NGC Employee External Access Login Instructions

Access Using the One Badge or One Time Password Token
Purpose

This document provides instructions on how to access the Northrop Grumman externally accessible web sites.

General Information

- To access the Northrop Grumman Portal, you must have the following credentials:
  - A Northrop Grumman domain login account. If you haven’t used your Northrop Grumman domain login account in 60 days or longer, please call the IT Service Desk at 855-737-8364 to enable it.

  AND

  - A Northrop Grumman issued One Badge

  OR

  - A Northrop Grumman issued One Time Password (OTP) Token. If you do not have a One Time Password token, call the IT Service Desk at 855-737-8364 to obtain one.

- OTP tokens and One Badges work in conjunction with Northgrum domain accounts for strong dual factor authentication.
- All users should follow the instructions in section II (Recommended Browser Settings) initially. Otherwise, the trusted website message will continue to appear upon each login.

Questions?

If you have questions, please contact the IT Service Desk at 855-737-8364.
Table of Contents

SECTION I – ONE TIME PASSWORD TOKEN/ONE BADGE AUTHENTICATION .............................................................................................................. 4
SECTION II – RECOMMENDED BROWSER SETTNGS FOR INTERNET EXPLORER .................................................................................................................. 9

ENABLE MIXED CONTENT MESSAGE POP-UPS .................................................................................................................................................................. 9
ADD ‘HTTPS://*.MYNGC.COM’ AS A TRUSTED SITE .................................................................................................................................................. 10
ENABLE AUTOMATIC CACHING .............................................................................................................................................................................. 11
USER AUTHENTICATION ....................................................................................................................................................................................... 12
## Section I – One Time Password Token/OneBadge Authentication

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
<th>Screen Shots</th>
</tr>
</thead>
</table>
| 1.   | a. Open a web browser window  
      b. Enter https://www.myngc.com  
      c. Select ‘myNGC Corporate Portal’ option from the right-hand menu.  
      d. If you are accessing 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 Shots](image1.png) ![Screen Shots](image2.png) |
2. From the 'Choose Your Login Method' window select 'Northrop Grumman Employee'.

Logging in via this method requires either a **NGC-issued** One Time Password token or a NGC issued OneBadge. The Password token should look similar to the diagram below:

![Password Token Diagram]

3. If you are using an One Time Password token, select NG Employee One Time Password Token (OTP). If you plan to use your NG issued OneBadge, skip to step 5.

![One Badge Diagram]
4. 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)
Select the ‘Login’ button.

5. If you are using an NG issued One Badge for authentication, be sure your One Badge is in your card reader and select NG Employee OneBadge Only.
6. Please note that depending on the operating system that you are using, the screen to select your digital certificate could vary. Here are possible screens that you might see.

   a. You will be prompted to select your Northrop Grumman certificate. Click OK.

   b. You will next be prompted for your OneBadge PIN. Enter your PIN and click OK.
<table>
<thead>
<tr>
<th></th>
<th>Note: Users can also get to portal sites by entering the exact URL to the desired location in step 1 (instead of going to the main <a href="https://www.myngc.com">https://www.myngc.com</a> portal page). Follow the login instructions in steps 2 &amp; 3. Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="https://home.myngc.com">https://home.myngc.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://eide.myngc.com">https://eide.myngc.com</a></td>
</tr>
</tbody>
</table>
Section II – Recommended Browser Settings for Internet Explorer

### Enable Mixed Content Message Pop-Ups

Open an Internet Explorer browser window:

1. **Step Instructions**
   
   a. On the menu, select ‘Tools’, then ‘Internet Options’.
   
   b. Select the ‘Security’ tab.
   
   c. Select the ‘Local Intranet’ icon.
   
   d. Near the bottom of the screen, press the ‘Custom Level’ button.
   
   e. Now scroll down about half way and within the ‘Miscellaneous Section’ you will see ‘Display Mixed Content’, select the radio-button to ‘Enable’ this option.
   
   f. Press the ‘OK’ button.
   
   g. Then, press ‘Yes’ button on the pop-up message.

**Screen Shots**

![Internet Options](image)

![Security Settings](image)
**Add ‘https://*.myngc.com’ as a Trusted Site**

2. Open an Internet Explorer browser window:
   
a. From the menu, select ‘Tools’, then ‘Internet Options’.
b. Select the ‘Security’ tab.
c. Select the ‘Trusted Sites’ icon.
d. In the ‘Add this website to the zone:’ box, type ‘https://*.myngc.com’ (without any quotes or spaces). The asterisk character ( *) is obtained by using shift+8.
e. Press the ‘Add’ button.
f. Press the ‘Close’ button.
g. Now, press the ‘OK’ button.
### Enable Automatic Caching

3. Open an Internet Explorer browser window:
   - a. From the **menu**, select **Tools**, then **Internet Options**.
   - b. Select the **General** tab.
   - c. In the **Browsing History** section, press the **Settings** button.
   - d. On the **Settings** screen, select the radio-button **Automatically**.
   - e. Lastly, press the **OK** button.

![Enable Automatic Caching](image_url)
<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
<th>Screen Shots</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>User Authentication</strong></td>
<td>![Image of Internet Explorer settings]</td>
</tr>
<tr>
<td></td>
<td>Open an Internet Explorer browser window:</td>
<td>![Image of Internet Explorer settings]</td>
</tr>
<tr>
<td></td>
<td>a. On the menu, select ‘Tools’, then ‘Internet Options’.</td>
<td>![Image of Internet Explorer settings]</td>
</tr>
<tr>
<td></td>
<td>b. Select the ‘Security’ tab.</td>
<td>![Image of Internet Explorer settings]</td>
</tr>
<tr>
<td></td>
<td>c. Select the ‘Internet’ icon.</td>
<td>![Image of Internet Explorer settings]</td>
</tr>
<tr>
<td></td>
<td>d. Near the bottom of the screen, press the ‘Custom Level’ button.</td>
<td>![Image of Internet Explorer settings]</td>
</tr>
<tr>
<td></td>
<td>e. Now scroll down all the way and under ‘User Authentication’ you will see Automatic logon with current username and password.” Select that radio-button.</td>
<td>![Image of Internet Explorer settings]</td>
</tr>
<tr>
<td></td>
<td>f. Press the ‘OK’ button.</td>
<td>![Image of Internet Explorer settings]</td>
</tr>
<tr>
<td></td>
<td>g. Then, press ‘OK’ button on the pop-up message to save this setting.</td>
<td>![Image of Internet Explorer settings]</td>
</tr>
</tbody>
</table>