What do I need to access password protected areas of OASIS?

In addition to a Northrop Grumman issued OASIS User ID and password, all users who access password-controlled information will be required to hold a Medium Level of Assurance (MLOA) hardware digital certificate.

There are several types of (MLOA) hardware digital certificates. The majority of OASIS users will be using MLOA certificates issued by Exostar. We also accept US Government issued CAC (Common Access Card), certificates issued to some Tier 1 suppliers, as well as IdenTrust, and WidePoint ORC certificates.

If you don't have a Northrop Grumman OASIS User ID/password please contact your Northrop Grumman buyer to sponsor an access request.

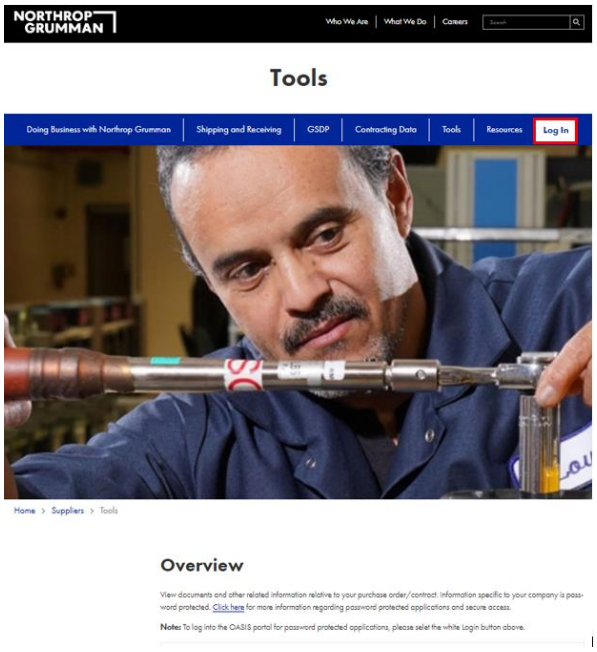
When will I know whether or not I will need to use my digital hardware certificate?

You will need to use the Exostar USB token when logging into the OASIS Portal. You must have an account with User ID and password to log into the portal. Contact your Northrop Grumman buyer for assistance with setting up an account if you do not already have one.

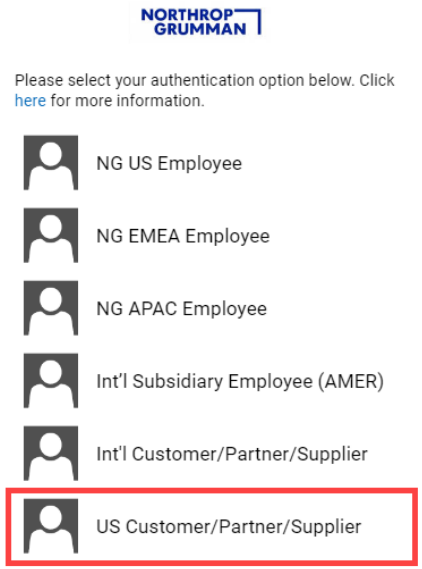
How do I login to the OASIS Portal?

Go to this link to log in using your authentication certificate: [Tools - Northrop Grumman]

1. Click "Log In"



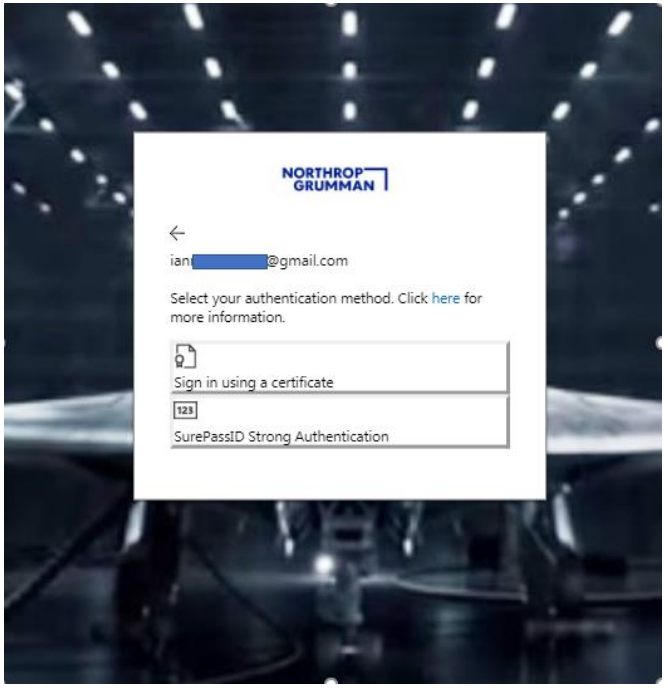
2. Select "US Customer/Partner/Supplier"



