Managed Access Gateway (MAG) User Guide

November 2023

Contents

Document Versions

Version	Impacts	Date	Owner
MAG 6.14	• Remove One-Time Password from First-Time Login process • Update Password Policy	May 2020	B. Nair
MAG 7.0	• Self-Registration • New Organization Adoption Invitation registration process • Dashboard • Purchasing • Credentialing • Activation • Authentication	February 2021	Beena Nair
MAG 7.3	• My 2FA Credentials Section	August 2022	Sam Boateng
MAG 7.5	• Proofing and credentialling enhancements • Credential management enhancement • Accepting Terms and Conditions • Reports enhancements • Login and registration UI enhancements	April 2023	Sam Boateng
MAG 7.6	• Update on add user page full name • Bulk Uploads enhancements • Locked requests fixed • Stronger Password Security features • Resent Activation Email fixed	August 2023	Sam Boateng
MAG 7.7	• Acceptable use policy message • Account locked out failed attempts • Updated text in FIS renewal email • 2FA email confirmation	November 2023	Sam Boateng

Introduction

Exostar's Managed Access Gateway (MAG) is a secure Identity and Access Management solution for highly regulated industries including Aerospace & Defense. With the cloud-based Exostar MAG Platform, users can administer accounts, purchase and activate credentials, access their partner applications, and more.

Getting Started

For your organization to access partner applications behind MAG, your company requires an account. Your partner company invites your organization to complete registration via email, for their applications.

Before users can access an application, the Organization or Application Administer must accept terms and conditions. Once an organization is registered, users require their own account. The account's MAG Organization Administrator can create user accounts or send self-registration invitations to users. After users register, they receive login information.

Additionally, a partner company's application may require a multi-factor credential (such as Exostar's Federated Identity Service (FIS) Digital Certificates or Phone One Time Password [OTP]). Using a multi-factor credential along with username/password, mitigates security risks by providing a stronger assurance level and better identity protections than conventional username/password technologies vulnerable to theft. You will be unable to access a partner company's application if you do not have the proper credential or if terms and conditions have not been accepted.

Organization and User ID Information

When an organization's account is created in MAG, the account is assigned an Organization ID. The Organization ID is a unique identifier for the organization. Once the organization account is created, users can be associated with the account. A user account is assigned a unique User ID. The User ID format is last name, first initial and typically a four-digit number (e.g. doej_1234).

Roles

MAG is a role-based solution. Users can be assigned a single role or multiple roles. Once the organization is established, Organization Administrators can add or remove roles for each user. The sections below provide additional information per role.

Exostar's Training Team hosts bi-monthly Organization and Application Administrator Trainings that provides an overview of the MAG solution, basic navigation, and basic administrator functionalities. Please visit the Training Registration page to sign-up for upcoming sessions.

Organization Administrator

The Organization Administrator is responsible for performing activities on behalf of their organization. An organization can have a single or multiple Organization Administrators. Organization Administrator responsibilities include:

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

Application and FIS Administrator

Application Administrators can only manage requests for applications they are administering, and they are responsible for approving or denying access to that specific application. When users request access to an application, the request is routed to an Application Administrator for approval. An organization can have a single or multiple Application Administrators. Additional responsibilities may include:

- Accepting Terms and Conditions for their specific applications.
- Requesting access to applications on behalf of users.
- Suspending access to applications.

User

Users have no administrative privileges for their organization's MAG account and use MAG to login and access their partner's applications.

Adoption Administrator

Adoption Administrators are responsible for inviting suppliers to use MAG and subscribing them to their partner's applications. Exostar must assign the Adoption Administrator role. For more information, please visit the Adoption Administrator page on my.exostar.com.

Service Provider (SP) Administrator

There are two types of SP Administrator roles: *administrative* and *view only*. The SP Administrator role with administrative permissions allows users to approve or deny access for specified partner applications, as well as to resend provisioning records. The SP Administrator role has view only permissions. Additionally, SP Administrators can run reports. The SP Administrator role is only available to partner companies. For more information on this role, please visit to Service Provider Administrator page on my.exostar.com.

Organization Steward

The Organization Steward role allows a single user to exercise administrative control over groups of designated organizations. Organization Stewards have the same privileges and responsibilities as Organization Administrators and Application Administrators for all applications the organizations are subscribed to. For instructions on how to obtain the Organization Steward role, please reference the Organization Steward section on my.exostar.com.

Bundle Administrator

Partner companies that have a bundled product require a Bundle Administrator. The Bundle Administrator is responsible for approving or denying bundled requests.

LOGIN INFORMATION

Your MAG account was created for you to access partner applications. You must activate your account, which includes completing permanent password and security questions/answers set-up.

Account Activation

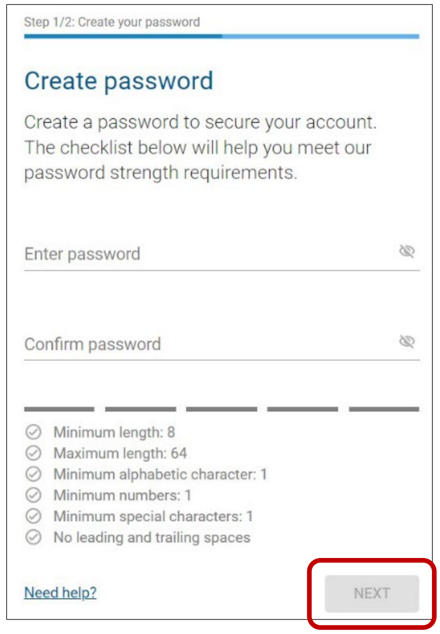
To complete account activation:

1. Locate the email with the subject line **Activate your Exostar Account**. Click the **ACTIVATE MY ACCOUNT** button in the body of the email.

NOTES:

- Users receive email reminders to complete account activation on the 14th day, the 28th day, the 42nd, as well as 14 days before the 180-day expiration period.
- Every reminder email provides a new activation link and when a user receives a new reminder email, the activation link in the old email expires.
- If a user selects an expired activation link, the system prompts the user to enter their email address. Once the email address is validated, the user is sent a new account activation link.

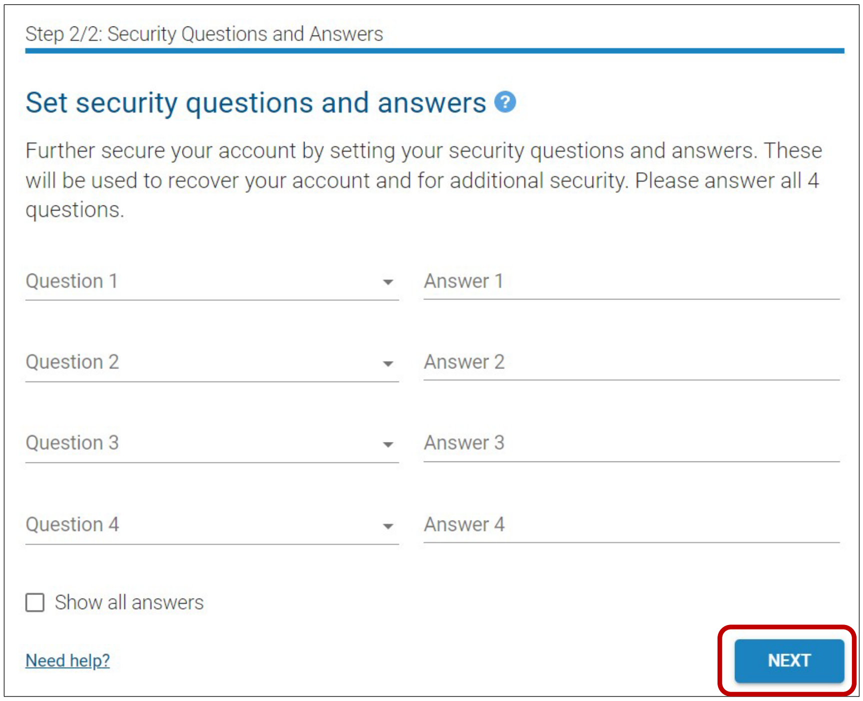
2. Create your new pass and confirm your password again. Once complete, click **NEXT.**
   NOTE: Make sure your password meets the requirements listed on the screen.



PASSWORD REQUIREMNETS: Your new password must meet the following requirements - *it must be a minimum of 15 characters, 1 alphabetic character, 1 numeric character and 1 special character. Leading and trailing white spaces are not permitted.*

IMPORTANT: *Passwords are checked against a breached password list - (https://haveibeenpwned.com/), to ensure that users are not using a password that was already compromised on another website. Users will receive an error when a password is part of breached compromised list.*

3. Select four unique security questions from the drop-down list and enter an answer for each question. Click **NEXT** to complete the account activation process. The MAG Dashboard displays.



Resend Account Activation Email

If you have not completed account activation or misplaced your account activation email, follow the directions below for the system to resend the email:

1. Navigate to the MAG Login screen.
2. Input your Email Address or User ID. Click **Next**.
3. The system displays an **Account not Activated** message. Click the **Resend Activation Email** link.
4. Follow the Account Activation instructions once you will receive the new email.

Subsequent Logins

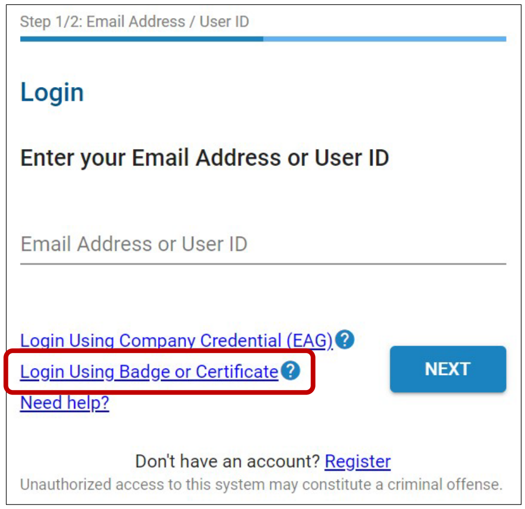
Users who completed account activation, follow the steps below for all subsequent logins to MAG:

1. Go to https://portal.exostar.com.
2. Enter your **User ID/Email**. Click **Next**.
3. Enter your **Password.** Click **Next**.

NOTE: Upon successful login, the MAG Dashboard displays.

Advanced Login Options

If you are accessing partner applications with Federated Identity Service (FIS) certificates, Third-Party Credentials (such as DoD CAC Card, NASA PIV Card, NGC One Badge), or Exostar's Enterprise Access Gateway (EAG) service, and you are not automatically prompted for the credential, select the **Login Using Badge/Certificate** link from the login screen.



Password Login Issues

This sections reviews common password login issues that you may run into:

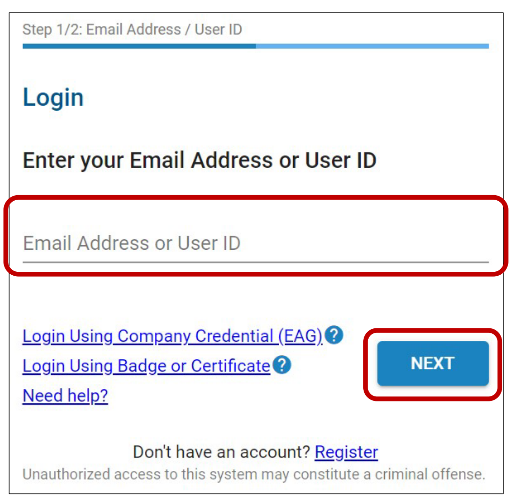
- Forgotten password for an active account
- Account locked (too many unsuccessful password attempts)
- Expired password

NOTE: These options are not available if your MAG account is linked to your corporate network log-in via Enterprise Access Gateway (EAG). If you have issues accessing your account, refer to the EAG User Guide or contact Exostar Customer Support for additional information.

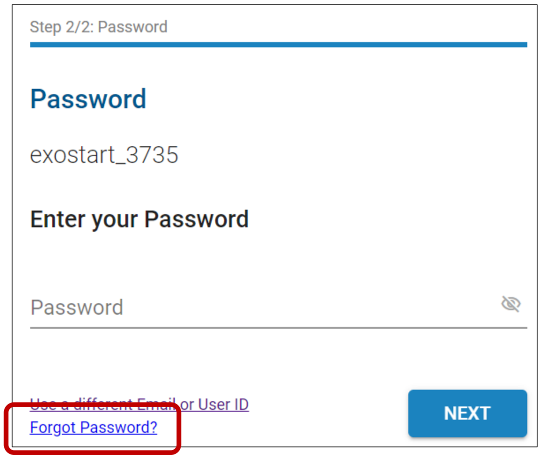
Forgot Password for an Active Account

Follow the steps below if you have an active MAG account and do not remember the password:

1. Access the [MAG login]() page and input your email address or user ID. Click **NEXT**.

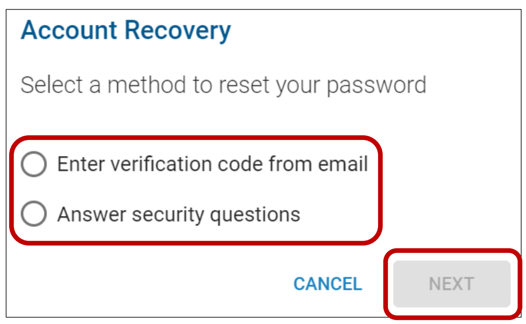


2. Select the **Forgot Password?** link.



3. On the **Account Recovery** page, select the desired recovery method. Click **NEXT**.

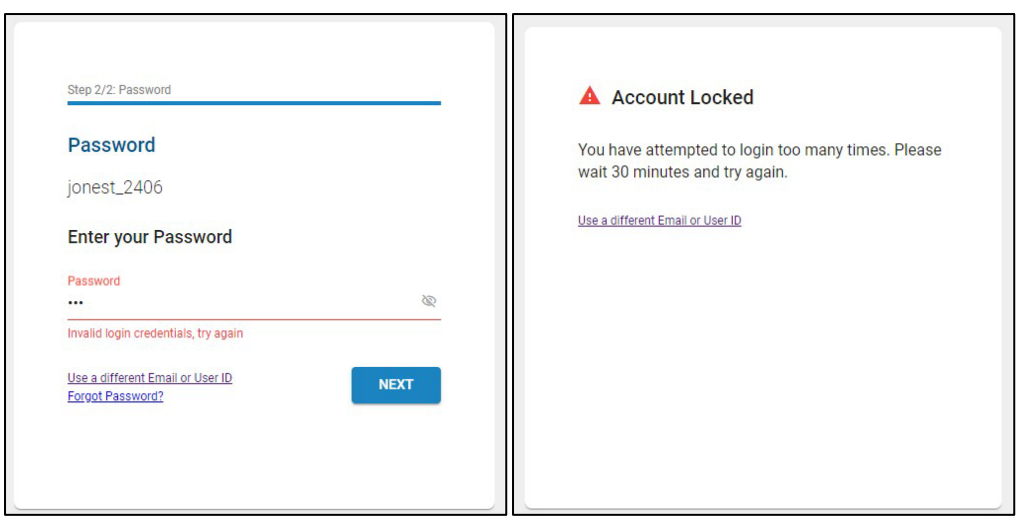
NOTE: If you registered with a credential, a screen will display for Account Recovery for verification via phone, Hardware Token and Mobile ID only display if the user registered with that credential.



4. Depending on the recovery selection, follow the prompts and click **Next**. The **Create New Password** screen displays. Enter your new password twice and click **Next**.

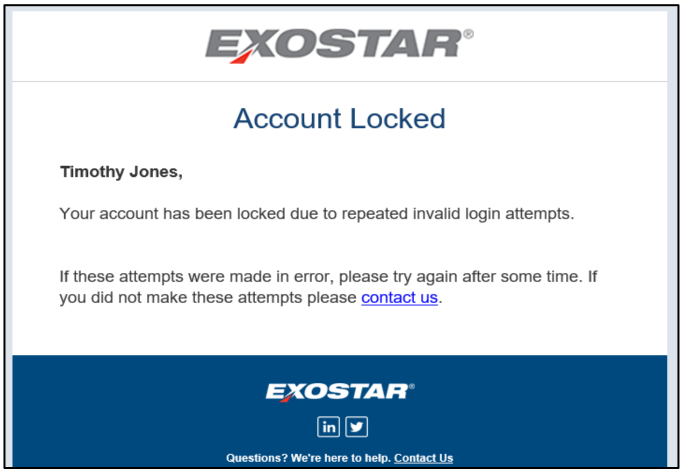
Locked Account

If you enter the wrong password three times, the system will lock your account. You will have to wait thirty (30) minutes before trying to login again.



Once your account is locked, you will receive an email notification that your account has been locked due to multiple failed login attempts.

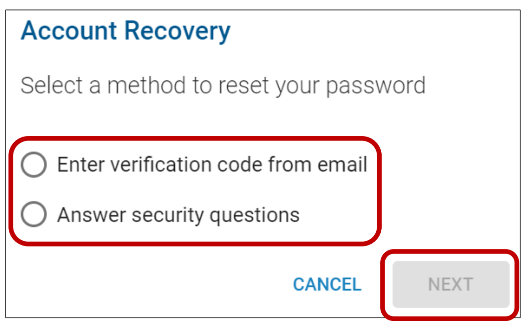
If you made the error, please wait thirty minutes and try again. If you did not make this error, please contact Support to reset your password.



Expired Password

If you attempt to log in and your password expired, you will receive an expired message. Follow the steps below to reset your password:

1. Click **Reset**.
2. On the **Account Recovery** page, select the desired recovery method. Click **Next**.



3. Depending on the recovery selection, follow the prompts and click **Next**.

NOTE: Select the **Verify a different way** link to make a different selection, if necessary.

4. The **Create New Password** screen displays. Enter your new password twice and click **Next**.

DASHBOARD TAB

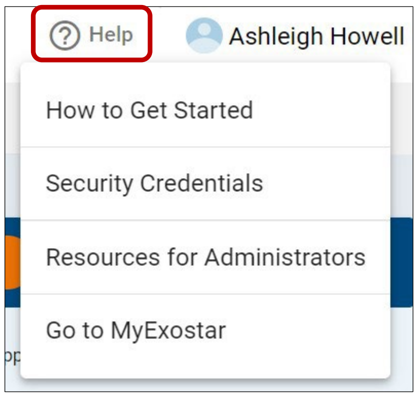
When you log-in to MAG, the dashboard displays. Please see the sections below for more information on each portion of the dashboard.

Top Header

The top header provides a **Help** dropdown menu and a **Profile** dropdown menu, available in the top, right corner.

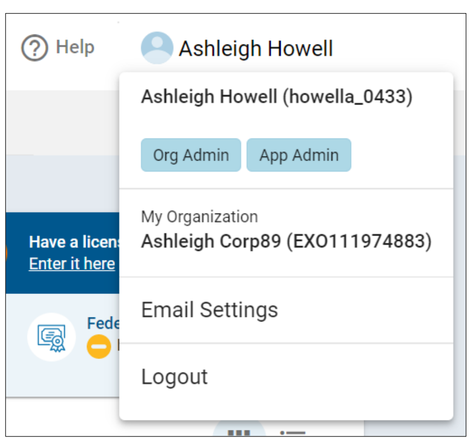
The **Help** menu provides the following information:

- **How to Get Started**: This option opens the MAG Get Started page on my.exostar.com, which provides instructions and videos on the registration and credentialing process.
- **Security Credentials**: This option opens the MAG Get Started page directly on Step 4, to complete the credentialing process.
- **Resources for Administrators**: This option opens the MAG Admin Resources page, which provides a button per administrator role.
- **Go to MyExostar**: This option opens Exostar's self-help portal, which houses all application-specific content, guides and videos.



The **Profile** (your name) menu provides the following information:

- **User Information**: This section provides user-specific information, and when clicked, redirects to the My Account tab.
- **Organization Information**: This section provides organization-specific information, and when clicked, redirects to the Organization Details page.
- **Email Settings**: This option is specific to Organization Administrators, Application Administrators, Service Provider Administrators, Service Provider Administrators (Read Only), and EPAs. This option allows administrators to manage email notifications from the MAG system.
- **Logout**: Select this to log out of the MAG application.



