



Tactics, Techniques, and Procedures for Activating your "PIV Authentication" Certificate

12 February 2019

DOD EE TTP-6 (original) Version 2.3

EXECUTIVE SUMMARY

This Tactics, Techniques, and Procedures (TTP) document describes the processes for activation of the PIV Authentication Certificate on a Common Access Card, which they will then use to authenticate to DoD Enterprise Email (EE).

DOCUMENT REVISIONS LIST

VERSION	DATE	DESCRIPTION OF CHANGES	ORGANIZATION
1.0	23 Jan 13	Initial (Army) Version	HQDA CIO/G6 (LTC Barclay)
1.1	23 Jan 15	Updates based on RSS changes, updated screenshots, adding trusted sites to Java security	PO EE, PEO EIS, (Peter Barclay)
1.2	24 Feb 15	Additional of clarification on why PIV Auth certs are required	DISA, DMDC, PEO EIS
2.0	15 May 15	Beta site functionality move to main RSS site. URL and screenshots updated	DMDC, Army PEO EIS - PO EE
2.1	11 Apr 18	Additional URL in Java Control Panel, new screenshots.	NETCOM
2.2	11 Nov 18	Update Java screenshots to ver 8 and certificate selection	GCE
2.3	2 Feb 19	Update version numbers	GCE

TABLE OF CONTENTS

1 Why is the PIV Authentication certificate required?	
2 The PIV Authentication Certificate Activation Process	1
3 System Requirements	1
4 Ensure that your computer will trust the websites	2
5 Installing the DoD Trust Chain	5
6 Verifying ActivClient for the Department of Defense configuration	
7 Access RAPIDS Self Service portal	
8 Confirmation	
9 What can be done to make the PIV Authentication requirement "go away"?	
10 Applet Log	
11 Supporting Documentation	
A. Verifying Versions of IE, JRE, and ActivClient	
Internet Explorer (IE)	
Java Runtime Environment (JRE)	
ActivClient	
B. Verifying Bit Versions of IE, JRE, and ActivClient	
Internet Explorer (IE)	
Java Runtime Environment (JRE)	
ActivClient	
TABLE OF FIGURES	
Figure 1 – Java icon in the Control Panel	
Figure 2 – The Java Control Panel	3
Figure 3 – Security tab in the Java Control Panel	
Figure 4 – Adding sites to the Exception Site List	
Figure 5 – Control Panel – Programs and Features	
Figure 7 – Modify Program	
Figure 8 – US Department of Defense configuration	
Figure 9 – 03 Department of Defense configuration	
Figure 10 – RAPIDS Self Service website	
Figure 11 – Consent to Monitor	
Figure 12 – CAC Login to RSS	
Figure 13 – Selecting ID certificate	
Figure 14 – Select the correct CAC and click "Activate PIV Certificate"	
Figure 15 – Ready to activate the PIV Auth certificate	
Figure 16 – Reading data from the CAC – 0%	
Figure 17 – Accepting the Java applet	
Figure 18 – Update Confirmation	
Figure 19 – Starting PIV Activation request to Post Issuance Portal	
Figure 20 – Request to the LCM User Portal	
Figure 21 – Enter CAC PIN	
Figure 22 – Activating PIV Authentication Certificate	
Figure 23 – Update Complete	
Figure 24 – Launching ActivClient	
Figure 25 – Opening My Certificates	
Figure 26 – Verifying all four certificates are visible	
5 - 7 5 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 -	

1 Why is the PIV Authentication certificate required?

The Under Secretary of Defense for Personnel and Readiness and the DoD Chief Information Officer (CIO) will mandate that all DoD Components transition NIPRNet PKI-enabled IT resources use the PIV Auth certificate for authentication. While new CACs issued since February 2018 have the PIV Auth certificate activated, older CACs might not have that PIV Auth certificate activated. The RAPIDS self-service portal (RSS) provides for this capability. ID Card Office Online (IDCO) is also an acronym for the RAPIDS self-service portal.

Note – RSS and IDCO acronyms are used interchangeably.

2 The PIV Authentication Certificate Activation Process

Being able to use a PIV Auth cert is a two-step process. Activate the PIV Auth certificate using RAPIDS Self Service (RSS), and then make the certificate available to Windows.

