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 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 a NGC issued One Time Password token, 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 ......................................................................................................................................................................................... 4
  Logging In the First Time via One Time Password Token ........................................................................................................................................... 4
  Subsequent Login Instructions ..................................................................................................................................................................................... 16

SECTION II – ACCESS VIA DOD (CAC) OR OTHER CERTIPATH/FEDERAL BRIDGE PARTNER CERTIFICATES ............................................................................... 19
  Logging In the First Time ......................................................................................................................................................................................... 19
  Subsequent Login Instructions .................................................................................................................................................................................. 24

SECTION III – RECOMMENDED BROWSER SETTINGS FOR INTERNET EXPLORER ........................................................................................................ 28

SECTION IV - GETTING HELP .................................................................................................................................................................................. 29
  Possible Common Issues ......................................................................................................................................................................................... 29
  First Point of Contact ......................................................................................................................................................................................... 30
  The Service Desk .............................................................................................................................................................................................. 30
  Escalation Contact ........................................................................................................................................................................................... 30
Section I – One Time Password Token

Logging In the First Time via One Time Password Token

<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="image1.png" alt="Screen Shot" /></td>
</tr>
<tr>
<td></td>
<td>a. Open a web browser window.</td>
<td><img src="image2.png" alt="Screen Shot" /></td>
</tr>
<tr>
<td></td>
<td>b. Enter <a href="https://www.myngc.com">https://www.myngc.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Select ‘myNGC Customer/Partner Portal’ option from the right-hand menu.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. When you see the bottom screenshot on the right, select the 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).</td>
<td></td>
</tr>
</tbody>
</table>

From here you will login, change your temporary directory password, and create a PIN.
2. From the ‘Choose Your Login Method’ window select ‘Supplier/Customer/Partner.’

3. Select ‘One Time Password Token (OTP).’

Logging in via this method requires a **NGC-Issued One Time Password**. It should look similar to the diagram below:
4. Enter your user information into the 3 fields displayed:
   a) ‘User Name’: Enter your **username** which was emailed to you. This is your username for future logins.
   b) ‘Password’*: Enter your **temporary directory password**.
   c) ‘OTP Passcode’: Enter your **temporary OTP passcode**, which was emailed to you.
   d) Select the ‘Login’ button.
5. You will now be prompted to change your password.
   
a. ‘Old Password’: Enter your temporary directory password, which was emailed to you.

b. ‘New Password’: Enter a new password that is at least 8 but no more than 14 alphanumeric characters. Your new password **MUST** contain at least one upper case character, at least one lower case character, and at least one digit. (Special character can also be used (,”’~!@#$%^&*()_+-=[]\{}|;:<>/?, .).

c. ‘Confirm New Password’: Re-type the new password.

d. Select the ‘Change Password’ button.
When this screen appears, select the ‘CONTINUE’ button
You have successfully created a new directory password.

**FROM THIS POINT FORWARD** you will use this new directory password for logging on. Please note that this password must be **changed every 90 days**. You will be prompted to do this when the time approaches.
7. You must now login again with your Username, new Directory password and Temporary One Time Password (OTP). Enter information, Click ‘Login.’

8. You should now be into the programs portal. You must set your PIN for your OTP token. From the External Partners section, click on the ActivIdentity Partner Account Mgt link.
9. From the **AAA Web Help Desk** you will set your OTP PIN and provide answers to the security questions.  
*If you receive any errors during this process, refresh your browser page.*

a. Select ‘**Directory (Network) password**’.
b. ‘**Enter your username:**’ Enter your **userID**.
c. Select the ‘**OK**’ button.
10. You will now be prompted for your Directory (Network) Password:
   a. **What is your Directory (Network) password?**
      Enter the new directory password created in Step 5.
   b. Select the ‘OK’ button
| Step 11 | You will now activate your token.  
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a.      | Press the ON button for 1 second, an 8 digit # will appear.  
| b.      | ‘Enter the one-time password:’ Enter 8 digits that appear on token.  
| c.      | Click ‘NEXT’.  

| Step 12 | Enter a PIN of your choice into the PIN: and Confirm PIN: fields, and then click **Set PIN**.  
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a.      | The PIN **must** be between 4 and 8 **alphanumeric characters**.
13. You will now set your security questions answers for your ActivIdentity token. Click on **Change answers to security questions.**
14. You will now be prompted to provide answers to security questions.
   a. Answer all 4 security questions.
   b. Select the ‘Set’ button

The security answers will be used to authenticate your identity when you phone the Northrop Grumman Service Desk.
15. When this screen appears, please close your browser.