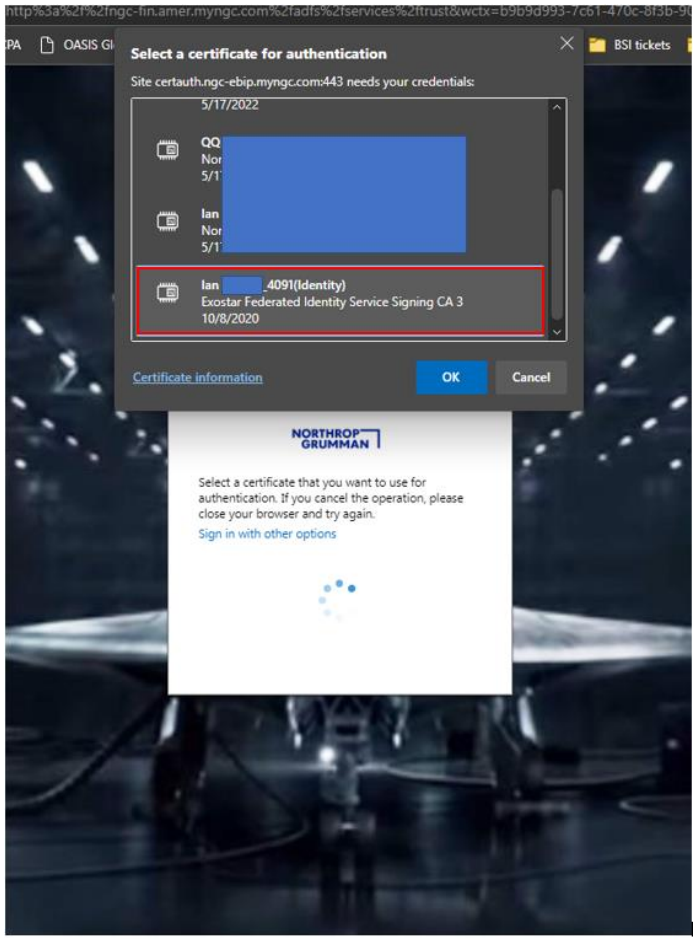
3. Enter your work email address and click “Next”

4. Select “Sign in using a certificate” if you are using an Exostar, CAC card, IdenTrust, WidePoint ORC, or similar certificate

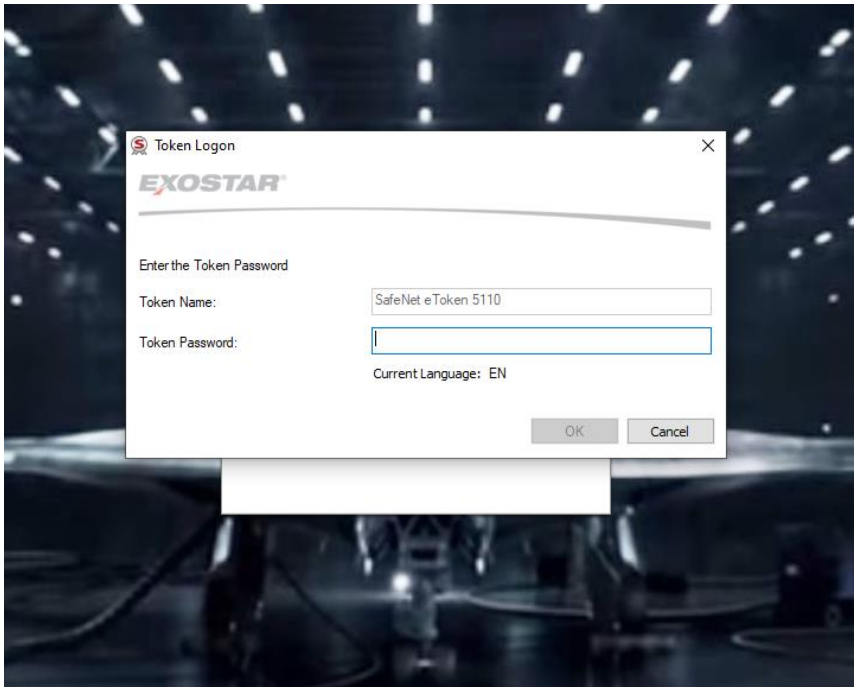
   Select “SurePassID Strong Authentication” if you are logging in using SurePass