The RAPIDS Self Service portal has many features and capabilities but has two different options for activating the PIV Auth certificate. This document is about using that new capability.

3 System Requirements

To take advantage of the time-saving benefits that RSS-IDCO provides to Sponsors and family members, your computer must meet the following minimum system requirements:

- Installed Browser and Programs: Your computer must have the following installed to run RSS-IDCO. See *Verifying Versions of IE, JRE, and ActivClient* to determine which versions are installed on your computer:
 - Internet Explorer (IE) 7 or higher (IE 11 is current),
 - Java Runtime Environment (JRE) (1.7.151- b33 or 1.8.144 or higher, version 8 update 201 is current)
 - ActivClient (we recommend version 7.1.0.190 + FIXS1711008 or higher), please note that older versions than 7.1x have reached end-of-life and are no longer supported by HID
- Bit Versions: IE, JRE, and ActivClient must be the same bit version (all 32-bit or all 64-bit) so that you can perform CAC updates successfully on your computer. See Verifying Bit Versions of IE, JRE, and ActivClient to determine the bit version.
- Trusted Site: RSS-IDCO must be listed as a Trusted Site so that you can perform CAC transactions online. See <u>Adding RSS-IDCO as a Trusted Site</u> for instructions.

4 Ensure that your computer will trust the websites

The new PIV Auth activation capability makes use of some enhanced Java features and we have found that most DoD computers don't trust the DMDC websites providing the Java application. Although you can set either IE or Java to trust the websites, it is simplest to have Java trust those sites.

1) Open the "Control Panel" on your computer and then double-click the Java icon to open the Java Control Panel.



Figure 1 – Java icon in the Control Panel

2) On the Java Control Panel, select the "Security" tab.

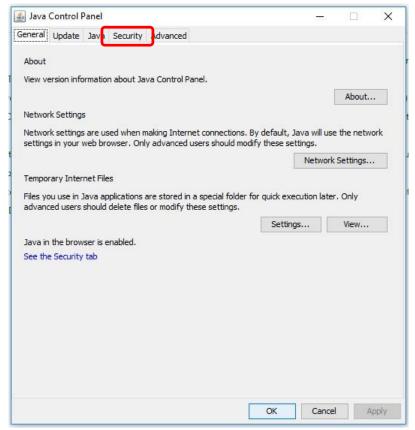


Figure 2 – The Java Control Panel

- 3) On the Security tab, make sure the following three sites are in the "Exception Site List" area:
 - https://www.dmdc.osd.mil
 - https://pki.dmdc.osd.mil
 - https://idco.dmdc.osd.mil

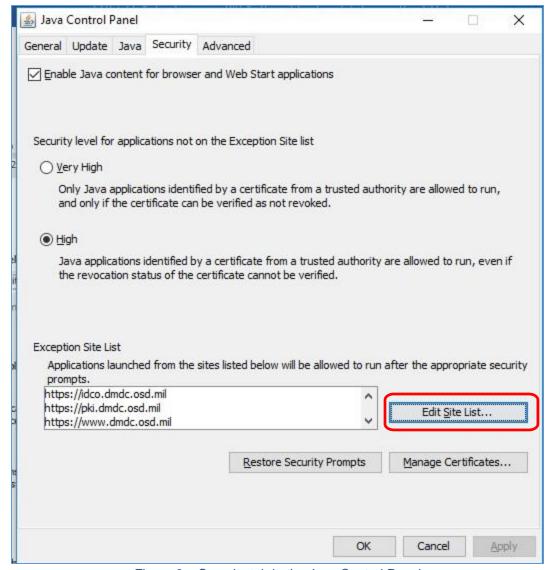


Figure 3 – Security tab in the Java Control Panel

- 4) If those three sites are not listed, they will need to be added. Click the "**Edit Site List...>**" button.
- 5) Add the three URLs (site addresses) to the Location list, clicking the **<Add>** button to add each new line in the table.

