Managed Access Gateway (MAG)
Application Administrator and Federated Identity Service Administrator Guide

February 2021

CONTENTS

DOCUMENT VERSIONS

Version	Impacts	Date	Owner
IAM Application and FIS Administrator Guide (MAG 6.10)	• Last MAG Access Date column added when using View Users sub-tab	November 2018	S. Puthanveetil
MAG 6.11	• Changed the product name from IAM to MAG	April 2019	S. Puthanveetil
MAG 6.14	• Remove One-Time Password from FTL • Update Password Policy	June 2020	B. Nair
MAG 7.0	• Self-Registration • New Organization Adoption Invitation registration process • Dashboard • Purchasing • Credentialing • Activation • Authentication	February 2021	B. Nair

Introduction

This role-based guide covers the primary actions performed specifically by users with the Application Administrator and Federated Identity Service (FIS) Administrator role. For a more comprehensive guide, please reference the Managed Access Gateway (MAG) User Guide on the MAG Downloadable Guides page.

Exostar's Training Team offers bi-monthly Organization and Application Administrator training. Please see the MAG Webinars page for registration information and upcoming event dates.

Application Administrator

The Application Administrator (App Admin) is responsible for approving or denying access to specific applications. When users request access to an application, the request is routed to the 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

Federated Identity Service (FIS) Administrator

The FIS Administrator (FIS Admin) is responsible for approving or denying access for FIS digital certificate requests. When users request FIS certificates, the request routes to the FIS Application Administrator for approval. An organization can have a single or multiple FIS Administrators.

Additional responsibilities include:

- Accept terms and conditions for FIS
- Request access on behalf of users to FIS
- Suspend access to FIS

Accept Terms & Conditions

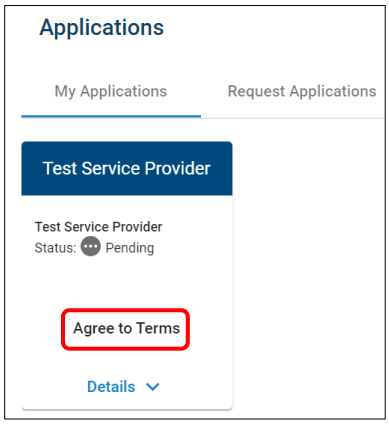
If you are an Application Administrator, and terms and conditions have not been accepted for your designated application, an **Agree to Terms** button displays next to each application.

Application Administrators are only able to accept terms and conditions for applications they administer. FIS Administrators can accept terms and conditions for FIS.

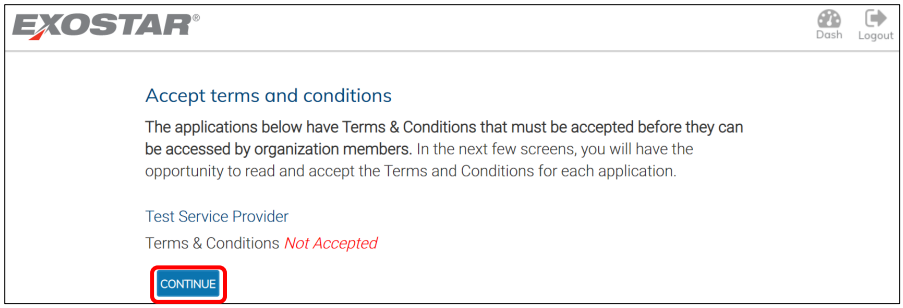
NOTE: Besides the Application Administrator, Organization Administrators and Organization Stewards can accept terms and conditions. Users within your organization are not able to access the application until the **Service Agreement** for the application is accepted.

To accept terms and conditions:

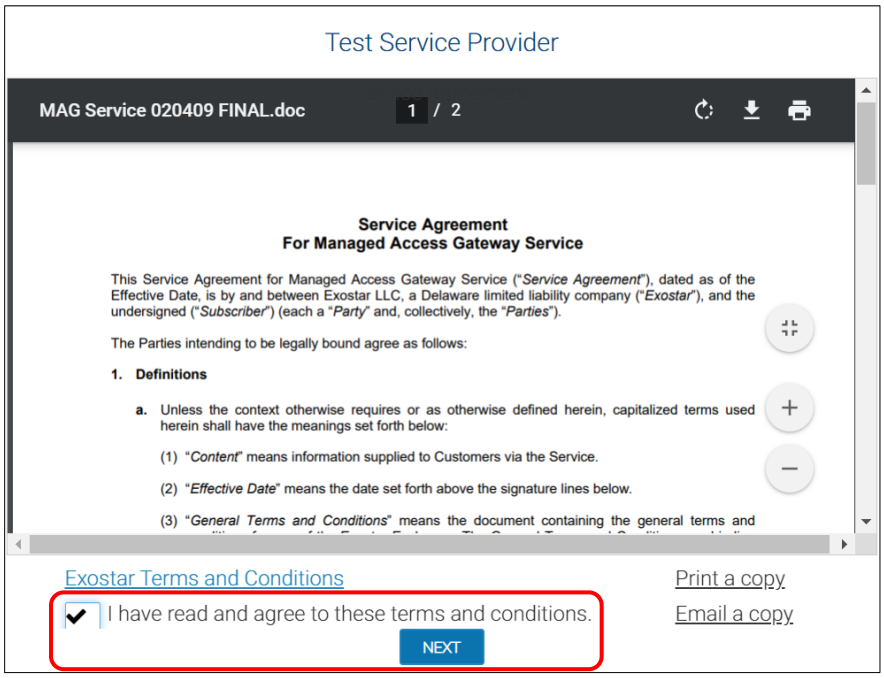
1. Locate the desired Application tile on the MAG Dashboard. Click **Agree to Terms**.



2. Click **Continue**.



3. If accepting, review the **Terms and Conditions**, and check the box for **I have read and agree to these terms and conditions.** Click **Next**.



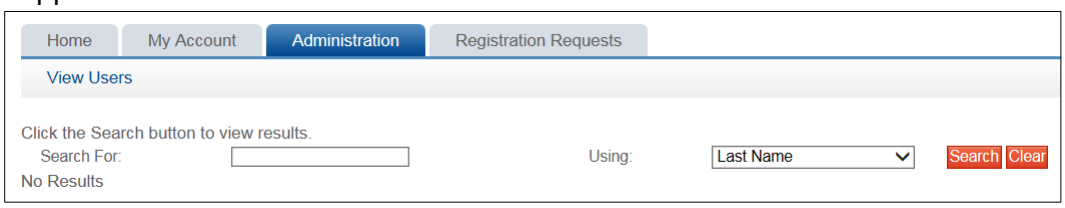
Your organization is now successfully subscribed to the application. Organization and Application Administrators for the application can start subscribing users within their organization to the application. If your organization is a part of a stewardship group, Organization Stewards can also subscribe users to applications. 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 remain in **Pending Acceptance of Terms & Conditions** status.
- Until acceptance occurs, Organization Stewards, Organization and Application Administrators for the application cannot start subscribing users within their organization to the application.
- Users cannot start requesting access to the application.

ADMINISTRATION TAB

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



View Users

The View Users sub-tab allows Administrators to complete user management activities such as request and suspend application access and FIS access for users. If suspending access, comments are required.

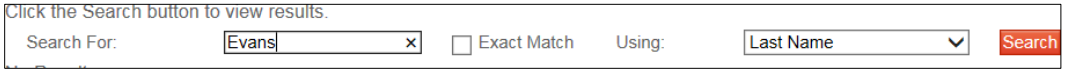
NOTE: If you are an Application Administrator requesting access to an application on behalf of a user, the request does not require manual approval and automatically bypasses Application Administrator approval.

Search

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

To complete a search:

1. Select search type (e.g. View Users or View Organizations).
2. Select search criteria from the drop-down menu and 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

Reference search criteria definition for assistance.

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 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

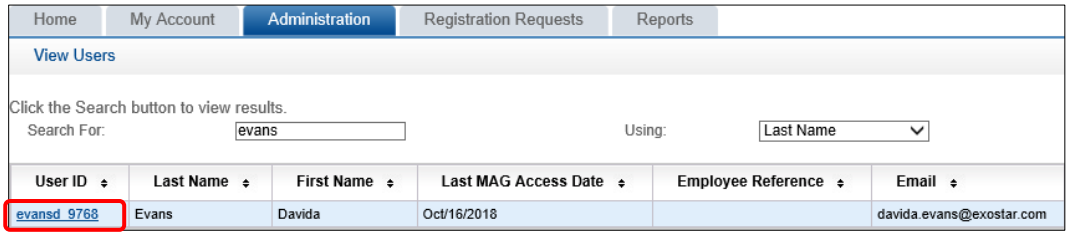
User ID	Unique identifier for the user

Last Name	Last name of user
First Name	First name of user
Last MAG Access Date	Last date user logged into Exostar's MAG account
Email	Email address of user
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 account
Org Name	Name of organization

