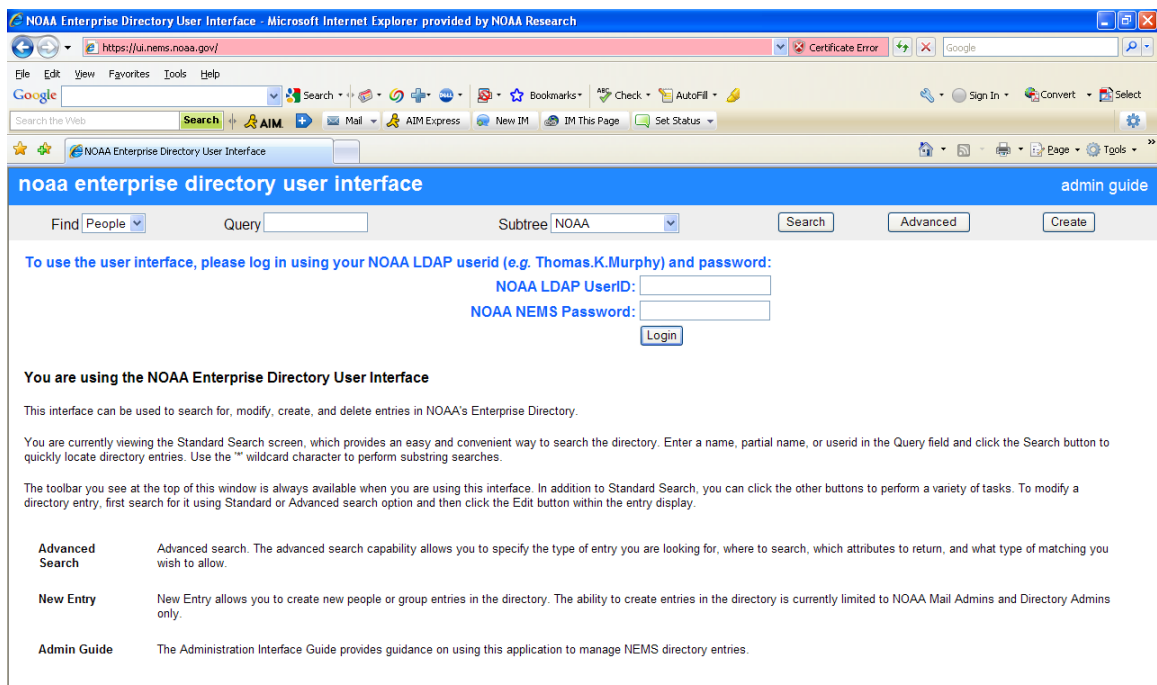


Email – Change Password

To change your email password:

- Log into NOAA Webmail User Interface at: <https://ui.nems.noaa.gov>
- You will see a login screen to the NOAA Enterprise Messaging System (NEMS) User Interface



The screenshot shows a Microsoft Internet Explorer browser window displaying the NOAA Enterprise Directory User Interface. The address bar shows the URL <https://ui.nems.noaa.gov>. The page title is "noaa enterprise directory user interface" and there is an "admin guide" link in the top right corner. The main content area features a search interface with a "Find" dropdown menu set to "People", a "Query" input field, a "Subtree" dropdown menu set to "NOAA", and buttons for "Search", "Advanced", and "Create". Below the search fields, there is a login section with the text: "To use the user interface, please log in using your NOAA LDAP userid (e.g. Thomas.K.Murphy) and password:". This is followed by two input fields: "NOAA LDAP UserID:" and "NOAA NEMS Password:", and a "Login" button. Below the login section, there is a heading "You are using the NOAA Enterprise Directory User Interface" and a paragraph of introductory text. At the bottom, there is a table with three rows: "Advanced Search", "New Entry", and "Admin Guide", each with a brief description of its function.

Advanced Search	Advanced search. The advanced search capability allows you to specify the type of entry you are looking for, where to search, which attributes to return, and what type of matching you wish to allow.
New Entry	New Entry allows you to create new people or group entries in the directory. The ability to create entries in the directory is currently limited to NOAA Mail Admins and Directory Admins only.
Admin Guide	The Administration Interface Guide provides guidance on using this application to manage NEMS directory entries.

