

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 certificates. The majority of OASIS users will be using MLOA certs issued by Exostar. We also accept US Government issued CAC (Common Access Card) and certificate issued to Boeing, Lockheed Martin, and Raytheon employees. IdenTrust and Widepoint ORC certificates are also accepted.

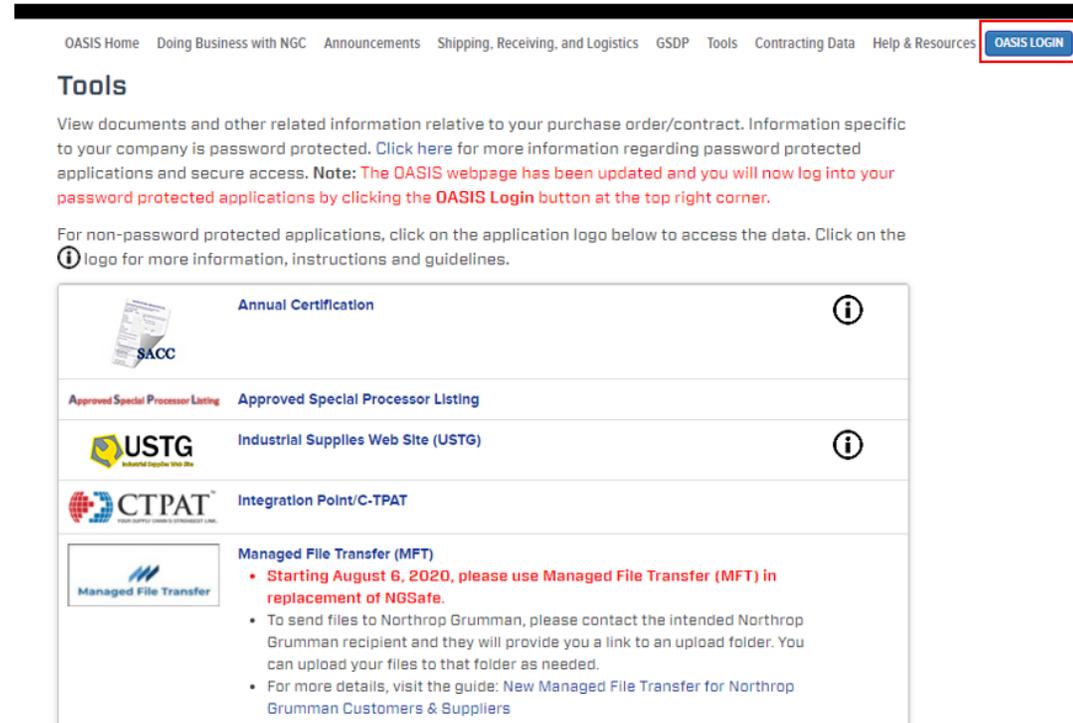
If you don't have a Northrop Grumman OASIS User ID/password please contact your NG buyer to sponsor your request.

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

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

Go to this link to log in using your Exostar certificate: [Tools \(northropgrumman.com\)](https://tools.northropgrumman.com)

Click OASIS LOGIN:



The screenshot shows the OASIS Tools page. At the top, there is a navigation bar with links: OASIS Home, Doing Business with NGC, Announcements, Shipping, Receiving, and Logistics, GSDP, Tools, Contracting Data, Help & Resources, and a highlighted OASIS LOGIN button. Below the navigation bar is the 'Tools' section header. The main content area contains a paragraph explaining that documents are password protected and provides a link for more information. A note states that the OASIS webpage has been updated and users should log in using password protected applications by clicking the OASIS Login button. Below this is a list of tools, each with a logo, a title, and an information icon (i). The tools listed are: Annual Certification (with a SACC logo), Approved Special Processor Listing, Industrial Supplies Web Site (USTG), Integration Point/C-TPAT, and Managed File Transfer (MFT). The MFT tool has a detailed description and a list of instructions.

OASIS Home Doing Business with NGC Announcements Shipping, Receiving, and Logistics GSDP Tools Contracting Data Help & Resources **OASIS LOGIN**

Tools

View documents and other related information relative to your purchase order/contract. Information specific to your company is password protected. [Click here](#) for more information regarding password protected applications and secure access. **Note: The OASIS webpage has been updated and you will now log into your password protected applications by clicking the OASIS Login button at the top right corner.**

For non-password protected applications, click on the application logo below to access the data. Click on the **i** logo for more information, instructions and guidelines.

	Annual Certification	i
	Approved Special Processor Listing	
	Industrial Supplies Web Site (USTG)	i
	Integration Point/C-TPAT	
	Managed File Transfer (MFT) <ul style="list-style-type: none">Starting August 6, 2020, please use Managed File Transfer (MFT) in replacement of NGSafe.To send files to Northrop Grumman, please contact the intended Northrop Grumman recipient and they will provide you a link to an upload folder. You can upload your files to that folder as needed.For more details, visit the guide: New Managed File Transfer for Northrop Grumman Customers & Suppliers	

Select NGC US, then click Supplier / Customer / Partner:



Warning !!

Access to Northrop Grumman's computer network ("Network") is only for authorized users and for authorized purposes. Transmission via the Network of export controlled information abroad or to a foreign person in the U.S. is an export which requires U.S. Government export authorization. You have no expectation of privacy in any information passing through or stored on the Network. Communications and data that pass through or are stored on this Network are monitored and may be intercepted, searched, disclosed or used for any lawful purpose.



Location



Role



Validate

Choose Location

- U** NGC US
- E** NGC EMEA
- A** NGC APAC
- I** Int'l Customer Partner-Access
- X** US External

Select your Role

- N** Northrop Grumman Employee
- P** Supplier / Customer / Partner

Please be advised that by accessing company and/or personal information on this computer, such information may be left within the computer's memory and could be accessed by others. If you are concerned about others potentially accessing such information it is recommended you access your personal information via Northrop Grumman owned equipment or your personal computer.

1-855-737-8364

Employee Login Help

External Supplier / Customer / Partner Help

2. The National Notary Association (NNA) sends an email to the individual (user) who purchased the digital hard 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 the next steps.

What do I do if I forgot my Exostar pin/password number?

It is very important that you don't forget the pin/password number for your Exostar digital hard certificate. The pin/password cannot be reset. Exostar will reissue your digital hard certificate for a fee. Contact Exostar's Customer Service at: +1 703-793-7800

I have an OASIS User ID/password and digital hard certificate and still cannot access the OASIS Portal.

The type of error message you're getting will determine resolution. These are some of the 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. Your Northrop Grumman OASIS point of contact can fix this issue.
 - ii. You are selecting the wrong certificate when logging in. For example, if your Exostar certificate is what our system is using and you select an IdenTrust certificate when logging in instead. You can fix this by selecting your Exostar certificate instead of the IdenTrust certificate.
 - iii. Your Exostar certificate expired.
 - iv. Sometimes when you've logged in for too long or too much information is cached in your browser, the browser cannot pick up the Exostar certificates. You can remedy this by clearing your browser cache, closing down the browsers, unplug the Exostar token and plug it back in.
 - v. A security tool or setting at your company is preventing your certificate from reaching out 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 and you're connecting to it. Later you log in and hit the US central server and you can log in fine.
 - ii. A security tool is blocking our website.

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

We do **not** recommend Mac as a computer to access our systems. Exostar certificates generally do not work with Mac computers and Windows OS is preferred.

