Contents

Introduction .................................................................................................................................................. 5
Getting Started .............................................................................................................................................. 5
Organization and User ID Information ...................................................................................................... 5
Roles .............................................................................................................................................................. 6
Organization Administrator ....................................................................................................................... 6
Application Administrator ............................................................................................................................. 6
User ............................................................................................................................................................ 7
Adoption Administrator ............................................................................................................................. 7
Service Provider (SP) Administrator ........................................................................................................... 7
Organization Steward ................................................................................................................................ 7
Bundle Administrator ................................................................................................................................ 7
Login Information .......................................................................................................................................... 7
First Time Login .......................................................................................................................................... 8
Retrieve Lost First Time Login Information .............................................................................................. 10
Logging In after First Time Login ............................................................................................................... 12
Advanced Log-in Options .......................................................................................................................... 12
Forgotten User ID and Password ................................................................................................................ 12
Forgotten User ID for an Active Account ................................................................................................. 13
Forgotten Password for an Active Account .............................................................................................. 14
Expired Password for an Active Account ................................................................................................. 15
Forgotten Security Questions/Answers ................................................................................................... 17
Password Reset Errors ............................................................................................................................. 18
Navigation ................................................................................................................................................... 19
Home Tab ................................................................................................................................................ 19
Application Management ........................................................................................................................... 20
Application Status .................................................................................................................................... 21
Accept Terms & Conditions ...................................................................................................................... 22
Request Access to Single Applications Excluding FIS ........................................................................... 24
Request Access to an Application Group ................................................................................................. 25
Request FIS Digital Certificates ............................................................................................................... 26
Request Access to Suspended Application .............................................................................................. 28
My Account Tab ....................................................................................................................................... 29

Copyright ©2018 Exostar LLC. All rights reserved
Edit Profile............................................................................................................................................ 29
Determine Role and Organization ID .................................................................................................. 30
View Organization Details.................................................................................................................... 30
Determine Administrators .................................................................................................................... 30
Determine Applications your Organization is Subscribed to ............................................................ 31
Enterprise Access Gateway (EAG) Settings ...................................................................................... 31
Restrict Credentials or Information from Search Results ................................................................. 31
Identify Small Disadvantaged Business Status ................................................................................. 33
Change Email ....................................................................................................................................... 34
Change Password................................................................................................................................. 35
Change Security Questions .................................................................................................................. 36
Unable to Edit Personal Information ............................................................................................... 36
Manage Certificates ............................................................................................................................. 36
Learn about FIS Digital Certificates .................................................................................................. 37
Manage OTP......................................................................................................................................... 37
Learn about OTP ................................................................................................................................... 37
Connect Accounts ............................................................................................................................... 37
Account Connection Rules .................................................................................................................. 38
Logging into a Connected Account ................................................................................................... 39
Administration Tab .................................................................................................................................. 40
View Users ........................................................................................................................................... 40
Change Role ....................................................................................................................................... 40
Modify Application Access .................................................................................................................. 41
Reset Password ................................................................................................................................. 42
Restrict Profile Access Attribute......................................................................................................... 42
Add New User ...................................................................................................................................... 43
Subscribe to Application ..................................................................................................................... 44
User Upload ......................................................................................................................................... 45
Bulk Actions ......................................................................................................................................... 45
Registration Requests Tab ................................................................................................................... 45
Authorize or Deny User........................................................................................................................ 45
Authorize or Deny Application Access ............................................................................................... 46
Authorize FIS ......................................................................................................................................... 48
Unable to Approve or Authorize........................................................................................................ 49
Introduction
Exostar's IAM Platform (formerly known as MAG) is a secure Identity and Access Management solution for highly-regulated industries including Aerospace & Defense. With the cloud-based Exostar IAM Platform, users can administer accounts, purchase and activate credentials, access their partner applications, and more.

Getting Started
In order for your organization to access partner applications behind Exostar’s IAM Platform (MAG), your company requires an account. Your partner company will invite your organization to complete registration via email. Please note you can register for Boeing Supply Chain Platform, SourcePass, and Exostar’s Federated Identity Service here without receiving an invitation from a partner company. You can also register for the Boeing 787 Supply Chain Platform here. Although Boeing applications are available for public registration, please work with your Boeing contact to confirm if a registration needs to be completed.

When an organization is invited to use Exostar’s IAM Platform (MAG), the invitation recipient is responsible for designating the Organization and Application Administrator roles for their organization. These individuals are responsible for administering users and authorizing access to partner applications for your organization’s account.

Users need to access their partner company’s application after completing first-time login. Before users can access an application, the Organization or Application Administrator must accept terms and conditions. Once an organization is registered, users require their own account. The account’s Exostar IAM Platform (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.

For assistance with getting started with Exostar, please reference the Getting Started Quick Reference Guides.

