



# Mobile Credentialing Unit Setup Guide

Version 2.1.0

April 29, 2019



The information contained in this document is proprietary and may not be transmitted or disclosed to anyone outside of the Government or authorized representatives without written permission.

## Revision Table

Version	Primary Author(s)	Description of Version	Date Completed
1.0	DXC Technology	Initial Draft	10/04/2017
1.1	DXC Technology	Updated ActiveX Controls to v4.3, Java to Update 151, and PCA Version.	12/14/2017
1.2	DXC Technology	Updated PCA and Java	01/31/2018
1.2.1	DXC Technology	Added Local Print instructions	02/07/2018
1.4.0	Perspecta	Added ActivClient Hotfix 7.1.0.210, updated Java 8 to Update 181, and updated Assured Identity controls. Removed Windows Hosts File Entries section from Re-Image instructions. This section is not needed.	07/20/2018
1.4.1	Perspecta	Updated software versions to: ActiveX Controls v4.3.1, CyberArmed PCA v1.5.12.1865, CyberArmed PCA BioAdaptor v1.6.56, CyberArmed PCA Activation Module v1.6.1.1 and CyberArmed BioAdaptorConfigure v1.1.0.	09/28/2018
2.0.0	Perspecta	Added section 1.6 Camera Settings. Updated ActiveX Controls, ActivClient Hotfix, PCA, Java 8 to update 191.	01/09/2019
2.1.0	Perspecta	Updated to the following versions: ActivClient Hotfix 7.1.0.244, Java 8 Update 201, USAccess AICSmartcardControl 1.0.0, USAccess CU Desktop Shortcuts 3.0.0, USAccess Install Manager CU 6.0.0, USAccess Network Test Tool 8.0.0, USAccess System Info 6.0.0.  Updated Scheduler icon on desktop to AI Scheduler, and directed it to the new AI Scheduler. Assured Identity icon goes directly to Enrollment application rather than AISSO menu.	04/29/2019

# Table of Contents

<b>1.0</b>	<b>Mobile Credentialing Unit Setup</b> .....	<b>1</b>
1.1	Who Is Needed for Setup?.....	1
1.2	How Long Will it Take to Setup? .....	1
1.3	Component Unpacking.....	1
1.4	Credentialing Unit Set-Up .....	2
1.5	Workstation Setup.....	2
1.6	Camera Settings .....	5
1.7	USB Cables.....	7
1.8	Power on the Laptop.....	10
1.9	Enter System ID in Site Manager.....	11
<b>2.0</b>	<b>Testing the MCU</b> .....	<b>11</b>
2.1	Network Test Tool.....	11
2.2	Testing Enrollment .....	13
2.3	Testing Activation .....	14
<b>3.0</b>	<b>Software Uninstall</b> .....	<b>17</b>
<b>4.0</b>	<b>Software Re-Install</b> .....	<b>20</b>
4.1	Mobile CU Prerequisites .....	20
4.2	Software Being Installed .....	20
4.3	Software Install.....	21
4.4	Software Re-Install Configuration .....	23
4.4.1	Configure Suprema Fingerprint Reader.....	23
<b>5.0</b>	<b>Manual Configuration after Re-Image</b> .....	<b>26</b>
5.1	Java 8 Configuration .....	26
5.1.1	DeploymentRuleSet.jar File .....	26
5.1.2	Disable Java Auto Update (optional) .....	28
5.2	Install Certificates.....	29
5.3	Add USAccess Portals as Trusted Sites.....	34
5.4	Configure ActivClient for Certificate Deletion on Card Removal (Optional).....	36
5.5	Configure ActivClient to Disable the Card Blocked Message (Optional) .....	37
5.6	Enable Transport Layer Security (TLS) .....	38
5.7	Allow Pop-ups from the CMS Portal.....	39
5.8	TLS Registry Updates .....	40
5.8.1	Registry Instructions for 64-bit Windows.....	40
5.8.1	Registry Instructions for 32-bit Windows.....	41
<b>6.0</b>	<b>MCU Local Printer Setup</b> .....	<b>43</b>
6.1	Site Requirements.....	43
6.2	Printer Unpack and Set Up .....	43
6.2.1	Unpacking the Printer.....	43
6.2.2	Assembling the Printer .....	44
6.3	Installing the Cartridges .....	49
6.3.1	Installing the Printer Film.....	49
6.3.2	Installing the Transfer Film.....	51
6.3.3	Installing the Laminate .....	54
6.3.4	Installing the Cleaner Roll .....	56
6.4	Card Input Cartridge and Output Hopper.....	57
6.5	Connect the Printing Unit .....	58

