AKO Email Shutdown

Quick Reference Guide

NETWORK ENTERPRISE CENTER

This guide explains how the Army is shutting down AKO Email and outlines steps you must take to ensure a smooth transition to full DoD Enterprise Email usage. You can perform all of these steps yourself without an IT technician, but feel free to request help if you prefer to work through the process with assistance or if you encounter any problems.

What is happening to AKO Email?

EXORD 058-11 directed the migration of email services to DoD Enterprise Email (DEE) and ordered the shutdown of all non-tactical legacy email systems, which includes AKO Email.

31 March 2015

Mailboxes on NIPRNet and SIPRNet AKO email systems will be shut down. AKO will continue to forward email for CAC holders until 30 June 2015.

1 July 2015

AKO will stop forwarding email. Any messages addressed to accounts @us.army.mil will be bounced back to the sender as undeliverable. You may still see the "user@us.army.mil" identifier as your username when logging in to Army websites, but it will no longer be a valid email address.

What steps is the Army taking?

The Army is actively transitioning from AKO Email to Enterprise Email:

- Since early 2014, all CACs are issued with the holder's Enterprise Email address.
- Website and application owners are verifying that emails and notifications sent to AKO Email addresses will be updated by 30 June 2015 to send to Enterprise Email or other email addresses.

What steps do I need to take?

To ensure a smooth transition, you should:

- Immediately stop distributing your AKO Email address and advise everyone to use your Enterprise Email address instead.
- Review your various accounts, contact information, and subscriptions that might use your AKO Email address and update them to either your Enterprise Email address or a personal email address (whichever is more appropriate for that particular use).

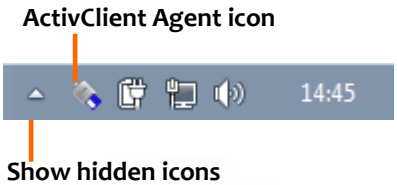
  Utilities ♦ Banks, credit cards, and financial institutions ♦ Mailing lists and newsletters ♦ Professional associations, social groups, and sports leagues ♦ Social media sites ♦ Commercial or subscription sites like Amazon or Netflix ♦ Emergency contacts for family members, such as those for a child's school or a spouse's employer ♦ Backup email for password recovery on commercial email services such as Gmail or Hotmail

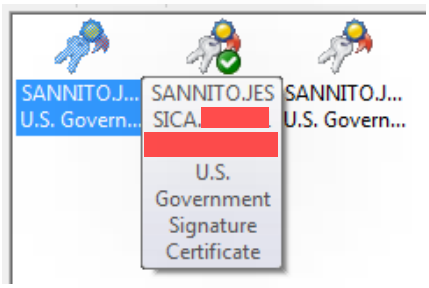
- Check your CAC to ensure that it has your Enterprise Email address on the certificate. If the CAC uses your AKO Email address, update the certificates on the CAC. Instructions are on the following pages.

Are you a DUAL PERSONA with MULTIPLE CACs? Check the certificates on BOTH cards and update them with the correct Enterprise Email addresses (.mil for the military CAC and .civ or .ctr for the other one).

Check Your CAC Certificate

1. In the notification area at the bottom right corner of your primary screen, locate the **ActivClient Agent** icon. (You may have to click the **Show hidden icons** arrow to find it.) Double-click the icon to open the program.
2. In the right window pane, double-click **My Certificates**. You will see icons for three certificates, or four if you are a dual persona with multiple CACs.
3. To see the full name of a certificate, hover over its icon. Locate either the **Signature Certificate** or the **Encryption Certificate** and double-click the icon to open it.
4. Locate the **Email** field and check to see whether it shows your AKO address (us.army.mil) or your Enterprise Email address (mail.mil).





AKO EMAIL (us.army.mil)
Continue following this guide to prepare your CAC for the AKO Email shutdown.

ENTERPRISE EMAIL (mail.mil)
Your CAC is ready for the AKO Email shutdown. You do not need to take further action.

Decrypt Your Files

We use two different methods of encryption:

- **BitLocker** – With BitLocker, the whole hard drive is encrypted.
  - A laptop with BitLocker will show a black screen with white letters at startup and ask you to enter a PIN. A desktop with BitLocker will not ask you for a PIN at startup.
  - To determine if your desktop computer uses BitLocker, click the **Start** button and select **My Computer**. In the list of drives that appears, locate the **OSDisk (C:)** drive. If the icon has a lock and key on it, then BitLocker is in use.

