. Review and verify the information you have entered. You may click **Modify** to make any necessary changes or **Cancel** to cancel this transaction. Click **Submit** to complete.

6. The confirmation page displays. The user will receive an email containing the account activation link.



From: Exostar UAT Administrators <CustomerService@exostar.com>
To: tcambetes
Subject: Exostar's Healthcare/Life Sciences Partner has invited you to access their applications via Exostar

You have been invited to activate your account in Exostar's Secure Access Manager. This service is used to provide secure access to your Partner's business and collaboration tools.

To complete the activation of your account please click the following link:
https://secureaccess.exostartest.com/idprov/accesslogin/Process1Otp.faces?p1=dXNlckFjY2Vzc0FjY3RSZWY9MTIyMS00MDMyLTQwMjUtMzQ1NCZwYXNzd2QxPWJJT2pzOTBCZFlLdmtUUFBJemdfZEE1b3hBZF9BSU1vc3VKUi0tSlBQemM9

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

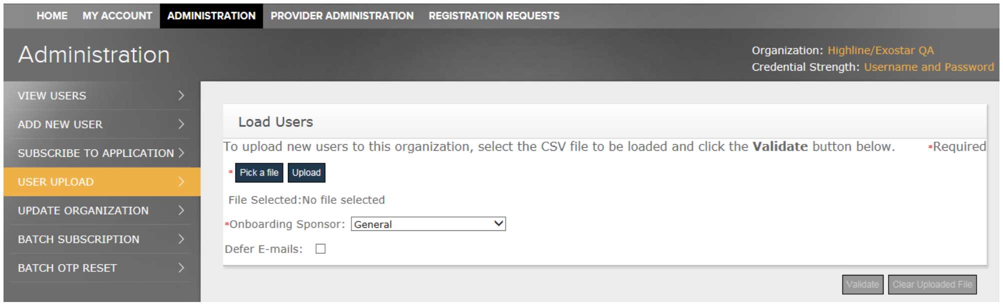
User Upload

Uploading users into SAM 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 the user and organization information directly and seamlessly.

To begin, prepare a CSV file containing user and organization information. See Appendix for samples and templates of acceptable .csv file formats. When preparing the file, include either a R-IDP User ID or a password for each user:

- **R-IDP**: provisions the user directly using enterprise credentials
- **Password**: provisions the user only in SAM with the username/password. If the user's organization is enabled with EAG, the user may later link to their enterprise credentials for SSO.

1. Access the **Administration** tab. Click **User Upload** link.



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

To upload new users to this organization, select the CSV file to be loaded and click the **Validate** button below. *Required

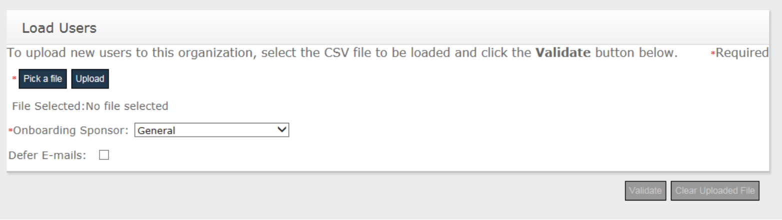
File Selected:No file selected

*Onboarding Sponsor: General

Defer E-mails: □

2. To upload new users to your organization, create a .csv file that contains user information. See **Appendix** 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**.



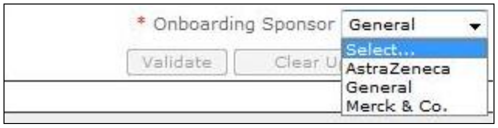
To upload new users to this organization, select the CSV file to be loaded and click the **Validate** button below. *Required

File Selected:No file selected

*Onboarding Sponsor: General

Defer E-mails: □

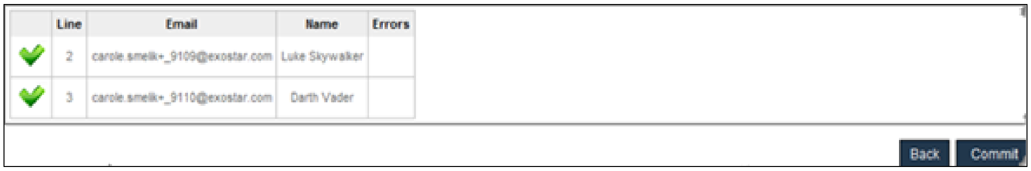
4. Using the drop-down menu, select the **Onboarding Sponsor**.



Note: The **Onboarding Sponsor** selected will affect branding, help links and content specific to that sponsor.

5. With the file selected and onboarding sponsor selected, click **Validate**. The system examines the file. If the system detects errors, they are reported on the screen.

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



	Line	Email	Name	Errors
✓	2	carole.smelik+_9109@exostar.com	Luke Skywalker	
✓	3	carole.smelik+_9110@exostar.com	Darth Vader	

7. The system successfully created the user accounts. Depending on the type of access granted, the appropriate emails are sent to the user.

Notes:

- If users are created with the *Defer E-emails* option enabled, **no first time login emails will be sent to the user**. 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 within the users 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 SAM Login Page (https://secureaccess.exostar.com) and enter their email address or User ID. SAM will then link the user to the proper RIDP.
- If an 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 SAM Login page and enter their email address or user ID.
- User not uploaded with an R-IDP ID will receive the **Account Activation** email.

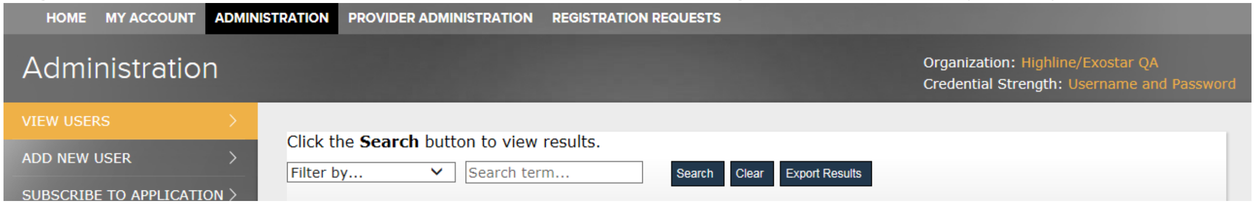
User Self-Registration

Admins may direct users to the **Self-Registration** portal to initiate their SAM account registration. The **Self-Registration** website is: https://secureaccess.exostar.com/userRegistration.

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

How to Locate and Modify Users

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



Administration

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

Click the **Search** button to view results.

You can use the search filters to help narrow your search.

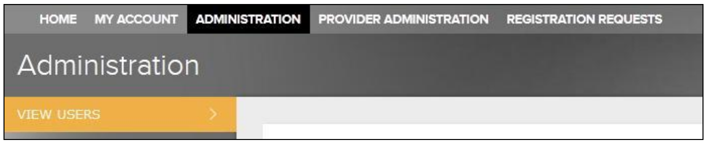
Once a user is located, you may view and update their user profile and/or role, and the applications to which they have access from the user's **Details** page.

A user's details page contains two sections:

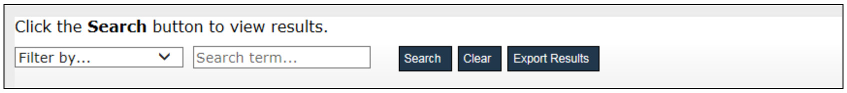
1. **User Profile**: you can view and update the details of the individual's profile.
2. **Application Settings**: you can view and update a user role, application access and SAM access. You can also reset the user's one-time password.

To locate and update a user's account:

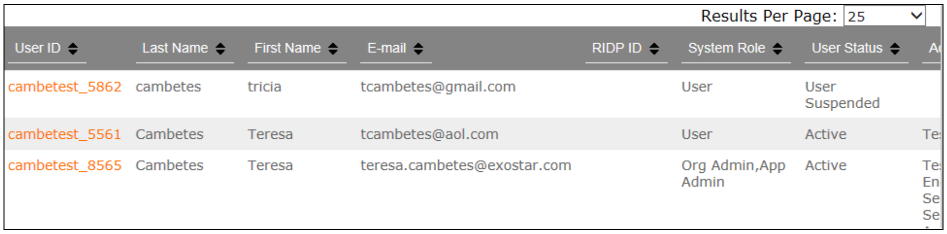
1. Access the **Administration** tab on the SAM portal. Click **View Users**.



2. To search for a user, you can use search filters to narrow your search, or view the complete list of users in your Organization. Enter search criteria, or simply click **Search** to list all users in your organization.

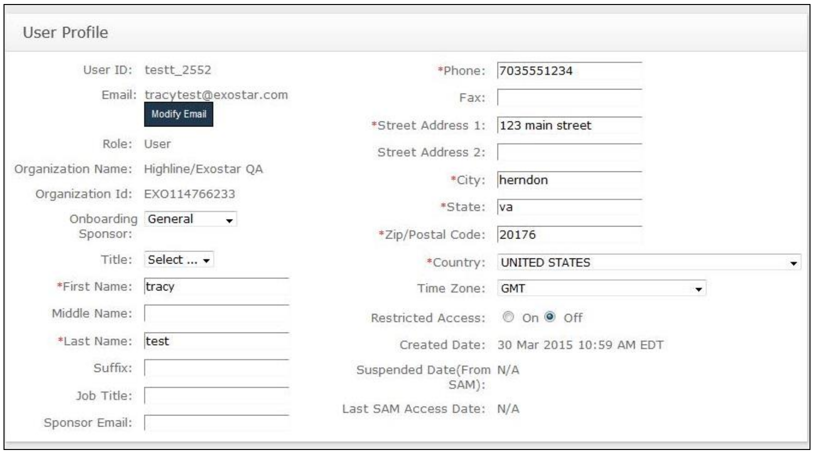

Click the **Search** button to view results.

