

# Managed Access Gateway (MAG) Federated Identity Service Administrator Guide

August 2022



**CONTENTS**

- Document Versions..... 3
- Introduction ..... 4
- Federated Identity Service (FIS) Administrator ..... 4
- Accept Terms & Conditions ..... 4
- Administration Tab ..... 6
  - View Users ..... 6
    - Search ..... 6
    - Search Field Definitions..... 6
    - View User Search Criteria..... 6
    - View User Results Fields..... 7
    - Determine Role ..... 7
    - Modify Application Access ..... 8
- Registration Requests Tab ..... 9
  - Authorize or Deny FIS ..... 9
  - View Complete Email Address..... 10
  - Unlock Pending Requests ..... 12

**DOCUMENT VERSIONS**

<b>Version</b>	<b>Impacts</b>	<b>Date</b>	<b>Owner</b>
IAM FIS Administrator Guide (MAG 6.10)	<ul style="list-style-type: none"><li>• Last MAG Access Date column added when using View Users sub-tab</li></ul>	November 2018	S. Puthanveetil
MAG 6.11	<ul style="list-style-type: none"><li>• Changed the product name from IAM to MAG</li></ul>	April 2019	S. Puthanveetil
MAG 6.14	<ul style="list-style-type: none"><li>• Remove One-Time Password from FTL</li><li>• Update Password Policy</li></ul>	June 2020	B. Nair
MAG 7.0	<ul style="list-style-type: none"><li>• Self-Registration</li><li>• New Organization Adoption Invitation registration process</li><li>• Dashboard</li><li>• Purchasing</li><li>• Credentialing</li><li>• Activation</li><li>• Authentication</li></ul>	February 2021	B. Nair

## INTRODUCTION

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

## 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 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

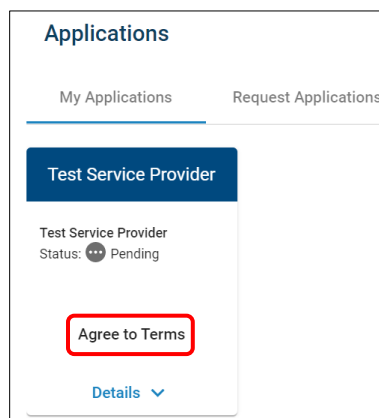
## ACCEPT TERMS & CONDITIONS

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

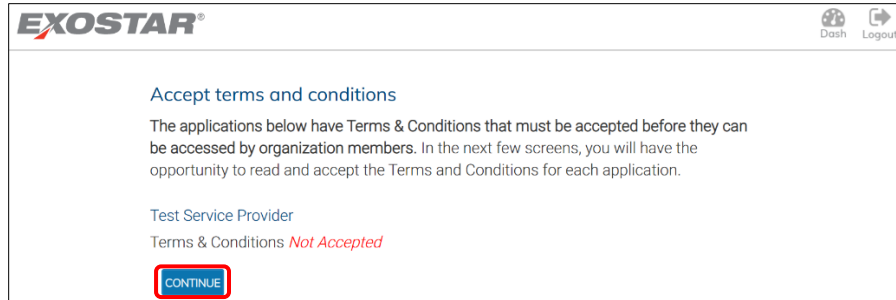
**NOTE:** Users within your organization are not able to access the FIS application until the **Terms & Conditions** are accepted.

