Table of Contents

How to get a CVR Account/Invitation
Steps to Success

CVR invitations have been sent to all Navy users. If you did not receive an invite, check the following:

1. **Verify your DUTY ORGANIZATION in milConnect* is correct**. Go to https://www.dmdc.osd.mil/milconnect. Click on **Update personal contact info**, A *DS Logon* screen will appear, select the **CAC** tab, then click the **Login** button, select your Authentication (PIV) certificate, then click **OK**. On the *Update and View My Profile* screen, click on the **CIV**, **MIL**, or **CTR** tab, whichever applies to you. **Ensure the *Duty Organization* selected is "United States Navy".** For example, if you are a US Marine working at a Navy HQ/Command with a @navy.mil email address and your Duty Organization is USMC you will not receive an email invitation; simply changing the Duty Organization to "United States Navy" will trigger the invitation once the systems update, **usually the next day.**
2. **Verify your DUTY SUB ORGANIZATION in milConnect* is correct** (located directly below the Duty Organization)**. The Duty Sub Organization MUST be a Navy organization**. Invitations are only sent to users in Duty Sub Organizations that were selected for CVR on-boarding. Every Navy Duty Sub Organization has been selected. If you selected a non-Navy Duty Sub Organization that was not ready to on-board, no CVR account was created and no CVR invitation would be sent. (On NMCI, the user's display name is updated by milConnect, so that can help determine if you've selected the correct Duty Sub Organization)
3. **Verify your PRIMARY PERSONNEL EMAIL in milConnect* is correct** (located further down the page). **This should be the same as your NMCI email address and MUST be a *.mil, *.gov, and DoD-controlled *.edu domain**. Invitations can only be sent to *.mil, *.gov, and DoD-controlled *.edu domains. If the Primary Personnel Email listed in milConnect is other than a *.mil, *.gov, or a DoD-controlled *.edu domain, use the "How to Change Your E-mail Address in milConnect" directions on the following page to change it. (The milConnect Primary Personnel Email is the same address as registered to your CAC)
4. **Submit the updates.** Once the *Duty Organization, Sub Duty Organization*, and *Primary Personnel Email* is updated and/or verified, scroll to the bottom of the page and click the **Submit** button.

How Do New Employees Get a CVR Account?

Personnel who are new to DoD will automatically get a CVR account when all of the following are true:

- They are registered in DEERS (i.e. receive a CAC)
- They set a valid e-mail address on their CAC (i.e. .mil, .gov, or DoD-controlled .edu)
- They update their CIV/MIL/CTR profile in milConnect with a valid *Duty Organization* ("United States Navy") and *Duty Sub Organization* (i.e. current command)

If the user came from another part of DoD, they will keep their existing CVR account. If that account was not active, they should follow the steps described above.

How to Change Your E-mail Address Displayed in milConnect

There are two ways to update the email address, which is the email address on your CAC.

1 - Go to a RAPIDS ID Card Office

2 - Use the RAPIDS Self-Service website, which is accessible from home or work and is described below.

RAPIDS Self-Service Website

- Prerequisites:
  - Internet Explorer in Windows 10 (Chrome and Edge will not work)
  - The user should be on (either):
    - an NMCI seat
    - a personally-owned system w/both ActivClient 7.1 (or higher) *and* Java 8 Update 151 (or higher) installed
  - Internet Explorer settings:
    - Internet Explorer -> Tools -> Compatibility View Settings: "osd.mil" MUST appear in the list.
    - Internet Explorer -> Tools -> Internet Options -> Security tab: "https://*.osd.mil" MUST appear in the list.
  - Java settings - "Configure Java" control panel -> The Exception Site List *must* have the following 3 sites
    - https://www.dmdc.osd.mil
    - https://pki.dmdc.osd.mil
    - https://idco.dmdc.osd.mil
- Procedure:
  1. Using Internet Explorer, go to https://www.dmdc.osd.mil/identitymanagement
  2. Click the **CAC** tab and **Login** with any CAC certificate (do not login with the DS Logon or DFAS tabs)
  3. Click the **Websites Accepting DS LOGON** tab
  4. Select the RAPIDS Self-Service **ID Card Office Online (IDCO)**
  5. Click the **Change CAC Email** button
  6. When prompted check the box labeled **Change from email provided by your organization to another email address**, then click **Proceed**. This process will use Java to read the email on your CAC.
  7. Click **I accept** the risk and click **Run** to any Java Security Warnings (may take 2+ minutes).
  8. Regardless of any warning messages, enter your *actual* work e-mail address (even if it shows *exactly* the same address already).
  9. Continue to follow the prompts.
  10. If you receive a PIN prompt during the process (a small, rectangular window in the center of the window), *very carefully and slowly* enter your PIN, always ensuring that the cursor appears at the end of the text field as you do so.
  11. If an error message is received, reload the page (F5) and try again; however, if this happens repeatedly, you most likely will need a new CAC.