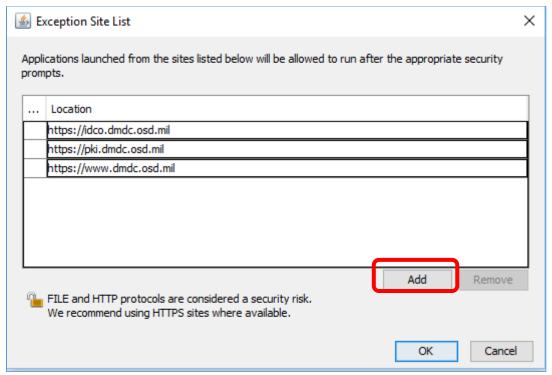


Figure 4 – Adding sites to the Exception Site List

6) Click **<OK>** once all three site addresses are listed and then click **<OK>** to close the Java Control Panel.

5 Installing the DoD Trust Chain

<u>If you are running IDCO from your home computer</u>, you will need to install the DoD certificate trust chain as it is not installed by default by Microsoft. You will need it to update your CAC (it should already be installed on your DoD workstation).

- 1) To install this DoD certificate trust chain, go to this location: https://iase.disa.mil/pki-pke/Pages/tools.aspx
- 2) If you scroll down that page look for a section called 'Trust Store'. Within Trust Store is a subsection titled 'InstallRoot 5.2: NIPR Windows Installer'.
- Select the appropriate link on your operating system either 32-bit Installer, 64bit Installer, or Non Administrator. A file will be downloaded to your local workstation.
- 4) Launch that .msi to install the DoD trust chain.

6 <u>Verifying ActivClient for the Department of Defense configuration</u>

STOP. This is for home use or contractor-owned owned workstations only. If you

are using a DoD government workstation, please skip this section!

It is possible your ActivClient is installed in the Federal PIV configuration – if so, you must change this to the Department of Defense configuration. To make this change do the following:

- 1) Launch Control Panel
- 2) Within Control Panel, select Programs and Features