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


Results Per Page: 25

User ID	Last Name	First Name	E-mail	RIDP ID	System Role	User Status	A
cambetest_5862	cambetes	tricia	tcambetes@gmail.com		User	User Suspended	
cambetest_5561	Cambetes	Teresa	tcambetes@aol.com		User	Active	Te
cambetest_8565	Cambetes	Teresa	teresa.cambetes@exostar.com		Org Admin,App Admin	Active	Te En Se Se

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



User Profile

User ID: testt_2552
Email: tracytest@exostar.com

Role: User
Organization Name: Highline/Exostar QA
Organization Id: EXO114766233
Onboarding Sponsor: General
Title: Select ...
*First Name: tracy
Middle Name:
*Last Name: test
Suffix:
Job Title:
Sponsor Email:

*Phone: 7035551234
Fax:
*Street Address 1: 123 main street
Street Address 2:
*City: herndon
*State: va
*Zip/Postal Code: 20176
*Country: UNITED STATES
Time Zone: GMT
Restricted Access: ○ On ● Off
Created Date: 30 Mar 2015 10:59 AM EDT
Suspended Date(From SAM): N/A
Last SAM Access Date: N/A

The **Modify Email** option allows you to update a user's email address. When an Org Admin modifies the email address, the user will receive an email containing an activation code and steps to follow to activate the new email address. The new email address is not reflected in SAM until the user completes the activation process. *(**Note**: This feature will not work with SSO/EAG users.)*

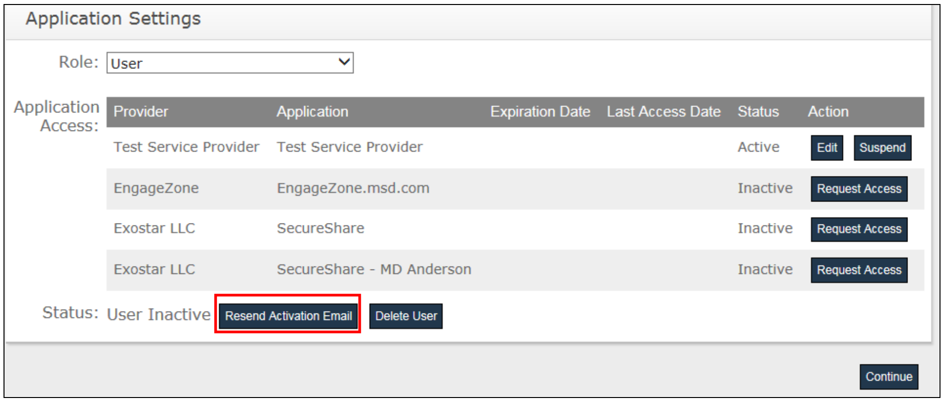
5. Verify the changes. You can click **Modify** to go back and make further changes or corrections, or **Cancel** to go back to the **Search** page. Click **Submit** to continue.

6. A confirmation page displays and the changes are saved in the system.

How to Resend Activation Email

In the **Application Settings** section of the **User Details** page, an Organization Admin can select to resend the **Activation Email** for inactive users.

1. Locate the user and access the profile page (as detailed above).
2. If a user account has an **Inactive** status, Org Admins can click **Resend Activation Email**.



Application Settings

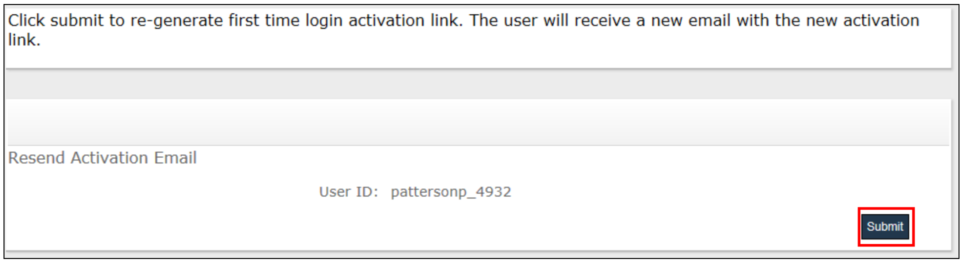
Role: User

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

3. A confirmation page displays. Click **Submit** to resend the email.



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

Resend Activation Email

User ID: pattersonp_4932

How to Suspend, Reactivate and Delete User Accounts

On the User Details page in the **Application Settings** section, there are several account access management features available including:

- Suspend, Edit and Reactivate access to an application
- Suspend access to SAM
- Permanently delete access to SAM

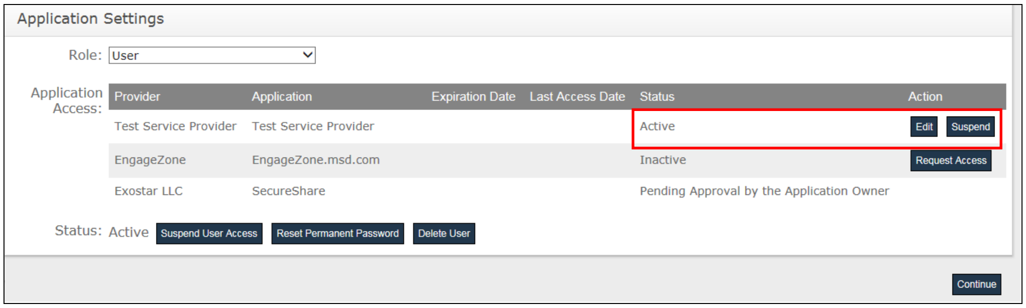
The system will notify users by email of a suspension or deletion action.

How to Suspend, Edit and Reactivate Application Access

1. Locate the user and access the profile page (as detailed above).
2. The Org Admin can **Suspend, Edit and Reactive** a user's access to an application.

   Click **Suspend** next to the appropriate application to suspend access to the solution.

   Click **Edit** to modify the subscription period for the solution.



Application Settings

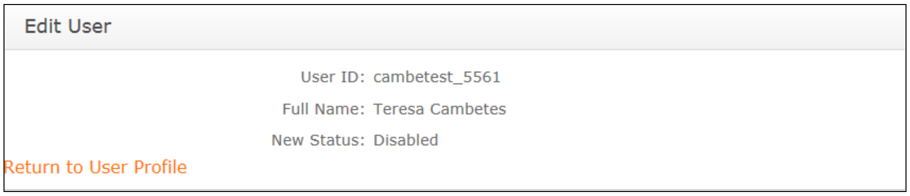
Role: User

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			Pending Approval by the Application Owner	

Status: Active

3. Click Continue. A confirmation page displays. The user status updates to **Inactive**.



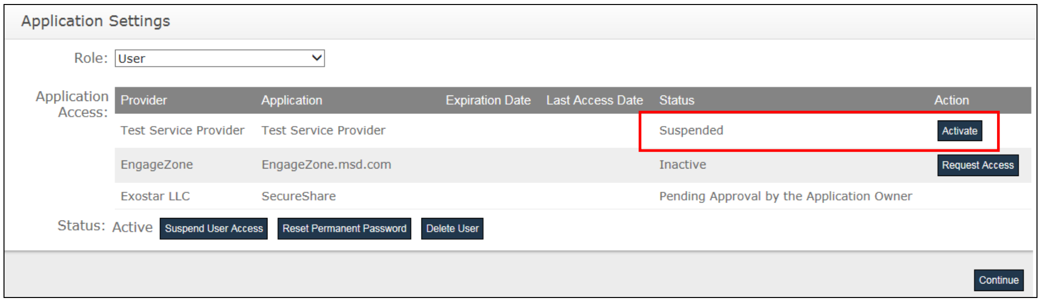
Edit User

User ID: cambetest_5561

Full Name: Teresa Cambetes

New Status: Disabled

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



Application Settings

Role: User

Application Access:

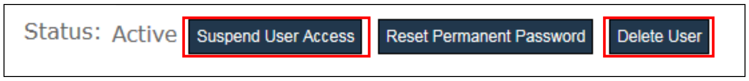
Provider	Application	Expiration Date	Last Access Date	Status	Action
Test Service Provider	Test Service Provider			Suspended	Activate
EngageZone	EngageZone.msd.com			Inactive	Request Access
Exostar LLC	SecureShare			Pending Approval by the Application Owner	

Status: Active

5. A confirmation page displays.

How to Delete a User Account in SAM

1. Locate the user and access the profile page (as detailed above).
2. The Org Admin can **Suspend** or **Delete** a user's access to SAM. To suspend access, click **Suspend User Access**. Click **Delete User** to permanently delete a user account in SAM.



Status: Active

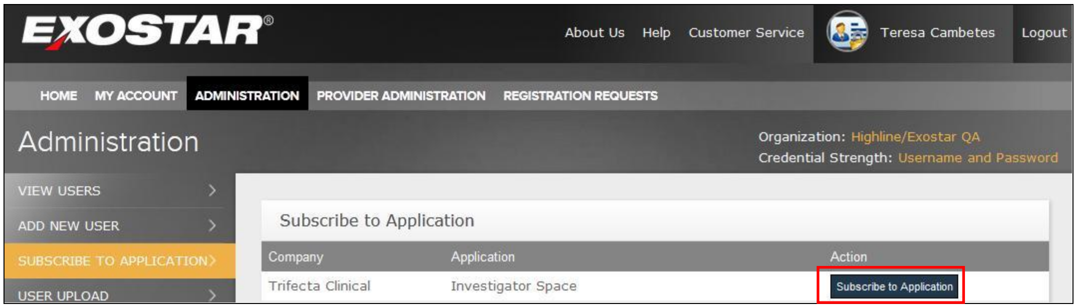
3. A confirmation page displays.