Organization and User ID Information
When an organization’s account is created in Exostar’s IAM (MAG) Platform, 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
Exostar’s Identity Access and Management (MAG) Platform is a role-based solution. Users can be assigned a single role or multiple roles. Once the organization is established, roles can be added or removed.

Organization Administrator
The Organization Administrator is responsible for performing administrative activities on behalf of their organization. Organization Administrators can complete a variety of activities such as adding, approving, deleting, and suspending user accounts. An organization can have a single or multiple Organization Administrators.

Organization Administrator responsibilities include:
• Accept terms and conditions for applications the organization is subscribed to.
• Create, suspend, unsuspend, delete user accounts individually or using the Bulk Upload function.
• Request, suspend, unsuspend, and delete applications for users individually or in bulk.
• Approve user accounts for users who completed self-registration.
• Request access to application on a user’s behalf.
• Subscribe the organization to public applications (e.g. Federated Identity Service [FIS])
• Reset user passwords.
• For organizations subscribed to Exostar’s Enterprise Access Gateway (EAG) service, subscribe users to EAG using Bulk Uploads or Bulk Actions upload functionality.
• Update user roles.
• Run reports.

Application Administrator (including FIS Administrator)
The Application Administrator is responsible for approving or denying access to specific applications. When users request access to an application, the request is routed to an Application Administrator for approval. Application Administrators can only manage requests for applications they are the Administrator for. An organization can have a single or multiple Application Administrators.

Additional responsibilities include:
• Accept terms and conditions.
• Request access on behalf of users.
• Suspend application access.
User
Users have no administrative privileges for their organization’s Exostar’s Identity and Access Management (MAG) account. Users will log into their account to access their required applications.

Adoption Administrator
Adoption Administrators are responsible for inviting suppliers to use Exostar’s Identity and Access Management (MAG) Platform and subscribing them to their partner company’s applications. The Adoption Administrator role is only available to partner companies.

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 company applications. The SP Administrator role has view only permissions. Additionally, SP Administrators can run reports. The SP Administrator role is only available to partner companies.

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 Quick Reference Guide.

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 Exostar Identity and Access Management (MAG) Platform account was created for you to access a company partner application. To complete your first-time login (account activation), you require:

- **User ID**: lastnamefirstinitial_xxxx.
- **One-time password**: no longer valid after you complete first-time login.
- **System generated password**: xxxx-xxxx-xxxx-xxxx; type (or use cut and paste) the password exactly as it appears in the email you receive, including the hyphens as depicted above.
Depending on how your account is created, the above information is sent to you via email, as follows:

<table>
<thead>
<tr>
<th>Number</th>
<th>Account created by?</th>
<th>One Time Password</th>
<th>System Generated Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>User (Self-Registration)</td>
<td>Created by the user</td>
<td>Via Account Registration email</td>
</tr>
<tr>
<td>2.</td>
<td>Organization Administrator (Org Admin)</td>
<td>Supplied by the Organization Administrator</td>
<td>Via Account Registration email</td>
</tr>
<tr>
<td>3.</td>
<td>Adoption Administrator</td>
<td>Via Account Registration email</td>
<td>Via Account Registration email</td>
</tr>
<tr>
<td>4.</td>
<td>Exostar</td>
<td>Via Account Registration email</td>
<td>Via Account Registration email</td>
</tr>
</tbody>
</table>

**First Time Login**
Follow the instructions below to complete the first-time login process:

1. Go to [https://portal.exostar.com](https://portal.exostar.com) and click the **First Time Login?** link.
2. Once you click the link, the following screen displays. Enter the information provided to you in the email from Exostar and the Captcha code:
   a. MAG User ID
   b. One-Time Password
   c. System Generated Password

   ![](image)

**IMPORTANT:** You must have both your one-time password, and system generated password to complete the login process.

3. Click **Continue**, and enter your new password twice. Use the password strength policy on the screen as reference. Once complete, click **Next**.

   ![](image)
4. On the **Password Reset Secrets** screen, select four unique questions from the drop-down list, and enter a response for each question.

![Password Reset Secrets Screen](image)

**IMPORTANT:** Please ensure you remember these **secrets**. You must provide answers to your secret questions if you need to reset your password in the future.

5. Click **Next**.
6. The **first-time login completed** window displays, indicating you successfully modified your password. Click **Continue** to proceed.

### Retrieve Lost First Time Login Information

If you misplace your credentials, follow the directions below to retrieve your first-time login information:

---

**IMPORTANT:** Please ensure you remember these **secrets**. You must provide answers to your secret questions if you need to reset your password in the future.
1. After clicking, **First Time Login? Establish your account** from the login page, click **Forgot any of the above information? Follow these steps** link.

   ![Let's secure your account](image)

   Keeping your account secure requires action on your part. You will be required to create a strong (secure) password and establish security questions and answers. You will then be able to log in to the Exostar platform with your user ID and password. For certain applications, you may be required to log in using a higher level of assurance.

