

MAG Application Access FAQs

Page Contents

- [Page Contents](#)
- [Jump to...](#)
- [Application not Accessible](#)
- [Activate Your Credential](#)
- [Credentials by Partner and Application](#)
- [Purchase a Stronger Credential](#)
- [Renew Expired Credential](#)
- [Log in with Credential](#)
- [Download the FIS MLOA Certificates](#)
- [Application Statuses](#)

Jump to...

- [MAG Overview](#)
- [MAG Get Started](#)
- [MAG Credentialing](#)
- [MAG Purchase, Renew & Pay](#)
- [MAG Billing and Support](#)
- [MAG FAQs and Troubleshooting Tips](#)
- [MAG Self-Help](#)

AG Application Access FAQs

e

Application not Accessible

If you are logged into your MAG account, but cannot access certain partner applications, it might be due to these common issues:



- You need to [activate your credential](#).
- You need a [stronger credential](#).
- Your [credential has expired](#).
- You need to [log into MAG with your credential](#).
- You still need to download the [FIS MLOA certificates](#).

Review the sections below to learn how to troubleshoot common access issues. Please see the [Credentials by Partner and Application](#) matrix to review acceptable credentials. For additional credentialing information, including purchase information, please visit the [MAG Credentialing FAQs](#) page.

ForumPass Defense customers: If you received a notice regarding account suspension due to inactivity, please click [here](#).

Activate Your Credential

How can I activate my credential?

You might not be able to access your partner application because your credential needs to be activated. Specifically, this applies to such credentials as [Phone OTP](#), [OTP Hardware Token](#), and [Exostar Mobile ID](#). Activation ensures your credential is attached to a specific MAG account. To activate your purchased credential:

Step 1. Log into your MAG account. In the **My 2FA Credentials** section, click the **Have a license key?** option.

Step 2. Click the link **Enter it here** link.

Step 3. Enter your **License key** and proceed to registration.

NOTE: If you purchased a Hardware Token, please begin the activation process after you receive the token in mail.

Credentials by Partner and Application

How do I know what credential to purchase?

The credential type is dependent upon the security requirements for the application you are accessing. Please review the table below, and if you cannot find the information or need additional assistance, please contact Exostar Customer Support or the representative of your partner organization.

Application/Customer Name	Acceptable Credentials
BAE Systems Board Portal	Inviter Specified
BAE Systems Portal	Email or User ID and Password + Phone OTP with proofing Email or User ID and Password + Hardware OTP Token with proofing Email or User ID and Password + Exostar Mobile ID with Proofing Email or User ID and Password + FIS MLOA Hardware Certificates DoD CAC NGC OneBadge Boeing SecureBadge Enterprise Access Gateway (EAG) – Level 3 or above NASA PIV Cards

<p>BAES UK Maritime Naval Ships Windchill Project</p>	<p>Email or User ID and Password + Phone OTP with or without Proofing</p> <p>Email or User ID and Password + Hardware OTP Token</p> <p>Email or User ID and Password + Exostar Mobile ID</p> <p>Email or User ID and Password + FIS MLOA Software or Hardware Certificates</p>
<p>Boeing Supplier Portal</p>	<p>Email or User ID and Password + Hardware OTP Token with Proofing</p> <p>Email or User ID and Password + FIS MLOA Hardware Certificates</p> <p>Enterprise Access Gateway (EAG)</p> <p>NGC OneBadge</p>
<p>Boeing SCP</p>	<p>Hardware OTP Token with Proofing</p>
<p>Boeing 787 SCMP</p>	<p>Hardware OTP Token with Proofing</p>
<p>Partner Information Manager (PIM)</p>	<p>Email or User ID and Password + Phone OTP Without Proofing</p> <p>Email or User ID and Password + Hardware OTP Token or Authy</p> <p>Email or User ID and Password + FIS MLOA Hardware Certificates</p> <p>Enterprise Access Gateway (EAG) or RIDP Users</p>
<p>Information Manager - HII</p>	<p>Email or User ID and Password + FIS MLOA Hardware Certificates</p> <p>DOD CAC</p> <p>NGC OneBadge</p>
<p>Lockheed Martin Aeronautical</p> <p>Aero JTD</p> <p>CSAS Web F-16</p> <p>EDCS Airlift</p> <p>EDCS F-16</p> <p>EDCS Palmdale</p> <p>F-22 Fleet Management Tool</p> <p>LM AeroSource F-35 Production</p> <p>Lockheed Martin OneAero</p> <p>Online Account Request System (OARS)</p> <p>Transportation Management System</p> <p>User Acceptance LM AeroSource</p>	<p>Email or User ID and Password + FIS Basic Certificates OR</p> <p>Email or User ID and Password + Hardware OTP Token</p> <p>Email or User ID and Password + FIS MLOA Software Certificates</p> <p>Email or User ID and Password + FIS MLOA Hardware Certificates</p> <p>Enterprise Access Gateway (EAG)</p> <p>NGC OneBadge</p>
<p>Lockheed Martin Procure to Pay (LMP2P)</p>	<p>Email or User ID and Password + Phone OTP with Proofing</p> <p>Email or User ID and Password + Exostar Mobile ID with Proofing</p> <p>Email or User ID and Password + Hardware OTP Token with Proofing</p> <p>Enterprise Access Gateway (EAG)</p> <p>Email or User ID and Password + FIS MLOA Hardware Certificates</p>
<p>ProcurePass Buysite (BAE Systems)</p>	<p>Email or User ID and Password</p>
<p>Raytheon Supplier Portal</p> <p>Raytheon SecureForms</p> <p>Raytheon Supply Chain Platform (RSCP)</p>	<p>Email or User ID and Password + Phone OTP with Proofing</p> <p>Email or User ID and Password + Hardware OTP Token with Proofing</p> <p>Enterprise Access Gateway (EAG)</p> <p>Email or User ID and Password + FIS MLOA Hardware Certificates</p>