My 2FA Credentials

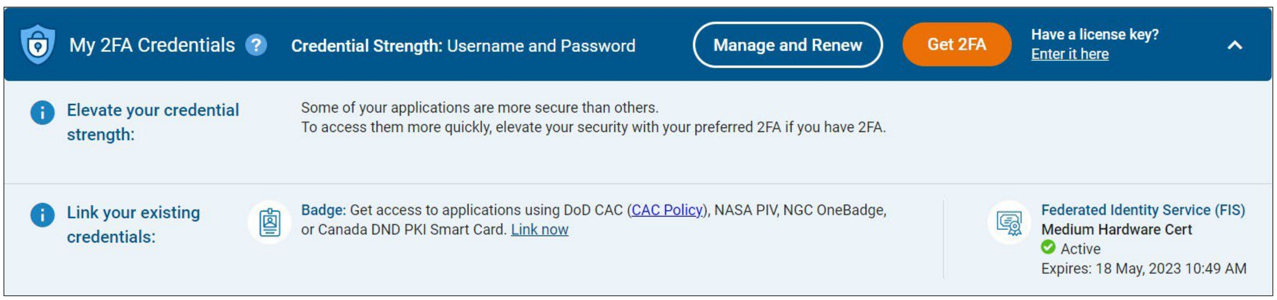
The 2FA module on the dashboard displays a snapshot of your 2FA credentials, as well as messages and clickable options to complete the process or manage existing credentials. Please note this section is collapsible via the arrow in the upper, right corner.

The following information displays:

- **Manage and Renew** button: Select this option to manage or renew your existing credentials via the **Manage OTP** page.
- **Get 2FA** button: Select this button to obtain a 2FA credential via Exostar's web store.

NOTE: If you already completed a 2FA purchase, an option displays **Have a License Key? Enter it here** link.

- **Elevate your credential strength**: Displays the credential to which you are currently logged-in (username and password, MLOA Hardware, OTP, etc.).
- **Link your existing credentials**: This section displays for you to link existing **Company Credentials**, as well as **Badges**.
- An FIS section also displays, if applicable.



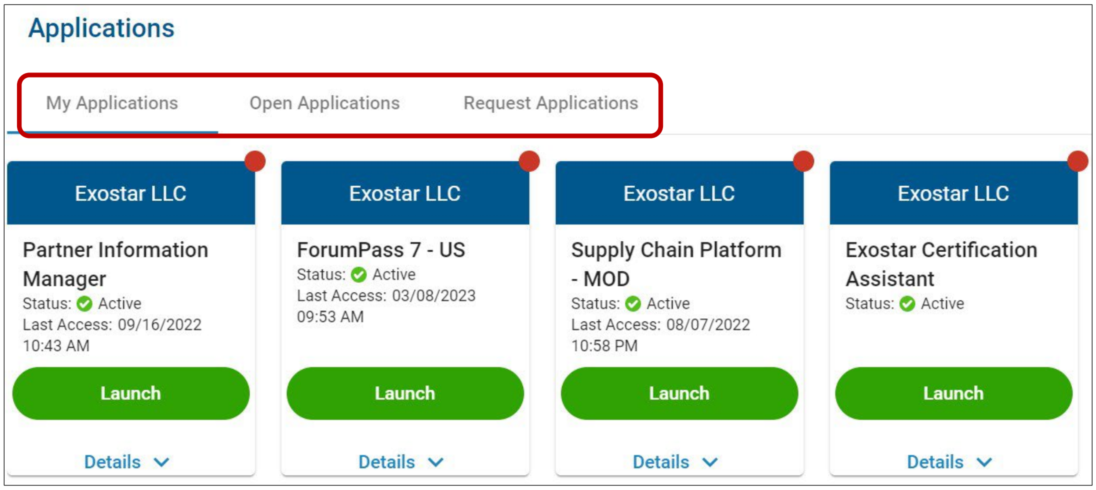
Applications

The Applications section provides an option to view in card or list view, and displays two tabs:

- **My Applications**: Lists all applications to which you have access. If you are logged in with the required credentials, select the **Launch** button to open that specific application. If you are not currently logged in with the required credentials, or do not have the required credentials, select the **Get 2FA** button to begin the process.
- **Open Applications**: This tab displays applications accessible to all users, without required approval, which have no active subscriptions. Currently, Certificate Assistant is the only open application displayed.
- **Request Applications**: Displays applications to which your organization is subscribed, but you do not personally have access. Click **Request Access** to begin the access process.

NOTE: In card view, select the **Details** button (displayed for each, individual application), to review the following:

- Announcements
- Application Status (if applicable)
- Acceptable Credentials
- Application Administrators (clickable to view administrator list)



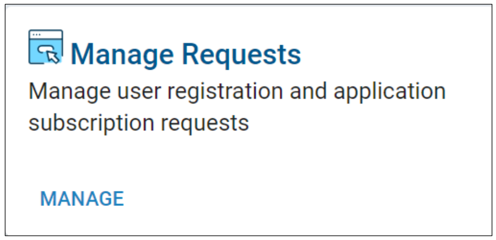
Application Status

Please see the comprehensive application status list below:

Status	Status Description	User Action
Active: Launch	Subscription is approved to access the application.	Click **Launch** to open the application in a separate browser window.
Active: Get 2FA	You have been granted access, but do not have 2FA set-up.	Purchase and complete credential set-up.
Pending: Approval	Organization or Application Administrator must approve your access request.	Contact your Organization or Application Administrator.
Pending: Pending Terms	Organization Administrator has not yet accepted Terms & Conditions for the application.	Contact your Organization Administrator.
Pending: Agree to Terms	Displays if you are the Organization or Application Administrator.	Select to open and agree to terms and conditions.
Pending: Pending Proofing	Specific to FIS Medium Level of Assurance, you must complete the in-person proofing process.	Contact Exostar Customer Support for information if in-person proofing **is complete**.
Pending: Download	FIS Certificates are ready for download.	Select to initiate certificate download.

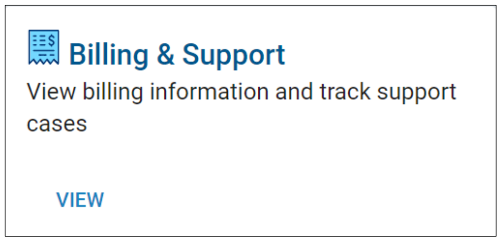
Manage Requests

This section provides a **MANAGE** link for you, as an Administrator, to manage user requests and application requests via the Administrator tab. Please note, you are directed to the relevant request page, depending on your administrator role.



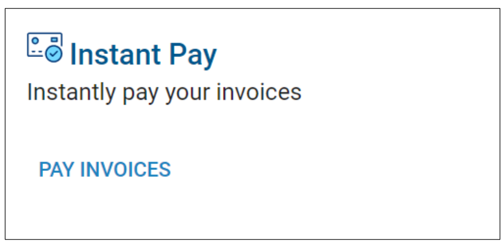
Billing & Support

This section provides a **VIEW** button to redirect to the Billing and Support page in Exostar's web store.



Instant Pay

This section provides a **PAY INVOICES** button, which redirects to the Instant Pay page on MyExostar.



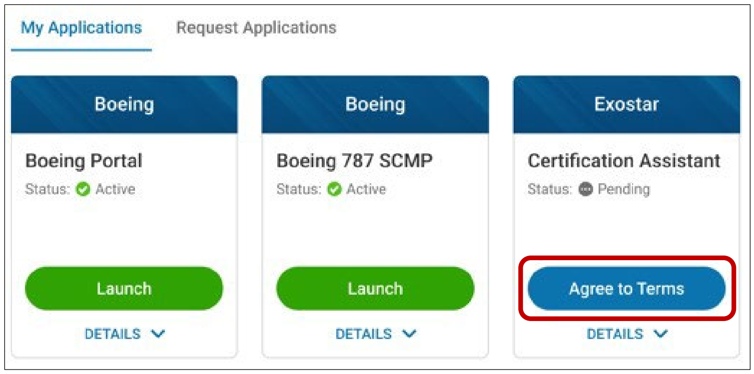
Accept Terms & Conditions

In order to access partner applications, Organization Administrators or an Application Administrator, *must* accept Terms and Conditions for those applications. Users within your organization are not able to access applications until Terms and Conditions are accepted.

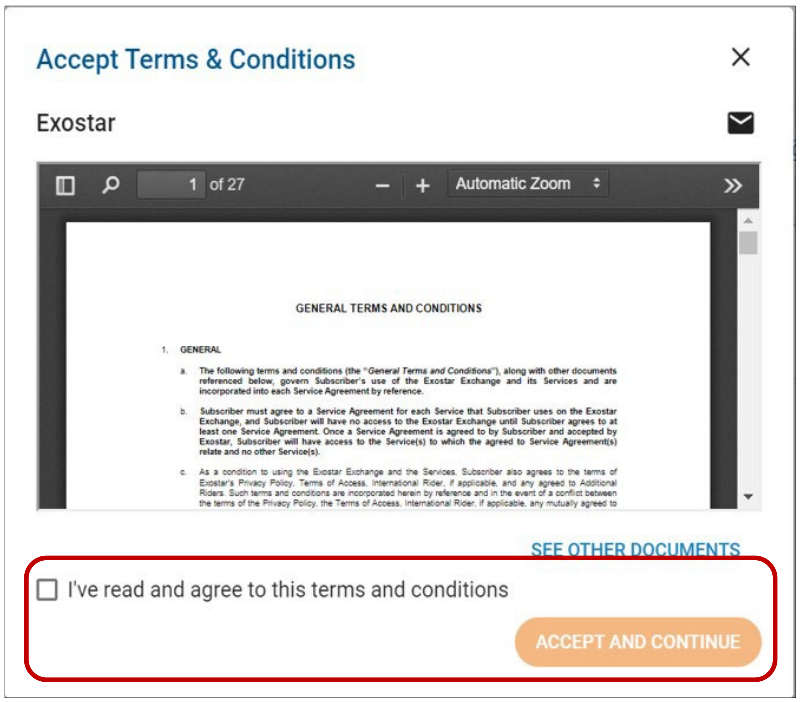
Organization Stewards access the **Accept T&C** sub-tab from the **Stewardship** tab. Organization Stewards need to reference the Organization Steward section for assistance.

To accept terms and conditions:

1. Click **Agree to Terms** for the desired application via the **Applications** tab.



2. Review the information. Click **CONTINUE**.



3. Once you review the Terms and Conditions, please a check in the box for **I've read and agree to these terms and conditions.** Click **ACCEPT AND CONTINUE**.

NOTE: Complete this process for all pending applications. The system automatically walks you through all pending applications.

4. After you have accepted all terms and conditions for the application(s), your organization will be successfully subscribed to the application(s). Users can now access the application(s).

NOTE: Organization and Application Administrators for the application can start subscribing users within their organization to the application, or users can start requesting access to the application.

What happens if you do not accept the Service Agreement?

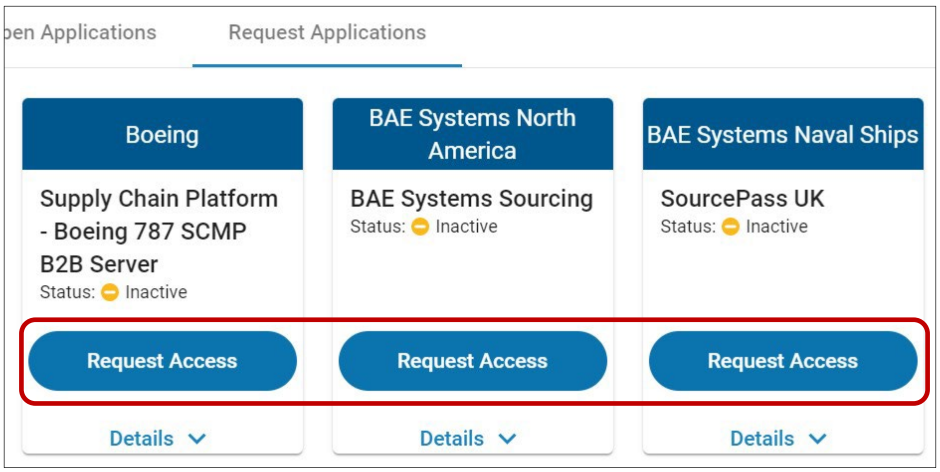
- If you do not accept terms and conditions by skipping the agreement, terms and conditions will remain in **Pending Acceptance of Terms & Conditions** status.

- Until Organization and Application Administrators accept the terms and conditions for the application(s), Admins cannot subscribe users within their organization the application and users cannot access the application(s).

Request Access to Single Applications (Excluding FIS)

If you need access to an application, an Administrator must grant you access. To request access to all single applications (other than FIS):

1. Click the **Request Access** button for the desired application, via the **Request Applications** tab.



2. Sponsor code and comments fields are optional. If you were provided a sponsor code, enter the sponsor code. Enter comments for the Application Administrator, SP Administrator, or Organization Steward to review. Click **Next**.

A confirmation page displays. The system routes the request to the Application Administrator for approval. For most applications, once the Application Administrator approves, you are granted access to the application. Please see the Application Status matrix to view application statuses.

Request Access to an Application Group

If you need to access a group of applications (for instance, Rolls-Royce eTools or the Raytheon Bundle:

1. Select **Request Access** for the desired application bundle.
2. Review all information. Click **Next**.

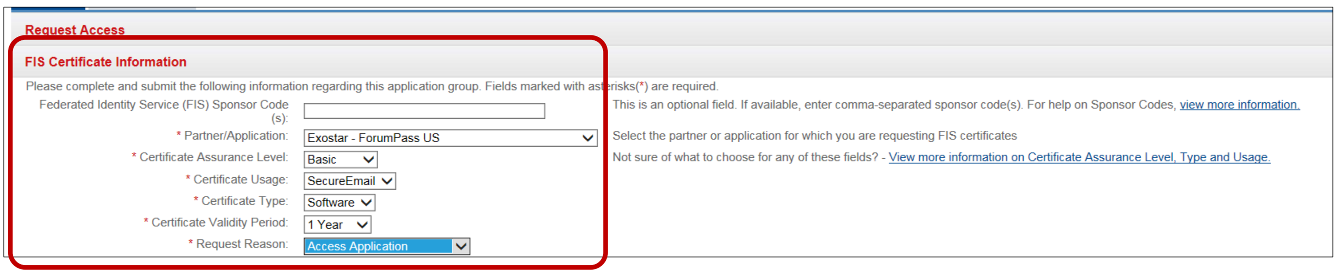
A confirmation page displays. The request routes to the Application Administrator for approval. For most applications, once the Application Administrator approves, you are granted access to the application. Please see the Application Status matrix to view application statuses.

If the application group includes FIS, and you are approved for a Basic Level of Assurance (BLOA) Digital Certificate, you will receive an approval email with a passcode to download your certificates.

Request FIS Digital Certificates

To request FIS access:

1. Click **Request Access** next to **Federated Identity Service (FIS).**
2. Enter **FIS Certificate Information** and select the correct information for the drop-down fields.

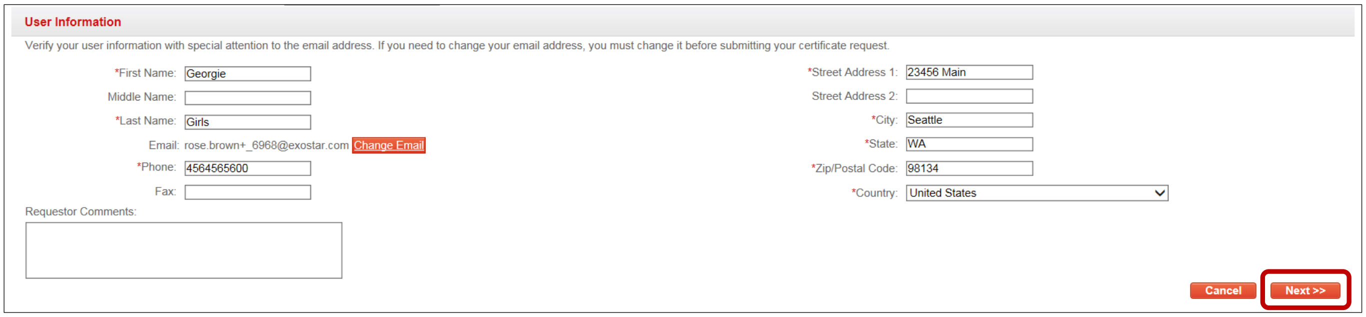


- **Sponsor Code**: If you were provided a sponsor code, enter the sponsor code. Optional.
- **Partner/Application**: This helps the FIS Administrator in approving your request with the appropriate information. You may select the **Other/Unspecified** option if you do not have this information.
- **Certificate Assurance Level**: You have the following options:
  - **Basic:** Basic Level of Assurance (BLOA)
  - **Medium:** Medium Level of Assurance (MLOA)
  - **Unknown**: If you select this, your FISA may take additional time to approve your request to ensure they approve you for the correct option.
- **Certificate Usage**: This option is only available when you select **Basic Level of Assurance**. Available usage options include **Identity**, **Secure Email,** and **Unknown**.
- **Certificate Type**: Depending on the assurance level selected, as well as the FIS subscription level of your organization's account, you may have all or some of the following options:
  - Software
  - Hardware
  - Unknown
- **Certificate Validity Period**: If you select **Basic**, you have the option to select **1** year. If you select **Medium** assurance, you are able to select from:
  - 1 year
  - 3 years
- **Request Reason**: Allows you to provide information to the FIS Administrator on why you need the certificates.

3. Review the **User Information** section.

NOTE: Please ensure you are using a valid email address (public email addresses such as Hotmail, Gmail, etc. are not allowed). If you request MLOA, it is important your first and last name match your identity documents.

Additionally, please ensure the address information is accurate. This is the address where a trusted agent will be dispatched to complete in-person proofing. Please ensure you do not have a PO Box listed.



NOTE: If you click to modify your email information, you will need to complete the email change process first. Once the email change is complete, you will need to restart the FIS request process.

4. Click **Next** to complete the application access request. A confirmation page will display.

What Happens Next?

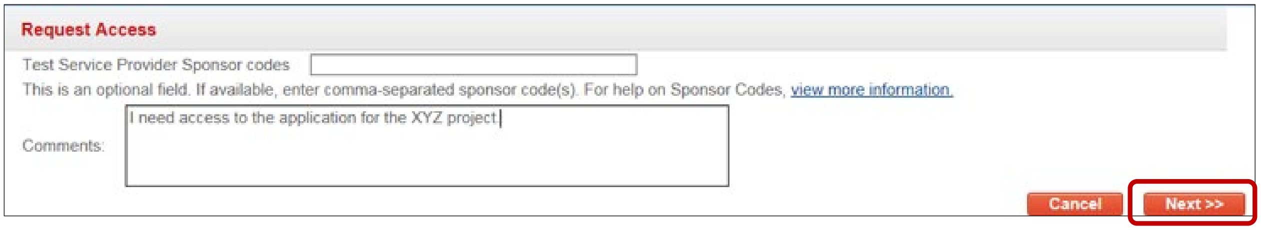
- The FIS Administrator receives a request to approve your FIS subscription. The FIS Administrator has the ability to modify your request.
- If your FIS Application Administrator approves a request for a BLOA Digital Certificate, you will receive an approval email with a passcode to download your certificates.
- If your FIS Application Administrator approves you for MLOA Digital Certificates, your request requires approval by Exostar (after purchase research), for an in-person proofing session with a trusted agent. After a successful proofing session, the trusted agent provides you a 16-digit passcode. The passcode is required to successfully download your certificates. You will receive an approval email from Exostar with instructions on how to complete the download process.

Request Access to Suspended Application

If the application you want to access is suspended, follow the steps below to request reactivation:

1. Click the **Reactivate Application** button for the desired application.

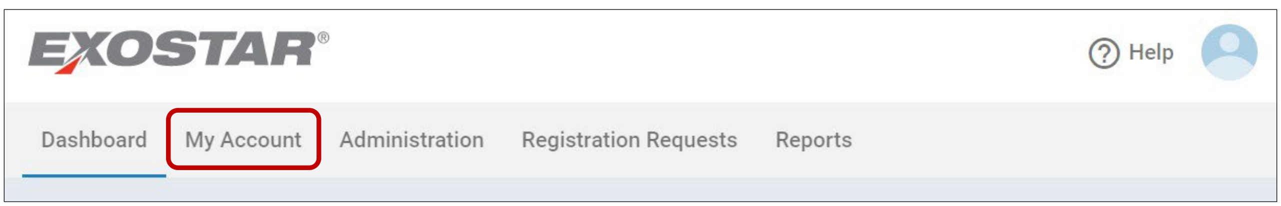
2. Enter comments. We suggest you include your access reason in your comments. Comments and sponsor code fields are optional. Click **Next**.