6.6	Installing the printer on the MCU.....	58
6.7	Installation and Configuration.....	60
6.2	Printer Configuration .....	61
6.3	Configure Local Print Utility.....	65
6.4	Designate Print Operation Role .....	69
6.5	Site Manager Set Up.....	69
6.6	Run Local Printing Connection Test .....	71
<b>Appendix A – Repacking the CU for Shipment.....</b>		<b>73</b>

## List of Figures

Figure 1:	CU Packed in Pelican Case.....	2
Figure 2:	Suggested Mobile CU Setup .....	3
Figure 3:	Surge Protector.....	3
Figure 4:	Laptop Power Cord and side of Laptop .....	4
Figure 5:	Hub Power Cord and Labeled Hub.....	4
Figure 6:	Camera on Tripod.....	4
Figure 7:	Camera Dial set to P.....	5
Figure 8:	Camera MENU Button .....	5
Figure 9:	Camera AF Button .....	5
Figure 10:	Camera Image Quality Menu.....	6
Figure 11:	Correct Camera Image Quality Setting.....	6
Figure 12:	H1 USB Cable and Flatbed Scanner .....	7
Figure 13:	H2 USB Cable, Camera Extension Cable, and Camera on Tripod.....	7
Figure 14:	Peripheral Connections to the Hub.....	8
Figure 15:	Hub Connections .....	8
Figure 16:	Right Side of Laptop Showing Hub Cable Connection .....	8
Figure 17:	Fingerprint Scanner Connection .....	9
Figure 18:	CAT6 Network Cable Connection.....	9
Figure 19:	Bottom of Flatbed Scanner .....	9
Figure 20:	Program Mode on Camera .....	9
Figure 21:	USAccess System Information Icon .....	10
Figure 22:	Site Manager System Info .....	10
Figure 23:	Network Test Tool Icon.....	11
Figure 24:	Network Tests .....	12
Figure 25:	MCU Network Test Log .....	12
Figure 26:	Enrollment Icon .....	13
Figure 27:	USAccess PIV Card Login Screen .....	13
Figure 28:	Authentication Certificate for Login.....	13
Figure 29:	Web Enrollment – Search Enrollee Page .....	14
Figure 30:	Activation Icon.....	15
Figure 31:	PIV and PIV-I Activation Options .....	15
Figure 32:	Welcome Screen.....	15
Figure 33:	Card Updates Detected .....	16
Figure 34:	CU Software Uninstaller .....	17
Figure 35:	List of Installed Applications .....	18
Figure 36:	Scanner Driver Uninstaller.....	18
Figure 37:	Canon Scanner Uninstall Complete.....	19
Figure 38:	Uninstall Complete.....	19
Figure 39:	Mobile CU Software Installer .....	21
Figure 40:	Turn On and Connect Card Printer.....	22
Figure 41:	Mobile CU Install Complete .....	22

