

PIV Certificate Activation Steps

In order to access DOD Enterprise Portal Service (DEPS) and/or Enterprise Email (EE), you will need to activate your PIV certificate if you are (or were) a dual persona user. The web site to do so is https://www.dmdc.osd.mil/self_service.

To use functions within RAPIDS Self Service to update your CAC you must have the following installed on your computer:

ActivClient (32-bit), JRE (32-bit) and a 32-bit browser (such as Internet Explorer 32-bit)

Or

ActivClient (64-bit), JRE (64-bit) and a 64-bit browser (such as Internet Explorer 64-bit)

Step 1 - After entering the link in your browser you should see the following.

Available Features/Actions

Sponsor:	Add/Change email address to receive initial or new Email Signature and Email Encryption Certificates Add Personnel Category Code to the User Principal Name of the Email Signature Certificate Activate the PIV Authentication Certificate Download applications View/Update contact information It is the Sponsor's responsibility to review and update all appropriate information as needed before requesting reissuance of ID cards for any family member.
Family Members:	View/Update contact information Request application for reissuance of ID card

For issues with your ID card or problems with sponsor or family member data, please contact your preferred RAPIDS ID card [facility](#).
For problems with this application [contact us](#).

Step 2 - Click 'Sign On'. You should see the following.

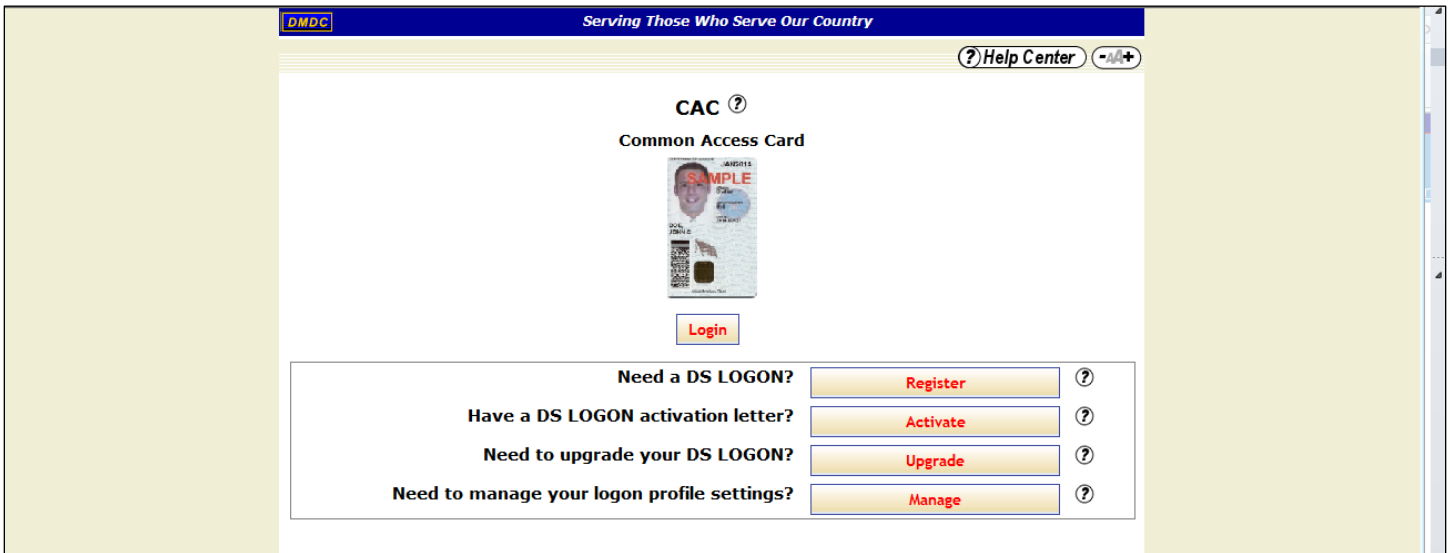
Self-Service Consent to Monitor

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG beneficiary self-service-authorized use only.