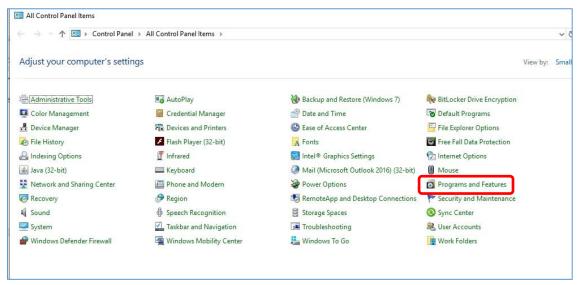


Figure 5 - Control Panel - Programs and Features

3) Select ActivID ActivClient and Change, then Next

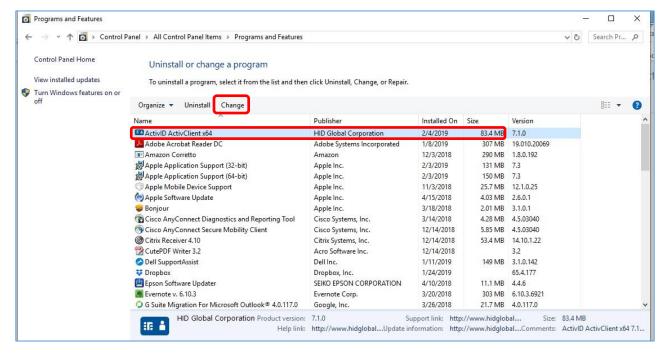


Figure 6 - Change ActivID ActivClient

4) Select **Modify**, then **Next**

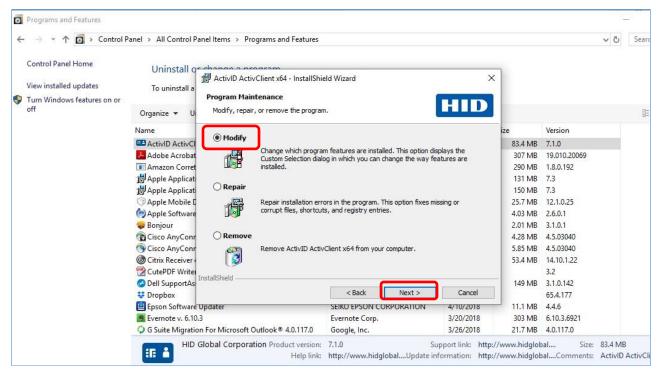


Figure 7 – Modify Program

5) Under Common Services choose US Department of Defense configuration

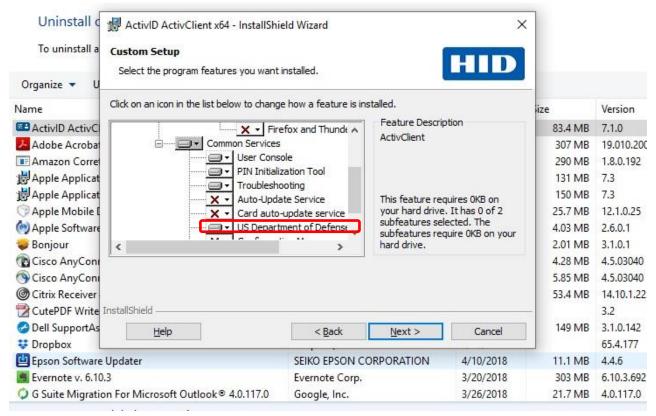


Figure 8 – US Department of Defense configuration

6) Select **Install** to complete change

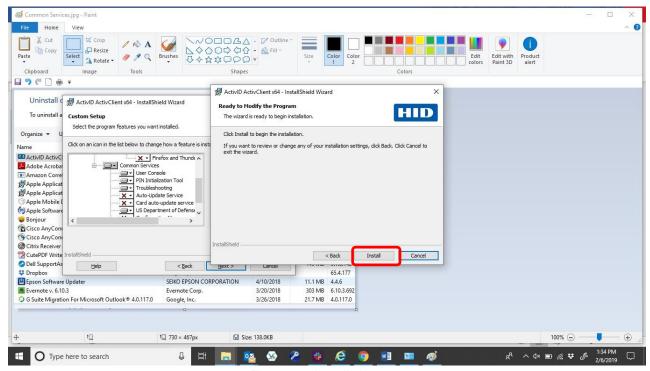


Figure 9 - Install changes

7 Access RAPIDS Self Service portal

- Ensure that your CAC is inserted into its reader and sign on to the RAPIDS Self Service Portal by going to: https://www.dmdc.osd.mil/self_service/
- 2) When the RSS website opens click the **<Sign In>** button.

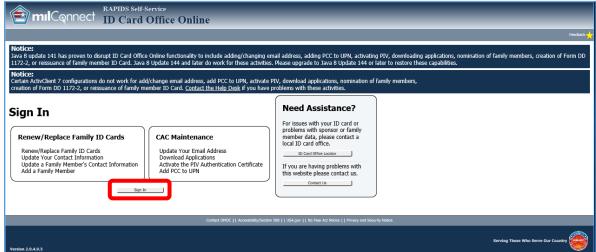


Figure 10 – RAPIDS Self Service website

3) Accept the DoD Notice and Self-Service Consent by clicking <OK>

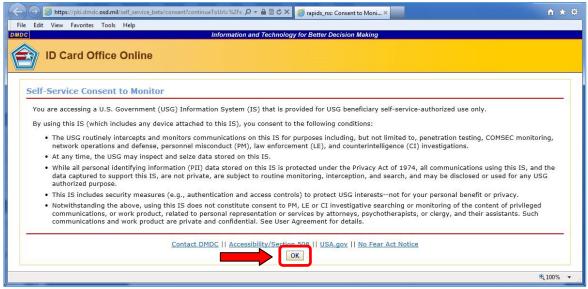


Figure 11 – Consent to Monitor

4) Click the < Login > button.



Figure 12 - CAC Login to RSS

5) When the dialogue box with your certificates pops us, select the "DoD ID" certificate and click the **<OK>** button.

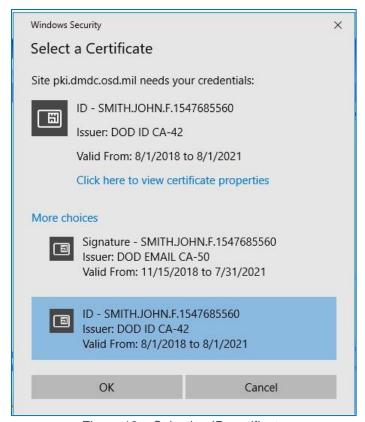


Figure 13 – Selecting ID certificate

6) Once the RAPIDS Self-Service webpage opens for you, select the "<Activate PIV certificate>".