- **EFS** – With EFS, you can encrypt specific folders or files so that only you can open them using your CAC. The names of the encrypted folders and files appear in green letters when you browse your computer. EFS is used on computers without BitLocker and by some people who need an extra layer of protection, or who were using EFS before they got BitLocker.

If you ONLY use BitLocker and do not have any folder or file names in green lettering, you can skip the rest of this section. If you use EFS or if you are not sure, follow these steps to decrypt the files BEFORE you update your CAC. Updating your CAC creates a new encryption certificate; you will not be able to open files encrypted with the old one.

1. Open your **Documents** folder.
2. Select all items that appear in green lettering. (*You can hold down the CTRL button while you click to select multiple items at once.*)
3. Right-click any of the selected items and click **Properties**.
4. On the **General** tab, click **Advanced**.
5. Uncheck the **Encrypt contents to secure data** box and click **OK**.
6. Back in the Properties window, click Apply.
7. Select **Apply changes to this folder, subfolders and files** and click **OK**.
8. A green progress bar will let you know how much time is left to decrypt. Decryption will take longer if you have more files or if the files are very large. When the decryption finishes, click **OK** to close the Properties window.

Any folder or file names that were green should now be black; this shows that they are decrypted. You can repeat these steps for any other locations where you have encrypted files, such as your Desktop.

Remove Your Current Email Certificates from Internet Explorer

1. Open **Internet Explorer**.
2. In the upper right corner, click the **gear icon**, then click **Internet options**.
3. In the *Internet Options* window, click the **Content** tab, then click the **Certificates** button.
4. In the *Certificates* window, the email certificates say **DOD EMAIL CA-##** after your name. You should have two current email certificates. Select both of them. (*You can hold down the CTRL button while you click to select multiple entries at once.*)

If there are email certificates in this list that are expired, you do not have to select and delete them. They allow you to read previously encrypted emails, but won't appear as an option when you log in to CAC-authenticated websites.

5. Click the **Remove** button, then click **Yes** to confirm. **Close** the *Certificates* window.
6. In the *Internet Options* window, stay on the **Content** tab and click the **Clear SSL state** button.
7. Close the *Internet Options* window and Internet Explorer.

Update the Email Address on Your CAC

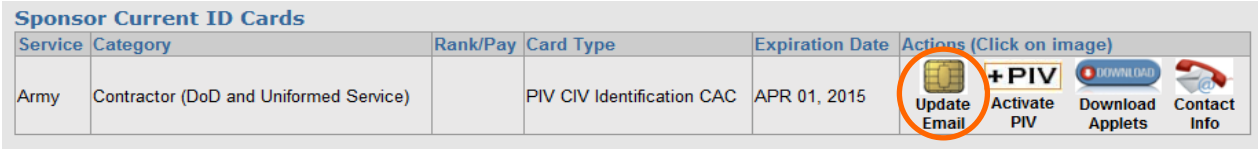
DUAL PERSONAS: If your computer is configured for dual personas, you will need to use a different computer for this step. Have the primary user log in to the computer, then insert your CAC into a secondary reader to log into the RAPIDS site.

Log in to the RAPIDS Self Service Portal

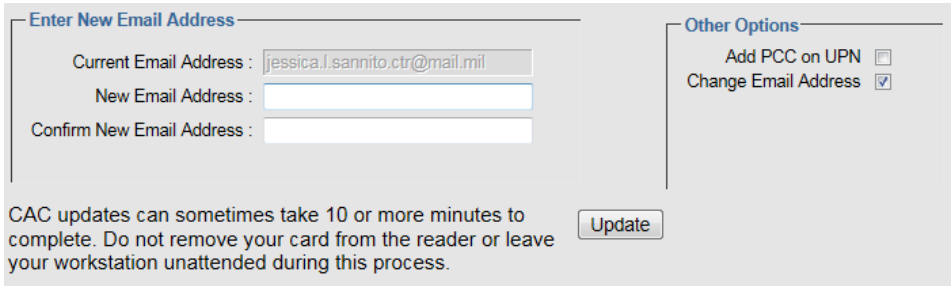
1. You must use the 64-bit version of Internet Explorer rather than the default 32-bit version. Click the **Start** button, then click **All Programs**. Near the top of the list, click **Internet Explorer (64-bit)**.
2. Navigate to the RAPIDS Self Service Portal at **https://www.dmdc.osd.mil/self_service** and click **Sign On** to access the RAPIDS application. Review the Self-Service Consent to Monitor and click **OK**.
3. Under the picture of a sample CAC, click the **Login** button.
4. When you are prompted to select a certificate, click your **NON-EMAIL certificate**. This is the one that lists the issuer as **DOD CA-##**. If needed, enter your CAC PIN and click **OK**.