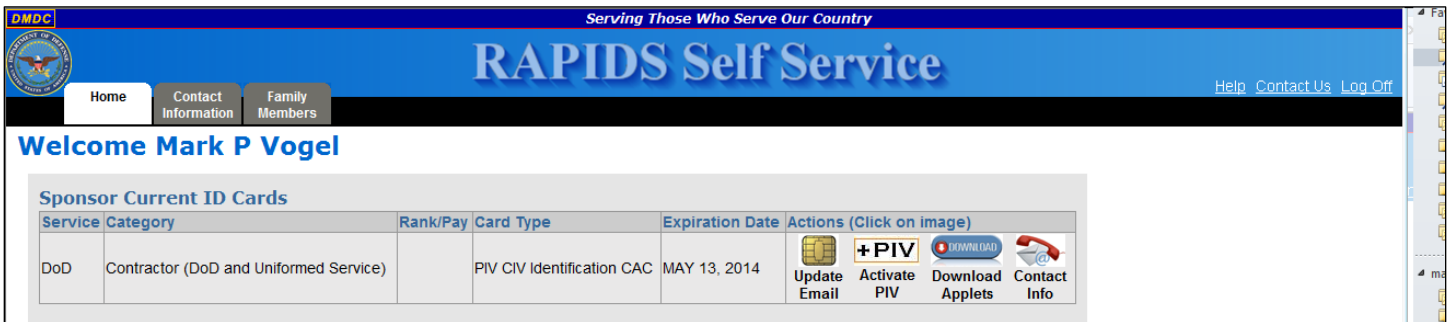
By using this IS (which includes any device attached to this IS), you consent to the following conditions:


- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- While all personal identifying information (PII) data stored on this IS is protected under the Privacy Act of 1974, all communications using this IS, and the data captured to support this IS, are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

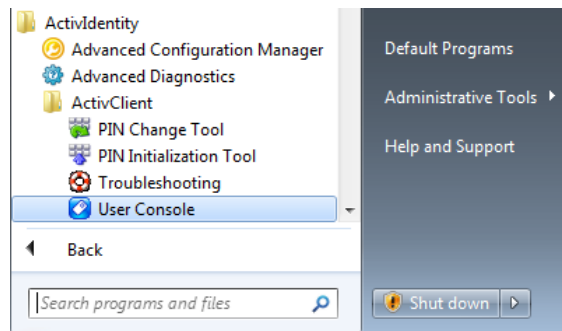
Step 3 - Click 'OK'. You should see the following.



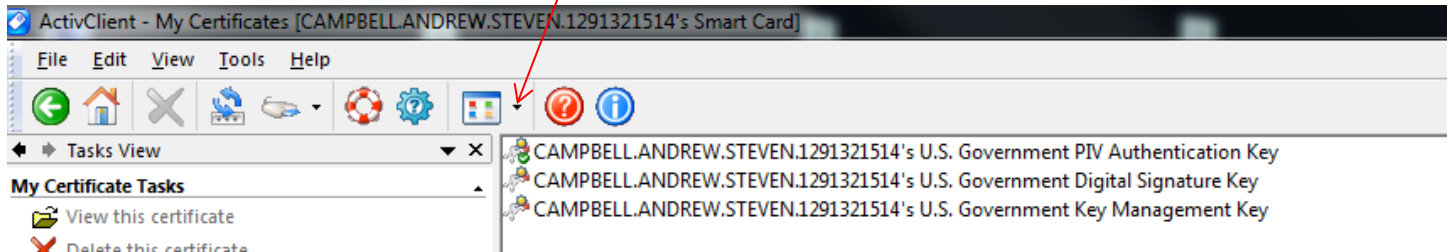
Step 4 - Click 'Login' and select your email certificate. You should see the following.