- Enter your current email user name and password and click the “Logon” button.
- Once you are logged in, type your name in the “Query” box and hit the “Search” button.
- When the search results come up, click on your name on the left side of the page.

- The NEMS User Interface will then display your email account information.

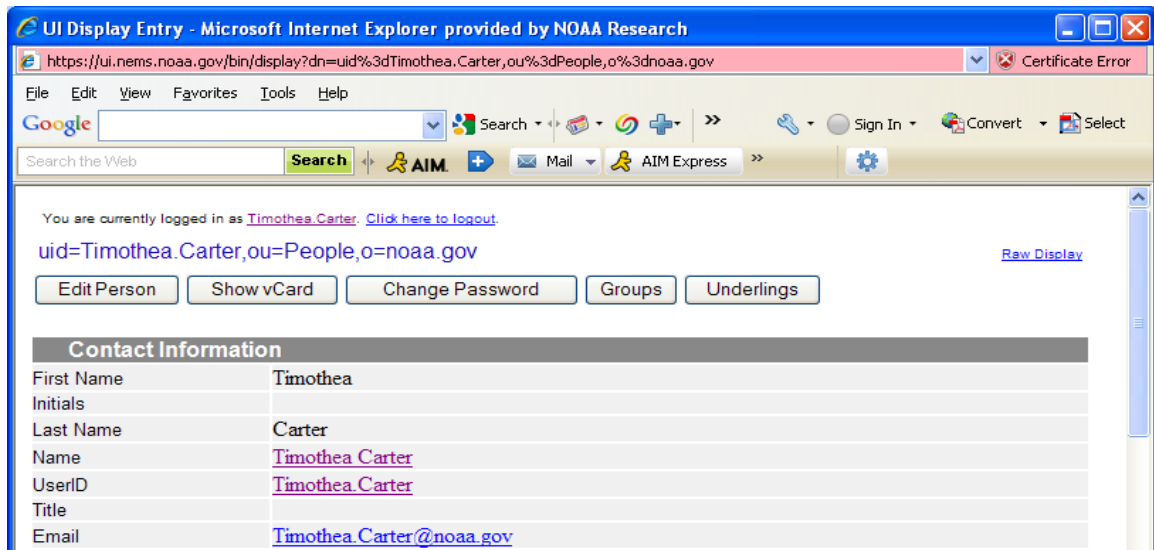


Fig 3

- Click the "Change Password" button at the top.

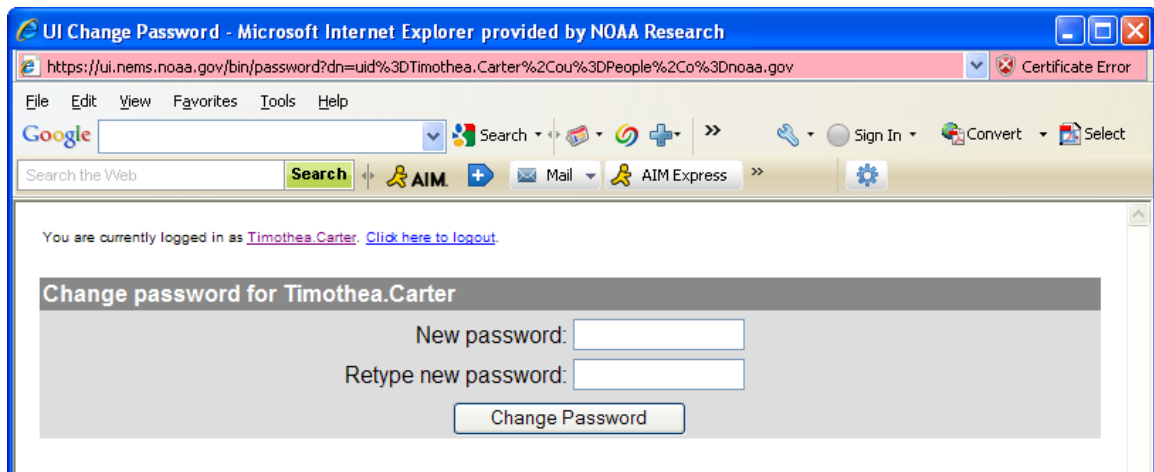


Fig 4

- Enter your new password in both fields and click the "Change Password" button.