How to Subscribe your Organization to an Application

The **Subscribe to Application** link allows an Org Admin to initiate an application subscription for their organization. ***Note****: Most applications are invitation-only, and require the Exostar EPA to complete the subscription*.

To subscribe your organization to an application:

1. Access the **Administration** tab. Locate the desired application and click **Subscribe to Application**.



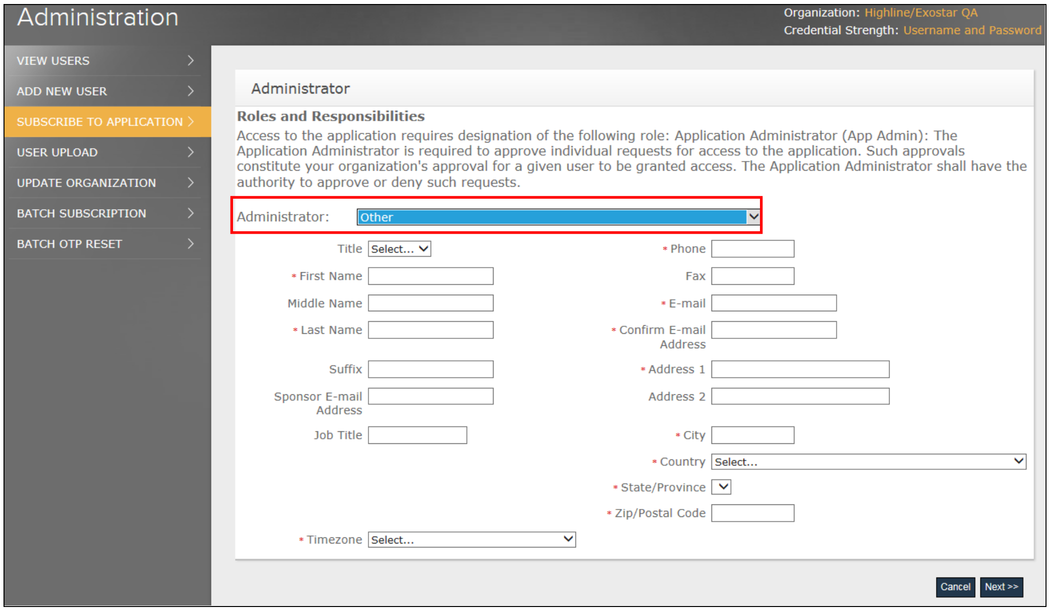
Administration

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

Subscribe to Application

Company	Application	Action
Trifecta Clinical	Investigator Space	Subscribe to Application

2. Complete the Administrator information page. You may choose to select an existing administrator from the drop down list or enter information for a new administrator. Click **Next**.



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

Administrator

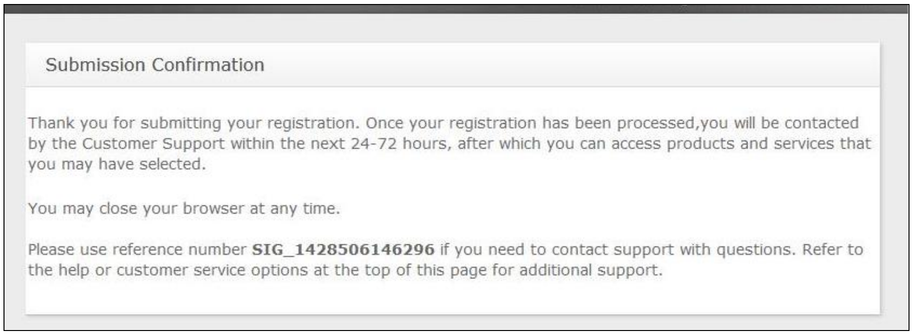
Roles and Responsibilities

Access to the application requires designation of the following role: Application Administrator (App Admin): The Application Administrator is required to approve individual requests for access to the application. Such approvals constitute your organization's approval for a given user to be granted access. The Application Administrator shall have the authority to approve or deny such requests.

Administrator: Other

Title	Select...	• Phone	
• First Name		Fax	
Middle Name		• E-mail	
• Last Name		• Confirm E-mail Address	
Suffix		• Address 1	
Sponsor E-mail Address		Address 2	
Job Title		• City	
		• Country	Select...
		• State/Province	
		• Zip/Postal Code	
• Timezone	Select...		

3. Confirm the administrator selection and information. Click **Next**.
4. The submission confirmation displays. The confirmation contains the reference number.



Submission Confirmation

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.

You may close your browser at any time.

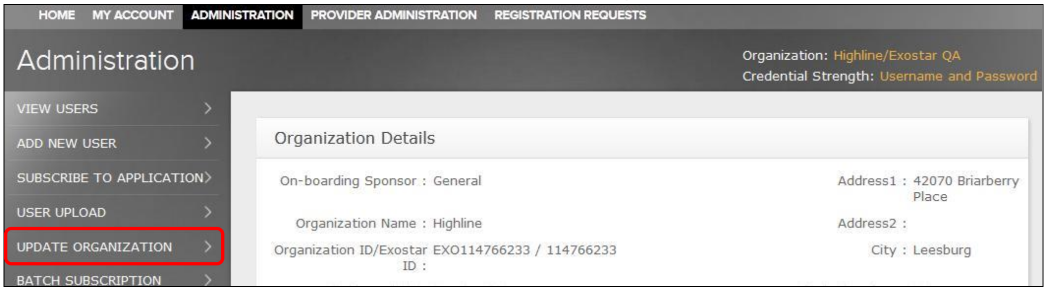
Please use reference number **SIG_1428506146296** if you need to contact support with questions. Refer to the help or customer service options at the top of this page for additional support.

How to Update Organization's Allowed Email Domains

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

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

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

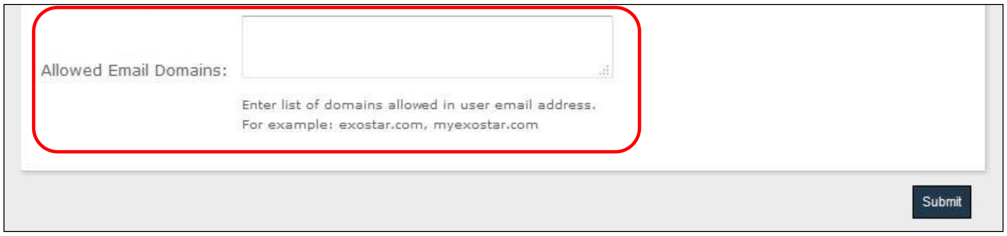


Organization: Highline/Exostar QA
Credential Strength: Username and Password

Organization Details

On-boarding Sponsor : General
Organization Name : Highline
Organization ID/Exostar ID : EXO114766233 / 114766233
Address1 : 42070 Briarberry Place
Address2 :
City : Leesburg

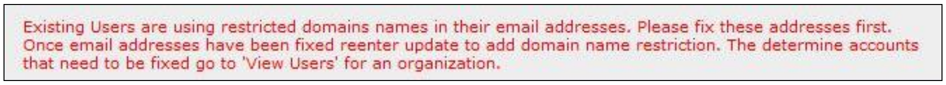
2. Enter email domains permitted for automatic provisioning. (**Example**: exostar.org). Click **Submit**.



Allowed Email Domains:

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, the following error is presented. Correct the list of domains to include all current user domains, or modify user emails to address in order to comply with the restriction.



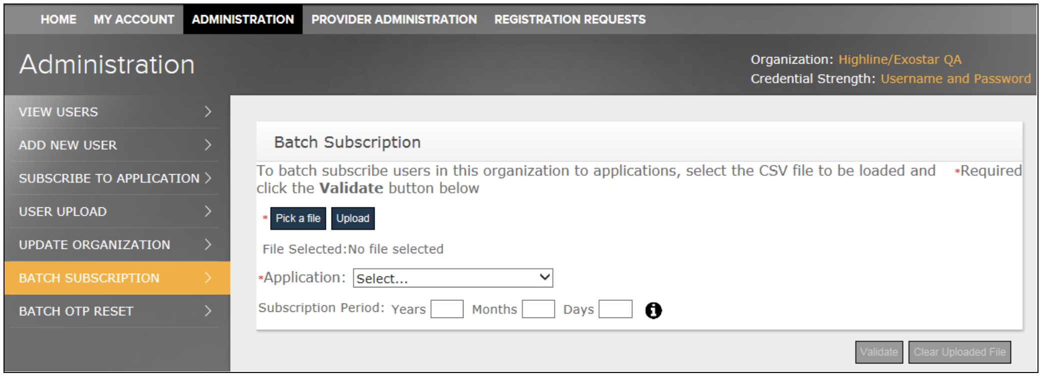
Existing Users are using restricted domains names in their email addresses. Please fix these addresses first. Once email addresses have been fixed reenter update to add domain name restriction. The determine accounts that need to be fixed go to 'View Users' for an organization.

4. Click **Submit**.

How to Add Multiple Users to an Application - Batch Subscription

Org Admins may choose to provision existing user accounts to a specific application in bulk using the **Batch Subscription** function. With this, administrators simply upload a .csv file containing user IDs and the subscription period (optional).