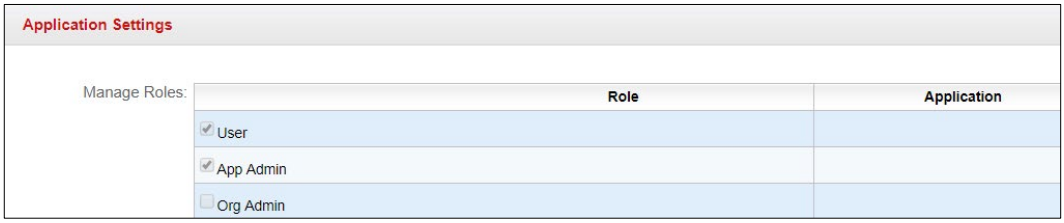
Determine Role

Application and FIS Administrators can determine a user's role by following the steps below:

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



4. Scroll to the **Application Settings** section to view the **Manage Roles** section. The Application field displays applications that the user is an Application Administrator for.

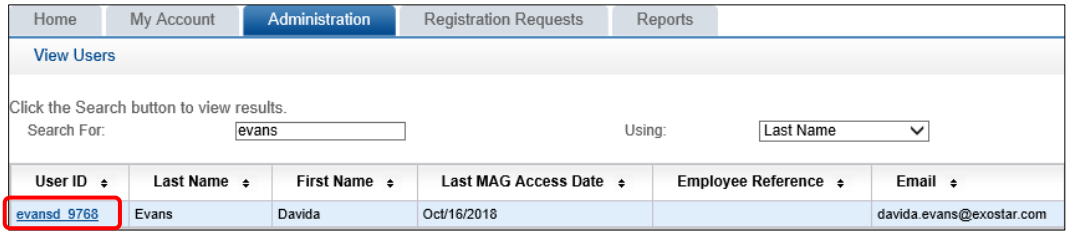


Modify Application Access

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

To modify application access:

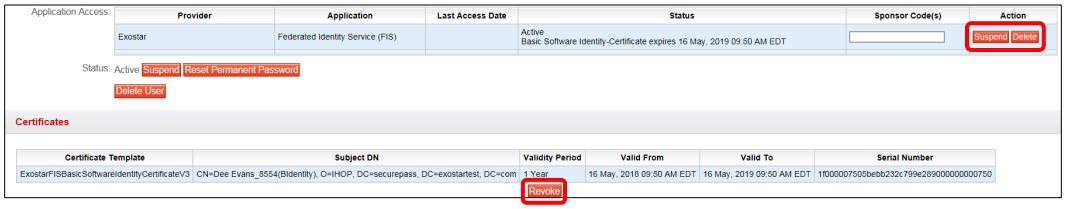
1. Click **View Users**.
2. Use the search filter menu or select **Exact Match** to narrow results. Click **Search**.
3. Click the hyperlinked **User ID.**



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.

   The Delete option removes the ability for you to modify the application. Additionally, application access is deactivated for the user.

   As the FIS Administrator, you can either revoke or suspend certificates. 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 is required to purchase new certificates.

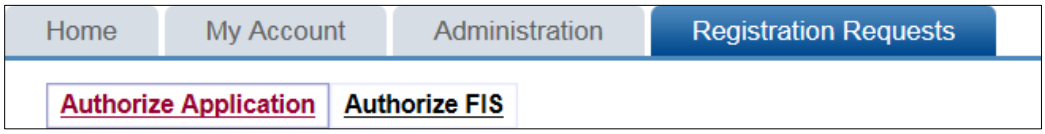


5. The user can request access to the application again from the **Request Applications** tab via the MAG Dashboard.

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

REGISTRATION REQUESTS TAB

Application Administrators administer application requests and FIS Administrators administer FIS requests from the Registration Requests tab.