Department of Commerce Password Requirements

All password changes must comply with the DoC Password Requirements policy (https://access.portal.noaa.gov/doc/CIO/ITSITnew/CITR_009_Password_Requirements.pdf). If the desired password does not comply with the policy you will receive a red error message with a description of the policy requirement that is not met by the password you entered.

A summary of the DOC password requirements taken from the NOAA IT Security Awareness training course (<http://noaa.learnsecuritywith.us/course/ac-main.asp>) can be found below.

NOAA General-Purpose System Password Policy

NOAA's general-purpose system password policy now reflects the DOC IT Security Program requirements for the management of passwords, passphrases, and PINs to support authentication for NOAA IT systems and/or applications.

DOC Password Requirements

1. Passwords must be created consistent with the following criteria.
 1. Passwords must have at least twelve (12) non-blank characters.
 2. Passwords must contain characters from at least three of the following four categories:
 1. English upper case characters (A...Z);
 2. English lower case characters (a...z);
 3. Base 10 digits (0...9); and
 4. Non-alphanumeric (For example, !,\$#%).
 3. Passwords must not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
 4. Six of the characters must not occur more than once in the password (e.g., 'AAAAAAA1n#!' is not acceptable, but 'A%rmp2g1n#!' and 'A%ArmA2gA1n!' are acceptable).
2. Passwords must not include any of following: vendor/manufacturer default passwords, names (e.g., system user names, part or all of your account name, family names), words found in dictionaries (i.e., words from any dictionary, spelled forward or backward), addresses or birthdays, or common character sequences (e.g., 3456, ghijk, 2468). Vendor-supplied default passwords, such as SYSTEM, Password, Default, USER, Demo, and TEST, must be replaced immediately upon implementation of a new system.
3. Systems or applications that have multiple passwords for different levels of access or authentication must have unique passwords for each level.
4. Passwords must be protected to prevent unauthorized use. Specifically:
 1. Passwords must not be shared except in emergency circumstances or when there is an overriding operational necessity as documented in an operating unit IT system security plan. Once shared, passwords must be changed as soon as possible.
 2. Group passwords (i.e., a single password used by a group of users) must not be used without some other mechanism that can assure accountability (such as separate and unique network User IDs).
 3. Group passwords must not be shared outside the group of authorized users and must be changed when any individual in the group is no longer authorized. Group passwords must never be re-used.

4. Passwords that need to be shared because of an overriding operational necessity, as well as group passwords, cannot be used to control access to other IT systems or applications on IT systems.
5. Passwords in readable form (e.g., written on paper) must be kept in a safe location and not stored in a location accessible to others. For example, safe locations include storage in a locked container accessible only by the user.
6. IT systems and workstations must not display or print passwords as they are entered.
7. User applications must not be enabled to retain passwords for later re-use or be configured to bypass authentication mechanisms. For example, Internet browsers must not be set to save passwords for re-use. However, use of password retaining programs is allowed provided that the retaining program requires authentication and stores passwords in an encrypted manner.
8. Passwords must not be distributed through non-encrypted electronic mail, voice-mail, nor left on answering machines.
9. Passwords must be changed as follows:
 1. At least every 60 days;
 2. Immediately if discovered to be compromised or one suspects a password has been compromised;
 3. Immediately if discovered to be in non-compliance with this standard; and
 4. On direction from management.
10. Do not reuse a password you have used any of the last 8 times you have changed your password or more recently than 2 years from when you last used the password.
11. Access to password files or password databases must be restricted to only those who are authorized to manage the IT system.
12. If a determination is made that a password has been compromised or is not in compliance with this standard, and if the password is not immediately changed, the account must be temporarily suspended until the password is changed.
13. Passwords for servers, mainframes, telecommunications devices (such as routers and switches), and devices used for IT security functions (such as firewalls, intrusion detection, and audit logging) must be encrypted when stored electronically.
14. Passwords, other than single-use (one-time) passwords, must be encrypted when transmitted across a wide area network or the Internet.