Managed Access Gateway (MAG) Overview

Page Contents

Jump to...

anaged Access Gateway (MAG) Overview

e

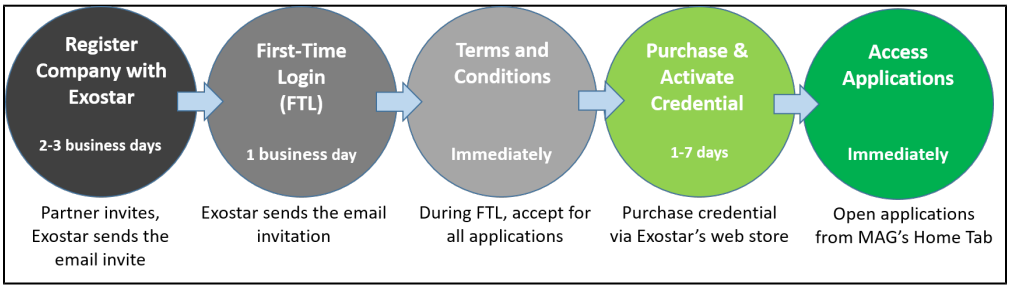
Overview

Exostar's Managed Access Gateway (MAG) is a secure identity and access management cloud service for the Aerospace & Defense industries. With MAG, organizations enjoy benefits like account management, web-based single sign-on user access, and a single place to connect to partner applications.

MAG is the partner of choice for highly regulated industries that have not yet implemented federation technologies. The cloud-based platform promotes quicker and more effective collaboration, while maintaining a secure and compliant atmosphere.

Click the arrows below to read further about the benefits of MAG, administrative roles available to users, and system requirements.

The chart below offers the overview of steps required to set up your company's secure MAG account. Please select image to enlarge:



Exostar's Managed Access Gateway (MAG) reduces the time and expense 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 MAG (A&D) credentials, so you will be able to do business faster. Exostar's MAG Platform will ensure that you have all necessary tools for secure and intelligent collaboration. With MAG, your company will enjoy the following benefits:

- A cloud-based, turnkey solution
- Ability to easily manage internal and external application users
- Strong authentication procedures for verifying user identities
- Simple and secure access to applications and data
- Streamlined communication across company divides
- Ability to protect collaborative spaces with additional security credentials
- Compliant with security regulations
- Desktop and mobile access

MAG users may be assigned administrative roles to help manage their company's MAG profile and access to applications and services. Read the synopsis of each role's duties and responsibilities. For further guidance, refer to our MAG Admin Resources page.

Adoption Administrator: Adoption Administrators are responsible for inviting external companies to MAG. They can also subscribe companies 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 MAG that require SP Administrator action can approve, deny or suspend application access.

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

Supported Operating Systems: Windows 8.1, Windows 10, and MAC
Supported Browsers: IE 11
Browsers Supported with Limitation*: Edge, FireFox, Safari, and Chrome

***Limitation**: (PKI) Digital Certificate Credential cannot be downloaded
How useful was this content?

Your Rating: Results: 80 rates

News and Announcements

- **MAG 6.15 Release**
- **MAG Webinars**