Figure 14 – Select the correct CAC and click "Activate PIV Certificate"

7) Once you click "Activate PIV certificate" you will get a confirmation screen. Click the **Proceed>** button.

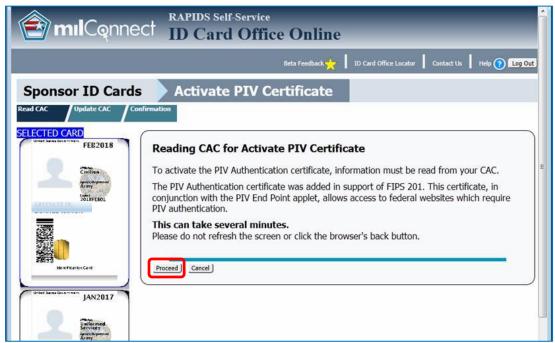


Figure 15 - Ready to activate the PIV Auth certificate

The Java applet will read the CAC.

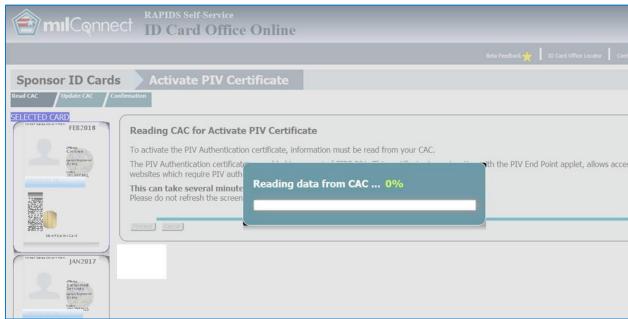


Figure 16 – Reading data from the CAC – 0%

8) The Java applet from the DMDC ID Card office software will appear and ask for confirmation to execute the applet. If you plan to use IDCO again you can select the 'Do not show again' button from the dialog display.



Figure 17 – Accepting the Java applet

Click "<Run>". to continue when you get the pop-up screen.

Once the Java applet executes, the portal will verify that you want to expose the PIV certificate and update the CAC.

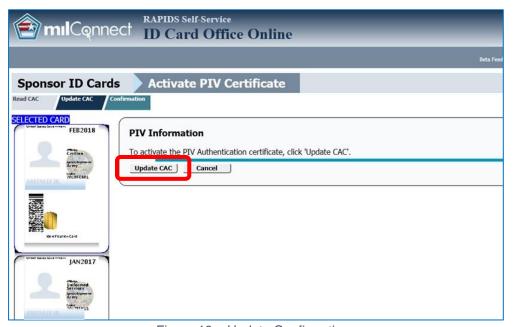


Figure 18 – Update Confirmation

9) DO NOT REMOVE THE CARD FROM THE READER. It can sometimes take a few minutes for the application to read all the details and then updated the CAC, exposing the certification. Be patient.

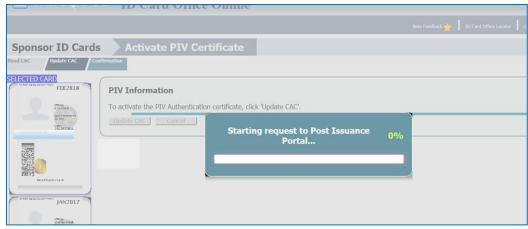


Figure 19 – Starting PIV Activation request to Post Issuance Portal

The application will walk through the process, contacting the portals necessary to complete the process.

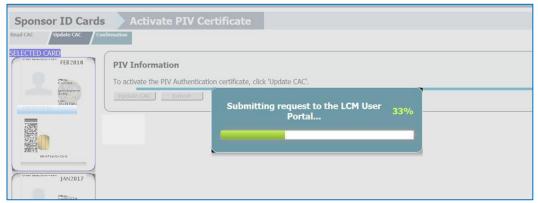


Figure 20 – Request to the LCM User Portal

There may be occasions when you will need to re-enter your PIN for your CAC. This is normal but be careful as the PIN entry popup will 'lose focus' during the PIN entry process and you might need to click within the PIN entry box multiple times before completing your PIN entry.