1. Access the **Administration** Tab. Click **the Batch Subscription** link.



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

Batch Subscription

To batch subscribe users in this organization to applications, select the CSV file to be loaded and click the **Validate** button below

*Required

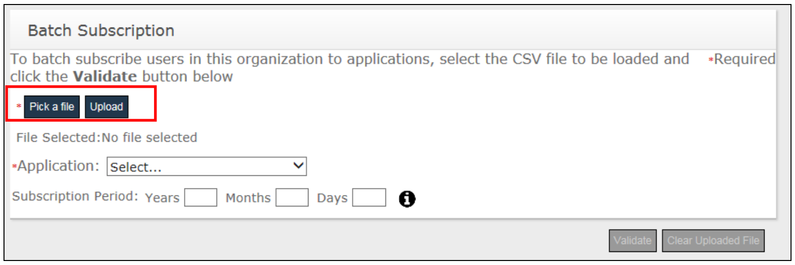
File Selected:No file selected

*Application: Select...

Subscription Period: Years Months Days

2. Click **Pick a file** to locate the file containing user information. (See **Appendix** for file formatting requirements).

Click **Upload** to upload the file.

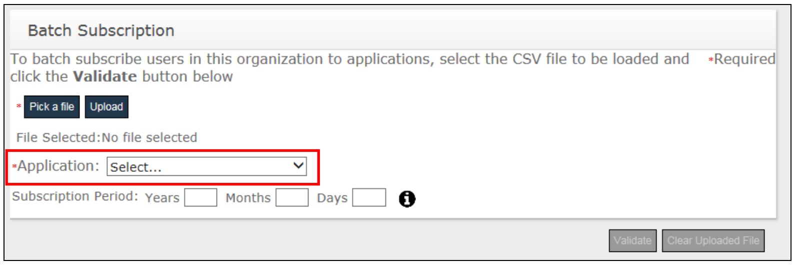


Batch Subscription

To batch subscribe users in this organization to applications, select the CSV file to be loaded and click the **Validate** button below

File Selected:No file selected

3. Select the application you want to add the users to. Click **Validate** to proceed.



Batch Subscription

To batch subscribe users in this organization to applications, select the CSV file to be loaded and click the **Validate** button below

File Selected:No file selected

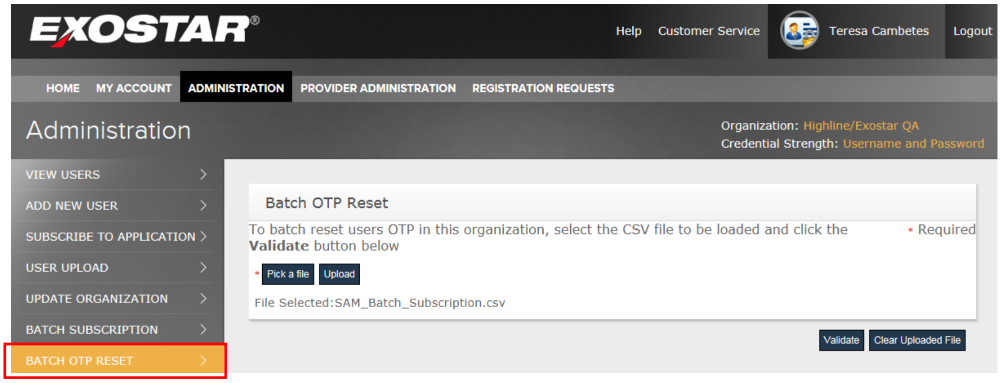
4. A confirmation message displays. Click **Commit** to load user subscriptions.

   Note: Users indicated with a green checkmark are granted access If any users are listed with a Red X mark, errors are listed and should be corrected.

How to Reset Inactive Accounts – Batch Reset

If there are multiple users who are inactive and activation emails need to be triggered for them, Org Admins can reset OTP accounts using the **Batch OTP Reset** function. This feature allows administrators to simply upload a .csv file containing user IDs.

1. Access the **Administration** Tab. Click **the Batch OTP Resets** link.



Administration

Organization: Highline/Exostar QA

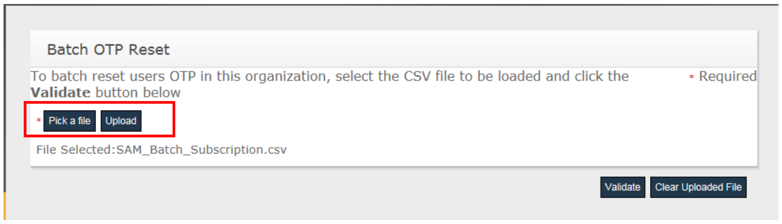
Credential Strength: Username and Password

Batch OTP Reset

To batch reset users OTP in this organization, select the CSV file to be loaded and click the **Validate** button below

File Selected:SAM_Batch_Subscription.csv

2. Click **Pick a file** to locate the file containing user information. (See Appendix for file formatting requirements). Click **Upload** to upload the file.



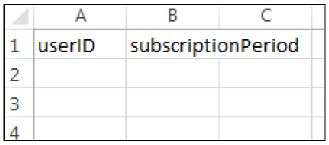
Batch OTP Reset

To batch reset users OTP in this organization, select the CSV file to be loaded and click the **Validate** button below

* Required

File Selected:SAM_Batch_Subscription.csv

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



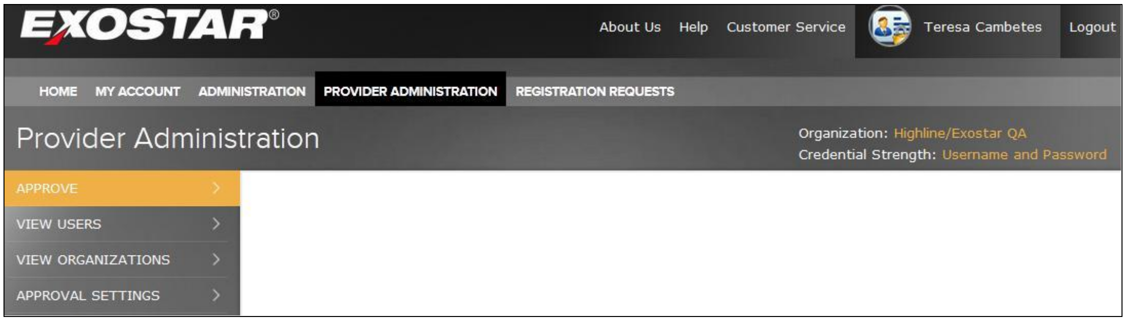
	A	B	C
1	userID	subscriptionPeriod	
2			
3			
4			

3. Click **Validate** to proceed.

4. A confirmation message displays. Click **Commit** to complete the reset.

The Provider Administration Tab - Service Provider Administrators

Service Provider Administrators (SP Admins) can access the **Provider Administration** tab in order to approve and provision users and organizations in specific applications. Often referred to as application owners, the SP Admin manages access to the application that they administer.



Provider Administration

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

- **Approve link**: displays the list of all users awaiting approval for access to the application.
- **View Users** link: allows the SP Admin to search for users subscribed to the application.
- **View Organizations link**: allows the SP Admin to search for organizations subscribed to the application.
- **Approval Settings** link: allows the SP Admin to add to the list of organizations whose users do not require your approval for access to the application.

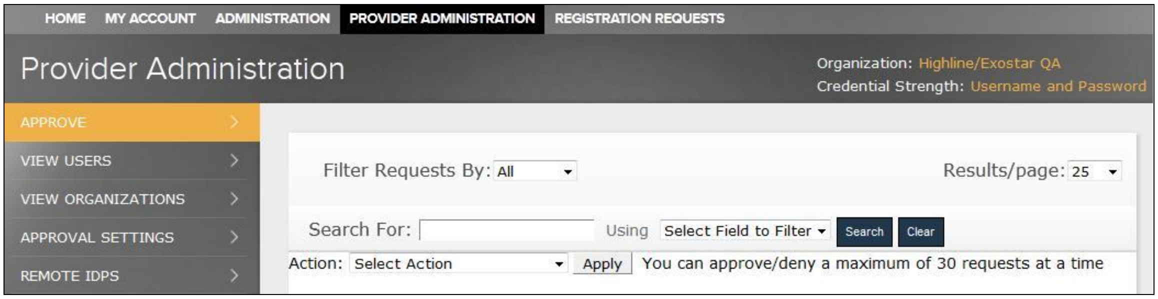
Approve: Approving User Access Requests

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

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

How to Filter and Search for Users

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



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

Filter Requests By: All

Results/page: 25

You can approve/deny a maximum of 30 requests at a time

2. Use the search filters and fields to locate a specific approval request.

   The following search filter fields are available:

   - **Filter Request By:** allows you to filter by All, New, and Pending requests
   - **Search For:** allows you to enter a search criteria, such as user name, user ID, or organization information

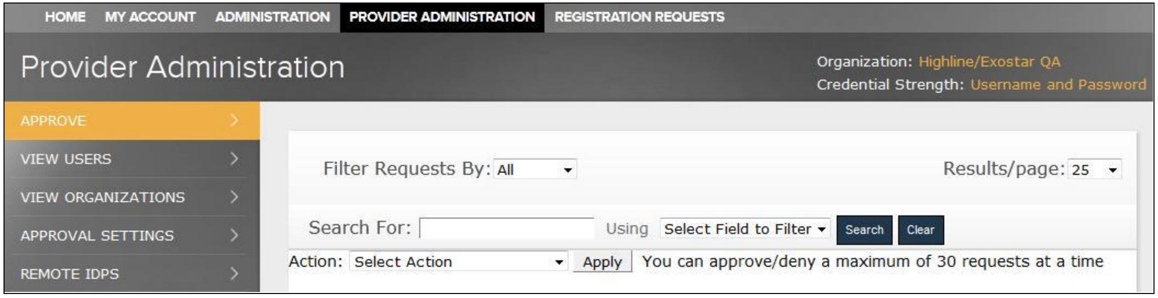
   Enter search criteria and click **Search**.

