External Supplier/Partner/Customer Login Instructions
Purpose

The purpose of this document is to provide the Northrop Grumman Corporation (NGC) external suppliers, partners and customers with instructions to log in with either a Northrop Grumman issued One Time Password token, a Northrop Grumman issued SurepassID soft or hard token, a DOD CAC, or other user certificates from Exostar, Verisign or IdenTrust ECA, Lockheed Martin CA, Raytheon CA or Boeing CA. It also shows a One Time Password user how to set their One Time Password token PIN. Access to the NGC environment and associated applications may be accessed by clicking the link under Program Application(s) provided by your sponsoring manager.

General Information

- Pay close attention to the instructions on each of the screens. The screens may appear the same; however, the fields may prompt you for different information.
- Access to the NGC environment and applications requires dual factor authentication that includes using an NGC issued One Time Password token, an NGC issued SurepassID token, a DoD CAC or a Certipath/Federal Bridge Partner Certificate.
- To maintain an active account, all external partners / customers must log into the system at least once every 90 days.
- If a user wishes to change the method of authentication, they should contact their NG sponsor.

If the previous authentication method was a One Time Password token, the One Time Password token must be returned to:

Northrop Grumman Corporation
Attn: Enterprise Security Shared Services
8710 Freeport Pkwy., Suite 100
Irving, TX 75063
Attn: AAO

Questions

Prior to contacting the Northrop Grumman Service Desk for assistance with login issues, please contact your project’s point of contact for assistance. If you have any additional login questions, please contact the Northrop Grumman IT Service Desk at 1-855-737-8364. Advise that you are an external partner or customer and that you are having problems with your extranet access/extranet account. At that point the Service Desk will validate your identify using the security questions you answered on your original access request form, create a help ticket, and work to resolve the reason for your call.
Table of Contents

SECTION I – ONE TIME PASSWORD TOKEN/SUREPASSID/DOD CAC/EXOSTAR/OTHER HW CERTS AUTHENTICATION ................................................................. 4
SECTION II – RECOMMENDED BROWSER SETTINGS FOR INTERNET EXPLORER .......................................................................................................................... 10
SECTION III - GETTING HELP .......................................................................................................................................................................................... 11
    POSSIBLE COMMON ISSUES .................................................................................................................................................................................. 12
    FIRST POINT OF CONTACT .................................................................................................................................................................................. 13
    THE SERVICE DESK ......................................................................................................................................................................................... 13
    ESCALATION CONTACT ................................................................................................................................................................................ 13
## Section I – One Time Password Token/SurePassID/DOD CAC/Exostar/Other HW Certs Authentication

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
<th>Screen Shots</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Prior to executing these instructions, make sure you have on-hand the information that was emailed to you (such as your username). See screenshot example.</td>
<td><img src="image.png" alt="Screen Shot" /></td>
</tr>
</tbody>
</table>
  
  **a.** Open a web browser window.  
  **b.** Click on the URL link in the “Program Application(s) section.  
  **c.** If you are accessing [https://eide.myngc.com](https://eide.myngc.com) and you see the bottom screenshot on the right, select **External Access (Employees, Partners)** option. Once you select this option, you will not receive this prompt again for 6 months (unless you clear browser cache/cookies).
2. **Under Select your Role, select “Supplier/Customer/Partner”.** If using a non-mobile device, you can type “P” or “p” and the method will be selected. If using a mobile device, just touch the “Supplier/Customer/Partner” option.

   Logging in via this method requires either an NGC-issued One Time Password (OTP) token, access via SurePassID, or Access Via a DOD Common Access Card (CAC) or other Certipath/Federal Bridge Partner Certificates including Exostar, ECA (Verisign or IdenTrust), Lockheed Martin, Raytheon, and Boeing.

3. If you are using SurePassID, select SurePassID. If using a non-mobile device, you can type “S” or “s” and the method will be selected. If using a mobile device, just touch the “SurePassID” option. If you are using One Time Password token (OTP), skip to step 6. If you are using a DOD CAC, skip to step 9. If you plan to use any other approved certificate including Exostar, ECA (Verisign or IdenTrust), Lockheed Martin, Raytheon, and Boeing, skip to step 10.
4. Enter your user information into the 2 fields displayed:
   a. ‘Username’: Enter your Northrop Grumman domain login account.
   b. ‘PIN’: Enter your SurePassID PIN that you set up.
   c. ‘Passcode’: Enter the 6-digit Passcode from your SurePassID token or smart phone app (as seen below) OR you can type in ONLY a ? in the Passcode field to use the push functionality of SurePassID (Push does NOT work with a hard token, only with the smart phone app).
      Please note: the comma will be entered automatically so there is no longer a need to add a comma!
   d. Select the ‘Login’ button.
   e. If you typed ? in the Passcode field, you will be prompted on your mobile device to accept the SurepassID code as seen here
   f. Once you select Approve, your access will be granted.