A confirmation page will display. The request routes to the Application Administrator for authorization. The Application Administrator will approve or deny access. If the application requires Service Provider (SP) Administrator approval, the request routes to the SP Administrator for final approval after Application Administrator approval.

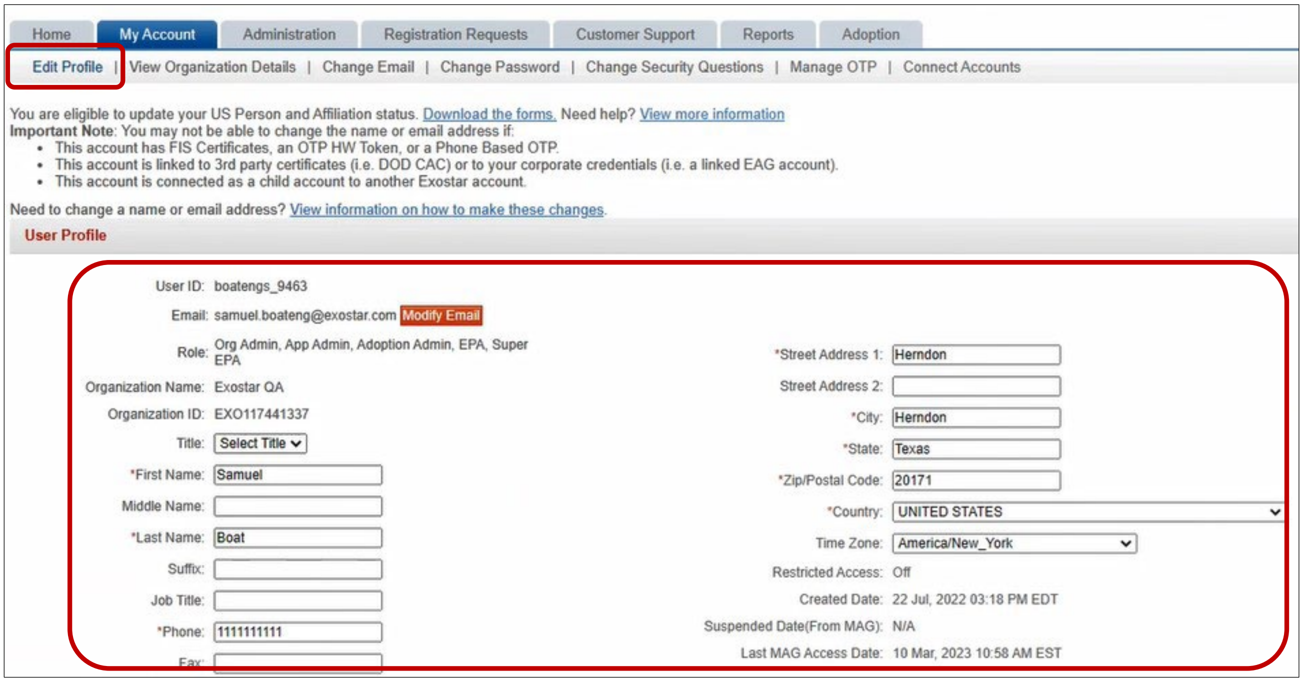
My Account Tab

The My Account tab provides information regarding your account. You can find information about your organization, including administrator information and managing credentials. Additionally, you can modify account information and connect qualified accounts.



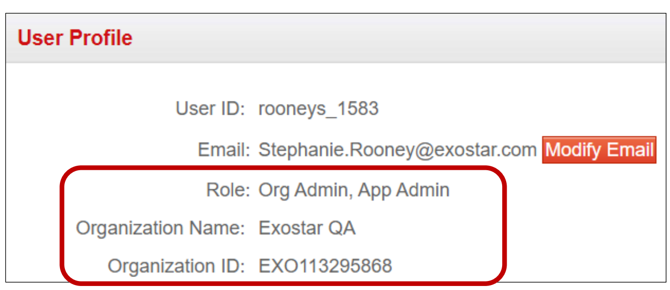
Edit Profile

Edit Profile allows you to modify your account information (e.g., name, address, etc). Users, whose organizations are subscribed to Exostar's Enterprise Access Gateway Service (EAG) or have third-party credentials, can complete the linking process from Edit Profile (see picture below).



NOTES:

- If your account has been linked to your corporate network account via Enterprise Access Gateway (EAG), your screen may look different.
- Not all profile information you update in the portal propagates across all your Exostar-enabled applications. You can update application-specific profiles within the respective application.
- **Restricted Access**: If you are accessing ForumPass, the ON/OFF setting is one of the factors that determines whether you can access **Restricted Profile** sites in ForumPass. If you have any questions regarding this setting, please contact your Organization Administrator.
- To determine your role and Organization ID, scroll down the User Profile to see your role and Organization ID.



View Organization Details

View Organization Details provides information about a user's organization. Users can determine who their Organization and Application Administrators are.

Determine Administrators

From **View Organization Details**, you can determine who your Organization and Application Administrators are by scrolling to the Organization Administrators and Application Administrations section of the page. The application column identifies the Application Administrator for that specific application.

Organization Administrators

First Name	Last Name	Email
Beena	Nair	beena.nair@exostar.com
Tim	Walter	Tim.Walter@exostar.com
Erica	Evans	erica.evans@exostar.com
Robert	Spezzano	Robert.Spezzano@exostar.com

Application Administrators

First Name	Last Name	Email	Phone	Application
Adrienne	Evans	adrienne.evans@exostar.com	5712131817	Federated Identity Service (FIS)
veena	Padigela	veena.Padigela@exostar.com	7037870500	Federated Identity Service (FIS)
Kurt	Wagner	robert.spezzano+_1107FF@exostar.com	5403456545	Boeing Supply Chain Platform
App Admin	Nair	beena.nair+_21@exostar.com	12345678	Test Service Provider
Robert	Spezzano	rspezzano1010C@qftgsivj.mailosaur.net	1230984567	Test Service Provider

Determine Subscribed Applications

From **View Organization Details**, determine which applications your organization is subscribed to and the application status via the **Application Settings** section. Active status indicates the application is active for the organization.

Application Settings

Application Access:

Provider	Application	Status
PIM	Partner Information Manager	Active
BAE Systems Naval Ships	SourcePass UK	Active
Test Service Provider	Test Service Provider	Active
Test Service Provider	Demo Service Provider	Active
Exostar LLC	Supplier Portal	Active

Enterprise Access Gateway (EAG) Settings

For users using the **Enterprise Access Gateway (EAG)** functionality, please reference the EAG User Guide for Identity and Access Management.

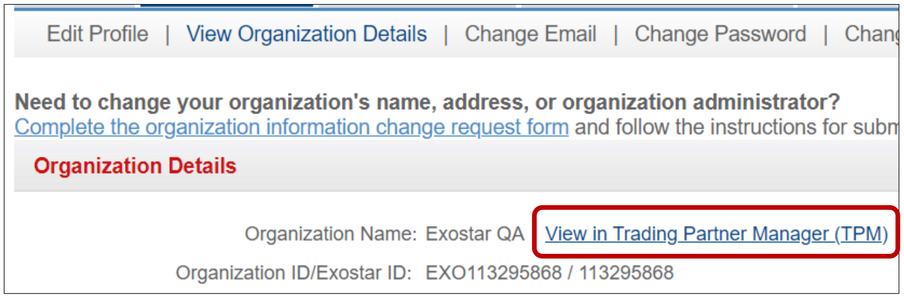
Restrict Credentials or Information from Search Results

Organization Administrators and Organization Stewards can restrict users within their organization from using OTP Hardware and Phone OTP credentials. They can also restrict visibility of the organization and associated users from displaying in application invitation search results completed by partner companies (i.e., buyers). Organization Stewards need to reference the

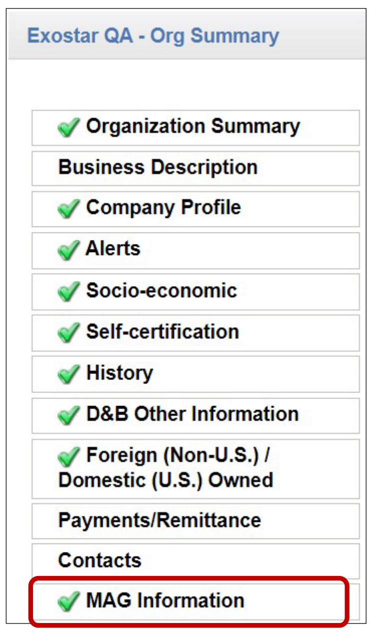
[Stewardship](#) section for assistance.

To Restrict:

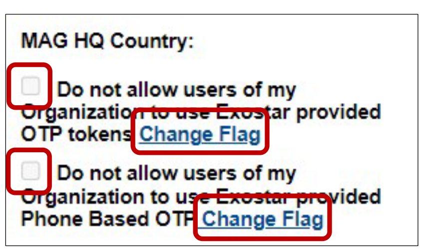
1. Go to the **My Account** tab, click **View Organization Details.**
2. From **View Organization Details**, click **View in Trading Partner Management (TPM)** in the **Organization Name** section.



3. The TPM information displays. Select **MAG Information**.

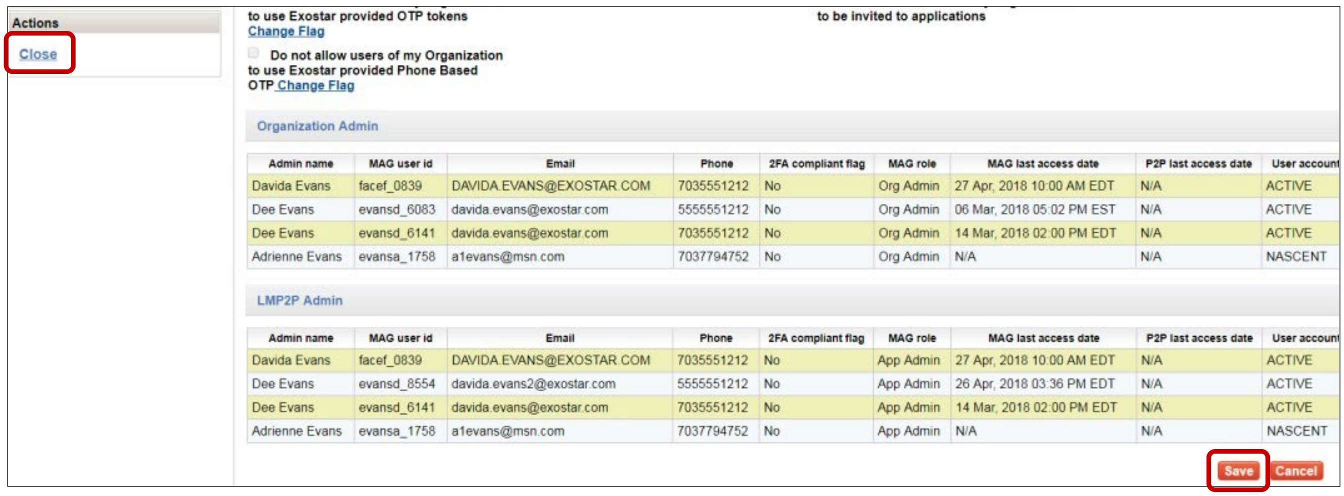


4. To restrict credentials, check the box for **Do not allow users of my Organization use Exostar provided OTP Tokens** or **Do not allow users of my Organization to use Exostar provided Phone Based OTP**. If the box is greyed out, click **Change Flag,** then check the box.



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

6. To complete, click **Save**. To close the window, click **Close**.



Organization Admin

Admin name	MAG user id	Email	Phone	2FA compliant flag	MAG role	MAG last access date	P2P last access date	User account
Davida Evans	facef_0839	DAVIDA.EVANS@EXOSTAR.COM	7035551212	No	Org Admin	27 Apr, 2018 10:00 AM EDT	N/A	ACTIVE
Dee Evans	evansd_6083	davida.evans@exostar.com	5555551212	No	Org Admin	06 Mar, 2018 05:02 PM EST	N/A	ACTIVE
Dee Evans	evansd_6141	davida.evans@exostar.com	7035551212	No	Org Admin	14 Mar, 2018 02:00 PM EDT	N/A	ACTIVE
Adrienne Evans	evansa_1758	a1evans@msn.com	7037794752	No	Org Admin	N/A	N/A	NASCENT

LMP2P Admin

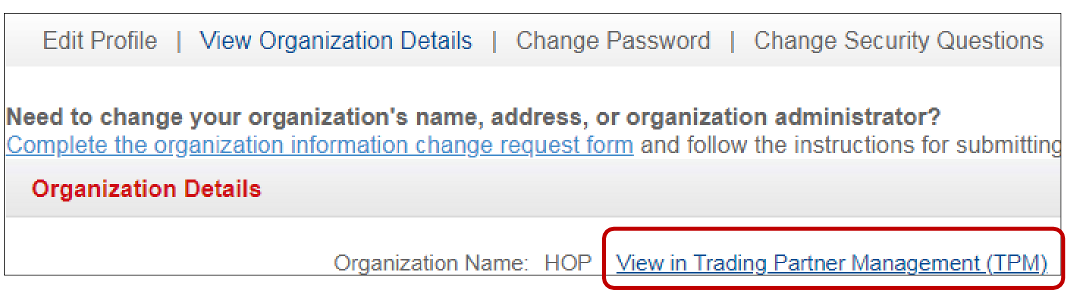
Admin name	MAG user id	Email	Phone	2FA compliant flag	MAG role	MAG last access date	P2P last access date	User account
Davida Evans	facef_0839	DAVIDA.EVANS@EXOSTAR.COM	7035551212	No	App Admin	27 Apr, 2018 10:00 AM EDT	N/A	ACTIVE
Dee Evans	evansd_8554	davida.evans2@exostar.com	5555551212	No	App Admin	26 Apr, 2018 03:36 PM EDT	N/A	ACTIVE
Dee Evans	evansd_6141	davida.evans@exostar.com	7035551212	No	App Admin	14 Mar, 2018 02:00 PM EDT	N/A	ACTIVE
Adrienne Evans	evansa_1758	a1evans@msn.com	7037794752	No	App Admin	N/A	N/A	NASCENT

Identify Small Disadvantaged Business (SDB) Status

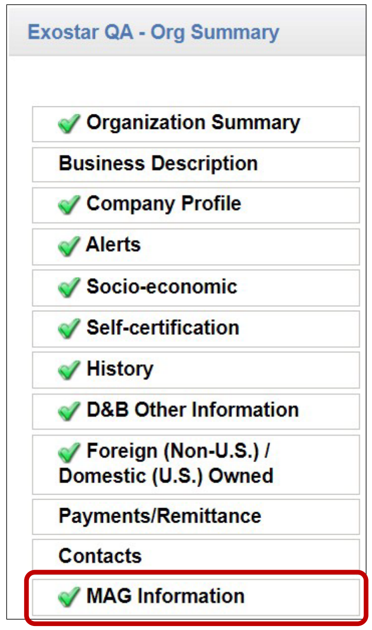
If your organization is a small, disadvantaged business (SDB), Organization Administrators and Organization Stewards can alert partner companies (buyers) of the organization's SDB status. Organization Stewards need to reference the Stewardship section for assistance.

To set the SDB flag:

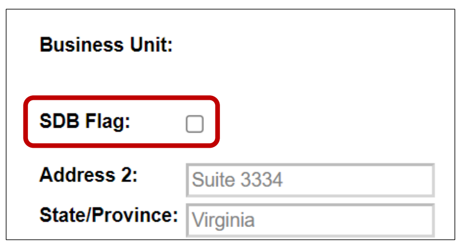
1. Go to the **My Account** tab. Click **View Organization Details.**
2. Select **View in Trading Partner Management (TPM)** in the **Organization Name** section.



3. TPM information will display. Select **MAG Information**.



4. Under the Business Unit section, check the box for **SDB Flag**. Then scroll down and click **Save**.

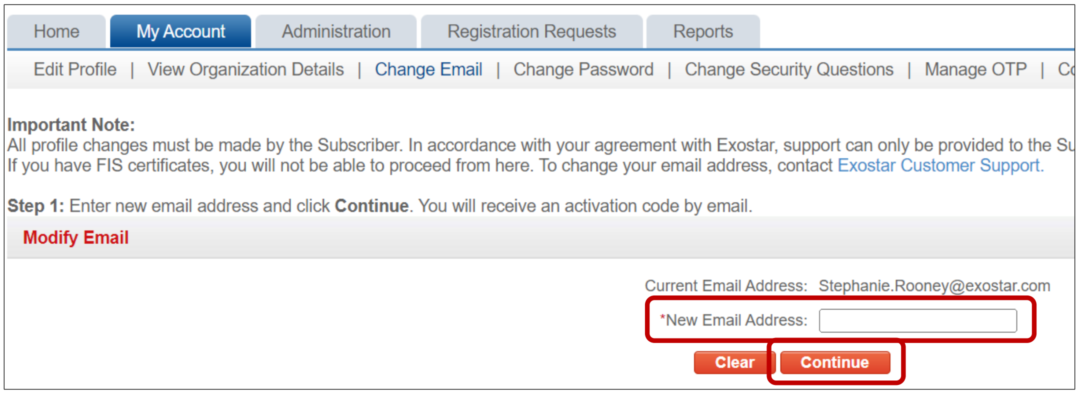


Change Email

Change Email allows you to update your email address. It is important to note if you have FIS certificates, you are unable to change your email address. You must revoke your certificates and purchase new certificates. **IMPORTANT**: CAC users are now able to update their email address.

To change your email address:

1. Navigate to the **My Account** tab, and the **Change Email** sub-tab.
2. Enter your new email address in the field provided. Click **Continue**.

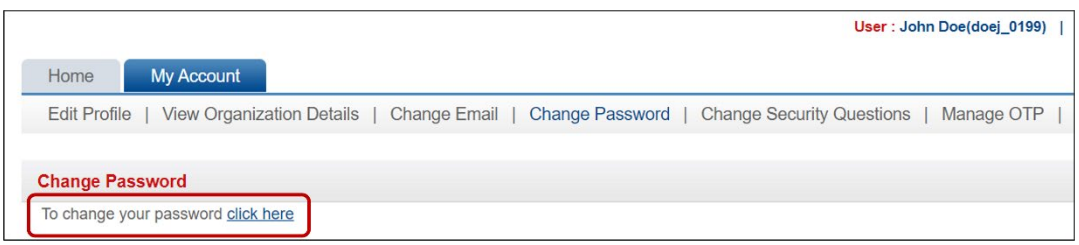


3. You will receive an email with an activation code. Next enter the Activation Code and click **Activate**. Your new email address is now active in the system.

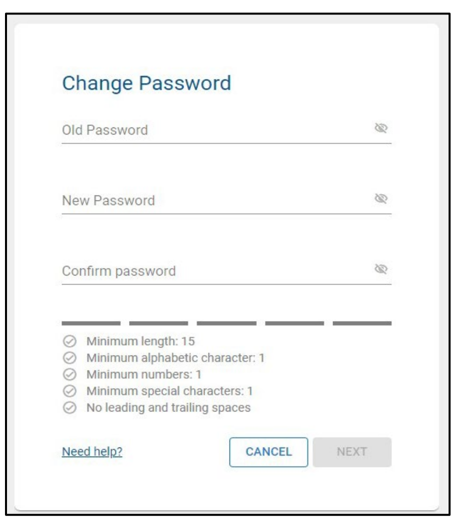
Change Password

Users can change their passwords under the **My Account** tab.

1. To change your password, select the **Change Password** sub-tab.
2. To change your password, select the "*To change your password click here*" link.