Figure 42: BioConfigure - Run administrator ..... 23

Figure 43: CyberArmed PCA Control Panel ..... 23

Figure 44: Simulate CMS Bio Verification ..... 24

Figure 45: Biometric Verification Window ..... 24

Figure 46: DeploymentRuleSet.jar Copied ..... 26

Figure 47: Java Control Panel with New Link ..... 27

Figure 48: Java Deployment Rule Set ..... 27

Figure 49: Disable Java Auto Update ..... 28

Figure 50: Launch MMC ..... 29

Figure 51: Add/Remove Snap-in ..... 29

Figure 52: Add Certificates ..... 29

Figure 53: Computer Account ..... 30

Figure 54: Complete Certificate Snap-in ..... 30

Figure 55: Certificate Snap-in Added ..... 30

Figure 56: Import Certificates ..... 31

Figure 57: Mobile CU Certificates ..... 31

Figure 58: Successful Certificate Import ..... 32

Figure 59: AssuredIdentityPrintService Certificate ..... 33

Figure 60: MMC Save Settings ..... 33

Figure 61: Group Policy Editor Launch ..... 34

Figure 62: Microsoft Group Policy Editor ..... 34

Figure 63: GPE Security Page ..... 35

Figure 64: Site to Zone Assignment List ..... 35

Figure 65: Zone Assignment ..... 36

Figure 66: GPE ActivClient Certificate Availability ..... 37

Figure 67: GPE ActivClient Notifications Management ..... 38

Figure 68: Advanced Tab in Internet Tools ..... 39

Figure 69: Pop-up Blocker Settings ..... 40

Figure 70: Fargo 5000 Card Printer ..... 43

Figure 71: Fargo 5000 Printer in Pelican Case ..... 44

Figure 72: Printer ..... 44

Figure 73: Dual Sided Printing Module ..... 45

Figure 74: Flipper to Printer Connections ..... 46

Figure 75: USB Connected to Printer Module ..... 46

Figure 76: Connect Flipper to Printer ..... 47

Figure 77: Screws for the Printer ..... 47

Figure 78: Lamination Module Connection ..... 48

Figure 79: Printer Tipped Over ..... 49

Figure 80: Lamination Screw Placement ..... 49

Figure 81: Open Lamination Module Cover ..... 54

Figure 82: Store Upgrade Tool ..... 54

Figure 83: Label Laminate Cartridges ..... 55

Figure 84: Card Input Cartridge ..... 57

Figure 85: Card Input Cartridge in Place ..... 57

Figure 86: Card Output Hopper ..... 58

Figure 87: Windows Control Panel ..... 59

Figure 88: Delete Existing HDP5000 Printers ..... 59

Figure 89: Printer Port ..... 60

Figure 90: Set As Default Printer ..... 61

Figure 91: Printer Properties ..... 61

Figure 92: Printer Configuration Security Tab ..... 62

Figure 93: Printer - Everyone Rights ..... 62

Figure 94: HDP5000 Printing Preferences ..... 63

Figure 95: Printing Preferences - Card Tab ..... 63

Figure 96: Advanced Setting Tab ..... 63

Figure 97: Device Options Tab ..... 64

Figure 98: Lamination Tab ..... 65

Figure 99: Local Print Utility ..... 66

Figure 100: Populate Printer Information ..... 66

Figure 101: Printer Serial Number and Consumable Levels ..... 67

Figure 102: Test Print Tab ..... 67

Figure 103: Check Card Stock Verification ..... 68

Figure 104: View Logs Button ..... 68

Figure 105: Sample Log File ..... 69

Figure 106: Successful Test Card Print ..... 69

Figure 107: Select Site Manager Role ..... 70

Figure 108: Site Search ..... 70

Figure 109: Workstations Link ..... 70

Figure 110: Add Workstation ..... 70

Figure 111: Add MCU Workstation Information ..... 70

Figure 112: Workstation List ..... 71

Figure 113: Add Printer to MCU ..... 71

Figure 114: Add Printer Information ..... 71

Figure 115: Local Printing Test ..... 72

Figure 116: Top Layer of Equipment Packing ..... 73

Figure 117: Equipment Packing ..... 73

Figure 118: Closed Latch ..... 74

## 1.0 Mobile Credentialing Unit Setup

Welcome to your new Mobile Credentialing Unit (MCU)! This unit **replaces** the LCS Kit at your site. Please refer to the *USAccess CU Deployment Process Guide* the MSO distributed, for more information on the differences between the old equipment and this new MCU, secure area requirements, and other important information.

**NOTE: MCUs are the property of Perspecta, they are not owned by the Agency.**

LCS Kits are the property of the agencies and will NOT be shipped back to Perspecta. Please contact your Agency Lead or Site POC about what to do with the LCS Kit equipment.