![Login Instructions Diagram]
5. If your credentials fail, you will see the page to the right. This means either your username or PIN or passcode from the SurePassID token were incorrect. Enter your credentials again and click Login.

If you cannot get past this page, then contact the Northrop Grumman IT Service Desk for assistance.

6. If you are using One Time Password token (OTP), select One Time Password Token. If using a non-mobile device, you can type “O” or “o” and the method will be selected. If using a mobile device, just touch the One Time Password Token option.
7. Enter your user information into the 2 fields displayed:
   a. ‘User name’: Enter your Northrop Grumman domain login account.
   b. ‘OTP Passcode’:
      Enter your PIN followed by:
      - the 8-digit # from the OTP token (characters joined with no spaces)
   c. Select the ‘Login’ button and your access will be granted.

8. If your credentials fail, you will see the page to the right. This means either your username or PIN or passcode from the OTP token were incorrect. Enter your credentials again and click Login.

   If you cannot get past this page, then contact the Northrop Grumman IT Service Desk for assistance.
9. If you are using a **DOD CAC** select “DOD CAC”. If using a non-mobile device, you can type “C” or “c” and the method will be selected. Click **Login** and skip to step 11.

   **Important:** Make sure you have inserted your smartcard/keyfob device.

10. If you are using any other approved certificate including **Exostar, ECA (Verisign or IdenTrust), Lockheed Martin, Raytheon, or Boeing** select “Exostar, Other HW Certs”. If using a non-mobile device, you can type “M” or “m” and the method will be selected. Click **Login**.

   **Important:** Make sure you have inserted your smartcard/keyfob device.
11. You will be prompted to select your certificate. Click OK.

Please note that depending on the operating system that you are using, the screen to select your digital certificate could vary. Here are two possible screens that you might see.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Image1.jpg" alt="Image 1" /></td>
<td><img src="Image2.jpg" alt="Image 2" /></td>
</tr>
</tbody>
</table>

12. You will next be prompted for your certificate PIN/Password. Enter your PIN/Password and click OK.

Please note that depending on the operating system that you are using, the screen to enter your PIN could vary. Here are two possible screens that you might see.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Image3.jpg" alt="Image 3" /></td>
<td><img src="Image4.jpg" alt="Image 4" /></td>
</tr>
</tbody>
</table>
Section II – Recommended Browser Settings for Internet Explorer

1. Go to Tools\Internet Options
2. Click on Advanced tab
3. In Security Menu
   a. Ensure TLS 1.0, TLS 1.1 and TLS 1.2 are checked.
   b. Ensure SSL 2.0 and SSL 3.0 are unchecked.
Section III - Getting Help

Possible Common Issues

Here are some possible issues you may see with some possible resolutions.

1. If, when accessing https://eide.myngc.com or any others that show the home realm discovery page (shown to the right), the browser spins for a few minutes and then a proxy error is displayed (as shown below), you most likely chose the wrong selection (should have selected External Access (Employees, Partners)).

The solution to this issue would be to clear your web browser cache and cookies and then retry. You should see the home realm discovery page again and will be able to select the correct option. External Access (Employees, Partners).
2. If you see the following screen, contact the service center.

**First Point of Contact**

The Service Center can help with basic issues such as a password reset or initial login problems. Contact the Service Center at 1-855-737-8364. Be sure to advise that you are an external partner or customer. Provide specifics relating to the problem you are having such as ‘cannot login for the first time’ or ‘forgot my password’. You will be required to validate your identity using the security questions and answers you provided in your original access request. If the Service Center is not able to resolve your problem immediately a ticket will be created. Be sure to get your ticket number for future reference.

**Escalation Contact**

Your Northrop Grumman sponsor is always your contact for any escalations that you may have.

**My Project is Over – What do I do?**

When your project or proposal is over you must advise NGC so that your access will be terminated. At all times this is done via your Sponsor. At the onset of your work an estimated date of completion was provided by your Sponsor. As this date was only an estimate it is possible that your access will be terminated earlier or after the estimated completion date. Some NGC-systems automatically notify when your end-date is approaching. In either case (early completion or extension) you must coordinate your continued or terminated access with your Sponsor. Upon completion of a project or proposal and termination of your access, you must return all equipment, such as a SecurID token, to Northrop Grumman as describe under ‘Purpose’ in this document.