**To accept terms and conditions:**

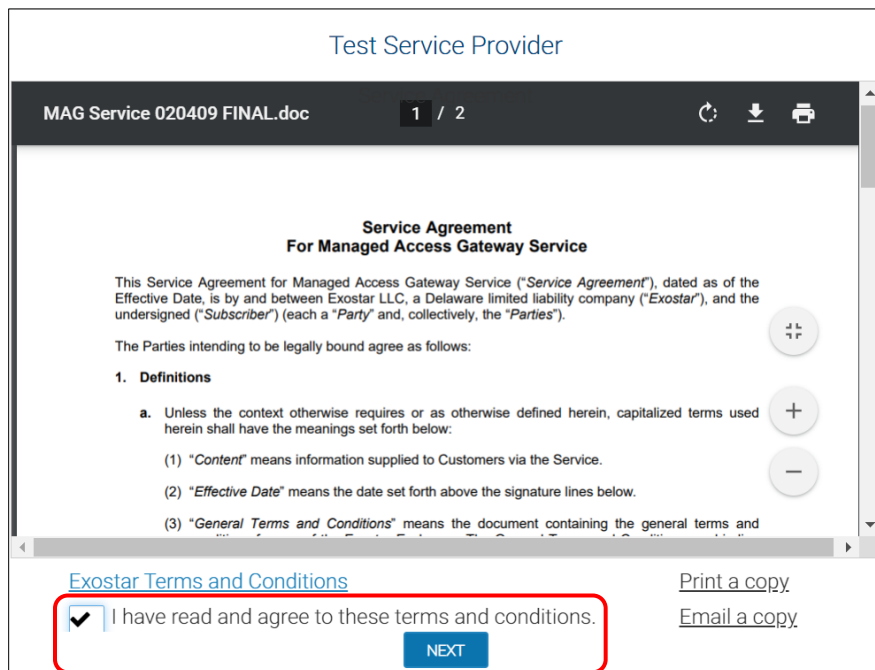
1. Locate the FIS Application tile on the MAG Dashboard. Click **Agree to Terms**.



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. The FIS Administrator can start subscribing users within their organization to the FIS application. Users also can start requesting access to the FIS 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, FIS Administrator's cannot start subscribing users within their organization to the FIS application.
- Users cannot start requesting access to the FIS application.

## ADMINISTRATION TAB

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.

### Search

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

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 will 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

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.

The screenshot shows the 'Administration' tab selected in a navigation menu. Below the menu, there is a 'View Users' section with a search bar containing 'evans' and a dropdown menu set to 'Last Name'. Below the search bar, a table displays search results. The first result is highlighted with a red box around the User ID 'evansd\_9768'.

User ID	Last Name	First Name	Last MAG Access Date	Employee Reference	Email
evansd_9768	Evans	Davida	Oct/16/2018		davida.evans@exostar.com

4. Scroll to the **Application Settings** section to view the **Manage Roles** section. The Application field displays only for the FIS application.

Application Settings		
Manage Roles:	Role	Application
<input checked="" type="checkbox"/>	User	
<input checked="" type="checkbox"/>	App Admin	
<input type="checkbox"/>	Org Admin	

## Modify Application Access

FIS Administrators can only modify FIS application 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**.

Home	My Account	Administration	Registration Requests	Reports	
View Users					
Click the Search button to view results.					
Search For:		evans	Using: Last Name		
User ID	Last Name	First Name	Last MAG Access Date	Employee Reference	Email
evansd_9768	Evans	Davida	Oct/16/2018		davida.evans@exostar.com

4. Scroll to **Application Settings**. Locate the FIS 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.

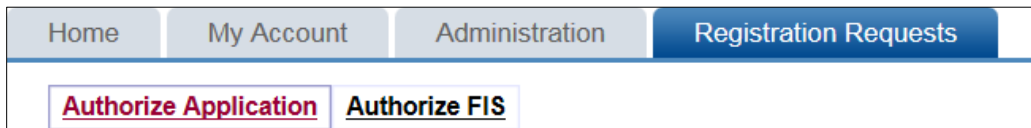
Application Access:	Provider	Application	Last Access Date	Status	Sponsor Code(s)	Action
	Exostar	Federated Identity Service (FIS)		Active Basic Software Identity-Certificate expires 16 May, 2019 09:50 AM EDT		Suspend Details
Status: Active <a href="#">Suspend</a> <a href="#">Reset Permanent Password</a>						
<a href="#">Delete User</a>						
Certificates						
Certificate Template	Subject DN	Validity Period	Valid From	Valid To	Serial Number	
ExostarFISBasicSoftwareIdentityCertificateV3	CN=Dee Evans_8554(Bidentity), O=IHOP, DC=securepass, DC=exostartest, DC=com	1 Year	16 May, 2018 09:50 AM EDT	16 May, 2019 09:50 AM EDT	110000075055ebb232c799e289000000000750	Revoke



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

## REGISTRATION REQUESTS TAB

FIS Administrators can administer FIS requests from the Registration Requests tab.



