

Identity and Access Management Platform (MAG)

Overview

Exostar's Identity and Access Management Platform (formerly known as MAG) is a secure identity and access management cloud service for the Aerospace Defense industries. With the Exostar IAM Platform, organizations enjoy benefits like account management, web-based single sign-on user access and a single place to connect to buyer partner applications they are doing business with.

Exostar's IAM Platform is the part-ner of choice for highly regulated industries who have not yet im-plemented federation technolo-gies. The cloud-based platform promotes quicker and more ef-fective collaboration, while main-taining a secure and compliant atmosphere.

Quick Reference

For more detailed information by topic, select from the buttons below to access the applicable content.



Get Started



Invite



Register/Activate



Purchase, Renew
& Pay



Learn

Workflow



Benefits

The Exostar IAM Platform reduces the time, expense, and exposure of establishing and maintaining external user accounts. It allows application owners to connect once and provide access to all validated external parties and users. Many of your business partners are likely already part of our large user community of Aerospace & Defense partners/suppliers with Exostar IAM Platform (A&D) credentials—so you will be able to do business faster.

Key Features

- Cloud-based, turnkey solution
- Manages internal and external users
- Enforces strong authentication policies to verify users
- Meets compliance regulations
- Provides simple and secure access to applications and data
- Streamlines communication
- Supports our large user community
- Reduces cost of credential users
- Supports multiple platforms, including mobile (iOS App and/or native mobile browser)

Roles and Responsibilities

Adoption Administrator: Adoption Administrators are responsible for inviting external companies, as well as external or internal users to Exostar's IAM Platform (MAG) and allows companies and users to be subscribed to applications.

Application and FIS Administrator: Application Administrators are 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 application they administer.

- Application Administrator additional responsibilities include:
 - Accept terms and conditions.
 - Request access on behalf of users.
 - Suspend application access.
- FIS Administrator additional responsibilities include:
 - Accept terms and conditions for FIS.
 - Request access on behalf of users to FIS.
 - Suspend access to FIS.

Organization Administrator: Organization Administrators are 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.

- Organization Administrator responsibilities include:
 - Accept terms and conditions for applications the organization is subscribed.
 - 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.

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 organization is subscribed.

Service Provider Administrator: The Service Provider Administrator role allows an application's Service Provider to administer access to the application. With this role, partner companies that have applications within Exostar's IAM Platform (MAG) that require SP Administrator action can approve, deny or suspend application access.

User: The User role does not have any administrative privileges.

System Requirements

Supported Operating Systems: Windows 7, Windows 8.1, Windows 10, and MAC

Supported Browsers: IE 8, IE 10, and IE 11

Browsers Supported with Limitation*: Edge, FireFox, Safari, and Chrome

***Limitation:** (PKI) Digital Certificate Credential cannot be downloaded.