Update the Email Address on Your CAC

1. The RAPIDS Self Service page will show a list of your current ID cards. Most people will only have one listed, but dual personas will have multiple entries. For the card that you want to update, click the **Update Email** icon.



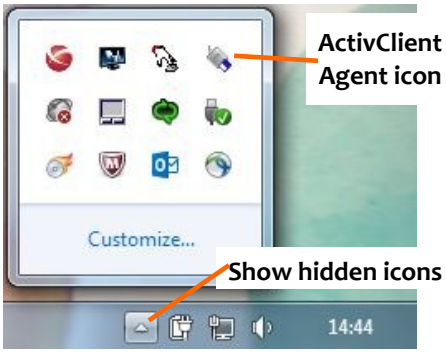
2. Wait a few minutes for the site to read your CAC. You will get a pop-up asking if you want to run the ID Card Office Online Applet. Click **Run**. You may need to wait a few more minutes for the site to finish reading your CAC.
3. Check the **Update Email Address** box, then type your Enterprise Email address in the **New Email Address** box and again in the **Confirm New Email Address** box. Click **Update**.



4. **DO NOT REMOVE YOUR CAC FROM THE READER OR RESPOND TO PROMPTS FOR YOUR CAC PIN** (such as those from other websites or from Outlook) **WHILE THE RAPIDS SITE IS UPDATING YOUR CERTIFICATES.** It can take 10 or more minutes for this process to finish. When the process is complete, you will see a message that says, "Congratulations! Your CAC has been successfully updated."
5. In the upper right corner of the site, click the **Log Off** link, then close Internet Explorer 64-bit.

Make New Certificates Available to Windows

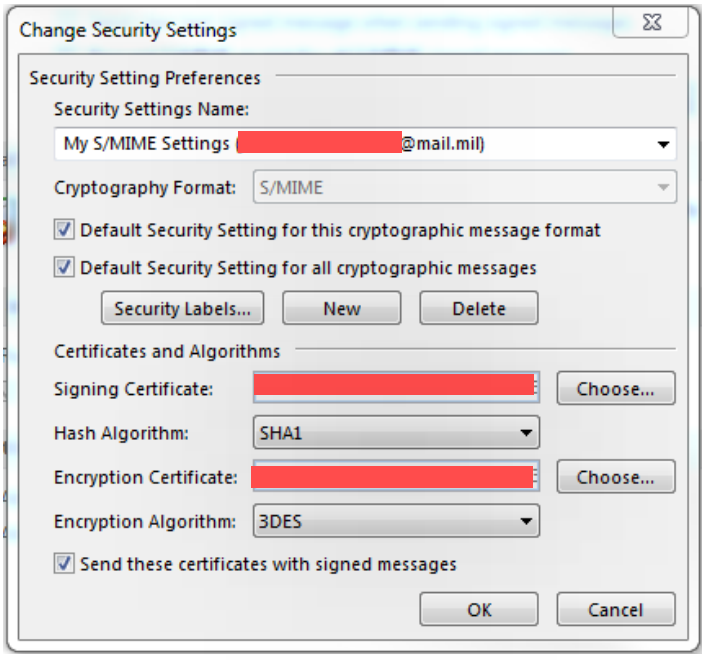
1. In the notification area at the bottom of the screen, next to the clock, click the **ActivClient Agent icon**, then click **Open**. The icon looks like an external CAC reader with a blue card sticking out. (*You may have to click the **Show hidden icons** arrow to see it.*)
2. In the ActivClient window, click **Tools** > **Advanced** > **Forget state for all cards**.
3. Click **Tools** > **Advanced** > **Make Certificates Available to Windows**. When ActivClient has finished loading your certificates, click **OK**.
4. Close ActivClient.