3. You will be redirected to a screen to **Change Password**.



4. Enter the new password and re-enter it again. Then click **Next**. Your password is now updated.

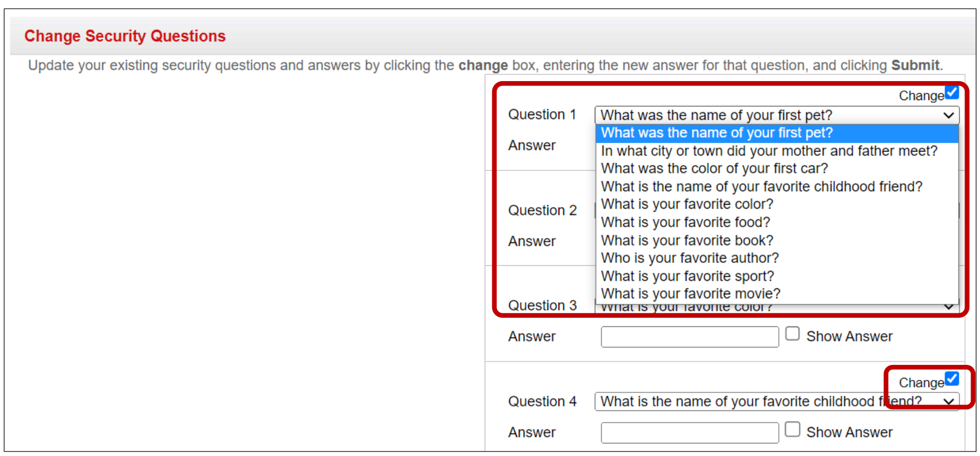
NOTE: Your new password must meet the following requirements - *it must be a minimum of 15 characters, 1 alphabetic character, 1 numeric character and 1 special character. Leading and trailing white spaces are not permitted.*

IMPORTANT: Passwords are checked against a breached password list - (https://haveibeenpwned.com/), to ensure that users are not using a password that was already compromised on another website. Users will receive an error when a password is part of breached compromised list.

Change Security Questions

Users can change their security questions under the **My Account** tab.

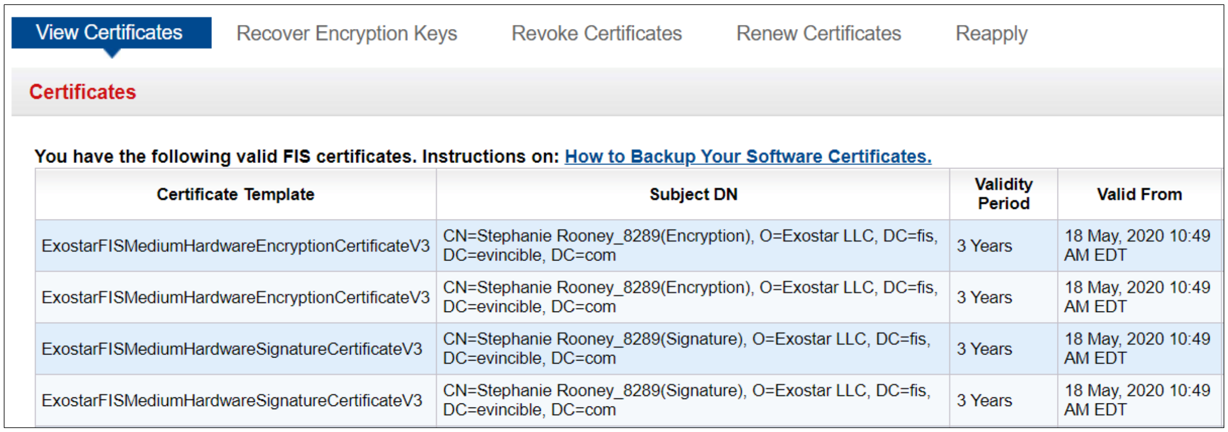
1. To change your security questions, go to **Change Security Questions** sub-tab.
2. Click the **Change box** to change the security question.
3. Then select the question from the drop-down list. Then enter your answer in the field provided.



NOTE: If your account is currently connected using EAG or Account Connections, you are not able to change your email and password.

Manage Certificates

Under the My Account tab, the **Manage Certificates** sub-tab only displays if you have active Federated Identity Service (FIS) Digital Certificates. Users can view installed certificates, recover encryption keys, revoke, renew, and reapply for certificates via this tab.



Certificate Template	Subject DN	Validity Period	Valid From
ExostarFISMediumHardwareEncryptionCertificateV3	CN=Stephanie Rooney_8289(Encryption), O=Exostar LLC, DC=fis, DC=evincible, DC=com	3 Years	18 May, 2020 10:49 AM EDT
ExostarFISMediumHardwareEncryptionCertificateV3	CN=Stephanie Rooney_8289(Encryption), O=Exostar LLC, DC=fis, DC=evincible, DC=com	3 Years	18 May, 2020 10:49 AM EDT
ExostarFISMediumHardwareSignatureCertificateV3	CN=Stephanie Rooney_8289(Signature), O=Exostar LLC, DC=fis, DC=evincible, DC=com	3 Years	18 May, 2020 10:49 AM EDT
ExostarFISMediumHardwareSignatureCertificateV3	CN=Stephanie Rooney_8289(Signature), O=Exostar LLC, DC=fis, DC=evincible, DC=com	3 Years	18 May, 2020 10:49 AM EDT

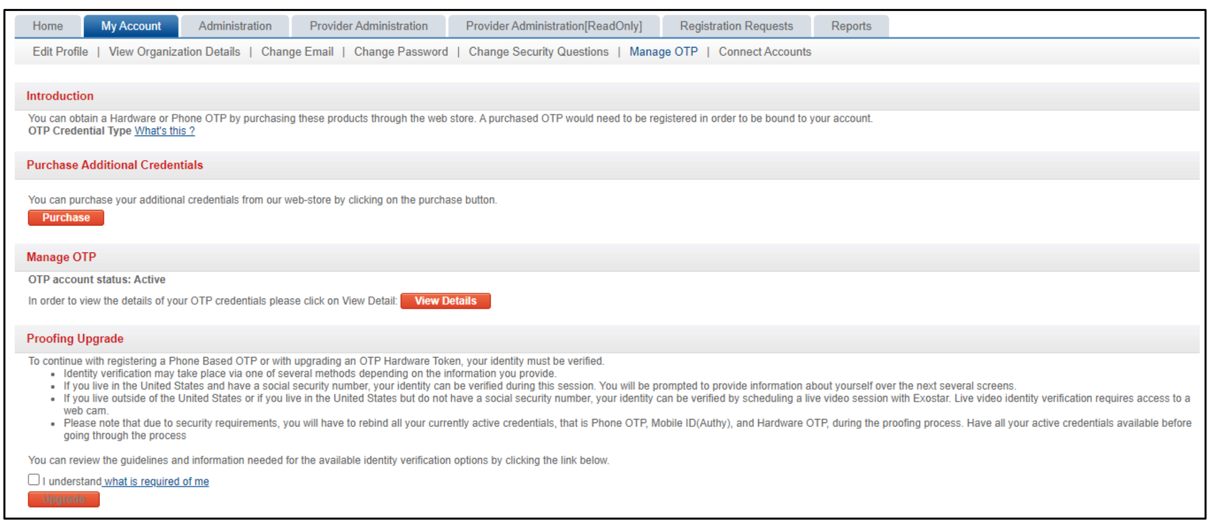
You will not see **Manage Certificates** if you have:

- Expired certificates (e.g., if your FIS status is **Inactive**),
- Your organization is not subscribed to FIS,
- Your organization has not accepted terms and conditions for FIS, or
- If FIS is in **Pending Application Administrator Approval**, **Pending Exostar Approval** or **Pending Proofing** status.

Manage OTP

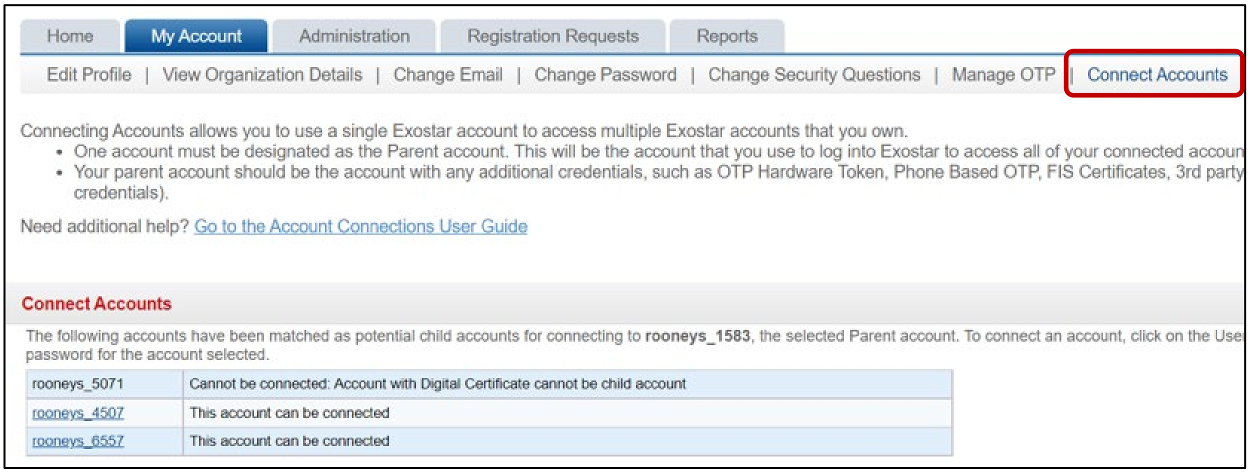
Under the My Account tab, users can manage OTP credentials.

1. Select the **Manage OTP** sub-tab, then you can choose to: Register credentials, complete a Purchase, Test your phone before you start using the service.



Connect Accounts

Connect Accounts allows you to connect multiple accounts in order to leverage credentials of one account to access applications associated with another account. Accounts are connected in a Parent (primary)-Child (secondary) hierarchy. Child accounts may be connected to the parent account. Users are given a choice of accounts to access when logging in with the parent account's credentials. The parent account's credentials can then be leveraged to access applications the child accounts to which they are subscribed.



Account Connection Rules

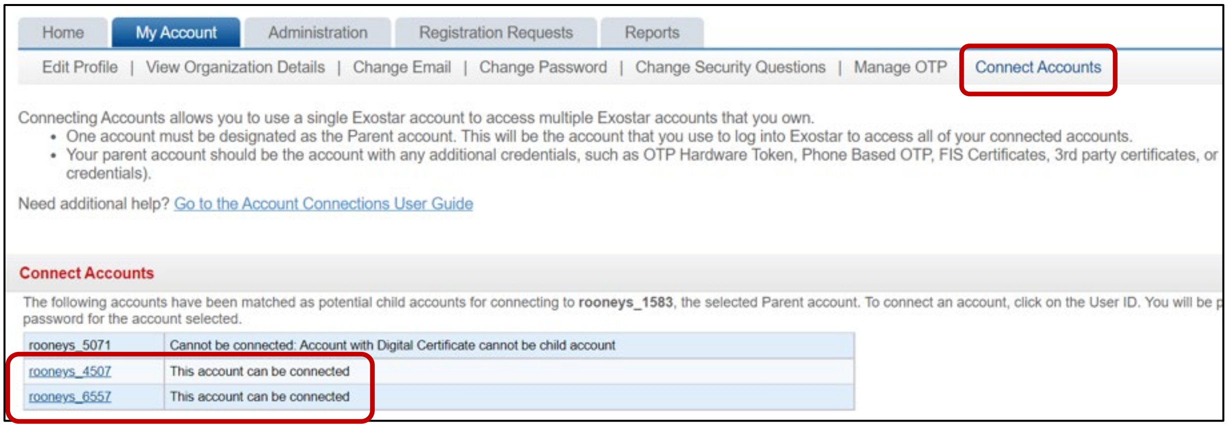
In order to connect a child account to a parent account, it must meet the following rules for eligibility:

- The first name, last name, and email address must match exactly between accounts.
- The child account cannot have any issued credentials (i.e. FIS Digital Certificates, Third Party Credentials such as a CAC Card, PIV card or NGC OneBadge; OTP Hardware Tokens, Phone OTP, Mobile ID, etc.) active on the account. You use the parent account's credentials once connection is complete.
- The child account cannot have a US Person Status attestation. If you have faxed Exostar a notarized US Person Attestation, please contact Exostar Customer Support to remove this attestation from the child account.

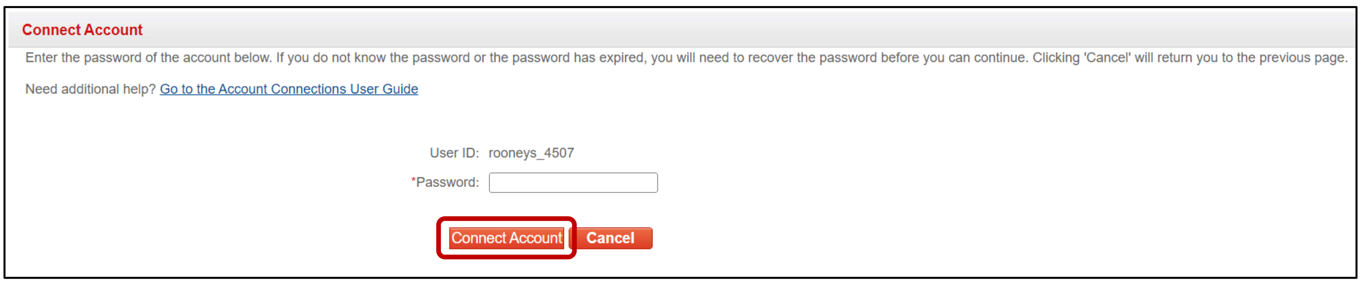
To connect accounts:

1. Under the **My Account** tab, click **Connect Accounts** sub-tab.
2. The **Connect Accounts** section displays any accounts with a matching first name, last name, and email address, as well as notes indicating whether the account is eligible for connection. Select an account to designate as a child.

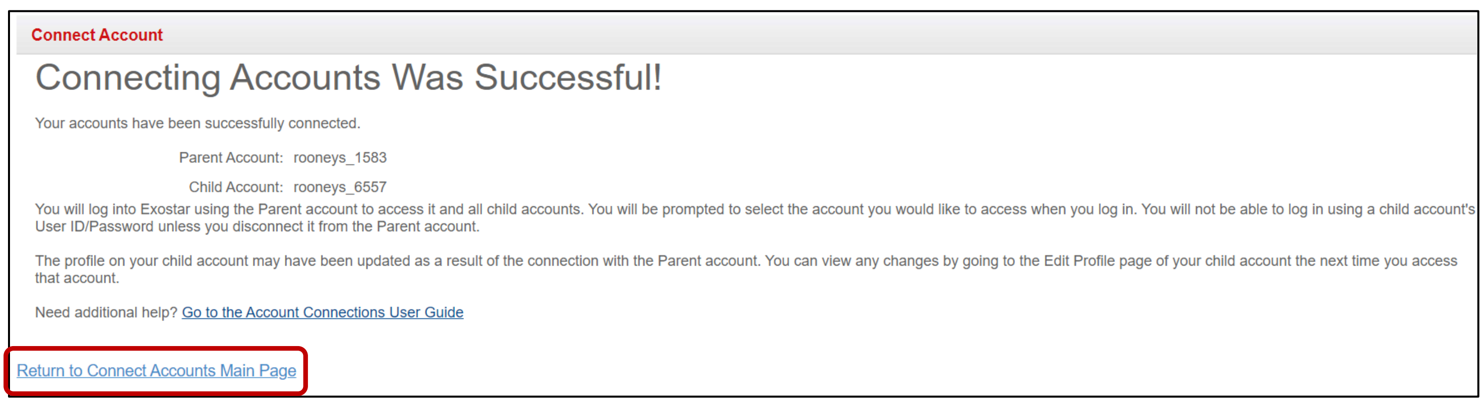
EXOSTAR®



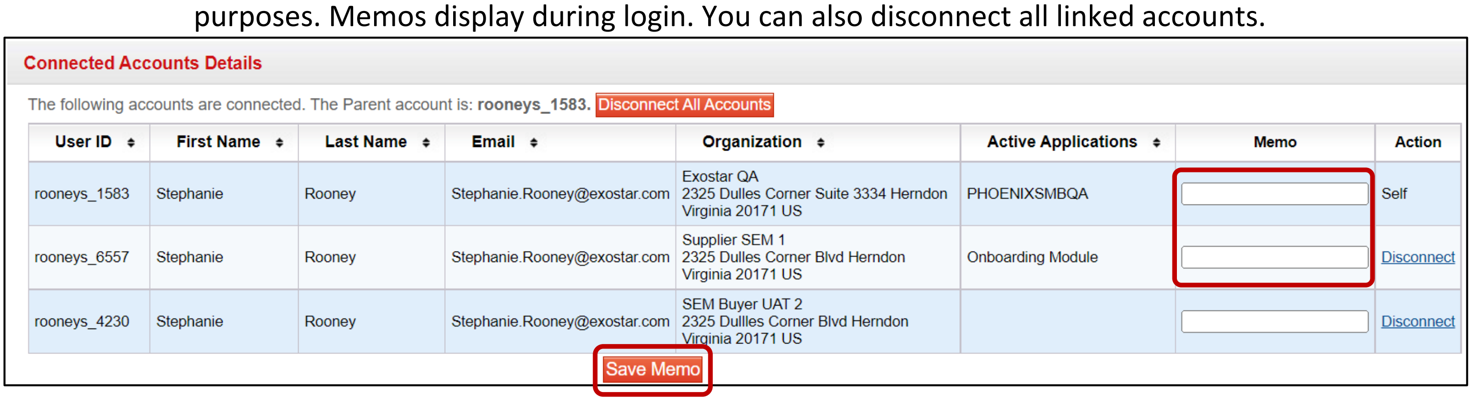
3. Enter the password of the account to which you want to connect. Click **Connect Account**.



4. A success notification displays. To add additional child accounts, click **Return to Connect Accounts Main Page**.



5. From **Connected Account Details**, you can add a memo to the account for organizational purposes. Memos display during login. You can also disconnect all linked accounts.

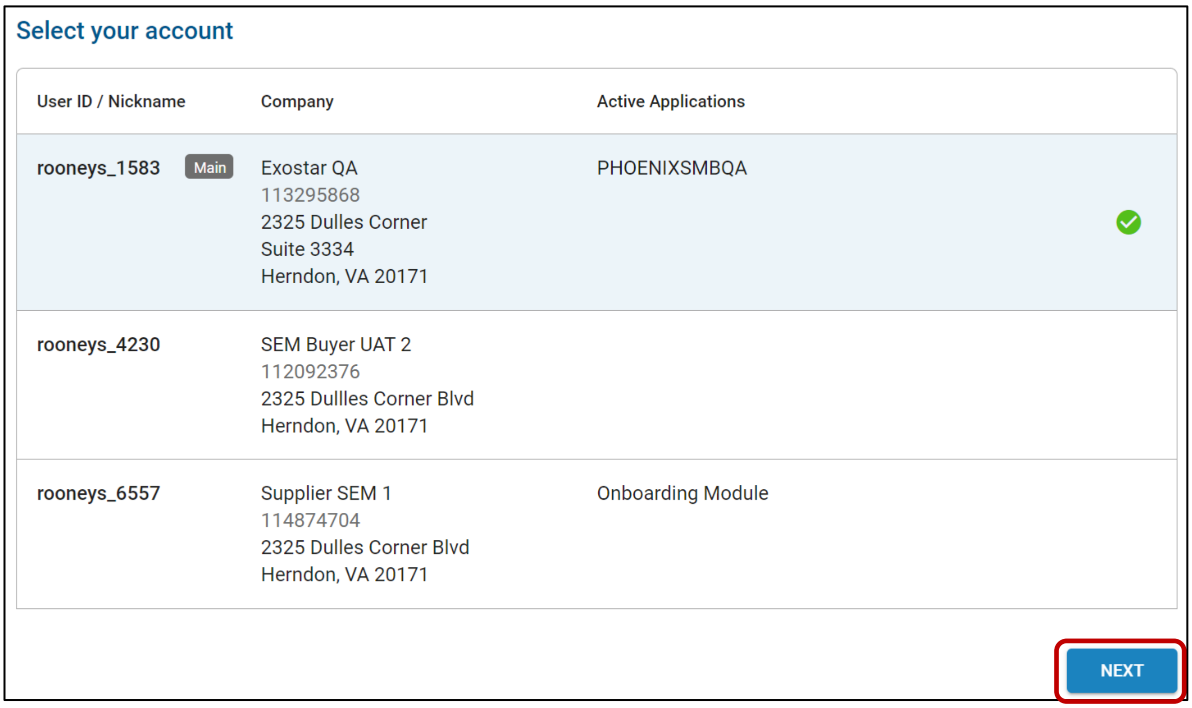


Login to Connected Account

After connecting accounts, you are required to login with your parent account credentials. If you try logging in using the child account (and not the parent account), you will receive the following message, **Your User ID/Password combination was not recognized**.

