FIS Administrator Responsibilities

Page Contents

Jump to...

- FIS Overview
- FIS Get Started
- FIS Register
- FIS Self-Help

S Administrator Responsibilities

e

This page provides step-by-step instructions on basic FIS Administrator responsibilities.

Action FIS Requests

Step 1. Log into Exostar's Managed Access Gateway (MAG).

Step 2. Click the **Registration Requests** tab.

Step 3. Click **Authorize FIS** to redirect to the **FIS Requests** queue.

Step 4. Filter/sort the requests by clicking the drop-down menus and column headers.

Step 5. Click the hyplerlinked **Request I**D for the request you want to process.

Step 6. Review user information and modify if required. Review the certificate attributes and if any fields have **Unknown**, review and select appropriate option. Add any comments you may want to add. If denying the request, you are required to enter the denial comments.

Step 7. Click **Approve** or **Deny**.

A confirmation screen displays.

> **NOTE:** Depending on your Organization’s subscriptions, you may be prompted to approve a user for Basic Level of Assurance (BLOA) or Medium Level of Assurance (MLOA). Please note MLOA certificates require the user to complete an in-person identity proofing appointment.

Request/Prepare Employment Verification Letter

The employment verification letter must be signed by the FIS Administrator or an authorized signatory within the organization, and provided to the user for their in-person proofing appointment.

Step 1. Log into MAG and follow the steps above to approve the user's FIS registration request.

Step 2. Request or prepare an employment verification letter.

Step 3. Sign the employment verification letter (the FIS Administrator's signature must be on the letter).

Step 4. Provide the letter to the user prior to the scheduled identity vetting appointment.

Step 5. Inform the user they must present this letter to the authorized individual facilitating the identity proofing.

> **NOTES**:
>
> - The employment verification letter is a crucial component to the successful completion of the identity proofing of the user. Failure on the part of the user to provide this letter results in failed identity vetting. Users are required to re-appear for their identity vetting appointment. This could incur an additional cost.
> - The employment verification letter should be printed on corporate letterhead, provide the applicant’s full name, employee number, assert the applicant’s affiliation with the organization, and be duly signed by the FIS Administrator/authorized signatory.

View User's Certificates

Step 1. Log into MAG.

Step 2. Click the **Administration** tab.

Step 3. Enter search criteria, or leave blank for all, and click **Search**.

Step 4. Review search results and change the number of results per page using the drop-down.

Step 5. Sort by a column (ascending or descending) by clicking the column header.

> **NOTE:** As an FIS Administrator, you can only view and not change a user’s profile information.

Revoke User's Certificates

FIS Administrators can revoke certificates for users within their organization. Once certificates are revoked, they can no longer be used. New certificates require purchase.

Step 1. Log into your MAG account.

Step 2. Go to the **Administration** tab, then click **View Users**.

Step 3. Complete user search.

Step 4. From results, click on the hyperlinked **User ID**.

Step 5. Scroll to the **Certificates** section. Click **Revoke**.

Step 6. Select the certificates you are revoking. You are required to select a revocation reason and enter comments. Click **Submit**.

Step 7. You receive a **Certificate Revocation Request** form. Click **Sign**.

Step 8. A signing page displays. Enter your MAG password in the **Passcode** field. Click **Sign**.

Step 9. Click **Done** (located in the lower, right corner of the page).

NOTES:

- Users can revoke their own certificates at any time.
- You should revoke a user’s certificates if you believe the security of those certificates have been compromised in any way.
- You should revoke a user’s certificates if they are no longer employed with your organization.
- Revocation of certificates is a permanent action. i.e., there is no way to recover those certificates and the user must reapply should they need those certificates.

How useful was this content?

Your Rating: Results: 5 rates