NOTE: Email changes **may take 24-48** hours to update milConnect and CVR

NOTE: Changing your CAC e-mail address results in creation of new encryption certificates. Users should publish their new certificates to the GAL (see NMCI Homeport for instructions). Users may need to download their old certificates to read older encrypted e-mail. Old certificates can be downloaded while connected from a NIPRNET workstation at https://ara-5.csd.disa.mil or https://ara-6.csd.disa.mil (these sites are inaccessible from the regular internet).

How to Reset CVR Password or Re-enable account
Steps to Success

AFTER verifying the above steps (and waiting 24-48 hours if changes were made), **go to the CVR Self-Service Portal** (https://account.cvr.mil/) **using Chrome or Microsoft Edge browser** and sign in with your PIV (non-email) Authentication certificate from your CAC to reset your password or re-enable your CVR account. If you are using google Chrome it does not tell you the name of your certificate (i.e.: email, authentication, etc.) it only tells you the serial number. If you don't choose the correct serial number, you will not gain access to the site and get an f5 error page. To find your correct serial number for authentication certificate go to:

In Google Chrome -

- Start Icon
- ActivID ActiveClient dropdown
- Choose User Console
- Double click authentication certificate
- Details tab

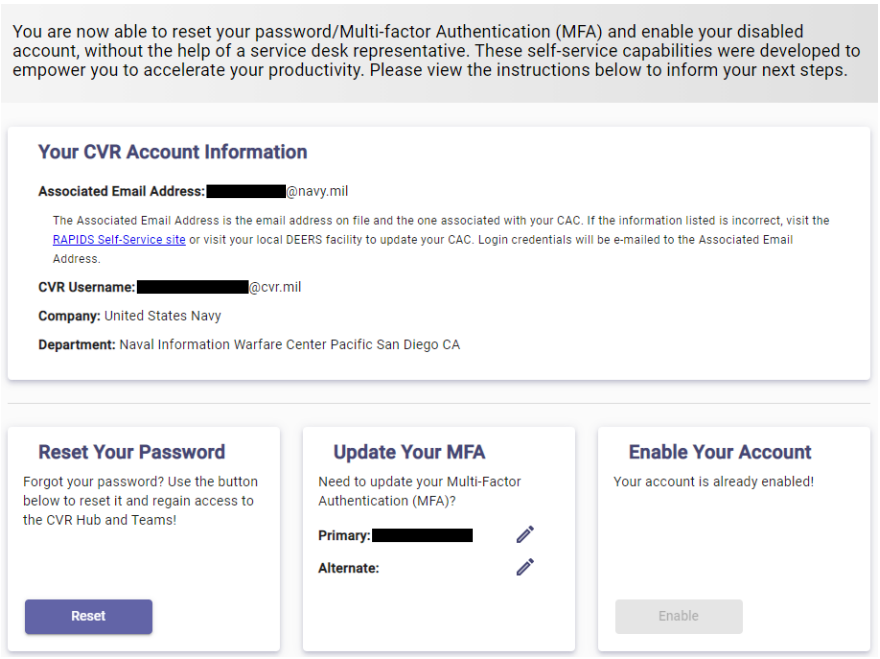
You will see your serial number in there.

When attempting to go to CVR Self-service Portal you may encounter errors related to outdated TLS security settings or "your session could not be established". If so, try the other browser (Chrome or Edge) and try multiple times. If still unsuccessful, contact NMCI.

In Microsoft Edge – check the TLS settings, un-check TLS 1.0, you should only be using TLS 1.1 and 1.2:

In the Windows menu search box, type Internet options.
Under Best match, click Internet Options.

- In the Internet Properties window, on the Advanced tab, scroll down to the Security section
- Check the User TLS 1.2 checkbox
- Click OK
- Close your browser and restart Microsoft Edge browser



If the Reset Your Password, Update Your MFA, and Enable Your Account buttons are grayed out, it's indicative of an account issue - the user will need to reach out to NAVY 311, the Tier 1 support desk for CVR.