   Please refer to your welcome email from Exostar and enter the user ID and one-time password below:

   - User ID:
   - One-time password:
   - System generated password:

   [Forgot any of the above info? Follow these steps]

2. Enter your **email address** and the **zip/postal code** used at the time of account creation. Create a **new password**, following the password guidelines provided. This is a one-time password to access your account, along with other details sent to you via email. Enter Captcha code and click **Submit**.

   ![Resend First Time Login Info](image)
3. You receive an email from Exostar Administrator alerting you your first-time login credentials have been reset. Click Login Now to complete first-time login. You require the one-time password you created above to login.

4. Follow the steps provided in the First-Time Login section.

Logging In after First Time Login
Users who complete first-time login follow the steps below for all subsequent access to Exostar’s IAM Platform (MAG).

2. Enter your User ID and password. Click Login. Upon successful login, the IAM Platform (MAG) application page displays.

Advanced Log-in Options
If you are using Exostar’s IAM Platform (MAG) with FIS Digital 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 appropriate option under Advanced Login Options. Third-Party Credential users should select Digital Certificates (Hardware).

Forgotten User ID and Password
You can change your password for the following three scenarios:
- Forgotten user ID for an active account
- Forgotten password for an active account
- Expired password
Note: These options are not available if your Exostar IAM Platform (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.

Forgotten User ID for an Active Account


2. Enter your Email Address and Zip/Postal Code for your Exostar IAM Platform (MAG) account. Click Continue.

3. A confirmation page displays. Your User ID is sent to the email address associated with your account.

NOTE: If you have multiple accounts associated with the same email address, you receive a message stating multiple user IDs were found for this email address. Contact Exostar Customer Support for assistance.
Forgotten Password for an Active Account
Follow the steps below if you have an active IAM Platform (MAG) account and do not remember the password.


2. Enter your User ID. Click Continue.
3. The **Answer Security Questions** screen displays. Select questions and enter answers. Click **Continue**.

![Answer Security Questions](image)

**NOTE**: Answers to security questions are case sensitive.

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

5. You receive a confirmation message indicating your password has been successfully changed.

![Password Reset Successful](image)

**Expired Password for an Active Account**

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

1. Click **Reset Password**.

![Login Error](image)
2. The **Answer Security Questions** screen displays. Select questions and enter answers. Click **Continue**.

![Answer Security Questions](image)

**NOTE**: Answers to the security questions are case sensitive. If you have forgotten the answers to your security questions, click **Forgot Security Questions/Answers**.

3. The **Create New Password** screen displays. Enter your new password twice, and click **Submit**.

![Create New Password](image)

4. A confirmation message displays indicating your password has been successfully changed.
Forgotten Security Questions/Answers

In the event you forget the answers to your security questions, follow the steps below to proceed.

1. Click the **Forgot Security Questions/Answers? – Follow these steps to reset your password** link.

2. Enter the **Email Address** and **ZIP/Postal Code** associated to this account. Click **Continue**.

3. You receive an email containing a temporary **system-generated password**.

5. The create New Password screen displays. Enter your new password twice, and click Submit.

![New Password Screen]

6. You receive a confirmation message indicating your password was successfully changed.

**NOTE:** This feature is not available if your Exostar IAM Platform (MAG) account is linked to your corporate network log-in via EAG. If you have issues accessing your account, refer to the [EAG User Guide](#) for quick reference, or contact Exostar Customer Support for additional information.

**Password Reset Errors**

You may encounter the error notifications below when trying to reset your password:

- **Multiple IDs:** The email address you used is associated with multiple user accounts. Contact Exostar Customer Support to resolve your access issue.

- **Email Address/Zip Code Combination is Incorrect:** You receive this error if:
  - You typed your email address or zip code incorrectly.
  - You do not have correct information.

If you continue to receive this error after trying multiple times, contact your Organization Administrator to reset your password.
Navigation
When you log-in to Exostar IAM Platform (MAG), the Account Management Home page displays. Depending on your role, this could include two or more tabs.

NOTE: To expand all sections, Click the +Expand All Sections or click the expander icon (>>) for the section.

Home Tab
The Home tab has a number of components and provides a dashboard view of your Exostar IAM Platform (MAG) account.

When you log-in to https://portal.exostar.com with your credentials, the system automatically identifies your credential strength.

NOTE: Listed applications vary depending on what your organization is subscribed to.