Publish New Certificates in Outlook 2013

1. Open Outlook and log in to your mailbox with your CAC PIN.
2. Click **File**. On the left menu, click **Options**. On the left side of the *Outlook Options* window, click **Trust Center**, then click the **Trust Center Settings** button. On the left side of the *Trust Center* window, click **E-mail Security**.
3. Delete your existing certificates:
    a. In the *Encrypted e-mail* section, find the **Default Setting** box and click the **Settings** button next to it.
    b. In the *Change Security Settings* window, find the **Delete** button in the middle of the window and click it until the box at the top of the window is blank. Click **OK** to close the window.
    c. Click the **Publish to GAL** button, then click **Yes** to remove your previously published settings. Click **OK** to confirm that the certificates were removed successfully.
4. Next to the **Default Setting** box, click the Settings button again. The *Change Security Settings* window should automatically fill in your name and certificates. Click **OK**.

    If the window is NOT filled in automatically, make sure the settings match these, then click **OK**.
    - **Security Settings Name**: Type your name.
    - **Cryptography Format**: S/MIME
    - Check both **Default Security Setting** boxes
    - **Signing Certificate**: Click **Choose** and select your **EMAIL** certificate
    - **Hash Algorithm**: Select **SHA1**
    - **Encryption Certificate**: Click **Choose** and select your **EMAIL** certificate
    - **Encryption Algorithm**: Select **3DES**
    - Check the **Send these certificates with signed messages** box.



5. Click the **Publish to GAL** button, then click **OK** to confirm.
6. Outlook will tell you that your certificates were published successfully. Click **OK** to dismiss the message, then close the Trust Center window.

Certificates are usually fully published right away, but sometimes it can take up to 24 hours for the changes to take effect. You may be unable to send or receive encrypted messages during this time. After 24 hours, please try sending again or ask the sender to resend to you. If you still cannot send or receive encrypted messages, please call AESD to submit a ticket.

Recover Your Old Email Certificate

In order to open encrypted email that was sent to you before you updated your CAC, you will need to recover the old email certificate. This recovery method stores your certificate so that Outlook can use it to open older encrypted messages, but you won't see it in your list of certificates when logging in to websites.

1. Go to the Automated Key Recovery site at https://ara-1.c3pki.chamb.disa.mil
   If this site is not working, use the secondary site at https://ara-2.c3pki.den.disa.mil
2. To log in, select your **NON-EMAIL certificate**, which lists the issuer as **DOD-CA##**. Click **OK** to acknowledge the security statement.
3. Wait while the site generates a list of your old e-mail certificates. Each certificate shows a date range for when it was valid. Locate the appropriate certificate, then click the **Recover** button next to that certificate. Click **OK** to acknowledge the security agreement.
4. Wait while the site generates your key and a one-time password. Click the blue **DOWNLOAD** link, then click **Open**.
5. A Certificate Import Wizard window will open. Move this window to one side of the screen so that you can still read the password on the key recovery site.
6. Click **Next** to start the wizard, and **Next** again to confirm the certificate file.
7. Type the password into the wizard exactly as it is displayed on the key recovery site, then click **Next**.
8. Click **Next** to accept the default certificate store, then click **Finish**.
9. You will get a message confirming certificate import. Click **OK**, then on the key recover site click **Logout**.

Encrypt Folders or Files

If your computer has BitLocker, then the whole hard drive is encrypted and you can skip this section.

If your computer does not have BitLocker or if some of your data requires extra protection, follow these steps.

1. Open your **Documents** folder.
2. Select all items that you want to encrypt. (You can hold down the CTRL button while you click to select multiple items at once.)
3. Right-click any of the selected items and click **Properties**.
4. On the **General** tab, click **Advanced**.
5. Check the **Encrypt contents to secure data** box and click **OK**.
6. Back in the Properties window, click Apply.
7. Select **Apply changes to this folder, subfolders and files** and click **OK**.
8. A green progress bar will let you know how much time is left to encrypt. Encryption will take longer if you have more files or if the files are very large. When the encryption finishes, click **OK** to close the Properties window.

The names of the items you selected should now be green; this shows that they are encrypted.

If you encounter any problems or need assistance,
please contact the Army Enterprise Service Desk (AESD) at 1-866-335-2769(ARMY) to submit a ticket.

If you are a dual persona with multiple CACs,
remember to update both cards with the correct Enterprise Email addresses.

Remember to check your non-Army accounts, subscriptions, and contact information
to update your email address if any of them use your AKO Email.