Multi-Factor Authentication (MFA)
Steps to Success

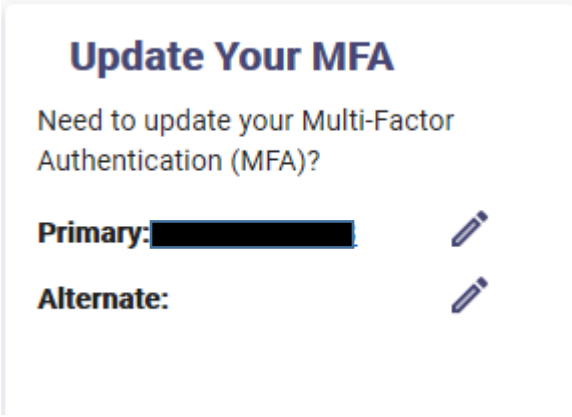
If you ARE able to temporarily access the original authentication phone:

Use that location to log in to https://aka.ms/mfasetup. There you can add a second phone number under "Alternate authentication phone". Note: phones do not have to be SMS-capable; you can receive a voice call to authenticate.

If you ARE NOT able to access the original authentication phone:

Go to the CVR Self-Service Portal (https://account.cvr.mil) to reset your CVR Multi-Factor Authentication (MFA). The next time you login to MS Teams you will be prompted to update the MFA device.

If you cannot get the text or call to verify your account you can now change the number before you log in or add an alternate number to use before trying to log in. Use the MFA Update tool on the CVR Self-Service Portal to edit the Primary and Secondary contact numbers.



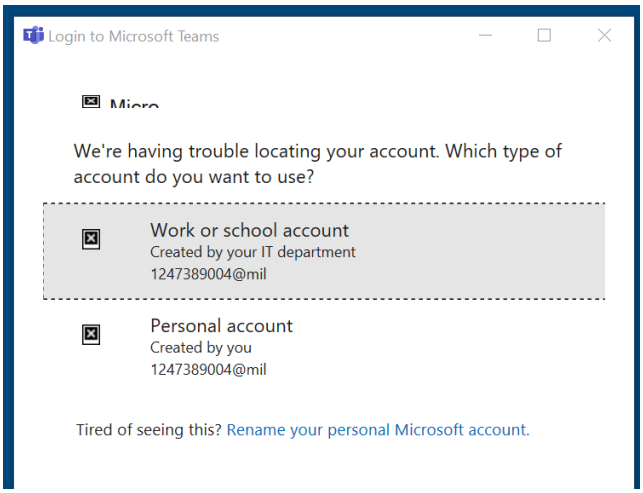
How Do I Sign In to MS Teams?

1. **Use the MS Teams application** on an NMCI computer

    a. In the Windows search bar type "Microsoft Teams" or click the Start button and select "Microsoft Teams" from the list of applications

    MS Teams loads slowly and can experience an error – it will ask you if you want to try again – please try again and again if necessary. If MS Teams does not load, it is an NMCI issue with the software, not your CVR account. Consider using a web browser to run MS Teams – see below

    b. Sign in – the user name will default to the CAC number@mil; replace this with the CVR user name provided (ends in @cvr.mil) and provided (temporary) password. If this screen opens, you have to sign out by going to the task tray at the bottom of the screen and right-click on the Teams icon and choose sign out. Then re-launch teams and login with appropriate account.



    c. Follow the prompts for verification, changing the password, and finally for "more information required" for Multi Factor Authentication (MFA).

2. **Use a web browser** – Microsoft Edge or Google Chrome (Microsoft Edge is able to perform most Teams functions on NMCI workstations, except audio & video. Still, there are some features that are not fully supported in the web client on any browser or computer - GFE or personal)
    a. Go to https://teams.microsoft.com
    b. Sign in with the @cvr.mil user name and provided (temporary) password

c. Follow the prompts – for verification and then change password and then the "more information required" for Multi Factor Authentication (MFA).

CVR MS Teams is a cloud base product and it can be accessed from any computer via the web with the proper user name, password, and MFA code. It works best on Edge, but will also work in Chrome

How Do I Keep My Account From Expiring?

For security purposes, CVR user accounts that have not had any successful logins within the **last 7 days** are automatically disabled. This is an ongoing process through the remaining life of the CVR environment.

To prevent disablement, one of the following activities needs to occur:

- Logging-in to Teams (web client, desktop app, or mobile app) using your username/password
- Accessing OneDrive, SharePoint, Forms, Office Online, etc.
- Participating in chat, meetings*, or Live Events*

NOTE: Joining meetings using guest links without logging into your CVR account, does not count as account activity.