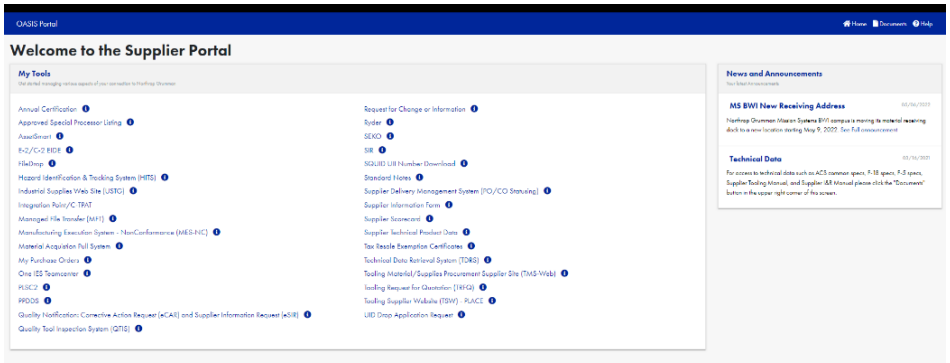
5. Select the Exostar or similar certificate and click “OK”
   In this example, we will use an Exostar certificate



6. Enter the Exostar token password and click “OK”



7. You should now be in the OASIS portal



How do I purchase an Exostar (MLOA) digital hardware certificate?
You may purchase the (MLOA) digital hardware certificate from Northrop Grumman's partner, Exostar, at the following link: Northrop Grumman Get Started - myexostar.com.

If you decide to buy the (MLOA) digital hardware certificate, please read all information and follow the directions on the Exostar website to complete a purchase.

What do I do after purchasing the (MLOA) digital hardware Certificate from Exostar?
After you have purchased the (MLOA) digital hardware certificate, you will be contacted by an Exostar representative via email.

1. You will be asked to verify that your computer system is compliant with the Exostar Dual Factor Authentication requirements.
2. The National Notary Association (NNA) sends an email to the individual (user) who purchased the digital hardware certificate to schedule a proofing appointment (in-person identity verification process). User brings all required documentation to the appointment and completes the in-person proofing.
3. Exostar mails the user a USB drive along with certificate download instructions.
4. User installs the required software to activate the USB drive (as applicable).
5. User logs on to Exostar's website to download the digital certificate onto their USB drive – **must be done within 30 days of the in-person proofing appointment**.
6. Once you've completed the process outlined above, you will contact your NGC OASIS point of contact for next steps.

What if I forgot my Exostar pin/password number?
It is very important that you do not forget the pin/password number for your Exostar digital hardware certificate. The pin/password cannot be reset. Exostar will reissue your digital hardware certificate for a fee. Contact Exostar's Customer Service at +1 703-793-7800

I have an OASIS User ID/password and (MLOA) digital hardware certificate and still cannot access the OASIS Portal.
The type of error message you are receiving will determine resolution. Below are some error messages you may encounter.

1. Access Forbidden
    a. This error message indicates that your certificate is not being read by our server. This can be caused by several issues:
        i. Your certificate is not input correctly in our system. Contact your Northrop Grumman OASIS point of contact.
        ii. You are selecting the wrong certificate when logging in. For example, our system is expecting you to use an Exostar certificate but instead you select an IdenTrust certificate. You can fix this by selecting your Exostar certificate instead of the IdenTrust certificate.
        iii. Your certificate has expired.

iv. Sometimes when you are logged in for a long time or too much information is cached in your browser, the browser cannot pick up the Exostar certificate. You can remedy this by clearing your browser cache, closing down the browser, unplugging the Exostar token and plugging it back in.
v. A security tool or setting at your company is preventing your certificate from reaching our authentication server. Your IT department must whitelist https://*.myngc.com in your trusted sites and security tools such as; ZScaler, Avast Anti-Virus, McAfee, etc

2. This website declined to show this page – HTTP 403
    a. This error occurs for a variety of reasons.
        i. A Northrop Grumman server is down i.e. US West server may be down when you're connecting to it. You log in later and hit the US central server and you can access OASIS just fine.
        ii. A security tool is blocking our website.

Can I access OASIS using my Exostar certificate from an Apple Mac computer?

We do **not** recommend using Mac computers to access OASIS. Exostar certificates generally do not work with Mac computers and Windows OS is preferred.