3. The search results display. Click the **Request ID** link to access the desired request.

How to Process User Access Requests

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

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



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

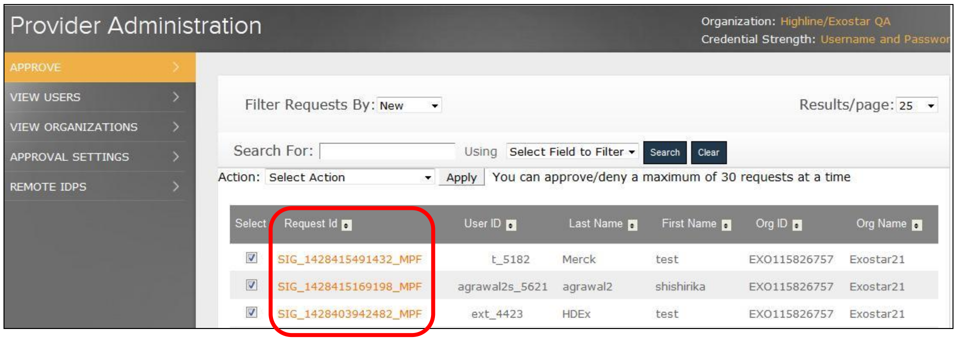
Filter Requests By: All

Results/page: 25

You can approve/deny a maximum of 30 requests at a time

2. To approve or deny an individual access request, select the desired request by clicking the **Request Id** link.

   To approval or deny multiple requests, select the desired requests by placing a checkmark in the box next to the **Request ID** link.



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

Filter Requests By: New

Results/page: 25

Search For:

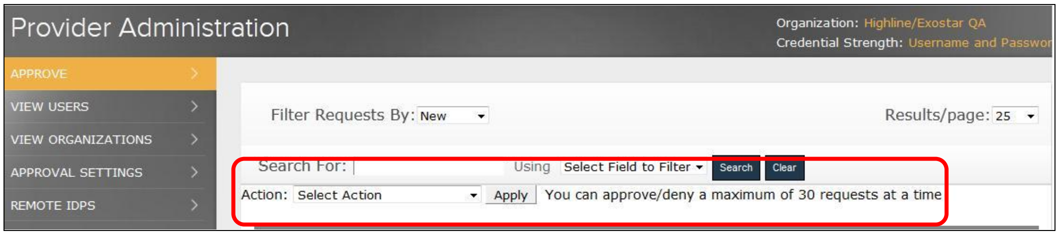
Using Select Field to Filter

Action: Select Action

You can approve/deny a maximum of 30 requests at a time

Select	Request Id	User ID	Last Name	First Name	Org ID	Org Name
☑	SIG_1428415491432_MPF	t_5182	Merck	test	EXO115826757	Exostar21
☑	SIG_1428415169198_MPF	agrawal2s_5621	agrawal2	shishirika	EXO115826757	Exostar21
☑	SIG_1428403942482_MPF	ext_4423	HDEx	test	EXO115826757	Exostar21

3. Select the desired **Action**.



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

Filter Requests By: New

Results/page: 25

Search For:

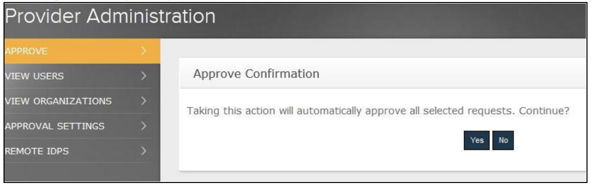
Using Select Field to Filter

Action: Select Action

You can approve/deny a maximum of 30 requests at a time

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

4. A confirmation message displays. The users will receive an email advising of approval.



Approve Confirmation

Taking this action will automatically approve all selected requests. Continue?

View Users: Locate and Update User Accounts

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

- Search for user accounts
- View user account details, including SAM Status, Active Applications, and Pending Applications
- Suspend and Restore a User's application access

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

How to Locate a User Account

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

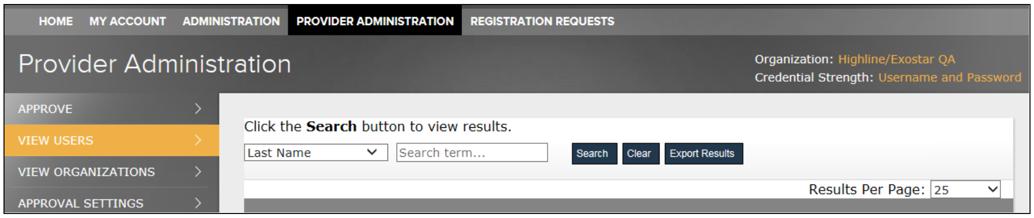
A user's details page contains two sections:

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

To locate a user:

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

2. Click the **View Users** link.



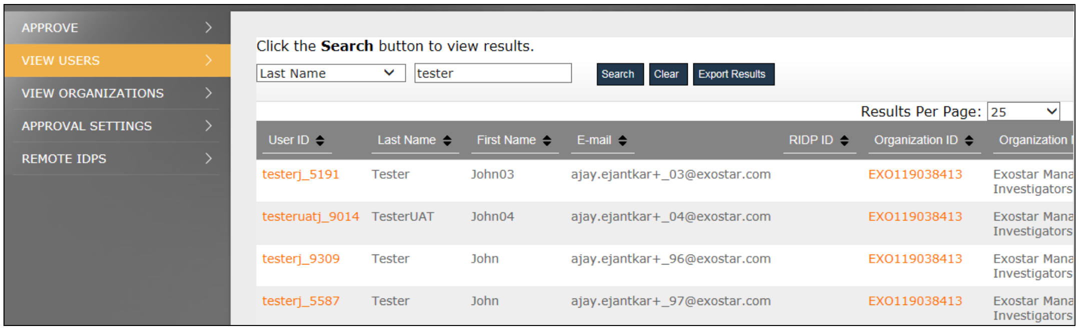
Organization: Highline/Exostar QA
Credential Strength: Username and Password

Click the **Search** button to view results.

Last Name | Search term...

Results Per Page: 25

3. Enter search criteria.



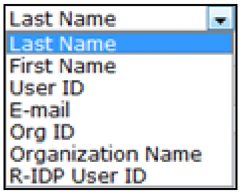
Click the **Search** button to view results.

Last Name | tester

Results Per Page: 25

User ID	Last Name	First Name	E-mail	RIDP ID	Organization ID	Organization I
testerj_5191	Tester	John03	ajay.ejantkar+_03@exostar.com		EXO119038413	Exostar Mana Investigators
testeruatj_9014	TesterUAT	John04	ajay.ejantkar+_04@exostar.com		EXO119038413	Exostar Mana Investigators
testerj_9309	Tester	John	ajay.ejantkar+_96@exostar.com		EXO119038413	Exostar Mana Investigators
testerj_5587	Tester	John	ajay.ejantkar+_97@exostar.com		EXO119038413	Exostar Mana Investigators

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



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

Note: There are two active links contained within each search result entry:

1. Click the **USER ID** link to view the profile for this particular user.
2. Click the **ORG ID** link to view the Organizational Details for this user.

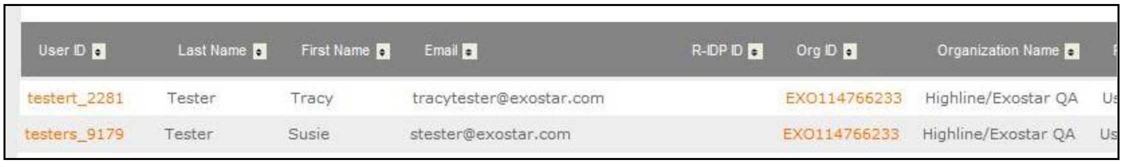
How to Suspend a User Subscription

There are times when a user may no longer require access to a specific application or resource, perhaps temporarily. However, the user needs 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:

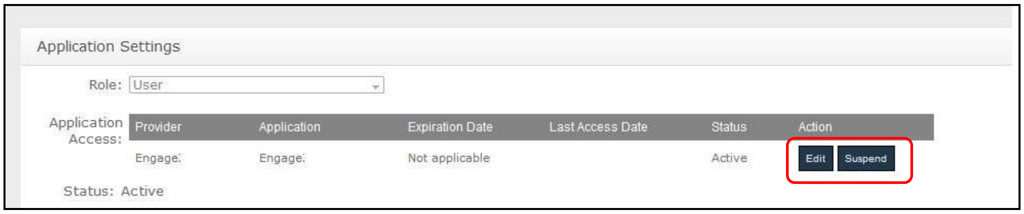
1. Login to SAM and access the **Provider Administration** tab.

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



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

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



Application Settings

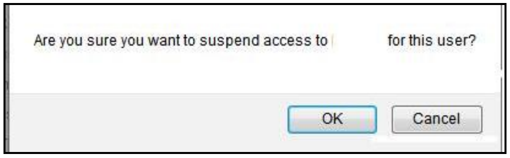
Role: User

Application Access:

Provider	Application	Expiration Date	Last Access Date	Status	Action
Engage:	Engage:	Not applicable		Active	Edit Suspend

Status: Active

4. A confirmation message displays. Click **OK**.



Are you sure you want to suspend access to for this user?

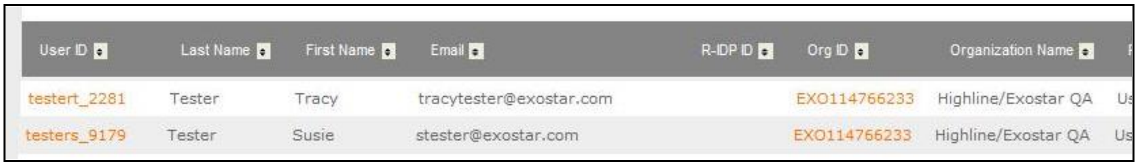
5. The user's account updates and their access to this application is suspended. An updated status for the user displays.