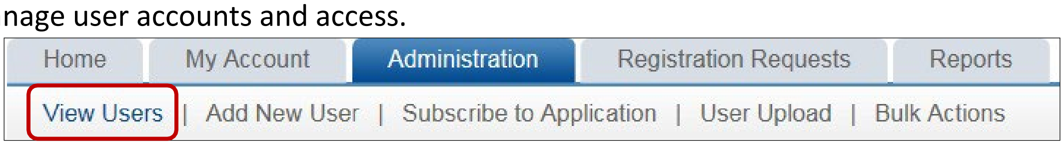
To login to your connected account:

1. After entering your parent account credentials, select the account you want to access. Click **Next** to complete the login process.



Administration Tab

Organization Administrators and Application Administrators can complete administrative tasks from this tab. Administrators can view information for all users linked to your organization, and can manage user accounts and access.



View Users

The View Users sub-tab allows Organization and Application Administrators to search and complete administrative functions, such as request and suspend application access for users. If suspending application access, comments are required. Additionally, Organization Administrators can manage user activities such as assign user roles, suspend, reset passwords and delete users. For assistance with searching, please reference the Search section.

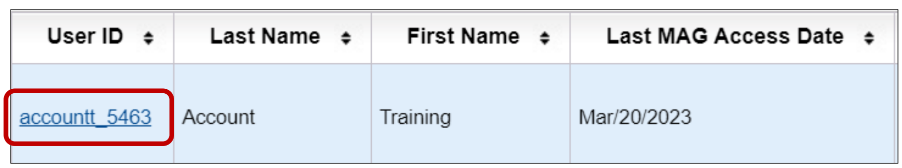
NOTE: If you are an Application Administrator requesting access to an application on behalf of a user, the request does not require manual approval and automatically bypasses Application Administrator approval.

Change Role

Organization Administrators and Organization Stewards can update user roles. It is important to note if you are the only Organization Administrator for your organization's account and you change your role, there will be no Organization Administrators for the account. To learn about role management as an Organization Steward, please reference the Organization Steward section.

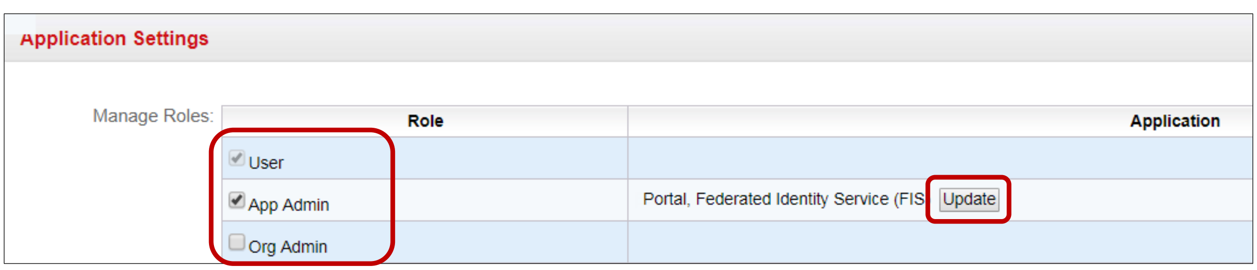
To change roles:

1. From the **Administration** tab, select the **View Users** sub-tab.
2. Enter search criteria. Click **Search**.
3. Select the **User ID** to access user details.



4. Scroll to the **Application Settings** section. Place a checkmark next to the desired role.

NOTE: If assigning the Application Administrator role or updating applications for a user to administer, you must select the application you want the user to administer by selecting **Update**. Applications that a user is an Application Administrator for, display in the **Service Providers** column.



5. After selecting **Update**, check the **Select** column for the applications you want the user to administer. Click **Done**.

Applications to Administer

Provider	Application	Select
SupplierPortal	Supplier Portal	☐
Test Service Provider	Demo Service Provider	☐
Test Service Provider	Test Service Provider	☐
exostar	PHOENIXSMBQA	☐

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

Employee Reference

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

To add employee reference to existing users:

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

Modify Application Access

Organization Administrators, Organization Stewards and Application Administrators can request or suspend user application access. FIS Administrators can modify FIS access. Application Administrators can only request or suspend application access for applications they administer. Once suspended, users are unable to access the application.

To modify application access:

1. From the **Administration** tab, select the **View Users** sub-tab.
2. Use the search filter menu or select **Exact Match** to narrow results. Click **Search**.
3. Click the hyperlinked **User ID.**

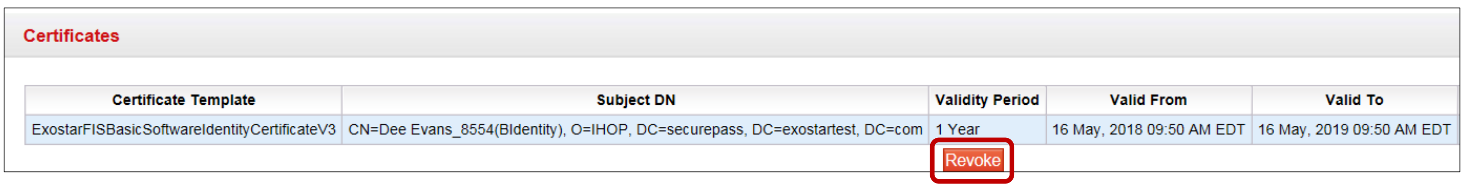
User ID	Last Name	First Name	Last MAG Access Date
accountt_5463	Account	Training	Mar/20/2023

4. In the **Application Settings** section, locate the application and click the appropriate action button.

NOTES:

- You are required to enter a suspension reason.

- Click **Activate** to unsuspend.
- **Delete**: removes the ability for you to modify the application. Additionally, application access is deactivated for the user.
- FIS certificates can either be **revoked** or **suspended**. If **suspending FIS**, the certificates are still active and can still be used. However, the user cannot renew or obtain additional certificates.
- **Revoke** is a permanent action and cannot be reversed. If a certificate is inadvertently revoked, the user requires new certificates and a purchase is required.



- Users can request access to the application again from their Dashboard tab.

Reset Password

Organization Administrators and Organization Stewards can reset a user's password. To learn about Organization Steward navigation, please reference the Organization Steward section.

To reset a password:

1. From the **Administration** tab, select the **View Users** sub-tab.
2. Enter and select search criteria. Click **Search**.
3. Select the required **User ID**.
4. Scroll to the **Application Settings** section of the page. Click **Reset Permanent Password**.

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

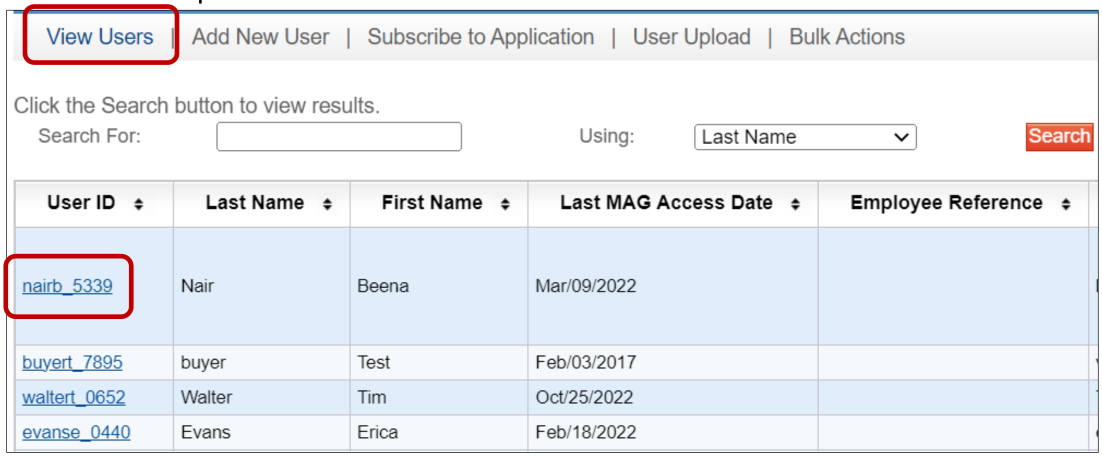
Restrict Profile Access Attribute

Organization Administrators and Organization Stewards can restrict access to ForumPass sites. ForumPass restricted profiles require users to have a user ID, password, Medium Level of Assurance (MLOA) certificate, restricted attribute enabled in MAG, and the TLS 1.0 setting. The **ON/OFF** setting is one of the factors that determines whether users can access restricted profile sites in ForumPass. To learn about Organization Steward navigation, please reference the Organization Steward section.

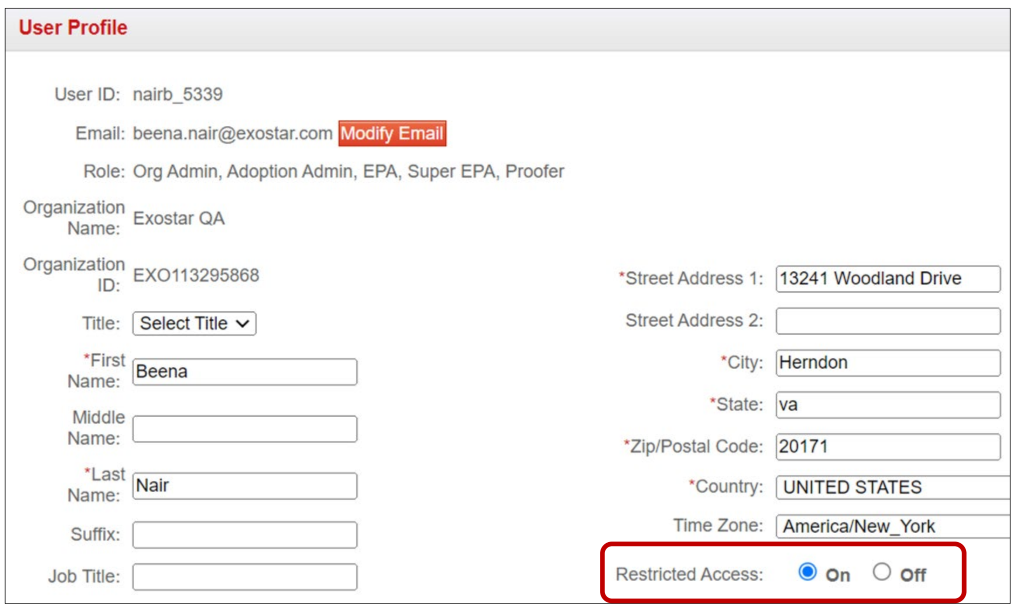
To restrict or remove the restriction attribute:

1. From the **Administration** tab, select the **View Users** sub-tab.
2. Enter and select search criteria. Click **Search**.

3. Select the required **User ID**.



4. From the **User Profile** section, select the desired radio button for **Restricted Access**.

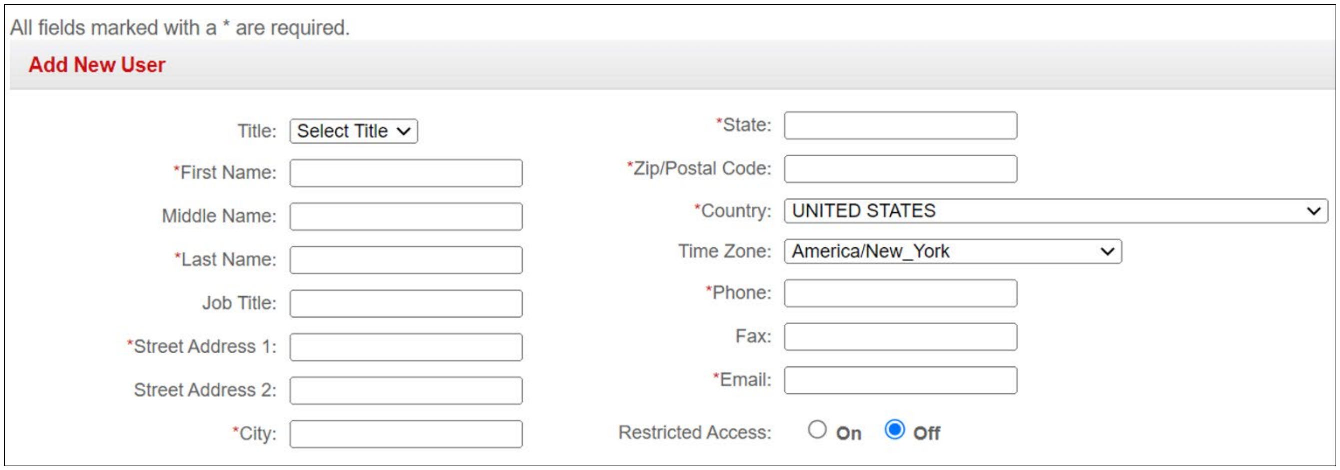


5. Scroll to the bottom of the page and click **Submit** to save the setting.

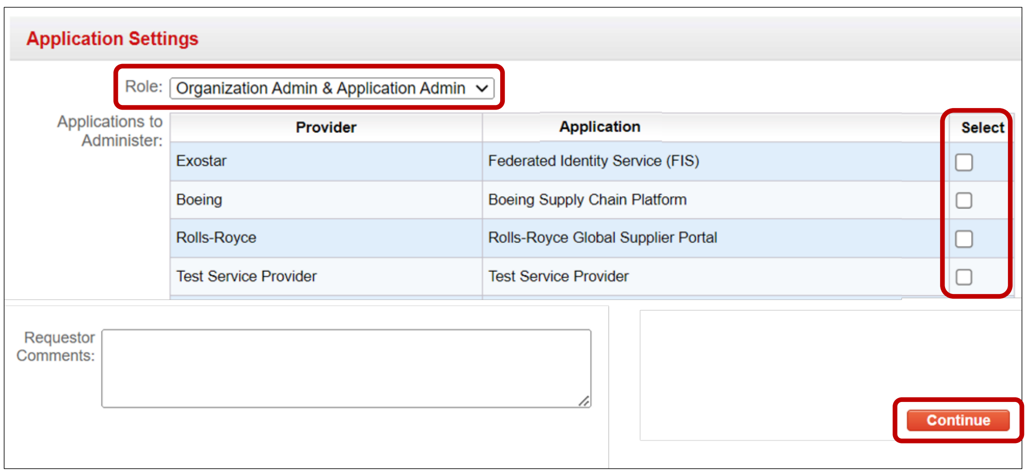
Add New User

The Add New User sub-tab allows Organization Administrators to create new user accounts for their organization. To add a new user:

1. Click the **Add New User** sub-tab from the Administration tab, then enter user's information and fill out all required fields.



2. Next select the user's role. Then select the applications the user needs access to.
3. Once you have entered all the user's information and selected the role(s) and application(s), click **Continue** to finalize the user's account.



4. Review the information you entered. Click **Submit**.
5. The user will receive an email notification to activate their account.

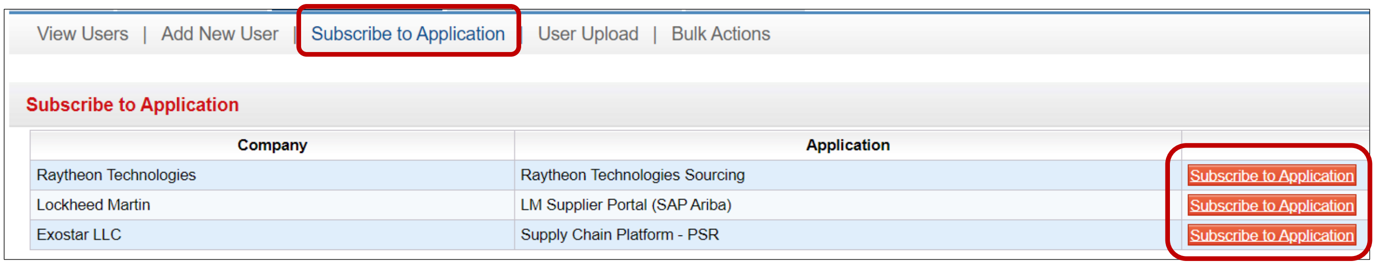
Send Self-Registration Invitation:

1. Send the user the self-registration URL: https://portal.exostar.com/userRegistration and your organization's Exostar Organization ID.
2. Once the user completes the invitation, you are required to action the request from your MAG account. For assistance with authorization, see how to Authorize User.

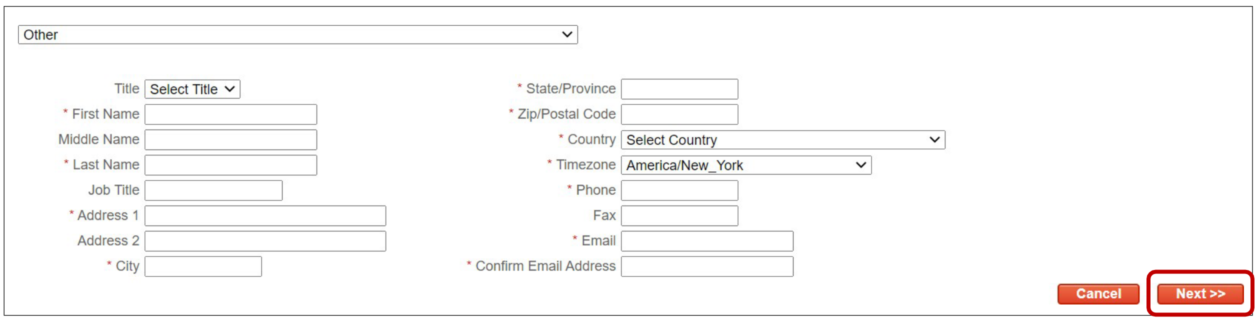
Subscribe to Application

Subscribe to Application allows Organization Administrators to subscribe to public applications their organization is not currently subscribed to. If the organization is subscribed to all available public applications, application subscription information is unavailable.

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



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



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

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

User Upload

User Upload allows Organization Administrators and Organization Stewards to add multiple users to an organization in a single instance using a .CSV file upload. The file upload can also be used to subscribe existing users to new applications. Reference the User Upload and Bulk Actions User Guide for assistance.

Bulk Actions

Bulk Actions allows Organization Administrators and Organization Stewards to delete, suspend, and/or unsuspend multiple user accounts and/or applications in a single instance using a .CSV file upload. Reference the User Upload and Bulk Actions User Guide for assistance.

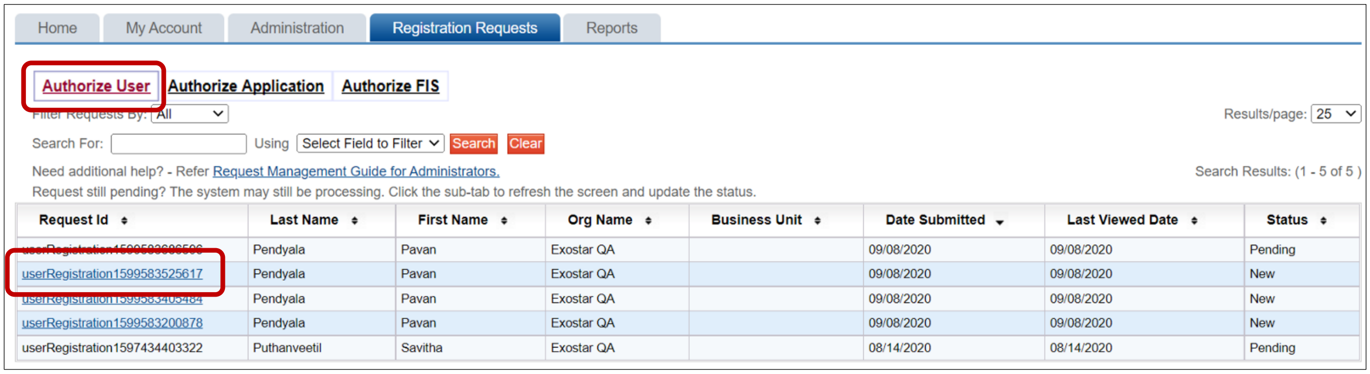
Registration Requests Tab

Users with administrative privileges for your organization have access to the **Registration Requests** tab. Organization Administrators can approve users who self-registered, Application Administrators administer application requests, and FIS Administrators administer FIS requests.