Rolls-Royce Global Supplier Portal	<p>Either of the following credentials are acceptable depending upon the application you need to access within GSP:</p> <p>Email or User ID and Password + FIS Basic Certificates OR</p> <p>Email or User ID and Password + FIS MLOA Software Certificates</p> <p>Email or User ID and Password + FIS MLOA Hardware Certificates</p> <p>Enterprise Access Gateway (EAG)</p> <p>NGC OneBadge</p>
Supply Chain Platform - BAE Systems	<p>Email or User ID and Password + Phone OTP with Proofing</p> <p>Email or User ID and Password + Hardware OTP Token with Proofing</p> <p>Email or User ID and Password + Exostar Mobile ID with Proofing</p> <p>Email or User ID and Password + FIS MLOA Hardware Certificates</p> <p>DoD CAC</p> <p>Enterprise Access Gateway (EAG) – Level 3 or above</p>
Supply Chain Platform - NNS	<p>Email or User ID and Password + FIS MLOA Hardware Certificates</p> <p>DOD CAC</p> <p>NGC OneBadge</p>

Purchase a Stronger Credential

How do I purchase or upgrade my current credential?

If you cannot access your application, double-check with your partner to see what kind of credential they require to access the specific application. If you need a stronger credential or an upgrade to your current credential in the form of Identity Proofing, follow the steps below to complete your purchase:

Step 1. Log into your MAG account, and navigate to the **My Account** tab.

Step 2. Click the **Manage OTP** tab, and select the purchasing option that addresses your credentialing situation. Scroll down and use the available buttons to either purchase a new credential, or add the proofing upgrade to your active credential.

Alternatively, you can also access Exostar's Web store by clicking the **Billing and Support** link, located in the bottom your MAG Home tab. Locate the desired credential, and follow the prompts to complete your purchase. We suggest using this option if the buttons under the Manage OTP sub-tab are temporarily unavailable.

Renew Expired Credential

How can I renew my expired credential?

If your credential is expired, please follow these steps to complete your credential renewal:

Step 1. Log into your MAG account, and click **Billing and Support** located in the bottom section of the Home tab.

Step 2. To renew expired credentials, click **Subscription Renewals** from the blue banner (top of page).

Step 3. Select the product from the drop-down menu, and select **Available Renewals**. Click **Add to Cart**. Follow the prompts to complete your renewal.

Log in with Credential

How do I ensure I am logged into MAG with my credential?

Step 1. From the Dashboard, click **Launch** from the application card or you may click on **Elevate Credential Strength** (green button) in the **My 2FA Credentials** section.

Step 2. The **Two-Step Verification** page displays with a list of 2FA credentials associated with your account.

Step 3. Select one of the methods and proceed with the authentication process.

Step 4. After you return to your MAG Dashboard, your credential strength updates and you should be able to open your application.

Download the FIS MLOA Certificates

How do I download and log in with my FIS MLOA certificates?

If you purchased, but forgot to download the FIS MLOA Hardware Digital Certificates, you won't be able to access the applications that require this certificate for access. Click [here](#) for instructions on how to complete the download, and then complete the steps below:

Step 1. If you are not automatically prompted to select your FIS MLOA Hardware certificates during login to MAG, close your browser and navigate to <https://portal.exostar.com>.

Step 2. Plug the FIS Hardware Token into your computer.

Step 3. Select the certificates option from the login screen.

Step 4. When the certificate prompt displays, select the certificate and click **OK**.

Step 5. Enter your token password.

NOTE: If you forget this password, you must go through the proofing process again, as this password cannot be reset.

Step 6. Verify you successfully logged in with your credential. The credential strength can be viewed in the **My 2FA Credentials** section on your Home tab. The credential strength field should display **Medium Hardware Cert**.

Application Statuses

I see that applications in my MAG account have different statuses. What do these statuses mean, and what should I do if some applications do not say "active"?

You can view the status of your applications from the **Dashboard** (home) tab (under the **My Applications** section) of your MAG account. Unless you see **Launch** under the application you want to use, you might need to wait or to reach out for help to Exostar Customer Support. Review the table below to see what each status means, and what action is required.

Exostar Application Status	User Action
Active	Click Launch to launch the application in a separate browser window.
Organization Registration Approval Pending	None
Pending Account Creation by the Application	If the application has been in this status for more than 24 hours, contact Exostar Customer Support .
Pending Approval by the Application Owner	If application has been in this status for more than 48 hours, contact Exostar Customer Support .
Pending Application Administrator Approval	Contact your Application Administrator for the application.
Pending Activation	Contact your Application Administrator for the SCP application.
Pending Acceptance of Terms & Conditions	Contact your Organization Administrator.
Inactive	If you need access to the application, click Request Access next to the inactive status. Your request transitions to Pending Application Administrator Approval .
Suspended	Click Reactivate Application . If you do not see Reactivate Application, work with your organization's Application Administrator for the suspended application.
Pending Exostar Approval	If application has been in this status for more than 48 hours, contact Exostar Customer Support .
Pending Proofing	Contact Exostar Customer Support for information if you completed your in-person proofing. This status applies only to MAG users who are awaiting proofing for FIS Medium Level of Assurance (MLOA) Certificates.

Questions? If you use an OTP credential, explore our library of [OTP FAQs](#).

How useful was this content?

Your Rating:

Results:

138 rates