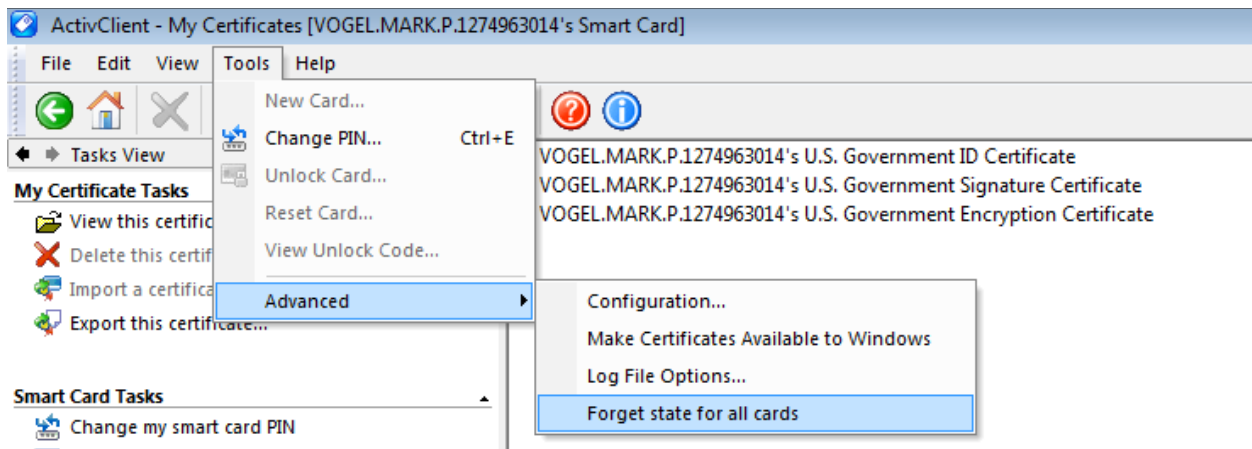
Step 5 - Click on 'Activate PIV' and follow the instructions. Once complete, you should be done with the RAPIDS web site. Next click on the Microsoft start button , go to the ActivIdentity folder, then the ActivClient Folder and click on 'User Console'.



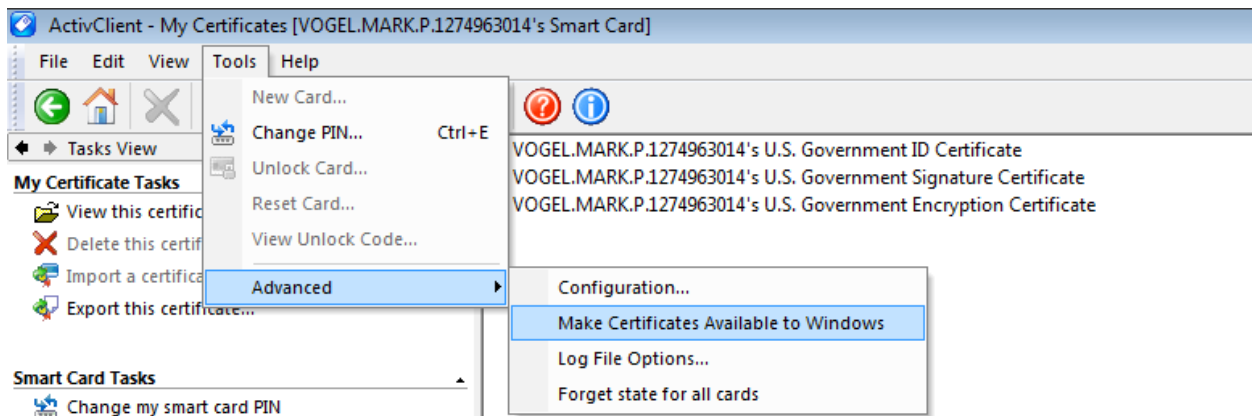
Step 6 – Double click on my certificates. Click on views and select list. You should now see a PIV Authentication Key certificate in your certificate list. If not, step 5 did not complete successfully.