Main components include:

- **User|Organization|Credential Strength**: User, Organization, and Credential Strength define your user ID, organization, and credential strength you are currently logged in with.
- **Credential Strength**: The following information may be presented under Credential Strength depending on what you logged in with:
  - Username & Password
  - Basic Software Certificate (displays Basic Software Cert)
  - MLOA Software (displays Medium Software Cert)
- MLOA Hardware (displays for FIS Hardware Digital Certificates and Third-Party Credentials and displays Medium Hardware Cert)
- OTP Hardware Token (displays Hardware OTP)
- Mobile ID (displays Mobile ID)
- Phone OTP (displays Phone OTP)

- **My Applications:** The applications listed in this section are based on applications your organization is subscribed to. The status of each application and available actions are provided next to the application name. If there are any special announcements for the application, and the **Announcements** column provides the information.

- **My Organization:** Provides information regarding your organization account along with available subscriptions. Displayed information is based on role.

- **My Tasks:** You may view all requests pending approval by you. Displayed information is based on role.

- **Account Summary:** Provides information about your account and roles for your Exostar IAM Platform (MAG) account.

- **Quick Links:** Provides links to various training demos and additional support links for quick reference.

**Application Management**

The Home tab displays all applications for which your organization has a subscription. You can view the status of applications and all available actions. If your organization is subscribed to an application group, it is listed under the **Application Groups** section. The page also displays any messages or announcements from Exostar or the application owner.
## Application Status

Applications may be in any of the below statuses:

<table>
<thead>
<tr>
<th>#</th>
<th>Status</th>
<th>Status Description</th>
<th>User Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Active</td>
<td>Subscription is approved to access the application.</td>
<td>Click <a href="#">Open Application</a> to launch the application in a separate browser window.</td>
</tr>
<tr>
<td>2.</td>
<td>Organization Registration Approval Pending</td>
<td>The organization’s request for subscription to the application has not yet been approved. Users cannot request access to the application. Approval can take up to 48 business hours.</td>
<td>None</td>
</tr>
<tr>
<td>3.</td>
<td>Pending Account Creation by the Application</td>
<td>The application has not yet been provisioned by the Service Provider (SP).</td>
<td>If the application has been in this status for more than 24 hours, contact <a href="#">Exostar Customer Support</a>.</td>
</tr>
<tr>
<td>4.</td>
<td>Pending Approval by the Application Owner</td>
<td>Request is pending approval by the SP Administrator. Approval time is determined by SP Administrator.</td>
<td>If application has been in this status for more than 48 hours, contact <a href="#">Exostar Customer Support</a>.</td>
</tr>
<tr>
<td>5.</td>
<td>Pending Application Administrator Approval</td>
<td>Application Administrator has not approved the subscription request or you have an active FIS subscription and have reapplied to get new certificates.</td>
<td>Contact your Application Administrator for the application.</td>
</tr>
<tr>
<td>6.</td>
<td>Pending Activation</td>
<td>SCP Application Administrator has not yet activated your SCP application subscription.</td>
<td>Contact your Application Administrator for the SCP application.</td>
</tr>
<tr>
<td>7.</td>
<td>Pending Acceptance of Terms &amp; Conditions</td>
<td>Organization Administrator has not yet accepted the Terms &amp; Conditions for access to the application.</td>
<td>Contact your Organization Administrator.</td>
</tr>
<tr>
<td>8.</td>
<td>Inactive</td>
<td>You are not subscribed to the application, but the organization is subscribed to the application.</td>
<td>If you need access to the application, click the <a href="#">Request Access</a> next to the inactive status. Your request is transitions to <a href="#">Pending Application Administrator Approval</a> (see status 5).</td>
</tr>
<tr>
<td>9.</td>
<td>Suspended</td>
<td>Your application access has been suspended.</td>
<td>Click <a href="#">Reactivate Application</a> next to the Application from the Home tab.</td>
</tr>
<tr>
<td>10.</td>
<td>Pending Exostar Approval</td>
<td>Specific to FIS Medium Level of assurance request, your request is pending approval by the Exostar Portal Administrator.</td>
<td>If application has been in this status for more than 48 hours, contact <a href="#">Exostar Customer Support</a>.</td>
</tr>
<tr>
<td>11.</td>
<td>Pending Proofing</td>
<td>Specific to FIS Medium Level of assurance request, you need to complete in-person proofing process.</td>
<td>Contact <a href="#">Exostar Customer Support</a> for information if in-person proofing has been completed.</td>
</tr>
<tr>
<td>12.</td>
<td>Login Requirements Not Met</td>
<td>Application access is restricted because the application requires a stronger assurance level.</td>
<td>Log into your account with the required credential. If you do not have a credential, you need to complete a purchase from <a href="#">Billing and Support</a> which can be accessed from your account. If you are unsure of what credential to purchase, contact <a href="#">Exostar Customer Support</a>.</td>
</tr>
</tbody>
</table>
Accept Terms & Conditions

If you are an Organization Administrator or Application Administrator and terms and conditions have not been accepted, you see View Service Agreement next to each application. Application Administrators are only able to accept terms and conditions for applications they administer. Organization Stewards will access the Accept T&C sub-tab from the Stewardship tab.