How to Reactivate a User's Subscription

SP Admins can reactivate a user's access to an application.

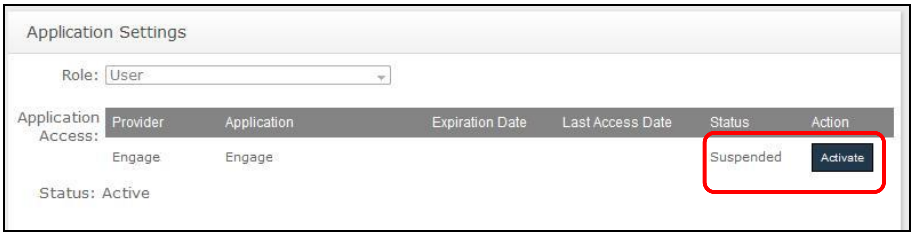
To reactivate a user account subscription:

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



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

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



Application Settings

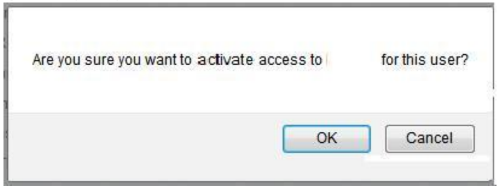
Role: User

Application Access:

Provider	Application	Expiration Date	Last Access Date	Status	Action
Engage	Engage			Suspended	Activate

Status: Active

4. A confirmation messagedisplays. Click **OK**.



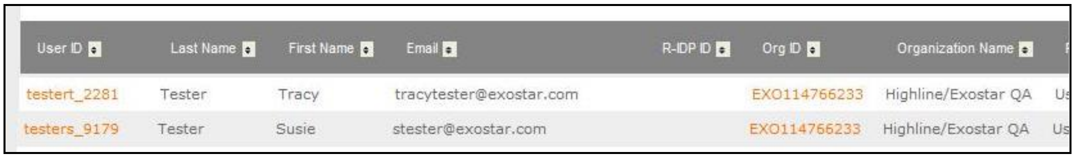
Are you sure you want to activate access to for this user?

How to Reset User's Permanent Password

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

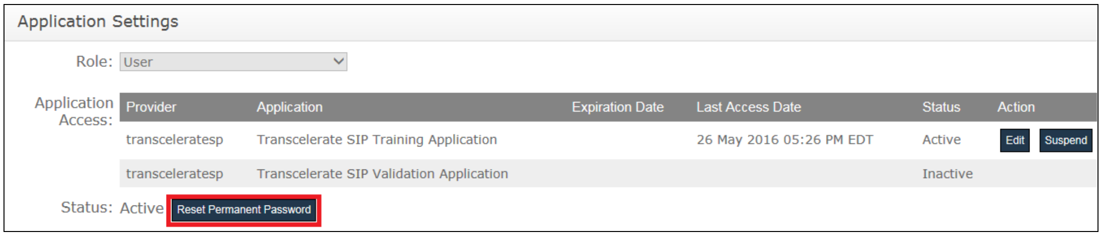
To reset a user's permanent password:

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



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

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



Application Settings

Role: User

Application Access:

Provider	Application	Expiration Date	Last Access Date	Status	Action
transceleratesp	Transcelerate SIP Training Application		26 May 2016 05:26 PM EDT	Active	Edit Suspend
transceleratesp	Transcelerate SIP Validation Application			Inactive	

Status: Active Reset Permanent Password

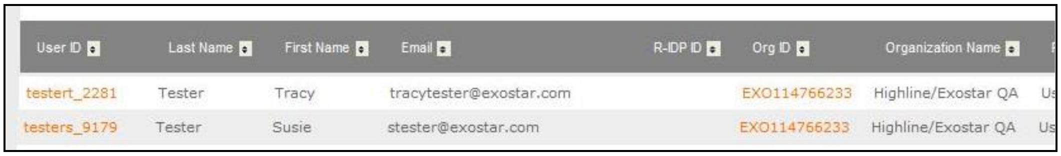
4. A confirmation message displays, and an email is sent to the user's email address. The email contains a system-generated password.

How to Resend Activation Email

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

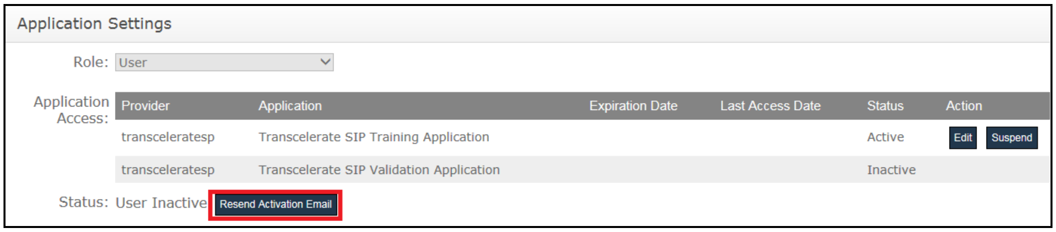
To resend the activation email: .

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



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

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



Application Settings

Role: User

Application Access:

Provider	Application	Expiration Date	Last Access Date	Status	Action
transceleratesp	Transcelerate SIP Training Application			Active	Edit Suspend
transceleratesp	Transcelerate SIP Validation Application			Inactive	

Status: User Inactive

4. A confirmation message displays.

View Organizations

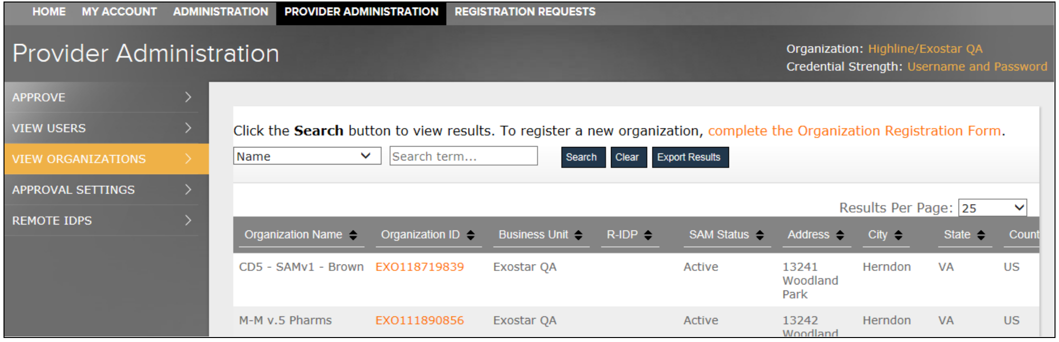
The View Organizations page provides SP Admins the ability to view and action organizations subscribed to their application. Administrators can also suspend and reactive organizational access to the resource.

SP Admins can take the following actions:

- Search for an Organization
- View Organization details, including Active Applications
- Suspend and Restore an Organizations application access

How to Locate an Organization

1. Login to SAM and access the **Provider Administration** tab.
2. Click the **View Organizatio**ns link .



Provider Administration

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

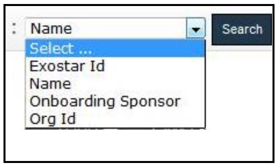
Click the **Search** button to view results. To register a new organization, complete the Organization Registration Form.

Name | Search term...

Results Per Page: 25

Organization Name	Organization ID	Business Unit	R-IDP	SAM Status	Address	City	State	Count
CD5 - SAMv1 - Brown	EXO118719839	Exostar QA		Active	13241 Woodland Park	Herndon	VA	US
M-M v.5 Pharms	EXO111890856	Exostar QA		Active	13242 Woodland	Herndon	VA	US

3. Enter search filters criteria. Then, select the desired search filter. Click **Search**.



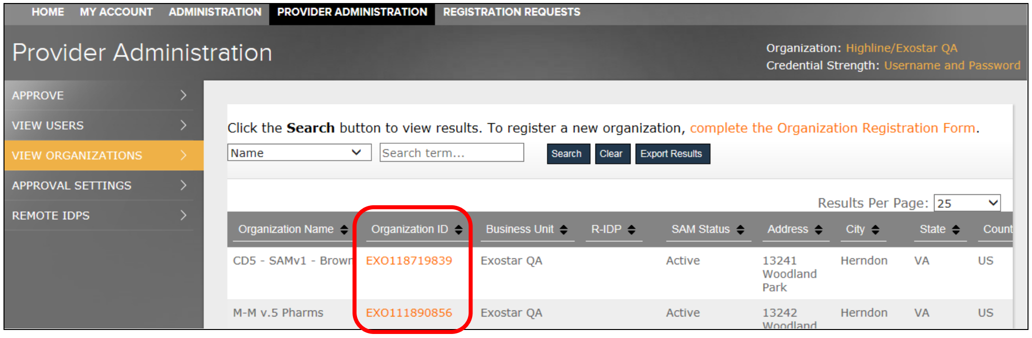
Note: You can leave the search criteria fields blank and a full list of all organizations will display.