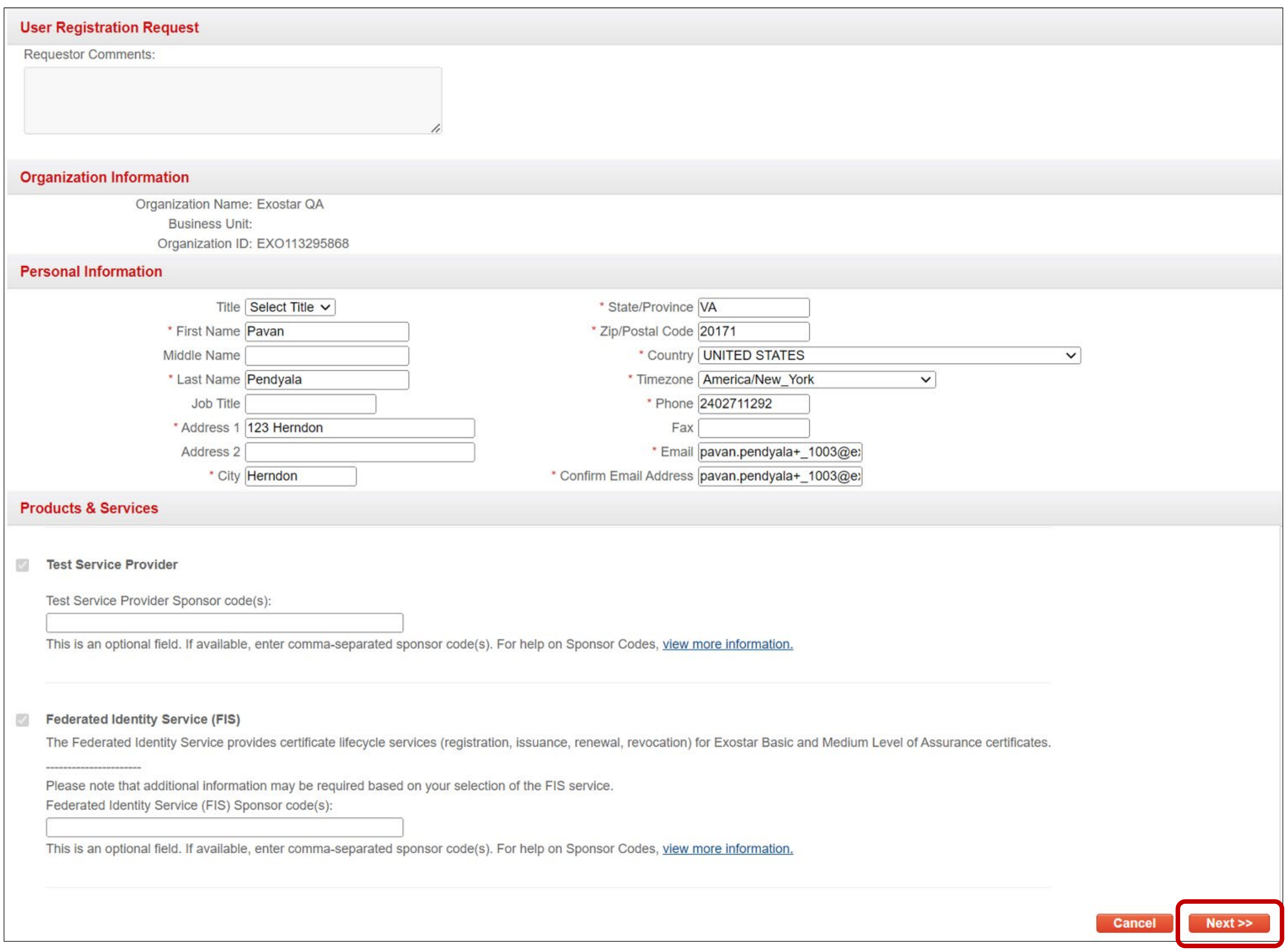
Authorize or Deny User

Under the Registration Requests tab, Organization Administrators can access the **Authorize User** sub-tab to approve or deny new user requests. To authorize or deny a user:

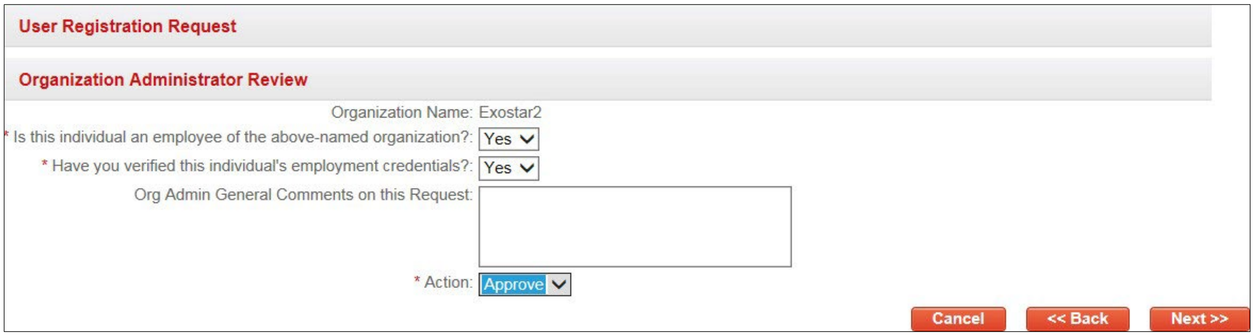
1. Click **Authorize User**.
2. Select the desired **Request ID**.



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



4. In the **Organization Administrator Review** section, answer questions by selecting from the drop-down menus. If approving, select **YES** for both questions. If denying, enter denial comments (required). Click **Next** to complete.

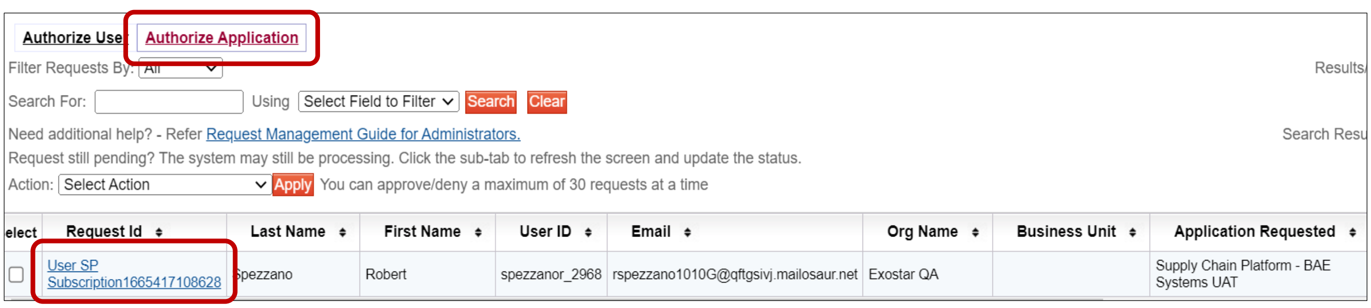


Once approved, a user ID is created, and the user receives instructions on how to complete account activation. If denied, the user receives a denial notification.

Authorize or Deny Application Access

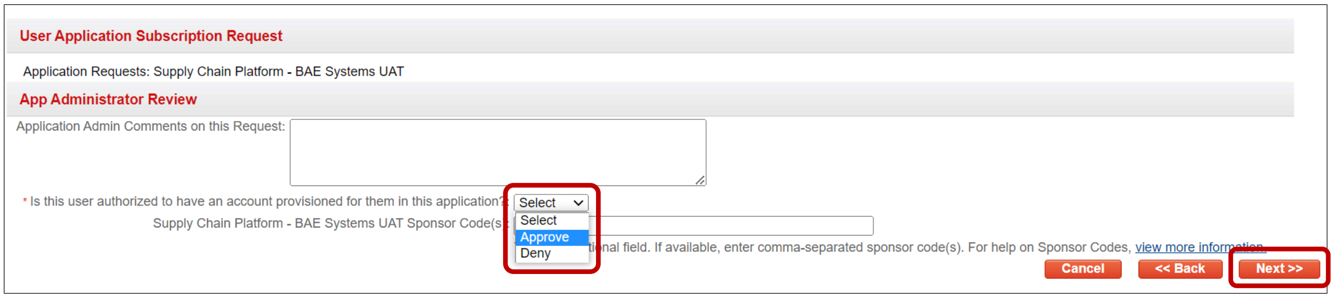
Application Administrators access the **Authorize Application** sub-tab to approve or deny requests individually or in multiples for application access. To authorize or deny requests individually:

1. Click **Authorize Application.**
2. Select the hyperlinked **Request ID**.



3. Review the user's information, if correct, click Next. *(NOTE: If the user requests reactivation of a suspended application, comments will display in the* ***User Application Subscription Request*** *section)*.

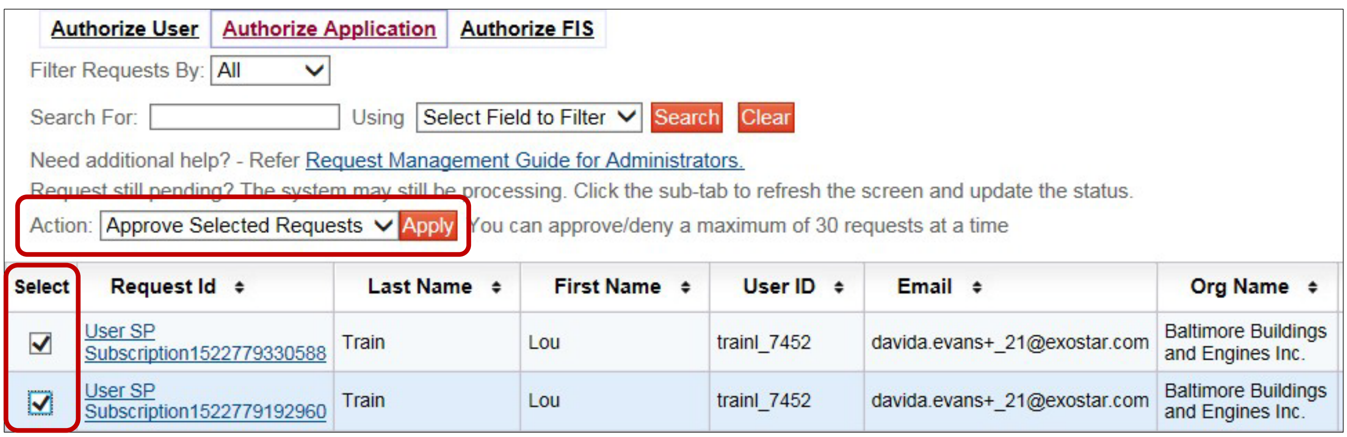
4. Select **Approve** or **Deny** from the drop-down menu. If denying, you must enter a denial comment. Sponsor code is optional. Click **Next**.



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

To administer multiple requests:

1. Click **Authorize Application.**
2. Place checkmarks next to the users you are approving or denying. From the **Action** menu, select **Approve** or **Deny Selected Requests** Click **Apply**. If denying, denial comments are required.



NOTE: If you are Application Administrator for multiple applications, please ensure you view the application requested column to verify you apply the appropriate action for the request.

3. Click **YES** to complete the action.

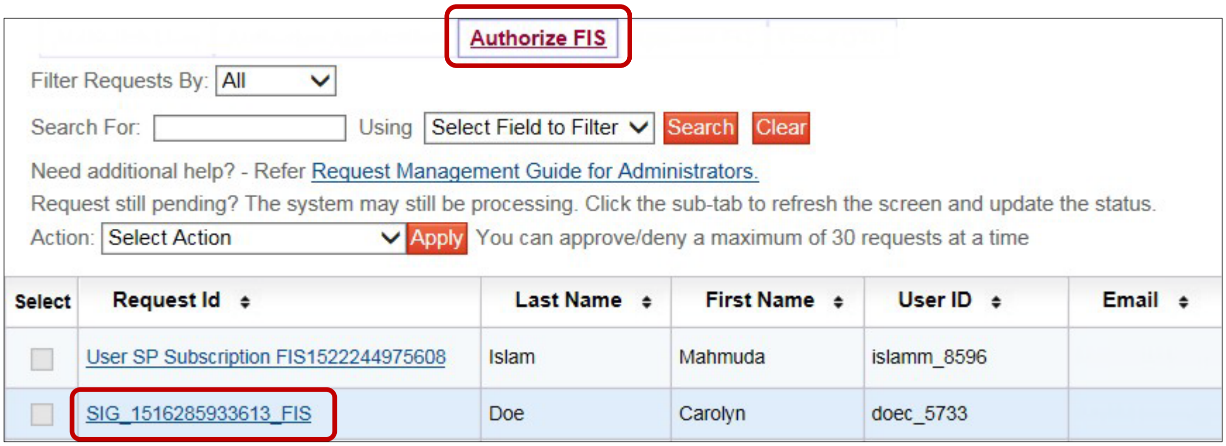
NOTE: Regardless of how the request for application was administered, the request is either approved (providing user access to the application), denied, or routes to the Application Owner for approval. An application's administrative approval workflow depends on what is set for the application. Additionally, users receive an email notification of the approval or denial.

Authorize FIS

FIS Administrators access the **Authorize FIS** sub-tab to approve or deny requests for FIS.

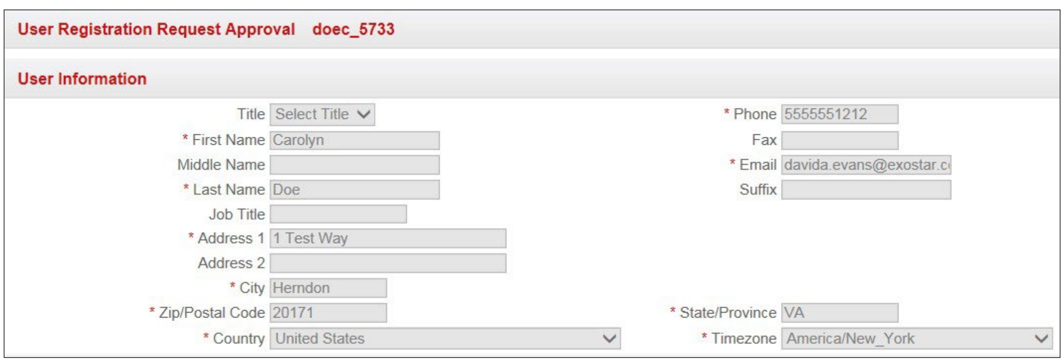
1. Click **Authorize FIS**.

2. Click the **Request ID**.



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

For example, Carolyn Doe is a match for doec_5733. If the request displays a first and last name of Carolyn Doe, but the user ID is smithj_1234, the request must be denied.

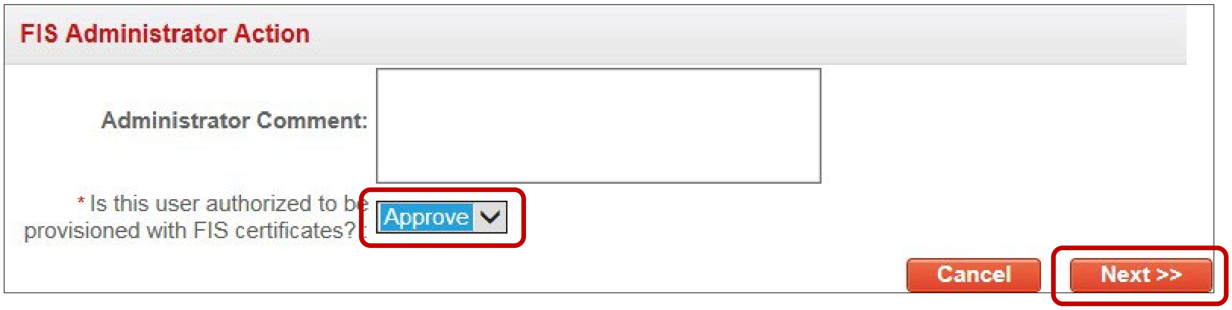


NOTE: If the user requested Medium Level of Assurance (MLOA) Digital Certificates, it is important their first and last name match their identity documents. Additionally, please ensure the address information is accurate. This is the address where a trusted agent is dispatched to complete in-person proofing.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

4. You can modify the following fields, if the user entered incorrect information:
    - **Partner/Application** that requires the digital certificates.
    - **Certificate Assurance Level**: Basic (BLOA), Medium (MLOA), or Unknown.
    - **Certificate Usage**: Only displays if user selects Basic
    - **Certificate Type**: Software, Hardware, or Unknown.
    - **Certificate Validity Period**: 1 or 3 years. Basic only offers 1 year.
    - **Request Reason**: Reason why user requires certificates.

5. From **FIS Administrator Action**, select **Approve** or **Deny.** If denying, you are required to enter

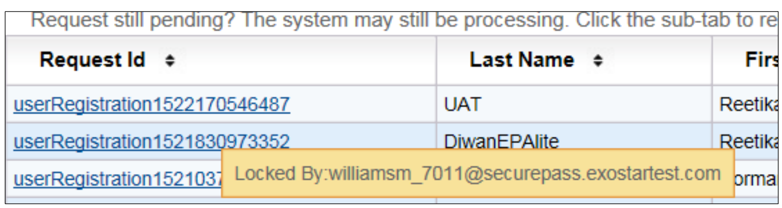
comments. Click **Next**.



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

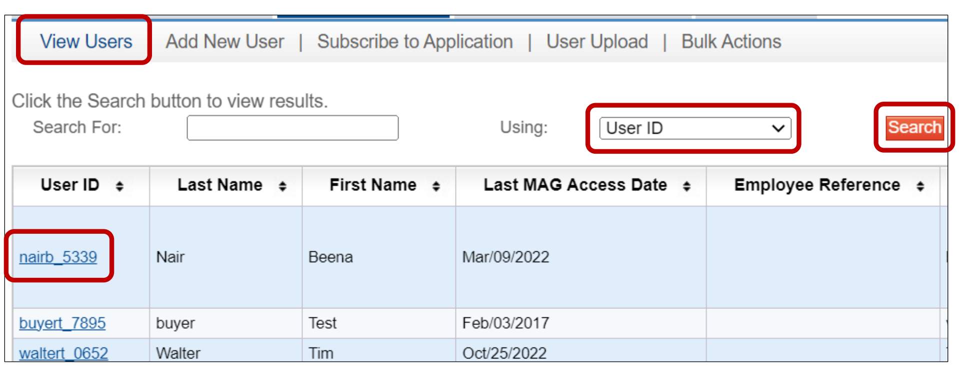
Unable to Approve or Authorize

If a request is **Pending**, you are unable to action the request because another administrator has locked the request. Place your cursor over the request ID to determine who locked the request. To unlock the request, contact the individual whose name displays (i.e. williamsm_7011).



If you are unfamiliar with the user ID of the locked request, to determine who to contact:

1. Go to the **Administration** tab. Then click **View Users** sub-tab.
2. Enter User ID in the **Search For** field. Select **User ID** from the search criteria drop-down menu. Click **Search**.
3. Results display. Click the hyperlinked **User ID** to access user details.



4. Contact the user to unlock the request.

Unlock Pending Requests

Requests transition to a pending status when a request is opened but not cancelled or processed.

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

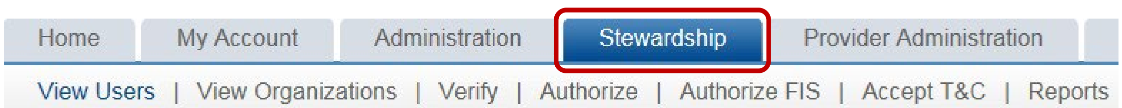
Request Id	Last Name	First Name	Org Name	Status
userRegistration1521830973352	DiwanEPAlite	Reetika	Exostar2	New
userRegistration1521037320799	Star	Norman	Exostar2	Pending

3. From the opened request, click **Cancel**. You are redirected back to the request queue.
4. Click the appropriate action sub-tab to refresh (Authorize User, Authorize Application or Authorize FIS).
5. The request now displays a status of **New**.