NOTE: Users within your organization are not able to access the application until the Organization or Application Administrator accepts the Service Agreement for the application. Organization Stewards need to reference the Organization Steward section for assistance.

1. Click View Service Agreement. For users completing a new organization registration invitation, you will be taken to step 2 after completing security questions.
2. Click Continue.

Great! Now let's accept terms & conditions.

The applications below have Terms & Conditions that must be accepted before they can be accessed by organization members. In the next few screens, you will have the opportunity to read and accept the Terms and Conditions for each application.

SourcePass

Terms & Conditions NOT Accepted

Exostar’s SourcePass is a comprehensive on-demand eSourcing solution which allows a Buyer to create events to request information (RFI), proposals (RFP), quotation (RFQ) for goods and services from Suppliers. The application is hosted in the US.

Continue

3. If accepting, review the terms and conditions, then check the box for I have read and agree to these terms and conditions. Click Agree to accept the agreement. Click Next.
4. Your organization is now successfully subscribed to the application. Organization and Application Administrators for the application can start subscribing users within their organization to the application. Users can start requesting access to the application.

![Image of Terms & Conditions Accepted]

Organization/Application administrator(s) have accepted the terms and conditions for the applications below. **Note: You will not be able to access any application in which Terms and Conditions have not been accepted by the Organization/Application Administrator.**

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 acceptance occurs, Organization and Application Administrators for the application cannot start subscribing users within their organization the application.
- Users cannot start requesting access to the application.

**Request Access to Single Applications Excluding FIS**
If you require access to an application, you have to be granted access.

1. To request access to all single applications (other than FIS), click **Request Access** under the **Status** column.
2. If you were provided a sponsor code, enter the sponsor code. You can also enter comments that can be reviewed by an Application Administrator, SP Administrator, and Organization Steward. Sponsor code and comments fields are optional. Click Next.

3. A confirmation page displays.

4. The request is routed 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 require access to an application group (such as Rolls-Royce eTools or the Raytheon Bundle), you have to be granted access.

1. Click the Request Access link under the Status column.
2. Review all information, and click **Next**.

3. A confirmation page displays.

4. 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.

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

**Request FIS Digital Certificates**

1. Click **Request Access**.
2. **Enter FIS Certificate Information.**

- **Sponsor Code:** If you were provided a sponsor code, enter the sponsor code. The sponsor code is optional.
- **Partner/Application:** This field displays a drop-down list of Partners/Applications, who may require you to have FIS certificates. 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 option to select **Basic** (Basic Level of Assurance known as BLOA), **Medium** (Medium Level of Assurance known as MLOA), or **Unknown**. Please note if you select **Unknown**, your FIS Administrator may take additional time to approve your request to ensure they approve you for the correct certificate option.
- **Certificate Usage:** This option is only available when you select **Basic Level of Assurance**. Available usage options include **Identity**, **Secure Email**, and **Unknown**. If you request FIS certificates to access ForumPass-US or ForumPass-EU applications, select **Identity** as the option for this field.
- **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 including name, address, and email address. Please ensure you are using a valid email address (public email addresses such as Hotmail, Gmail, etc. are not allowed). If you request Medium Level of Assurance (MLOA) Digital Certificates, 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 need to complete the email change process first. Once the email change is complete, you need to restart the FIS request process.

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

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

3. A confirmation page displays. The request routes to the Application Administrator for authorization. The Application Administrator will approve or deny access.

NOTE: 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 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.

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.

**Determine Role and Organization ID**

Follow the steps below to determine your role and organization ID.

1. From Edit Profile, view User Profile.
2. View 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 which application an individual is an Application Administrator for.
Determine Applications your Organization is Subscribed to

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.

<table>
<thead>
<tr>
<th>Application Access</th>
<th>Provider</th>
<th>Application</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exostar LLC</td>
<td>Exostar</td>
<td>Identiti</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(FTT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assurance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Tokens</td>
<td></td>
</tr>
</tbody>
</table>

Enterprise Access Gateway (EAG) Settings


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, then click View Organization Details.
2. From View Organization Details, click View in Trading Partner Management (TPM) in the Organization Name section.
3. TPM displays. Click **MAG Information**.

![MAG Information Icon]

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.

![Change Flag]

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**.

**Identify Small Disadvantaged Business 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.

1. To set the SDB flag, go to the **My Account** tab, then click **View Organization Details**.
2. From **View Organization Details**, click **View in Trading Partner Management (TPM)** in the **Organization Name** section.
3. TPM displays. Click **MAG Information**.

4. Check the box for **SDB Flag**. 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.

1. Enter your new email address, and click **Continue**. You receive an activation code via email to your new email address.
2. Enter the activation code from your email, and click **Activate**. Your new email address is now active in the system.

![Activation Process]

**Change Password**

Change Password allows users to change their password.