4. The search results displays. Click the **Organization ID** to view all org information, contacts, and administrators.

Suspend an Organization's Access

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

1. Locate the organization you would like to suspend access. Click on the **Org ID** for the applicable organization.



Provider Administration

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

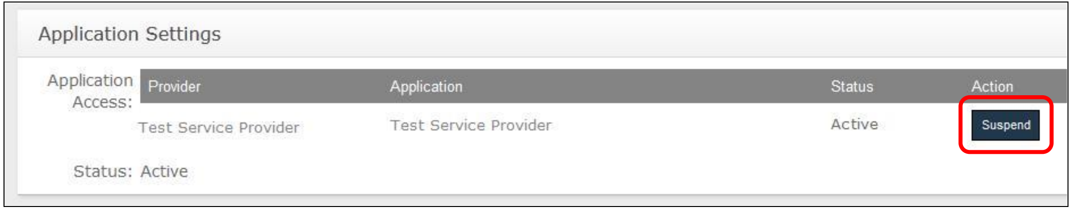
Click the **Search** button to view results. To register a new organization, complete the Organization Registration Form.

Name | Search term...

Results Per Page: 25

Organization Name	Organization ID	Business Unit	R-IDP	SAM Status	Address	City	State	Count
CD5 - SAMv1 - Brown	EXO118719839	Exostar QA		Active	13241 Woodland Park	Herndon	VA	US
M-M v.5 Pharms	EXO111890856	Exostar QA		Active	13242 Woodland	Herndon	VA	US

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



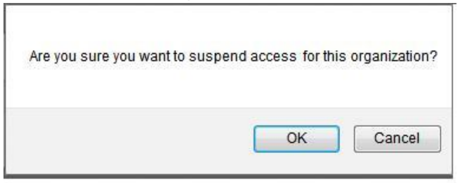
Application Settings

Application Access:

Provider	Application	Status	Action
Test Service Provider	Test Service Provider	Active	Suspend

Status: Active

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



Are you sure you want to suspend access for this organization?

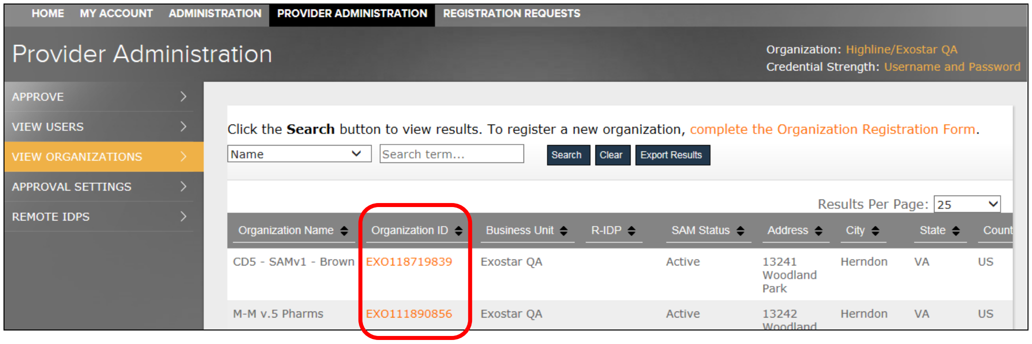
4. A confirmation message displays.

Reactivate an Organization's Access

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

To reactive access:

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



Provider Administration

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

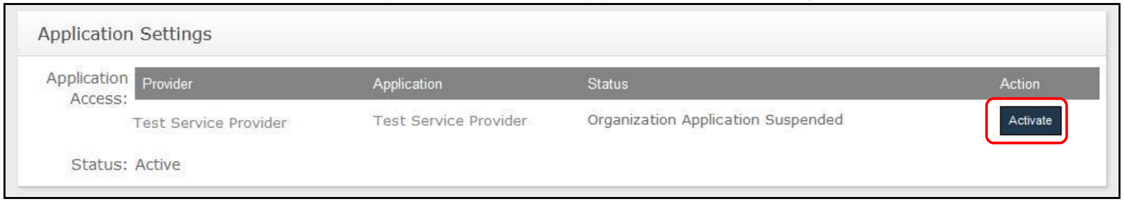
Click the **Search** button to view results. To register a new organization, complete the Organization Registration Form.

Name | Search term...

Results Per Page: 25

Organization Name	Organization ID	Business Unit	R-IDP	SAM Status	Address	City	State	Count
CD5 - SAMv1 - Brown	EXO118719839	Exostar QA		Active	13241 Woodland Park	Herndon	VA	US
M-M v.5 Pharms	EXO111890856	Exostar QA		Active	13242 Woodland	Herndon	VA	US

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



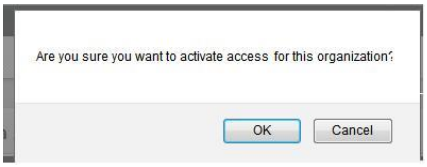
Application Settings

Application Access:

Provider	Application	Status	Action
Test Service Provider	Test Service Provider	Organization Application Suspended	Activate

Status: Active

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



Are you sure you want to activate access for this organization?

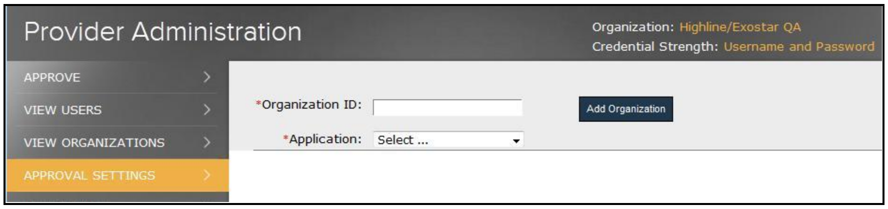
4. A confirmation message displays.

Approval Settings

The Approval Settings page allows SP Admins to set automatic approvals for all users from a given organization. For example, users from organizations in the ‘approved list’ do not need to be approved by a SP Admin.

How to Add an Organization to the Approved List

1. Login to SAM and access the **Provider Administration** tab.
2. Click the **Approval Setting** link.



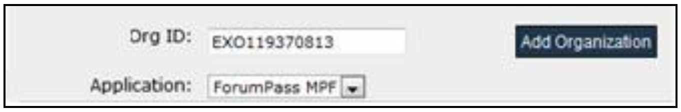
Provider Administration

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

*Organization ID:

*Application: Select ...

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



Org ID: EXO119370813

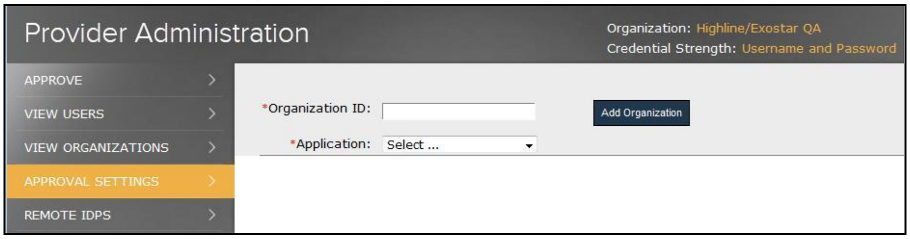
Application: ForumPass MPF

4. The page will refresh, now showing the organization on the approved list. ***Note****: You may add as many organizations as you wish to the approval list for each application*

How to Remove an Organization from the Approved List

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

1. Login to SAM and access the **Provider Administration** tab.
2. Click the **Approval Setting** link.



Provider Administration

Organization: Highline/Exostar QA

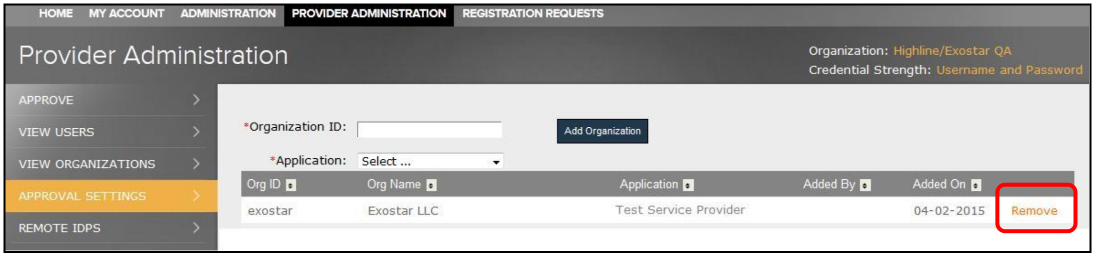
Credential Strength: Username and Password

*Organization ID:

*Application: Select ...

3. Use the search fields to locate the desired organization.

4. Click the **Remove** link to remove of an organization from the approved list.



Provider Administration

Organization: Highline/Exostar QA

Credential Strength: Username and Password

*Organization ID:

*Application: Select ...

Org ID	Org Name	Application	Added By	Added On	
exostar	Exostar LLC	Test Service Provider		04-02-2015	Remove

The Registration Requests Tab

The **Registration Requests** tab lists all pending user requests, which include requests for SAM access and requests for application access.

1. **Verify** link provides access to the list of all users who have self-registered, and are pending SAM access approval. These approvals are handled by the Org Admin.

2. **Authorize** link provides access to the list of all users who have been approved in SAM by the Organization Admin and are pending application access approval. These approvals are handled by the App Admin.

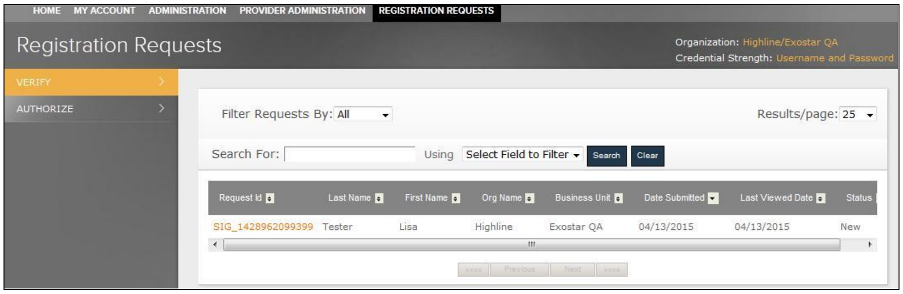
***Note**: The links available may depend upon your role. For example, the Org Admin role will not show the Authorize link.*

User Access Approvals (Verify Link)

An Organization Administrator will receive an email notice when a new user access request is pending. The **Verify** link will display all users who have been through the self-registration process and are awaiting SAM approval. An Org Admin will verify the user's registration information and confirm employment status prior to approval.