Step 7 – Go to Tools → Advanced and select 'Forget state on all cards'. Remove and reinsert the smart card in the smart card reader.



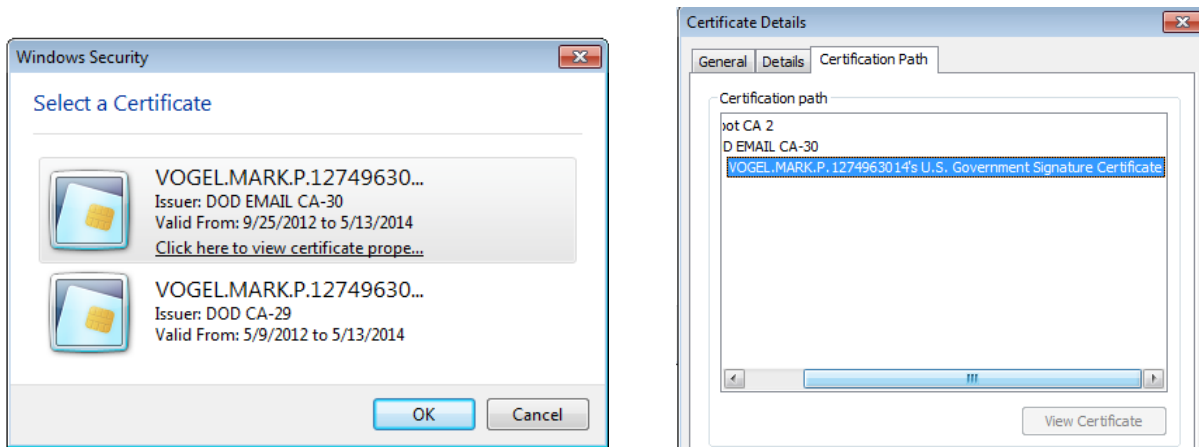
Step 8 – Go to Tools → Advanced and select 'Make Certificates Available to Windows'.



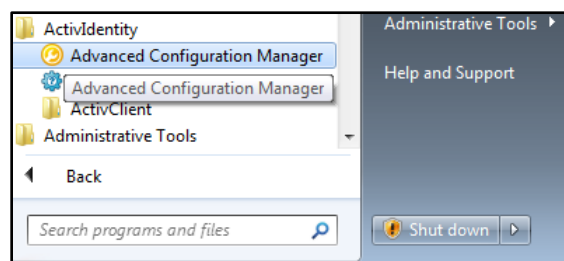
Step 9 – You should get a confirmation message similar to the following.



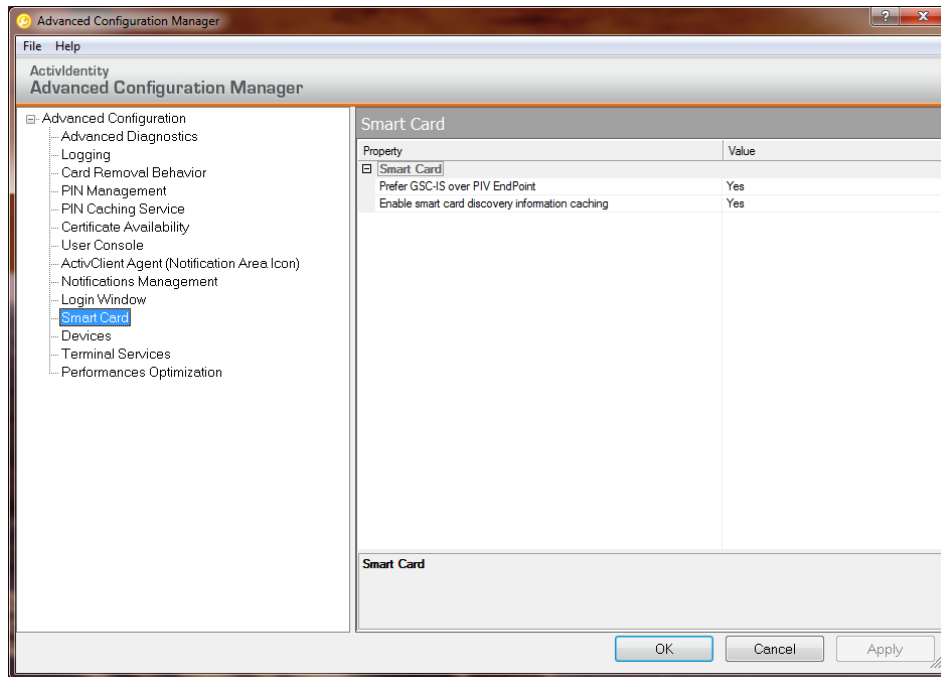
Step 10 - Your PIV certificate should now be available to you when you attempt to log into DEPS; you *MUST* select the PIV certificate in order to gain access. However, which certificate is the PIV certificate is not obvious. For each certificate in your list, click on the 'Click here to view certificate properties' link. Go to the 'Certification Path' tab and scroll all the way to the right. Continue with each certificate in the list until you find the PIV certificate.