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

Stewardship Tab

Users with the Organization Steward role can complete administrative tasks from this tab. The Organization Steward role allows a single user account to maintain complete administrative control over groups of designated organizations.



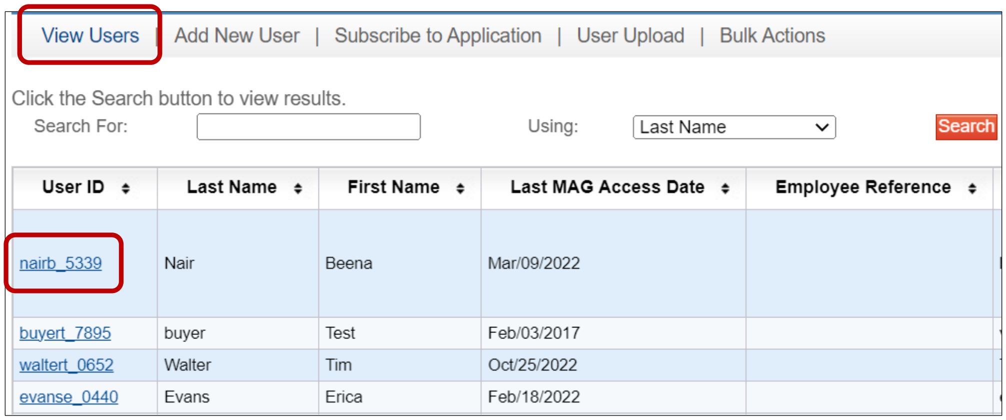
View Users

The View Users sub-tab allows Organization Stewards to search and complete administrative functions for all users within all organizations in the stewardship group. For assistance with administrative functions excluding role management, please see the Administration section. It is important to note that administrative activities are completed from the Stewardship tab.

Change Roles

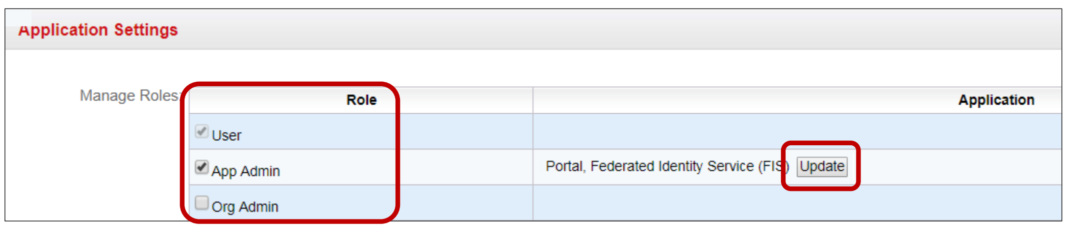
Organization Stewards can change user roles for users in their stewardship group. To change roles:

1. From the Stewardship tab, select the **View Users** sub-tab.
2. Enter search criteria. Click **Search**.
3. Click the **User ID** to access user details.

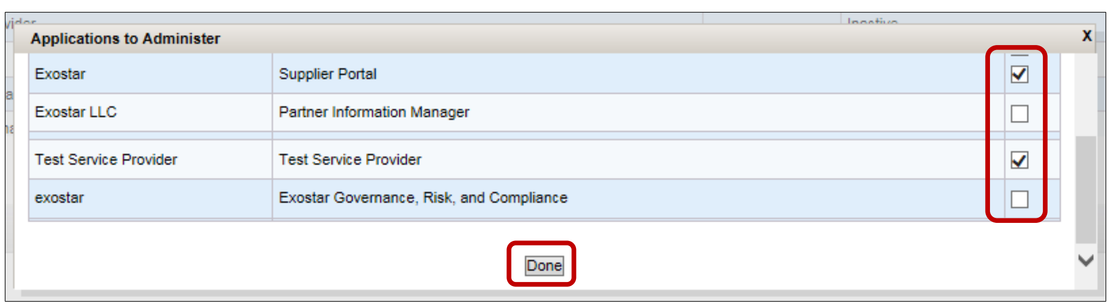


4. Scroll to the **Application Settings** section. Select the role from the **Role** drop-down menu.

NOTE: If assigning the Application Administrator role, select the application you want the user to administer by clicking **Update**.



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

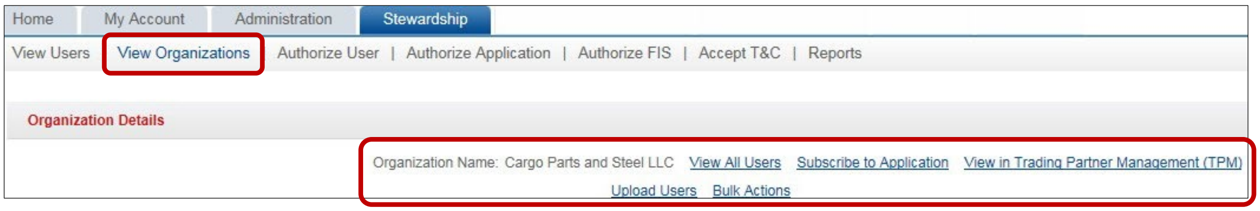


6. To complete role and/or application administration, scroll to the bottom of the page and click **Submit**.

View Organizations

View Organizations allows Organization Stewards to search for organizations included in their stewardship group. Organization Stewards can also subscribe organizations in their stewardship group to public applications, restrict credentials and information from partner company searches, identify an organization's small, disadvantaged business (SDB) status, and restrict profile access for restricted ForumPass sites.

Additionally, they can create, suspend, unsuspend, and delete user accounts using the user bulk upload function and request, suspend, unsuspend, and delete applications for users using the bulk actions upload function for organizations in their stewardship group. For assistance with identifying SDB status, restricting profile access for ForumPass site, user upload and bulk upload functions for organizations in your stewardship group, please see the Administration section. It is important to note these activities are completed from the Stewardship tab.



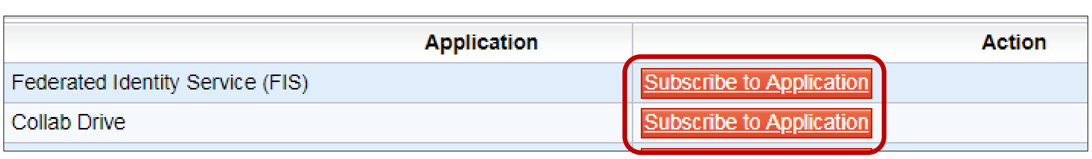
Subscribe an Organization to an Application

Organization Stewards access the **View Organizations** sub-tab to subscribe an organization to a public application.

1. Locate the organization by entering search criteria.
2. Click the **Org ID**.

3. Click **Subscribe to Application**.

4. Select the application or service to subscribe the organization to by clicking **Subscribe to Application.**



5. Select an existing Application Administrator from the drop-down menu or create new administrator. Click **Next**.

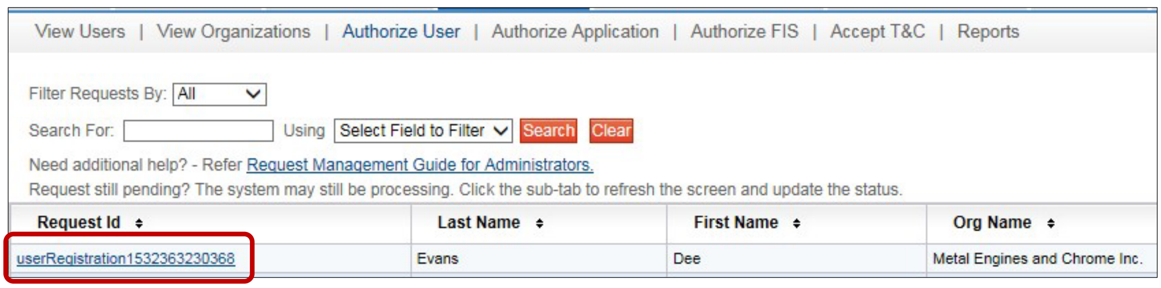
The request routes to Exostar for approval. It can take up to 48 business hours to process. If approved, the Organization Administrator, Organization Steward or Application Administrator for the application must accept terms and conditions before users can request access to the application.

For assistance with additional administrative functions, please see the Administration and View Organization Details sections. If completing activities for your stewardship group, access all functions from the Stewardship tab and not the Administration tab, Registration Requests tab or View Organization Details sub-tab (located from the My Account tab).

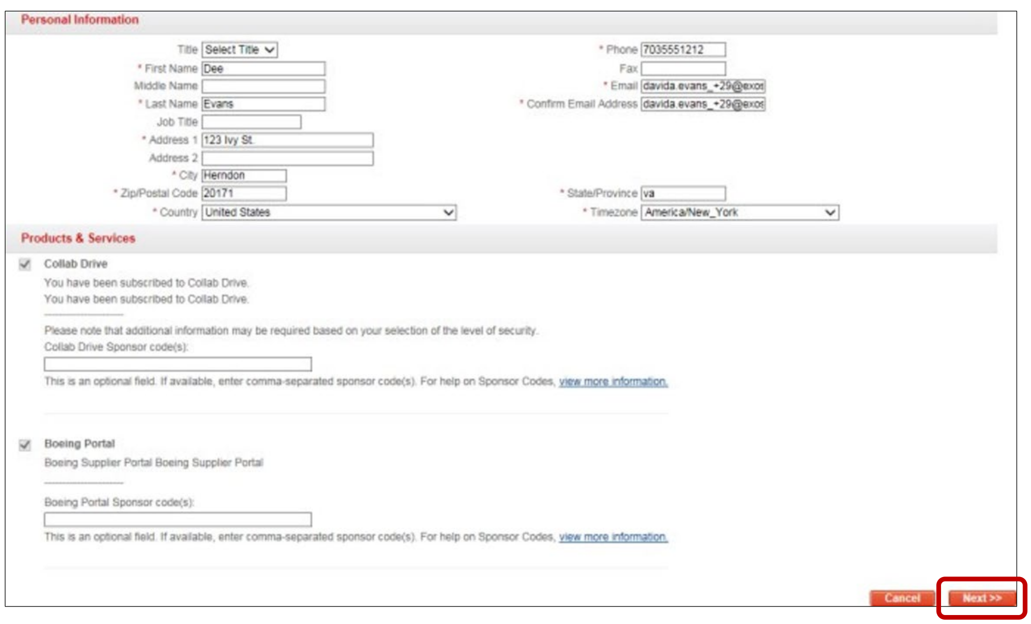
Authorize User

Organization Stewards access the **Authorize User** sub-tab to approve or deny new user requests for organizations in their stewardship group. To action a request:

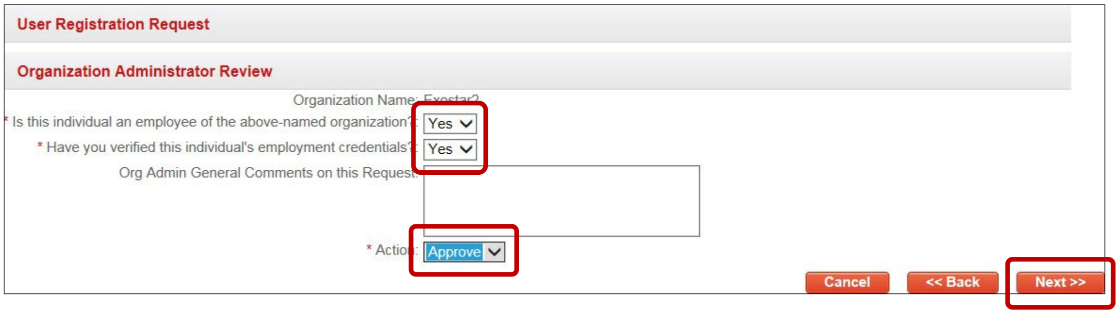
1. Click **Authorize User.**
2. Click the hyperlinked **Request ID**.



3. View request. modify personal information, if necessary. Then click **Next**.



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



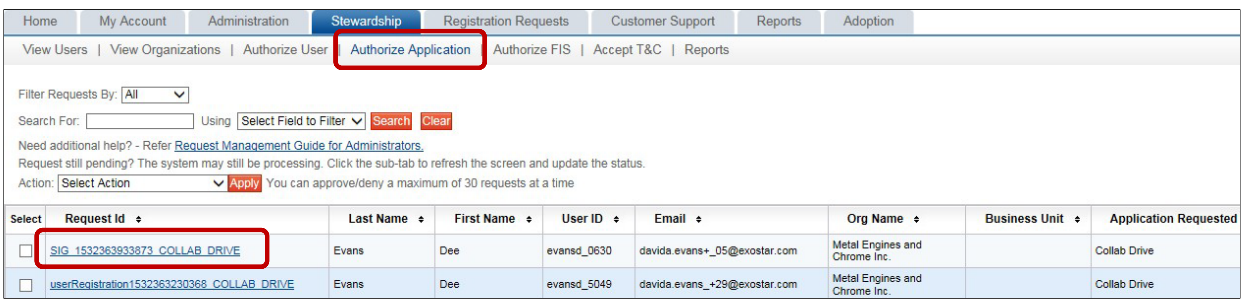
Once approved, a User ID is created, and the user receives instructions on how to complete account activation. If denied, the user receives a denial notification.

Authorize Application

Authorize allows Organization Stewards to authorize application requests for users in their stewardship group. You can view what application a user is requesting access to from the **Application Requested** column.

To authorize or deny requests individually:

1. From the **Stewardship** tab, select the **Authorize Application** sub-tab.
2. Click the hyperlinked **Request ID**.

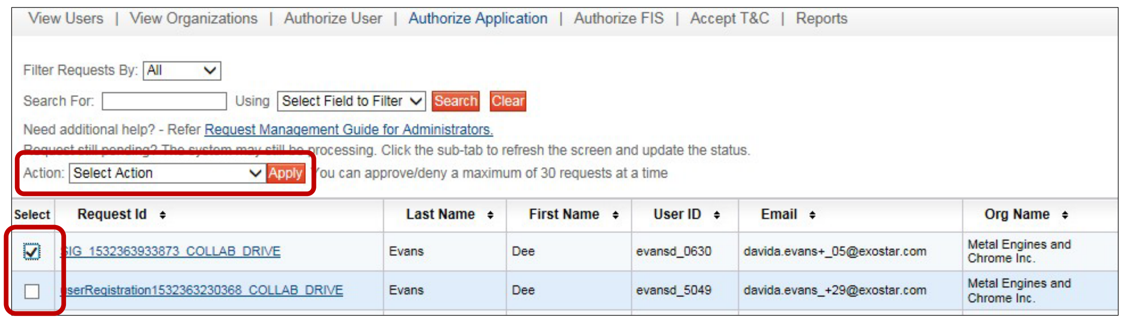


3. If the user requests reactivation of a suspended application, comments display in the **User Application Subscription Request** section if the user entered them. Review the information. Click **Next**.
4. Select **Approve** or **Deny** from the drop-down menu. If denying, you must enter a denial comment. Sponsor code is optional. Click **Next**.

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

To administer requests in multiples**:**

1. From the Stewardship tab, select the **Authorize Application** sub-tab.
2. Select the users you wish to approve or deny. From the **Action** menu, select **Approve** or **Deny Selected Requests,** click **Apply**. If denying, denial comments are required.



3. Click **YES** to complete the action.

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

Authorize FIS

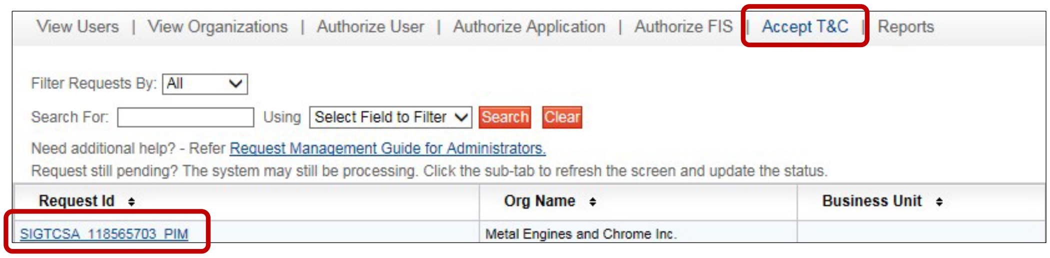
The Authorize FIS sub-tab allows Organization Stewards to approve or deny requests for Federated Identity Service (FIS) Digital Certificates for users within their stewardship group. For FIS authorization instructions, please reference the Authorize FIS section. It is important to note you complete this function from the Stewardship tab. Please see Federated Identity Service (FIS) Self-Help for more information.

Accept T&C

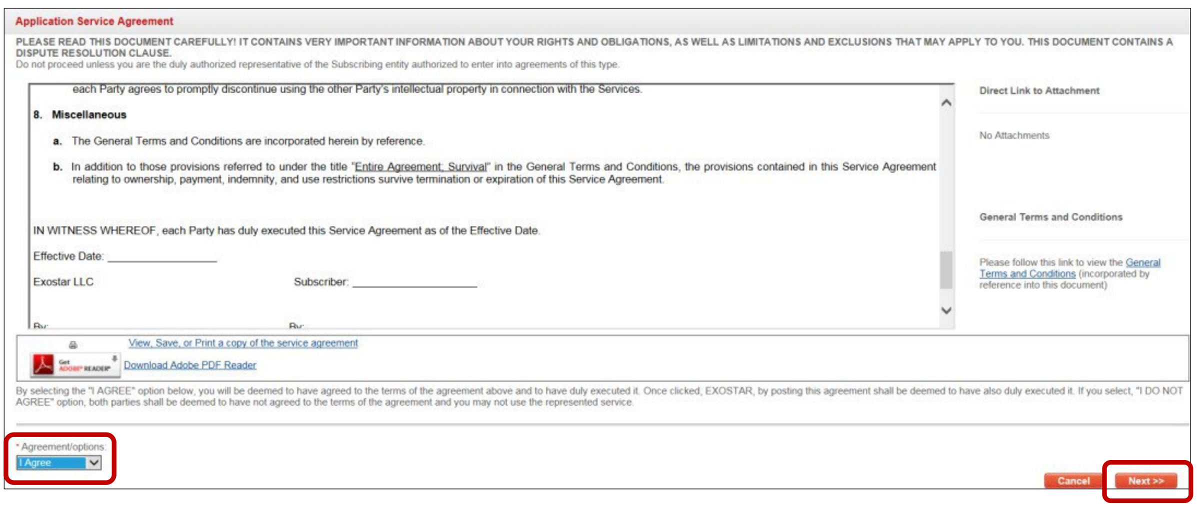
The Accept Terms and Conditions tab allows Organization Stewards to accept Terms and Conditions for the applications in their stewardship group. Once terms and conditions are accepted, users from the organization can request access to the application.

To accept terms and conditions:

1. From **Accept T&C**, click the hyperlinked **Request ID**.



2. Review the service agreement. To accept, select **I Agree** from the **Agreement/Options** menu. Terms and Conditions will not be accepted if you select, **I Do Not Agree**. Users are unable to access the application until Terms and Conditions are accepted. However, the organization's Organization Administrator or Application Administrator for the application can also accept Terms and Conditions.
3. Click **Next** to complete. If accepted, the organization is subscribed to the application and users can start requesting access.

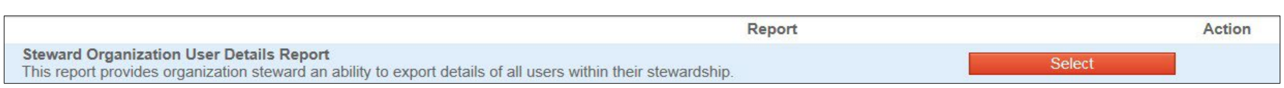


Pending Requests

If you are unable to complete an action using **Verify, Authorize,** or **Authorize FIS** please reference the Unable to Approve or Authorize section for assistance.

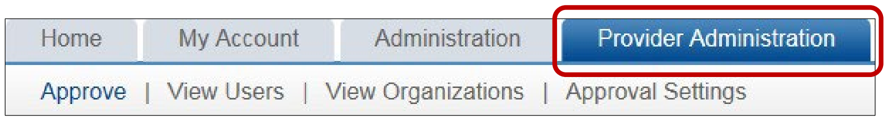
Reports

Reports provide the Organization Steward with relevant information on organizations and users within the stewardship group. Navigate to the Reports tab, and click **Select** to generate the report.