1. When user completes the self-registration process, the Org Admin will receive an email notifying them that there is a pending user request.

2. Login to SAM as an Org Admin and access the **Registration Requests** tab. Access the **Verify** link to view the list of pending requests.

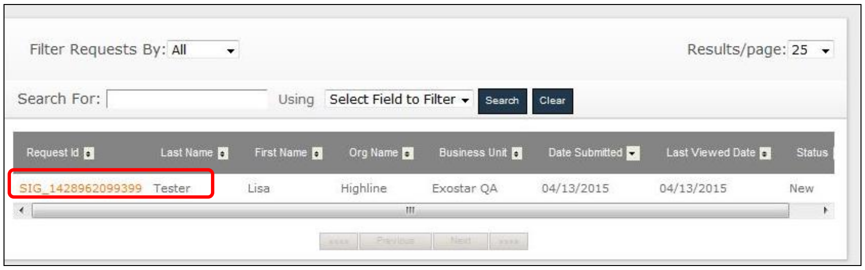


Organization: Highline/Exostar QA
Credential Strength: Username and Password

Filter Requests By: All
Results/page: 25
Search For: Using Select Field to Filter

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

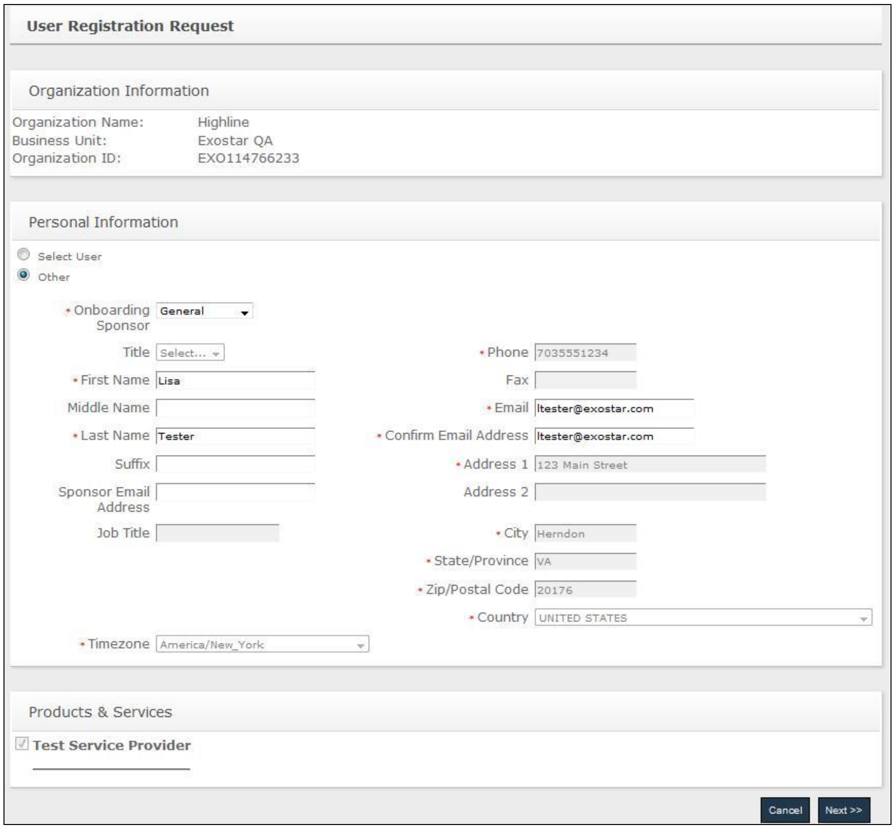
3. Click the **Request Id** link associated with the request you would like to approve.



Filter Requests By: All
Results/page: 25
Search For: Using Select Field to Filter

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

4. Review the **User Registration Request** information including the **Products & Services** access request. Click **Next.**



User Registration Request

Organization Information

Organization Name: Highline
Business Unit: Exostar QA
Organization ID: EXO114766233

Personal Information

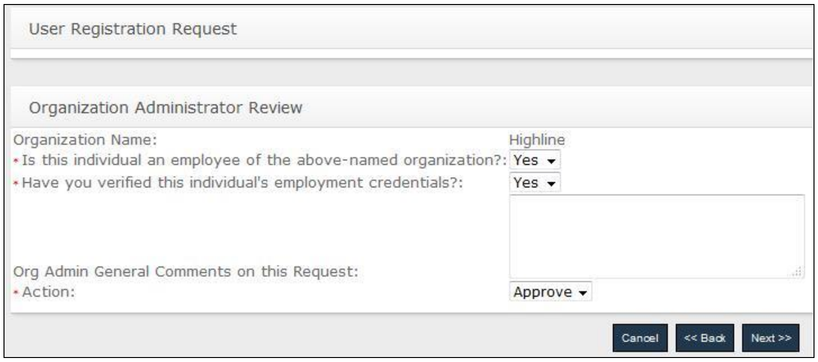
○ Select User
● Other

* Onboarding Sponsor: General
Title: Select...
* First Name: Lisa
Middle Name:
* Last Name: Tester
Suffix:
Sponsor Email Address:
Job Title:
* Timezone: America/New_York
* Phone: 7035551234
Fax:
* Email: ltester@exostar.com
* Confirm Email Address: ltester@exostar.com
* Address 1: 123 Main Street
Address 2:
* City: Herndon
* State/Province: VA
* Zip/Postal Code: 20176
* Country: UNITED STATES

Products & Services

☑ Test Service Provider

5. Complete all required fields confirming you have validated the user credentials. Click **Next**.



User Registration Request

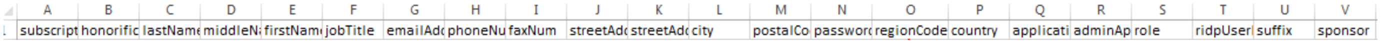
Organization Administrator Review

Organization Name: Highline
* Is this individual an employee of the above-named organization?: Yes
* Have you verified this individual's employment credentials?: Yes
Org Admin General Comments on this Request:
* Action: Approve

Note: If you select to **Deny** the request for access, you are then required to enter **Comments** to address the reason for denial.

6. A **Confirmation** page displays and the user is active in SAM.

Appendix A – CSV File Requirements – User Uploads



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1	subscript	honorific	lastName	middleN	firstNam	jobTitle	emailAdd	phoneNu	faxNum	streetAdd	streetAdd	city	postalCo	passworc	regionCode	country	applicati	adminAp	role	ridpUser	suffix	sponsor

Field	Cardinality/ Values	Response/Comments
subscription Period	Optional	Acceptable Options: #y#t#d#h#m#s e.g. 1y = 1 Year, 1y1t = 1 year + 1 month Leaving this value blank will default to the Application Maximum Subscription Duration (if provided)
Honorific	Optional	Acceptable options: Mr., Mrs., Ms., Dr.
Last Name	Required Max 32 characters	Accepts letters, numbers and printable special characters except for ‘<’ or ‘>’.
Middle Name	Optional Max 32 characters	Accepts letters, numbers and printable special characters except for ‘<’ or ‘>’.
First Name	Required Max 32 characters	Accepts letters, numbers and printable special characters except for ‘<’ or ‘>’.
Job Title	Optional Max 50 characters	Accepts letters, numbers and printable special characters except for ‘<’ or ‘>’.
Email Address	Required RFC822 compliant	Must be unique
Phone	Required Min 4 characters /Max 20 characters	Accepts only the following characters: Numbers, ‘-‘, ‘+’, ‘.’, ‘(‘, ‘)’, ‘e’, ‘t’, ‘x’ and embedded white spaces
Fax	Optional Min 4 characters / Max 20 characters	Accepts only the following characters: Numbers, ‘-‘, ‘+’, ‘.’, ‘(‘, ‘)’, ‘e’, ‘t’, ‘x’ and embedded white spaces
Street Address 1	Required Max 64 characters	Accepts letters, numbers and printable special characters except for ‘<’ or ‘>’.
Street Address 2	Optional Max 64 characters	Accepts letters, numbers and printable special characters except for ‘<’ or ‘>’.
City	Required Max 52 characters	Accepts letters, numbers and printable special characters except for ‘<’ or ‘>’.
Zip/Postal Code	Required Max 16 characters	Accepts letters, numbers and printable special characters except for ‘<’ or ‘>’.
RegionCode	Required	Accepts letters, numbers and printable special characters except for ‘<’ or ‘>’.
Country	Required	Must be in the form of ISO 3166-1 Alpha-2 Code (i.e. United States = US)
Applications	Required	Multiple applications must be separated by a semicolon ‘;’ Organization must be subscribed to the listed application(s)
Application Admin	Optional	Multiple applications must be separated by a semicolon ‘;’ User will be assigned the application administrator role for application(s) listed in the column Organization must be subscribed to the application(s) listed
Role	Required	User or Admin User will be assigned the organization administrator role if ‘Admin’ is listed in the column

R-IDP User ID	Optional	R-IDP User ID must be unique for the associated R-IDP Organization must be associated to an R-IDP Note: For Merck, the R-IDP User ID and the ISID are the same thing.
Suffix	Optional	4 Char Limit
Sponsor Email Address	Optional RFC822 compliant	75 Char Limit
RegionCode	Required	

Appendix B – CSV File Requirements – Batch Subscription

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