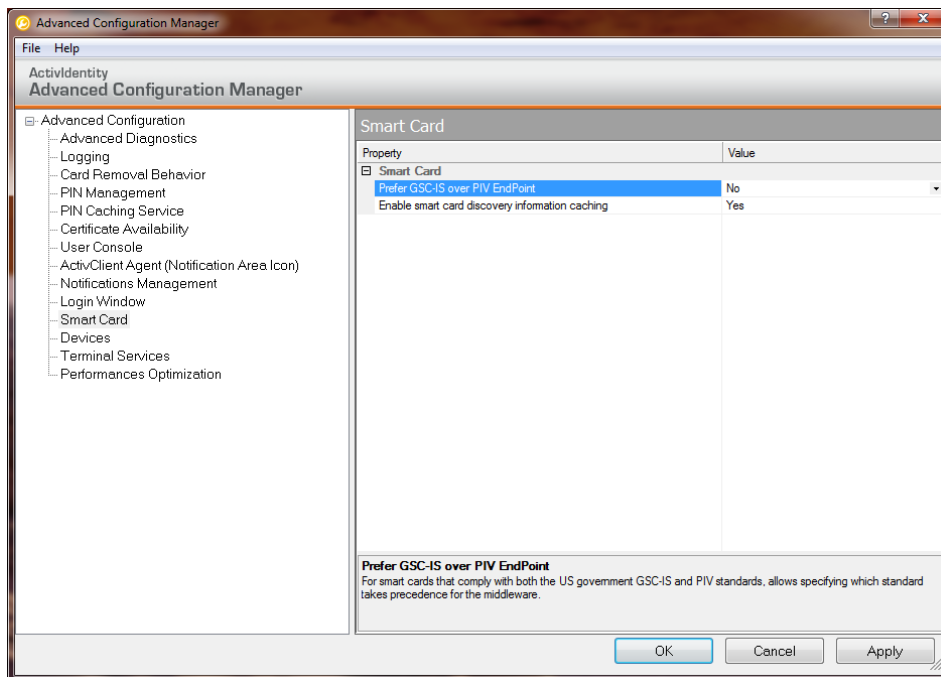
Step 11 – If your PIV is still not available after step 10, someone with administrator rights to the computer in question needs to open Active Client 'Advanced Configuration Manager'.



Step 12 – Select ‘Smartcard’ from the list.



Step 13 – From the Smart Card Window below select ‘Prefer GSC-IS over PIV EndPoint’ and change the value to no. Click ‘Apply’ and then ‘OK’.



Step 14 – Reboot the computer. The computer should then begin to recognize the PIV Certificate.

If you are an end user and you are still experiencing problems you will need to contact your level 1 service desk representative. If you call DISA Mechanicsburg level 2 service desk directly we will direct you to your level 1 service desk.