![Password Change Process]

Make sure your new password complies with the **Password Strength Policy**:

- Must contain a minimum of eight characters, and a maximum of 12 characters.

- Must contain at least four distinct characters:
  - One alphabetic character
  - One numeric character
  - One special character such as !,@,#,$,% etc.
  - Leading and trailing spaces are not permitted.
Change Security Questions
Change Security Questions allows you to update your security questions.

NOTE: If your account is currently connected using EAG or Account Connections, you are unable to change your email and password.

Unable to Edit Personal Information
If you purchased a product that requires identity proofing, such as an Exostar OTP Hardware Token, FIS Digital Certificates, or Phone OTP; account information (e.g. name, email address, etc.) cannot be modified while a proofing is pending. If you are unable to edit your profile information, you may need to cancel a pending identity verification request and reschedule once the information is corrected.

If using Account Connections, your name and email address can only be changed on your parent account. Changes made to the parent account apply to child accounts as well.

Manage Certificates
Manage Certificates 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.
You will not see **Manage Certificates** if you have expired certificates (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.

*Learn about FIS Digital Certificates*

For additional information about FIS, please reference the **FIS Guides**.

**Manage OTP**

Manage OTP allows you to manage OTP credentials. From here, you can complete a purchase, test your phone before you start using the service, view details about your activated credential, and elevate with your credential if you logged in with only username and password.

![Manage OTP screenshot](image)

**NOTE**: Purchase is only available from Manage OTP for users who have not activated OTP credentials.

*Learn about OTP*

Please reference **OTP Resources** to learn more about OTP.

**Connect Accounts**

Connect Accounts (known as Account Connections) 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-Child 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.
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. Click **Connect Accounts**.
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.
3. Enter the password of the account you will connect to. 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.

---

**Logging into a 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 be unable to login, and receive the following message, “Your User ID/Password combination was not recognized.”
1. After entering parent account credentials, select the account you want to access and click Continue.

2. You are logged into the selected account leveraging the parent account credential.

**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**

View Users allows Organization and Application Administrators to search and complete administrative functions. Administrators can complete user management activities 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 Organization Steward navigation, please reference the Organization Steward section.

To change roles:

1. Click View Users.
2. Enter search criteria then click Search.
3. Click the **User ID** to access user details.

![View Users](image)

4. Scroll to the **Application Settings** section. Select the role from the **Role** drop-down menu. If assigning the role of Application Administrator, you must select the application you want the user to administer by checking the box in the **Select** column.

![Application Settings](image)

5. To complete, scroll to the bottom of the page and click **Submit**.

---

**Modify Application Access**

Organization Administrators, Organization Stewards and Application Administrators can request or suspend application access for users. 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 learn about Organization Steward navigation, please reference the **Organization Steward** section.

To modify application access:

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

![View Users](image)

4. Scroll to **Application Settings**. Locate the application and click the appropriate action (i.e. Suspend). You are required to enter a suspension reason. Click **Activate** to unsuspend. 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.

![Image of certificate status options](image)

However, the user can request access to the application again from their Home tab.

**NOTE:** Comments are viewable by the Application Administrator, Organization Steward, or SP Administrator. If requesting access, sponsor code is not required.

**Reset Password**

Organization Administrators and Organization Stewards can reset a user’s IAM Platform (MAG) password. To learn about Organization Steward navigation, please reference the **Organization Steward** section.

To reset password:
1. Organization Administrators will access **View Users** from the **Administration** tab.
2. Enter search criteria then click **Search**. Select the required **User ID**.
3. Scroll to the **Application Settings** section of the page. Click **Reset Permanent Password**.
4. 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 the IAM (MAG) platform, 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. Go to the **Administration** tab, then click **View Users**.
2. Enter search criteria then click **Search**. Select the required **User ID**.

![View Users](image)

3. From the **User Profile** section, select the required radio button for **Restricted Access**.

![User Profile](image)

4. Scroll to the bottom of the page and click **Submit**. The setting is saved. To learn more about the additional settings for restricted access, please reference the **ForumPass User Guide**.

**Add New User**

Add New User allows Organization Administrators to create new user accounts for their organization.

To add a new user:

1. Click **Add New User** and enter user details.
2. Select the user’s role and select the applications you want to subscribe the user to.
3. Click **Continue**.
4. Click **Submit**.
5. The user receives 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 the Exostar Organization ID.
2. Once the user completes the invitation, you are required to action the request from your Exostar IAM Platform (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.

![Subscribe to Application](image)

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

![Application Administrator Form](image)

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

3. 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
Organization Administrators can access the Authorize User sub-tab to approve or deny new user requests.

1. Click Authorize User.
2. Click the hyperlinked Request ID.
3. View the request, and modify personal information, if necessary. Click **Next**.

![User Registration Request](image1)

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

![User Registration Request](image2)

5. Once approved, a user ID is created, and the user receives instructions on how to complete first-time login. 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. 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 and 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.