**FROM THIS POINT FORWARD** you will use the new directory password and OTP passcode (PIN + 8-digit token code). Refer to the email that you received from your Northrop Grumman sponsor, go to the Program Application(s) section and use the URL link for all future access. You can refer to the ‘Subsequent Login Instructions’ section if help is required.
**Subsequent Login Instructions**

<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></td>
</tr>
<tr>
<td>a.</td>
<td>Open a web browser window.</td>
<td></td>
</tr>
<tr>
<td>b.</td>
<td>Click on the URL link in the “Program Application(s) section.</td>
<td></td>
</tr>
<tr>
<td>c.</td>
<td>If you are accessing <a href="https://eide.myngc.com">https://eide.myngc.com</a> and you see the bottom screenshot on the right, select the 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).</td>
<td></td>
</tr>
</tbody>
</table>
2. From the ‘Choose Your Login Method’ window select ‘Supplier/Customer/Partner.’

3. Select ‘One Time Password Token (OTP).’
4. Enter your user information into the 3 fields displayed:
   a. ‘User Name’: Enter your username.
   b. ‘Password’: Enter your new directory password. This is the directory password that you created during your initial setup or reset after each 90 day interval.
   c. ‘OTP Passcode’: Enter your PIN followed by: the 8-digit # from the OTP token
   d. Select the ‘Login’ button.

You will now have access to your collaborative area. If you continue to have access issues please refer to the Getting Help section of this document.
Section II – 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

Logging in the First Time via Client Certificate

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
<th>Screen Shots</th>
</tr>
</thead>
</table>
| 1.   | **Important: Insert your smartcard/keyfob device.**  
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.  

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 the **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).  

From here you will login, and change your temporary directory password. |

Ex. External Partner / Customer Login Instructions  
via the myNGC Portal  
Page 19 of 30  
Northrop Grumman IT Service Desk  
Version 6.2, 8/21/2019
2. From the ‘Choose Your Login Method’ window select ‘Supplier/Customer/Partner.’

3. Select the option for your specific certificate.
   If you use a DOD CAC, select that option.
   If you use an Exostar, Lockheed Martin, Raytheon, Boeing, an ECA certificate from Verisign or IdenTrust, or any other approved Certificate Authority, select that option.
4. Regardless of which certificate you select, enter your user information into the 2 fields displayed:
   a. ‘**User Name**’: Enter the **username** that was emailed to you. This is your username for all future logins.
   b. ‘**Password**’: Enter your **temporary password** that was emailed to you.
   c. Select the ‘**Login**’ button.

5. 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.
6. 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.

7. If you enter the information in Step 4 correctly you will be prompted to change your password.

If the login screen reappears repeat Step 4. Be sure to enter your credentials correctly. Repeated errors will cause a lockout of your account.

a. ‘Old Password’: Enter your temporary directory password that was emailed to you and used in Step 4.

b. ‘New Password’: Enter a new password that is at least 8 but no more than 14 alphanumeric characters. Your new password MUST contain at least one upper case character, at least one lower case character, and at least one digit. (Special character can also be used ;":'"~ ! @ # $ % ^ & * ( ) _ + - = { } \ ; < > ? , . /).

c. ‘Confirm New Password’: Re-type the new password.

d. Select the ‘Change Password’ button.
<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>When this screen appears, select the ‘CONTINUE’ button.</td>
</tr>
<tr>
<td>9.</td>
<td>You have successfully created a new directory password. <strong>FROM THIS POINT FORWARD</strong> you will use this new directory password for logging on. Please note that this password will need to be <strong>changed every 90 days</strong>. You will be prompted to do this when the password expires. You must now <strong>login again with the new credentials</strong> that you just created. Go back and follow steps 2 through 6.</td>
</tr>
</tbody>
</table>
### Subsequent Login via Client Certificate Instructions

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
<th>Screen Shots</th>
</tr>
</thead>
</table>
| 1.   | **Important: Insert your smartcard/keyfob device.**  

Open an Internet Explorer browser window.

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.

1. a. Open a web browser window.
2. b. Click on the URL link in the “Program Application(s) section.
3. c. If you are accessing [https://eide.myngc.com](https://eide.myngc.com) and you see the bottom screenshot on the right, select the **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). | ![Screen Shot](image) |
2. From the ‘Choose Your Login Method’ window select ‘Supplier/Customer/Partner.’

3. Select the option for your specific certificate.
   If you use a DOD CAC, select that option.
   If you use an Exostar, Lockheed Martin, Raytheon, Boeing, or an ECA certificate from Verisign or IdenTrust, select that option.
4. Regardless of which certificate you select, enter your user information into the 2 fields displayed:
   a. ‘User Name’: Enter the username that was emailed to you. This is your username for all future logins.
   b. ‘Password’: Enter your new password. This is the password that you created during your initial login or reset after each 90 day interval.
   c. Select the ‘Login’ button.

5. 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.
6. **You will next be prompted for your certificate PIN. Enter your PIN 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.

You will now have access to your collaborative area. If you continue to have access issues please refer to the Getting Help section of this document.
Section III – 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 IV - 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 proxy server isn't responding]

   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.