PROVIDER ADMINISTRATION TAB

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



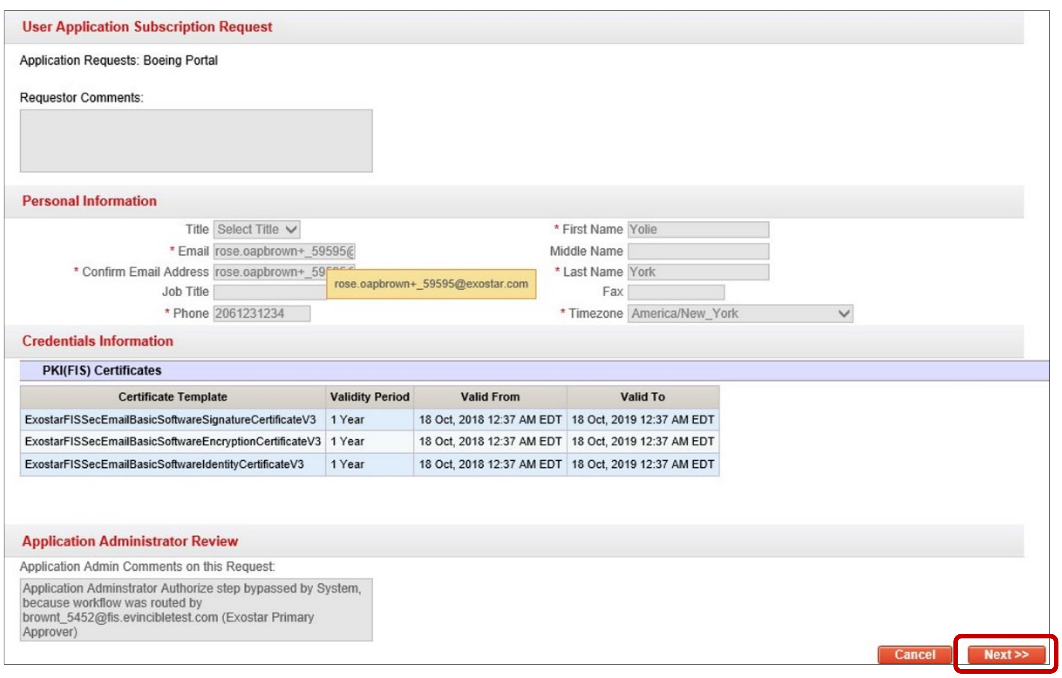
Approve

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

1. Click **Approve.**
2. Click the hyperlinked **Request ID**.

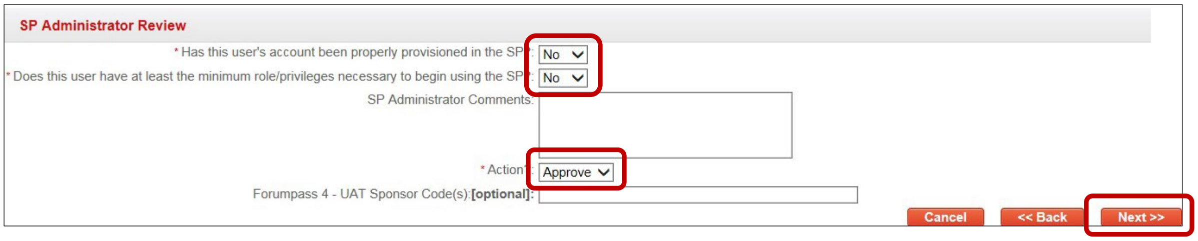
Select	Request Id	User ID	Last Name	First Name	Org ID	Org Name
☐	SIG_1530116451692_BSP	evansd_6801	Evans	Dee	EXO109701334	Exostar Test
☐	SIG_1529605513899_BSP	twentyj_3701	Twenty	June	EXO119809180	OAP ben two adoption/Exostar QA

3. Review the information. Click **Next**. To view the full email address, hover over the email address field.



NOTE: If user has registered multi-factor authentication credentials, such as One Time Password (OTP) Product or Federated Identity Service (FIS) Digital Certificates, information displays under the credential information section

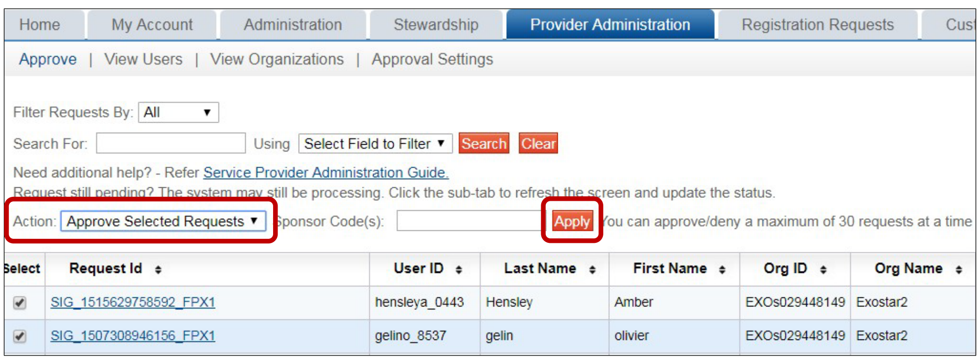
4. If approving, you must answer **Yes** to both questions. If denying, answer **No** to the questions. Denial comments are required.



NOTE: An application's administrative approval workflow depends on what is set for the application. Additionally, users receive an email notification of the approval or denial.

To administer multiple requests:

1. Select the users you are approving or denying. From the **Action** menu, select **Approve** or **Deny Selected Requests,** click **Apply**. You can select 30 requests at a time.



2. You will receive an **Approve Confirmation** screen. Click **YES** to complete approval. If denying, you must enter denial comments. Click **Submit**. Users receive an email with approval/denial status. Users receive an email notification of the approval or denial.

NOTE: Regardless of how the request for application access was administered, the request is either approved (providing user access to the application), denied, or routes to the Application Owner for approval. An application's administrative approval workflow depends on what is set for the application.

View Users

View Users allows SP Administrators to search for users subscribed to their application. From View Users, you can modify application access.

View Organization

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

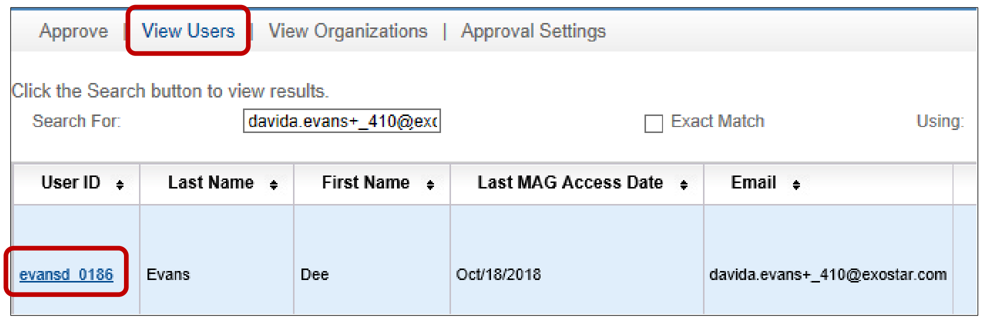
Modify Application Access

SP Administrators can modify application access for applications they administer. Modifying applications can be completed for users or organization. If suspending, users will be unable to access the application.

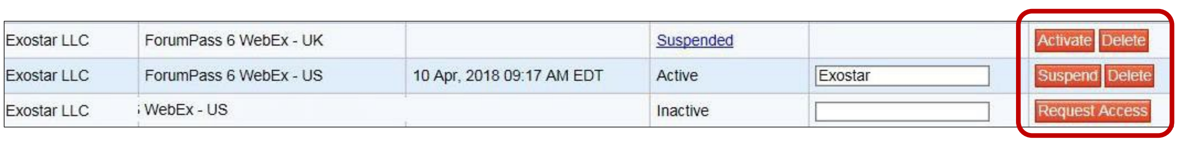
Users

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

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



4. To modify application access, scroll to **Application Settings**. Locate the application and click the appropriate action. You are required to enter a suspension reason. Click **Activate** to unsuspend. **Delete** removes the ability for you to modify the application.

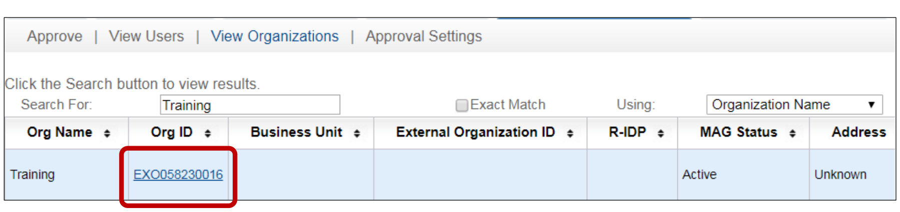


Additionally, application access is deactivated for the user. However, the user can request access to the application again from their Home tab.

Organizations

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

1. Click **View Organizations**.
2. Enter search criteria. Use the search filter menu or select **Exact Match** to narrow results. Click **Search**.
3. From results, click the hyperlinked **Org ID**.



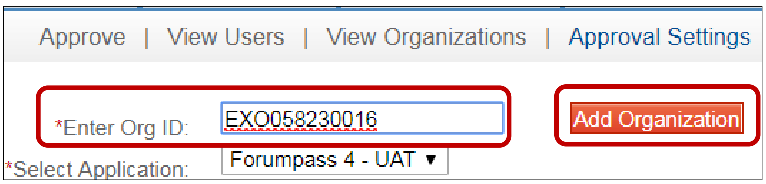
4. To modify application access, scroll to **Application Settings**. Locate the application and click the appropriate action. You are required to enter a suspension reason. Click **Activate** to unsuspend.

Approval Settings

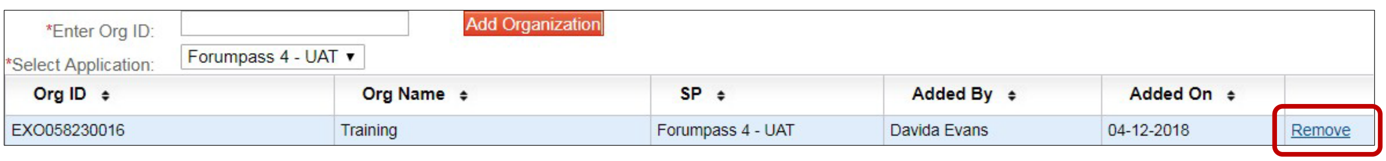
Approval Settings allows SP Administrators to add organizations for automatic approval for application requests. When organizations are added, all users who request access to a SP Administrator's application do not require SP Administrator approval.

To add or remove application settings:

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



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

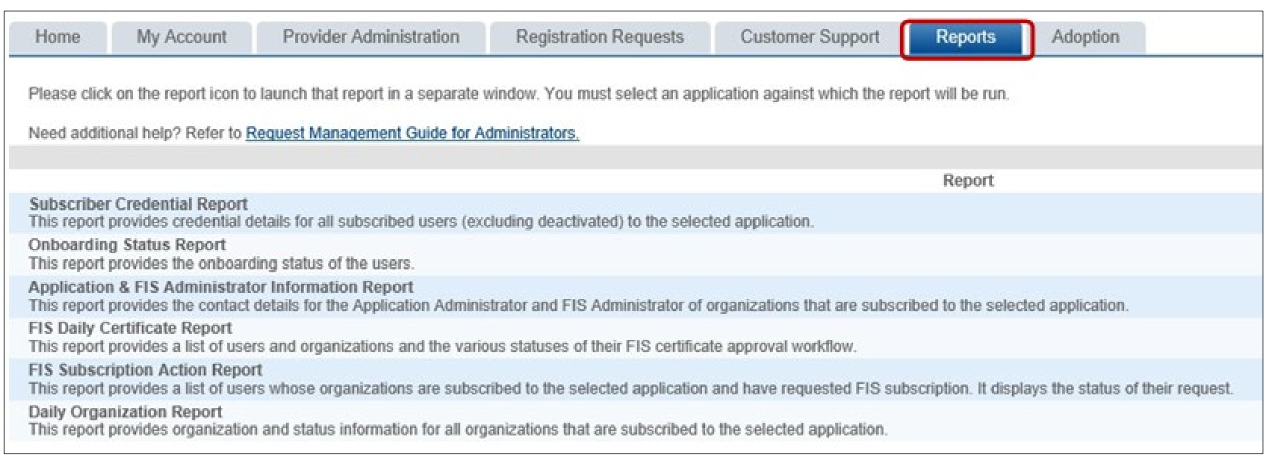


Reports Tab

The reporting feature is available to MAG Administrators. Organization Administrators, Application Administrators, Organization Stewards, and Adoption Administrators can generate reports, but their access to reports varies by role. Please review the table below to see what reports are available for your administrative role:

Reports	Organization Administrator	Organization Steward	Application Administrator	Adoption Administrator	Service Provider Administrator (SP Admin)	Service Provider Admin (Read only)	Exostar Portal Administrator (EPA)	EPA Lite	Customer Support	Is report in SSRS tool?
All Details Report	✓	✓					✓			✓
Application & FIS Administrator Information Report					✓	✓	✓			
Onboarding Status Report				✓			✓		✓	
Application Status Report	✓	✓	✓				✓			✓
Daily Organization Report					✓	✓	✓			
FIS Daily Certificate Report					✓	✓	✓			
FIS Subscription Action Report					✓	✓	✓			✓
Organization User Details Report	✓	✓								
Subscriber Credential Report					✓	✓	✓			✓
Steward Organization User Details Report (sub tab)		✓								

Reports can be launched directly from the **Reports** Dashboard. Click the Reports tab to access the list of reports available to you. Follow the prompts to generate your reports.



We encourage you to spend some time exploring reporting options to see what type of user data might make your administrative duties easier. Below we highlight reports that can be of particular use to Organization, Application, and Adoption Administrators.

Organization and Application Administrators have access to the following reports:

- All Details Report
- Organization User Details Report
- Application Status Report.

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

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

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

Onboarding Status Report is available to Adoption Administrators. This report allows to quickly track the onboarding of all companies invited by your organization to MAG. Have your suppliers registered for a MAG account, or invitations are still pending? Have they obtained their credentials and undergone identity proofing? Who is the point of contact for each individual company if the onboarding has stalled? Use this report to gain quick intelligence into where your partners are in their MAG onboarding journey.

Adoption Tab

Users with the Adoption Administrator role access this tab to use Exostar's Adoption Module, to invite organizations to access partner applications. For assistance with using the Adoption Module, please reference the Adoption Administrator Guide.

Search

Depending on role, search criteria and functionality varies for Administrators and Organization Stewards.

1. Select search type (e.g. View Users or View Organizations).
2. Select search criteria from the drop-down menu then enter search criteria in **Search For** field. Click **Search.**

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

View User Search Criteria

Last Name	Unique identifier for the user
First Name	Last name of user
User ID	Unique identifier for the user
Email	First name of user
R-IDP User ID	Email address of user
Employee Reference	Unique employee ID/reference for the user
Org ID	Organization ID for the Exostar MAG account
Organization Name	Name of organization
External User ID	User ID that partner company uses
External Organization ID	Organization ID that partner company uses

View User Results Fields

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

View Organization Search Criteria

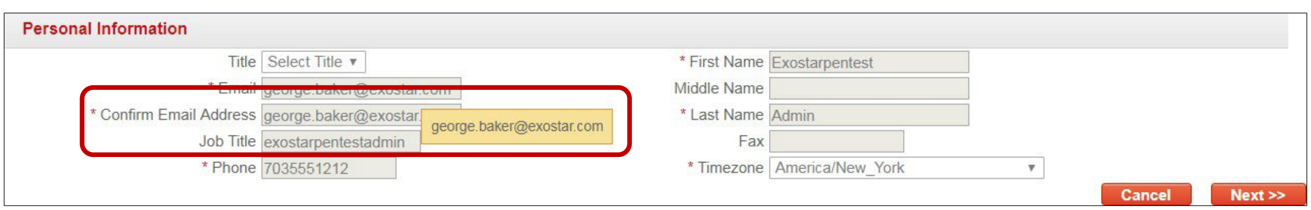
Org Name	Organization Name
Org ID	Organization ID for Exostar MAG Platform account
External Organization ID	Organization ID that partner company uses

Organization Results Fields

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

View Complete Email Address

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



Billing and Support

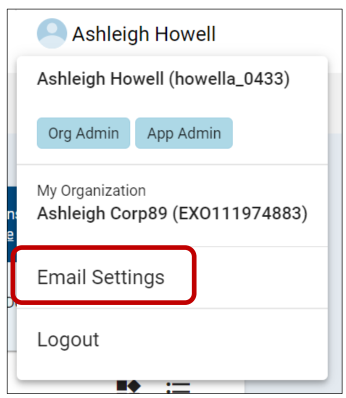
The Exostar Billing and Support Center is used to complete a variety of tasks including purchasing, making payments, viewing SCP transactions, opening support tickets, and more.

You must have the Exostar MAG Platform Organization Administrator role or Billing Contact role to pay Exostar SCP invoices.

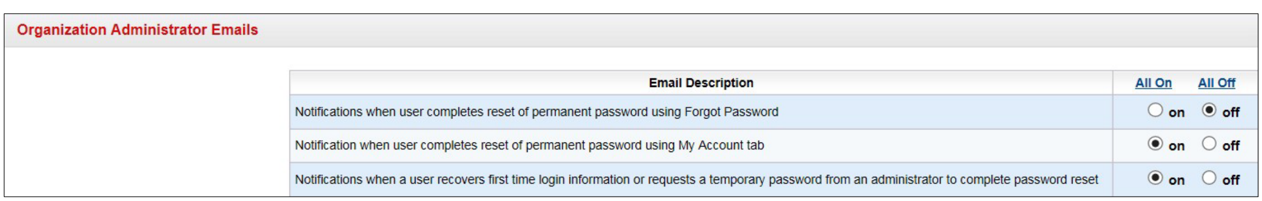
Email Settings

If you have an administrative role in MAG, you can adjust email notifications:

1. From your dashboard, in the top, right corner, select your Name. From the drop-down menu, select **Email Settings**.



2. Select the email notifications you want to adjust. The displayed information depends on role.



3. To complete, click **Submit.**

Change Authorization Requests

Change requests for the following events require **Change Authorization Form** completion:

- **Organization Administrator Change**: When the existing Organization Administrators are <u>no longer</u> available.

- **Email Address Change**: When a user has not completed first-time login or email domain name changed and the user cannot access the account requires an email address change.
- **Company Address Change**: When the company's address changed.
- **Company Name Change**: When the company's name changed.
- **Legal Name Changes**: When you change your legal name.

For assistance with change request completion, please reference the Change Authorization Requests section on MyExostar.

Account Disablement

If your account is in a state of inactivity, it may get suspended or deleted. Please see the reasons below about why your account may get **deleted** or **suspended**:

- **Account Activation not completed for more than 180 days:** If you have not completed account activation for your MAG account, your account is deleted. You are notified **30 days** prior to the deletion date, with instructions on how to complete account activation.
- **Application access suspension**: Each application has set parameters for the number of days of inactivity, which leads to access suspension. If your application access is due for suspension in 30 days or less, each time you log-in to your Exostar MAG Platform account, you are presented with a reminder to access the application, and the number of days to suspension. To ensure you do not lose access to the applications you need, it is good practice to log-in to your MAG account regularly, and access available applications.
- **Application access deletion:** If your application access has been suspended for **X** number of days, as specified by the application owner, your access to the application is deleted. You are notified regarding this deletion **30 days in advance**.
- **Active account deletion**: If the last active application subscription is suspended, your Exostar MAG Platform account is suspended **30 days after the application suspension**. You are notified regarding this suspension 30 days in advance. Contact Exostar Customer Support for information on how to re-establish application access.

MAG System Requirements

- **Supported Operating Systems:** Windows 8.1, Windows 10, and MAC
- **Supported Browsers:** IE 11
- **Browsers Supported with Limitation*:** Edge, FireFox, Safari, and Chrome
- ***Limitation**: (PKI) Digital Certificate Credential cannot be downloaded