5. 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. Select 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. 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. Pending requests display. **Click the Request ID.**

![Authorize FIS](image)

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’s user ID, first and last name matches their legal name.

![User Registration Request Approval](image)

4. 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 will be dispatched to complete in-person proofing. Please ensure the user does not have a **PO**
5. 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.

6. From **FIS Administrator Action**, select **Approve** or **Deny**. If denying, you are required to enter comments. Click **Next**.

   ![FIS Administrator Action](image)

7. 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 the status of 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).

![Request still pending](image)

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

1. Go to the **Administration** tab.
2. Enter user ID in the Search For field. Select User ID from the search criteria drop-down menu. Click Search.

![Image of search results]

3. Results display. Click the hyperlinked User ID to access user details.

![Image of user details]

4. You must 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 hyperlinked User ID.

<table>
<thead>
<tr>
<th>Request Id</th>
<th>Last Name</th>
<th>First Name</th>
<th>Org Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_registration15210301273992</td>
<td>Star</td>
<td>Norman</td>
<td>Exostar2</td>
<td>New</td>
</tr>
<tr>
<td>user_registration15210301273999</td>
<td>Star</td>
<td>Norman</td>
<td>Exostar2</td>
<td>Pending</td>
</tr>
</tbody>
</table>

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.

![Image of request statuses]

Reports Tab
The Reports tab provides reporting information. Access to this tab and available reports depends on role. Available file formats are .CSV, PDF and HTML.
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

View Users allows Organization Stewards to search and complete administrative functions for all users within all organization in the stewardship group. From View Users, Organization Stewards can complete user management activities such as request and suspend application access, assign user roles, as well as suspend and delete users. For assistance with administrative functions, please see the Administration section. It is important to note that administrative activities will be completed from the Stewardship tab.

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, 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 that these activities will be 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**.

   ![Click the Org ID](image1.png)

3. Click **Subscribe to Application**.

   ![Subscribe to Application](image2.png)

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

   ![Subscribe to Application](image3.png)

5. Select an existing Application Administrator from the drop-down menu or create new. If creating as new, you are responsible for communicating the One-time Password to the user. Click **Next**.

   ![Select Application Administrator](image4.png)

6. 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, you will 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).

Verify
Organization Stewards access the Verify sub-tab to approve or deny new user requests for organizations in their stewardship group.

1. Click Verify.
2. Click the hyperlinked Request ID.
3. View request. You can modify personal information. 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.

![User Registration Request](image)

5. Once approved, a user ID is created and the user receives instructions on how to complete first-time login. If denied, the user receives a denial notification.

**Authorize**

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

![Request Management](image)

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 and 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.

5. 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. Click Authorize.
2. Select 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.
3. Click YES to complete the action. 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
Authorize FIS 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 that you will complete this function from the Stewardship tab.
Accept T&C
Accept terms and conditions (T&C) allows Organization Stewards to accept terms and conditions for applications for organizations within the stewardship group. Once terms and conditions are accepted, users from the organization can request access to the application.

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 will be unable to access the application until the terms and conditions are accepted. However, the organization’s Organization Administrator or Application Administrator for the application can also accept the terms and conditions. You can come back and accept them if you decline acceptance.

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 reporting information. Select the report to view from the Action column. Available file formats are .CSV, PDF and HTML.

Provider Administration Tab
Partner companies with the Service Provider (SP) Administrator role can complete application approvals for applications that require SP Administrator approval, view users and organization information. From 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 individually:
1. Click Approve.
2. Click the hyperlinked Request ID.
3. Review the information. Click Next.
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 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 (i.e. suspend).

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 are SP Administrator for. 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.

1. To modify a user’s application access click View Users.
2. Enter search criteria. Use the search filter menu or select Exact Match to narrow results. Click Search.

![Search Screen]

3. From results, click the hyperlinked User ID.

4. To modify application access, scroll to Application Settings. Locate the application and click the appropriate action (i.e. Suspend). 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.

![Application Settings]

Organizations
You can modify access to your application for an entire organization. Once suspended, users are unable to access the application.
1. To modify an organization’s application access, click **View Organizations**.
2. Enter search criteria. Use the search filter menu or select **Exact Match** to narrow results. Click **Search**.

![Image of View Organizations](image)

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

**Approval Settings**

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

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

![Image of Enter Org ID and Select Application](image)

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

**Adoption Tab**

Users with the Adoption Administrator role access this tab to use Exostar’s Adoption Module. 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.).