### Authorize or Deny FIS

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

- Click **Authorize FIS**.
- Pending requests display. Click the **Request ID**.

The screenshot shows the FIS registration requests interface. At the top right, there is a red-bordered button labeled 'Authorize FIS'. Below it, there is a filter section with a dropdown menu set to 'All', a search bar, and buttons for 'Search' and 'Clear'. A message below the search bar reads: 'Need additional help? - Refer [Request Management Guide for Administrators](#). Request still pending? The system may still be processing. Click the sub-tab to refresh the screen and update the status.' Below this is an action section with a dropdown menu set to 'Apply' and a note: 'You can approve/deny a maximum of 30 requests at a time'. The main part of the interface is a table with the following data:

Select	Request Id	Last Name	First Name	User ID	Email
<input type="checkbox"/>	<a href="#">User SP Subscription FIS1522244975608</a>	Islam	Mahmuda	islam_8596	
<input type="checkbox"/>	<a href="#">SIG_1516285933613_FIS</a>	Doe	Carolyn	doec_5733	

- 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.

**User Registration Request Approval** doec\_5733

**User Information**

Title	Select Title ▾	* Phone	5555551212
* First Name	Carolyn	Fax	
Middle Name		* Email	davida.evans@exostar.c
* Last Name	Doe	Suffix	
Job Title			
* Address 1	1 Test Way		
Address 2			
* City	Herndon		
* Zip/Postal Code	20171	* State/Province	VA
* Country	United States ▾	* Timezone	America/New_York ▾

**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**.

**FIS Administrator Action**

Administrator Comment:

\* Is this user authorized to be provisioned with FIS certificates?: Approve ▾

Cancel
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 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.

**Personal Information**

Title: Select Title ▾

\* Email:

\* Confirm Email Address:

Job Title:

\* Phone:

\* First Name:

Middle Name:

\* Last Name:

Fax:

\* Timezone:

### 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).

Request still pending? The system may still be processing. Click the sub-tab to re

Request Id ↕	Last Name ↕	Firs
<a href="#">userRegistration1522170546487</a>	UAT	Reetika
<a href="#">userRegistration1521830973352</a>	DiwanEPAlite	Reetika
<a href="#">userRegistration1521037</a>	Locked By:williamsm_7011@securepass.exostartest.com	

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**.

Home | My Account | **Administration**

[View Users](#) | [Add New User](#) | [Subscribe to Application](#) | [User Upload](#) | [Bulk Actions](#)

Click the Search button to view results.

Search For:  x

Using:  ▾

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

Click the Search button to view results.

Search For:  Using:

User ID ↕	Last Name ↕	First Name ↕	Email ↕
<a href="#">williamsm_7011</a>	Williams	Matthew	matthew.williams@exostar.com

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.

Request Id ↕	Last Name ↕	First Name ↕	Org Name ↕	Status ↕
<a href="#">userRegistration1521830973352</a>	DiwanEPAlite	Reetika	Exostar2	New
<a href="#">userRegistration1521037320799</a>	Star	Norman	Exostar2	Pending

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

Request Id ↕	Last Name ↕	First Name ↕	Org Name ↕	Status ↕
<a href="#">userRegistration1521830973352</a>	DiwanEPAlite	Reetika	Exostar2	New
<a href="#">userRegistration1521037320799</a>	Star	Norman	Exostar2	New