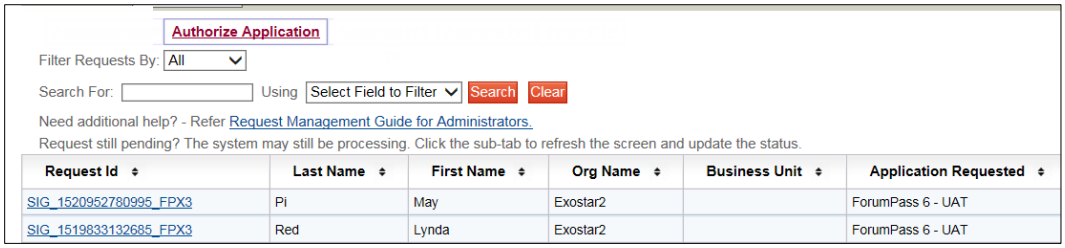


Authorize or Deny Application Access

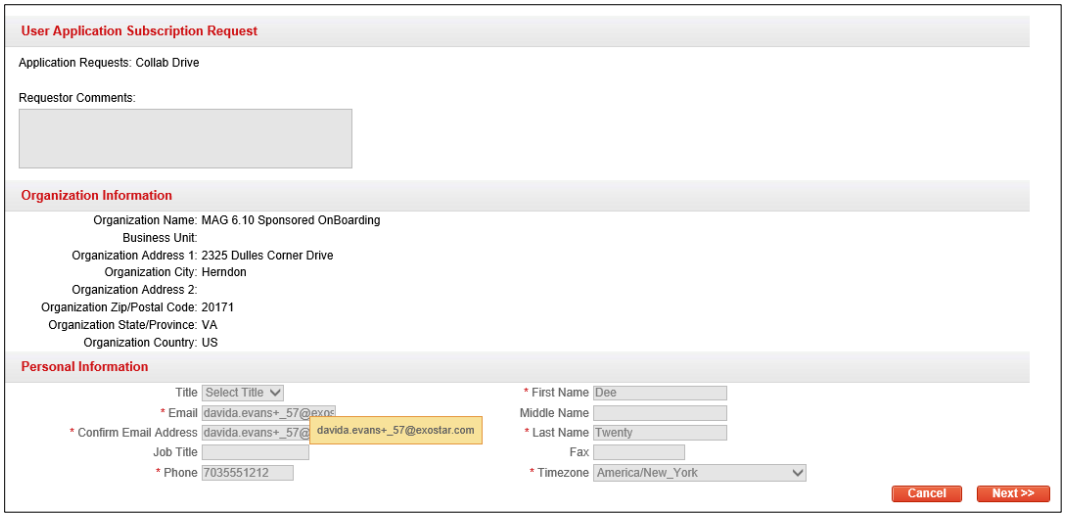
Application Administrators access the **Authorize Application** sub-tab to approve or deny requests individually or in multiples for application access.

To authorize or deny requests individually:

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

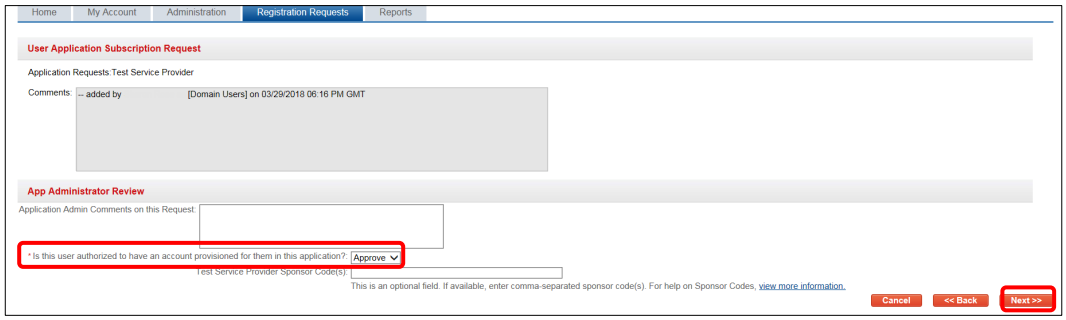


2. If the user requests reactivation of a suspended application, comments display in the **User Application Subscription Request** section. Review the information and click **Next**.



NOTE: To display full email address, hover over email address field with your mouse.