**Search Field Definitions**
**View User Search Criteria**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>Unique identifier for the user</td>
</tr>
<tr>
<td>First Name</td>
<td>Last name of user</td>
</tr>
<tr>
<td>User ID</td>
<td>Unique identifier for the user</td>
</tr>
<tr>
<td>Email</td>
<td>First name of user</td>
</tr>
<tr>
<td>R-IDP User ID</td>
<td>Email address of user</td>
</tr>
<tr>
<td>Org ID</td>
<td>Organization ID for Exostar IAM Platform (MAG) account</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Name of organization</td>
</tr>
<tr>
<td>External User ID</td>
<td>User ID that partner company uses</td>
</tr>
<tr>
<td>External Organization ID</td>
<td>Organization ID that partner company uses</td>
</tr>
</tbody>
</table>
**View User Results Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Unique identifier for the user</td>
</tr>
<tr>
<td>Last Name</td>
<td>Last name of user</td>
</tr>
<tr>
<td>First Name</td>
<td>First name of user</td>
</tr>
<tr>
<td>Email</td>
<td>Email address of user</td>
</tr>
<tr>
<td>R-IDP User ID</td>
<td>Remote Identity Provider User ID (information displays in the column if user has linked their account)</td>
</tr>
<tr>
<td>Role</td>
<td>Role(s) assigned to user.</td>
</tr>
<tr>
<td>MAG Status</td>
<td>Status of user’s access. Active status means user has completed first time login. Inactive status means user has not completed first time login.</td>
</tr>
<tr>
<td>Active Applications</td>
<td>Applications active for the user</td>
</tr>
<tr>
<td>Pending Applications</td>
<td>Applications pending approval by an Administrator</td>
</tr>
<tr>
<td>External User ID</td>
<td>User ID that partner company uses</td>
</tr>
<tr>
<td>External Organization ID</td>
<td>Organization ID that partner company uses</td>
</tr>
<tr>
<td>Org ID</td>
<td>Organization ID for Exostar IAM Platform (MAG) account</td>
</tr>
<tr>
<td>Org Name</td>
<td>Name of organization</td>
</tr>
</tbody>
</table>

**View Organization Search Criteria**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org Name</td>
<td>Organization Name</td>
</tr>
<tr>
<td>Org ID</td>
<td>Organization ID for Exostar IAM Platform (MAG) account</td>
</tr>
<tr>
<td>External Organization ID</td>
<td>Organization ID that partner company uses</td>
</tr>
</tbody>
</table>
### View Organization Results Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org Name</td>
<td>Organization Name</td>
</tr>
<tr>
<td>Org ID</td>
<td>Organization ID for Exostar IAM Platform (MAG) account</td>
</tr>
<tr>
<td>Business Unit</td>
<td>Unit of an organization representing a specific business function</td>
</tr>
<tr>
<td>External Organization ID</td>
<td>Organization ID that partner company uses</td>
</tr>
<tr>
<td>R-IDP</td>
<td>Remote Identity Provider (information displays in column if organization is using EAG.)</td>
</tr>
<tr>
<td>MAG Status</td>
<td>Status of organization’s account. Active status means the organization is active in Exostar’s IAM Platform (MAG).</td>
</tr>
<tr>
<td>Address</td>
<td>Organization’s Address</td>
</tr>
<tr>
<td>City</td>
<td>Organization’s City</td>
</tr>
<tr>
<td>State</td>
<td>Organization’s State</td>
</tr>
<tr>
<td>Country</td>
<td>Organization’s Country</td>
</tr>
<tr>
<td>Active Applications</td>
<td>Applications active for the organization.</td>
</tr>
<tr>
<td>Suspended Application</td>
<td>Applications suspended for the organization.</td>
</tr>
</tbody>
</table>

### 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 IAM Platform (MAG) Organization Administrator role or Billing Contact role to pay Exostar SCP invoices.
Email Settings
If you have an administrative role in Exostar’s IAM Platform (MAG), you can adjust email notifications.

1. Click the gear icon (upper, right hand corner of your account).

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

3. To complete, click Submit.

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

- **Organization Administrator Change:** When the existing Organization Administrators are no longer 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 Request Quick Reference Guide.
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:

- **First Time Login not completed for more than 180 days**: If you have not completed First-Time Login (account activation) for your Exostar IAM Platform (MAG) account, your account is deleted. You are notified 30 days prior to the deletion date, with instructions on how to complete the first-time log-in.

- **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 IAM Platform (MAG) 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 Exostar IAM Platform (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 IAM Platform (MAG) 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.
IAM System Requirements

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Browsers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FF 3.0+</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>T</td>
</tr>
<tr>
<td>Windows 7</td>
<td>RS</td>
</tr>
<tr>
<td>Windows 8</td>
<td>RS</td>
</tr>
</tbody>
</table>

(R) Recommended: Exostar Solutions will work with these browser/OS combinations.

(T) Tested: Exostar has conducted high-level testing of its Solutions to identify any critical issues. Support will be provided but may be limited to the extent issues have been identified.

(RS) Roadmap Support: Exostar recognizes the potential need for future support but has not conducted any testing to date. Inclusion in future roadmap scope is not guaranteed, but has been identified as a candidate.