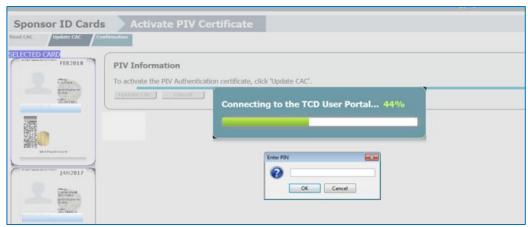


Figure 21 - Enter CAC PIN

The application will continue and will activate your PIV Authentication certificate.

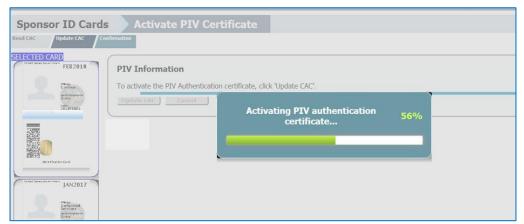


Figure 22 – Activating PIV Authentication Certificate

10) The application will continue and will complete the activation of your PIV Authentication certificate. When finished, it will notify you that the update is complete.



Figure 23 - Update Complete

11) Once the CAC update is complete, click on the Home button

NOTE: If the "Activate PIV Authentication Certificate" update process failed to run, or the update failed, the user will need to visit their local Defense Enrollment Eligibility Reporting System/RAPIDS (DEERS/RAPIDS) office to obtain a new CAC because the current CAC is too old and does not contain the PIV Auth certificate.

8 Confirmation

1) Open <u>ActivClient</u> by double clicking the CAC icon in the system tray (bottom right corner of the screen).



Figure 24 - Launching ActivClient

2) Now, double click <My Certificates>.

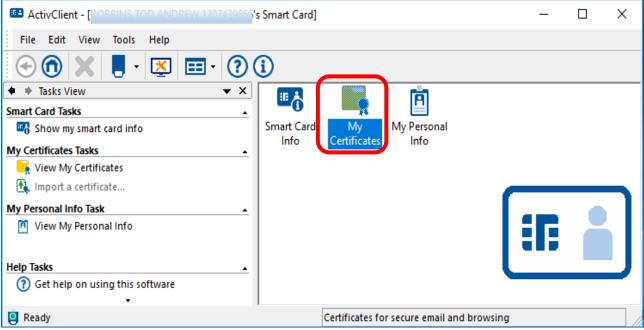


Figure 25 – Opening My Certificates

3) Ensure that four certificates are displayed like below:

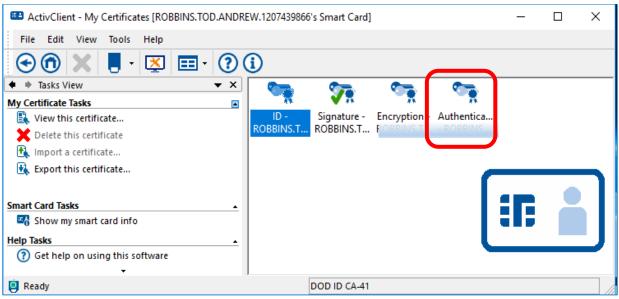


Figure 26 – Verifying all four certificates are visible

NOTE: If the Authentication Certificate is not displayed in this step, activation failed. The user will need to visit their local DEERS/RAPIDS office to obtain a new Common Access Card because the CAC is too old and/or does not contain the PIV Auth certificate.

9 What can be done to make the PIV Authentication requirement "go away"?

You can't. The important phrase to understand is "Once PIV Auth, always PIV Auth". Once an individual is required to use the PIV Authentication certificate to authenticate to enterprise services provided by DISA, the user will **always be required to use the PIV Authentication certificate**, even after they only have one CAC. The enterprise system can identify when a duplicate entry exists, and so both records are changed from using the email certificate to using the PIV Authentication certificate (because the credentials provided by the email certificates of an individual are identical and the system cannot distinguish between them using the email certificates).