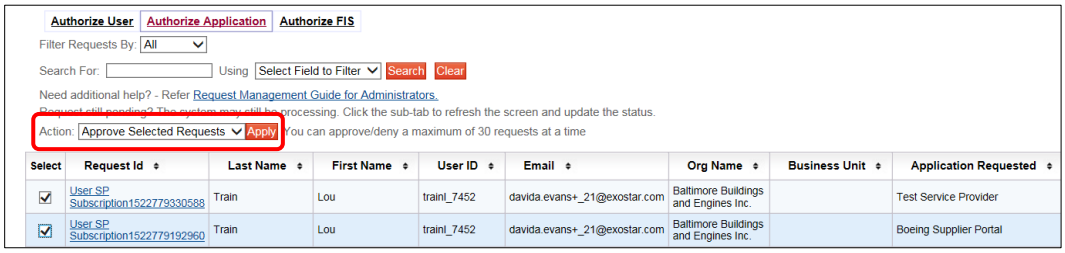
3. Select **Approve** or **Deny** from the drop-down menu. If denying, you must enter a denial comment. Sponsor code is optional. Click **Next**.



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. Select the users you are approving or denying. From the **Action** menu, select **Approve** or **Deny Selected Requests.**
3. Click **Apply**. If denying, denial comments are required.



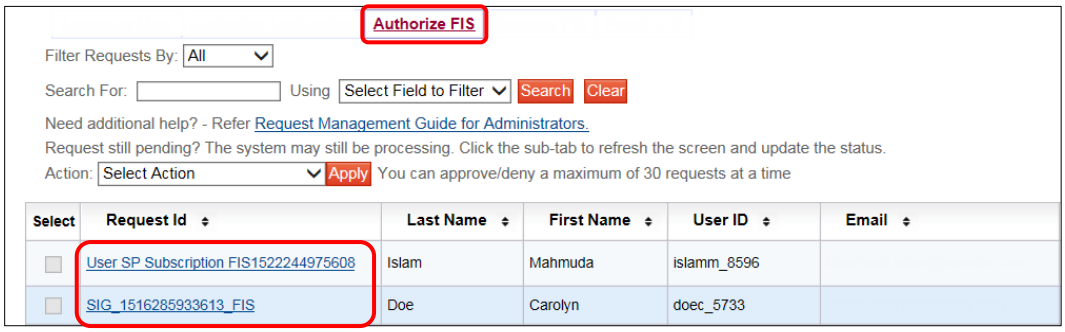
NOTE: If you are the Application Administrator for multiple applications, please ensure you view the **Application Requested** column to verify you apply the appropriate action for the request.

4. 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 or Deny FIS

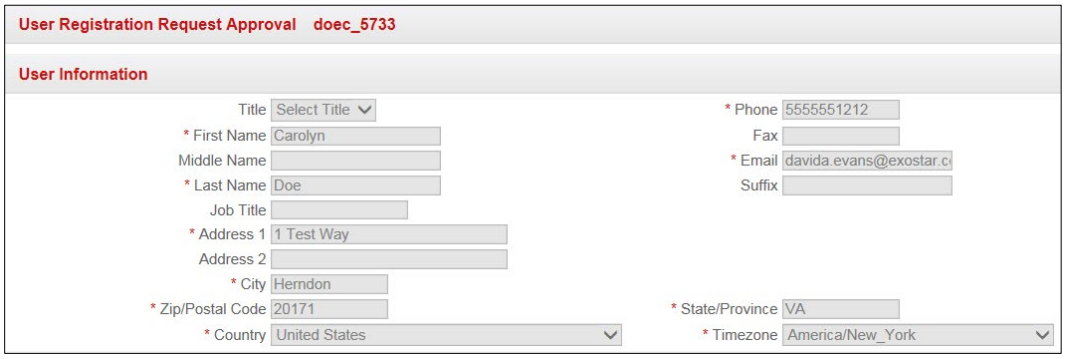
FIS Administrators access the **Authorize FIS** sub-tab to approve or deny requests for FIS. To action an FIS request:

1. Click **Authorize FIS**.
2. Pending requests display. Click the **Request ID**.



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

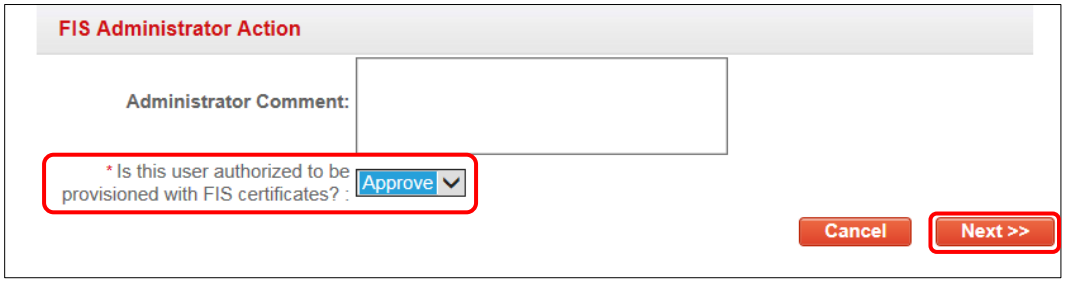
For example, Carolyn Doe is a match for doec_5733. If the request displays a first and last name of Carolyn Doe, but the user ID is smithj_1234, you must deny the request.



NOTE: If the user requested Medium Level of Assurance (MLOA) Digital Certificates, it is important their first and last name match their identity documents. 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.

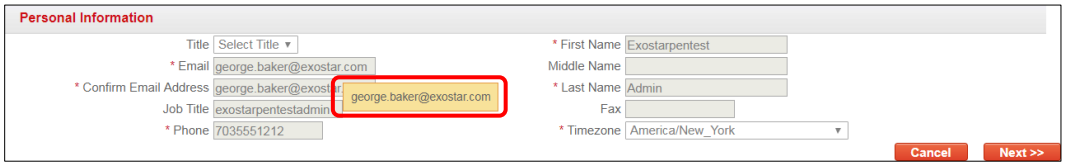
5. From **FIS Administrator Action**, select **Approve** or **Deny.** If denying, you are required to enter comments. Click **Next**.



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.

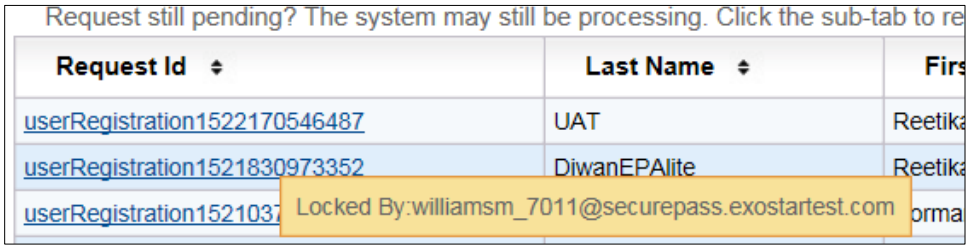
View Complete Email Address

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



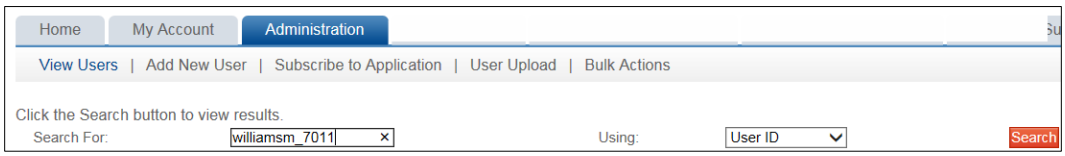
Unable to Approve or Authorize

If the status of a request is **Pending**, you are unable to action because another administrator 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).

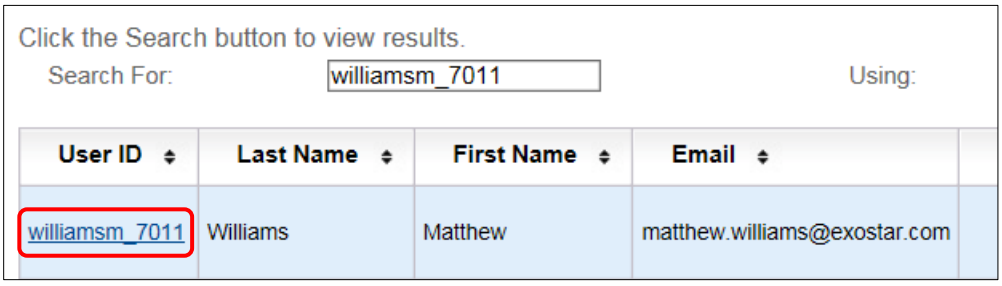


If you are unfamiliar with the user ID of the locked request, to determine who to contact:

1. Go to the **Administration** tab.
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. To unlock a pending request:

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

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). 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	New