**Please do NOT mix parts between MCU and LCS Kits.**

### 1.1 Who Is Needed for Setup?

1. Someone to unpack the equipment and connect it according to these instructions.
2. A Registrar who can run through a Test Enrollment and activation.
3. A Local or Agency Site Manager (ASM or LSM) who can add the Mobile CU System ID to the site in the Site Manager Portal. The ASM or LSM are roles in the USAccess system. If you do not know who your ASM or LSM is, please run the Role Assignment report in the Reports portal to find your role holders. This person is not needed in person but needs to be available by phone or email at the time of equipment setup.

### 1.2 How Long Will it Take to Setup?

Timing depends on what your agency needs to do to the MCU in order to connect it to your agency network. The timing described in this Guide describes connecting the MCU as-is. At a minimum, your agency must add an anti-virus program, as none is included on the MCU. Please allow extra time if your agency needs to re-configure any part of the system or add software, to allow it to connect on your agency network.

Unpacking and setting up the equipment should take approximately 30-60 minutes. Allow an additional 30 minutes after Setup for the system to receive any pending Windows updates that may or may not require a reboot. Update time may vary, depending on the speed of your Internet connection, and the timing of your shipment. Your MCU may not require any updates, or there may be some newly released patches to install since it was shipped. Allow another 30-60 minutes to test the system.

Total time **without agency-specific configuration**: Approximately 1 ½ to 2 ½ hours.

Please also check for any MCU Installer updates that may have been posted to the SFTP server since you received your MCU. IF the unit has been on site for a while, it may need an update.

### 1.3 Component Unpacking

If unpacking the kit in a location other than the secure MCU station area, ensure this area is also secure (locked room with limited access so equipment does not go missing). *Carefully* unpack all components to ensure the packing foam does not tear, and is available for reuse.

The Mobile CU contains a packing inventory list certifying the presence of all required contents when the kit was shipped. If a more recent version has been posted, please allow time to download and install the updated MCU installer.

**NOTE: Keep all packing supplies, including cable ties, for repacking.**

4. Open the Pelican case containing the Mobile CU. Contact your Site POC for the Pelican case combination.
5. Carefully remove all components. The Pelican case contents are shown below without packing materials.



Figure 1: CU Packed in Pelican Case

6. As you unpack the equipment, place all cable ties and packaging materials back in the travel case for future relocation.
7. Store the inventory list inside the travel case. When it's time to move the CU to another location, use the inventory list to ensure all the kit contents are sent on to the next location.

## 1.4 Credentialing Unit Set-Up

The Mobile CU must be set up and kept in a secure room that is locked when not in use by the Registrar or Activator. Complete the following steps to setup the Mobile CU for operation.

## 1.5 Workstation Setup

1. Make sure the power to the laptop and all equipment is turned OFF. The hub and peripherals will be plugged in initially with the power off.
2. Place all Mobile CU equipment on the table or desk where it will be used. Figure 2: Suggested Mobile CU Setup shows a recommended equipment layout. If you also plan to use Local Print now or in the future, allow at least three feet more desktop space for the printer.