10 Applet Log

If you encounter issues during your CAC update you might be asked to provide your applet log to the service desk for advanced troubleshooting. The applet log is in the following location: C:\Users\<User Name>\AppData\Local\Temp\rss_applet.log

11 **Supporting Documentation**

A. Verifying Versions of IE, JRE, and ActivClient

Internet Explorer (IE)

To verify the IE version:

Press **Alt+H** on your keyboard and click **About Internet Explorer**. The version number appears beside "Internet Explorer."



Java Runtime Environment (JRE)

To verify the JRE version:

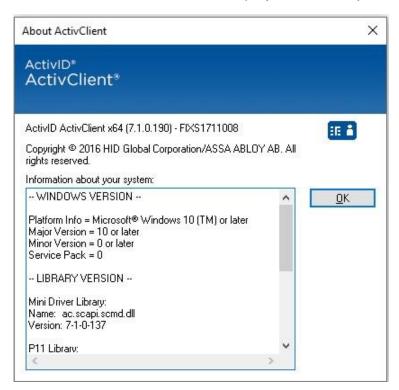
- 1. Click **Start** and select **Control Panel**.
- 2. In the upper-right corner, select **Small icons** in the *View by:* drop-down menu.
- 3. Click Java.
- 4. Under the **General** tab, click **About**. The version number displays in the "About Java" window.



ActivClient

To verify the ActivClient version:

- 1. Click **Start** and select **All Programs**.
- 2. Navigate to the ActivIdentity>ActivClient and select User Console.
- 3. In the "ActivClient" window, click **Help** and select **About ActivClient**. The version number displays in the "Major Version" section.



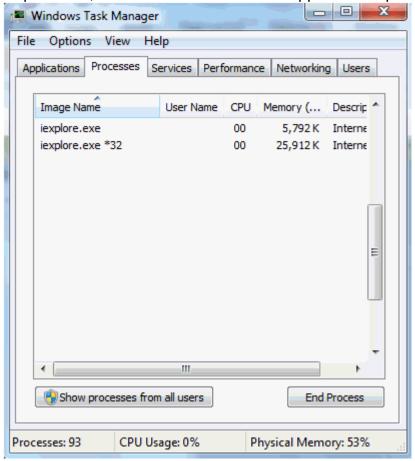
B. Verifying Bit Versions of IE, JRE, and ActivClient

Internet Explorer (IE)

To verify the bit version of IE:

- 1. Press Ctrl+Alt+Delete on your keyboard.
- 2. Click Start Task Manager.
- 3. In the "Task Manager" window, click the **Processes** tab.

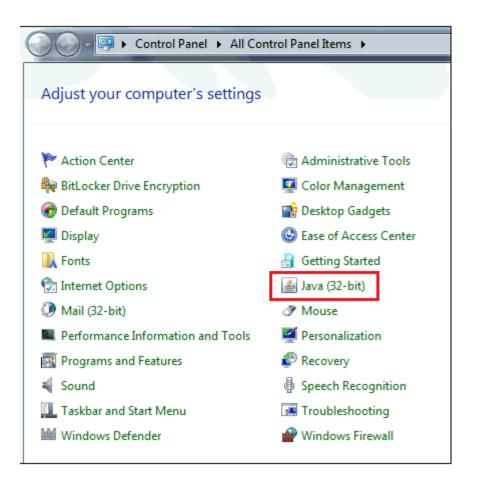
Locate "iexplore.exe" in the *Image Name* column. The 64-bit version of IE will appear as iexplore.exe; the 32-bit version of IE will appear as iexplore.exe *32.



Java Runtime Environment (JRE)

To verify the bit version of JRE:

- 1. Click Start and select Control Panel.
- 2. In the upper-right corner, select **Small icons** in the *View by:* drop-down
- 3. Locate "Java". The number that appears indicates the bit version.



ActivClient

To verify the bit version of ActivClient:

- 1. Click **Start** and select **All Programs**.
- 2. Navigate to the **ActivIdentity>ActivClient** and select **User Console**.
- 3. In the "ActivClient" window, click **Help** and select **About ActivClient**. The 64-bit version of ActivClient will appear as x64; the 32-bit version of ActivClient will appear as ().