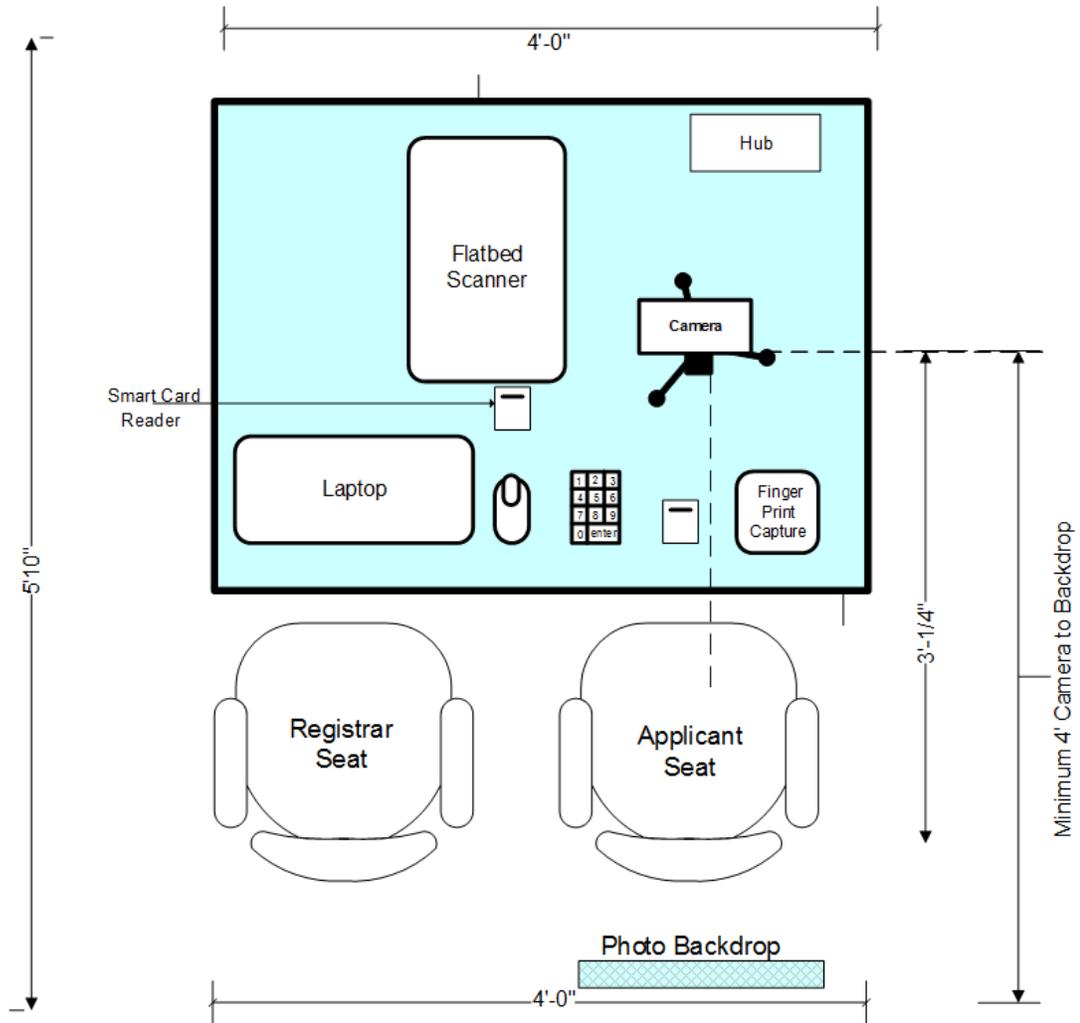


Figure 2: Suggested Mobile CU Setup

- Place the surge protector on the floor and plug it in to the electrical outlet.



Figure 3: Surge Protector

- Plug the Laptop power cord labeled "Laptop Power" into Laptop on the back right side. Plug the other end of the cord into the Surge Protector.



Figure 4: Laptop Power Cord and side of Laptop

5. Plug the Hub power supply cord (labeled “HUB Power”) into the Hub on the left side. Then plug the other end of the Hub power supply into the Surge Protector.



Figure 5: Hub Power Cord and Labeled Hub

6. Set up the camera and tripod by positioning the lens over one of the legs of the tripod to avoid the camera falling over. Tighten the knobs for Panning and Tilting on top of the tripod just below the camera.



Figure 6: Camera on Tripod

7. The camera power supply is already attached to the camera. Plug the other end of the camera power supply cord into the surge protector.

At this point, all power cords (three) are plugged into the Surge Protector.

## 1.6 Camera Settings

1. Ensure camera dial on top of the camera is set to “P”.



Figure 7: Camera Dial set to P

2. Check/Change the Image Quality settings on the camera.
  - a. On the back of the camera press the **MENU** button



Figure 8: Camera MENU Button

- b. Press the “**AF**” button to scroll until you reach the **Image quality** option on the camera’s view finder.



Figure 9: Camera AF Button

- c. Press the **SET** button once you are on the **Image quality** option screen.



Figure 10: Camera Image Quality Menu

- d. Confirm that the following option is selected.



- e. If any other image quality option is selected, press the “AF” button to scroll to the correct icon.
- f. Press “SET” again.

- 3. Once you have confirmed or selected the correct option, you should see the following on the camera’s view finder. Press **Menu** to exit. The view finder should be dark again.

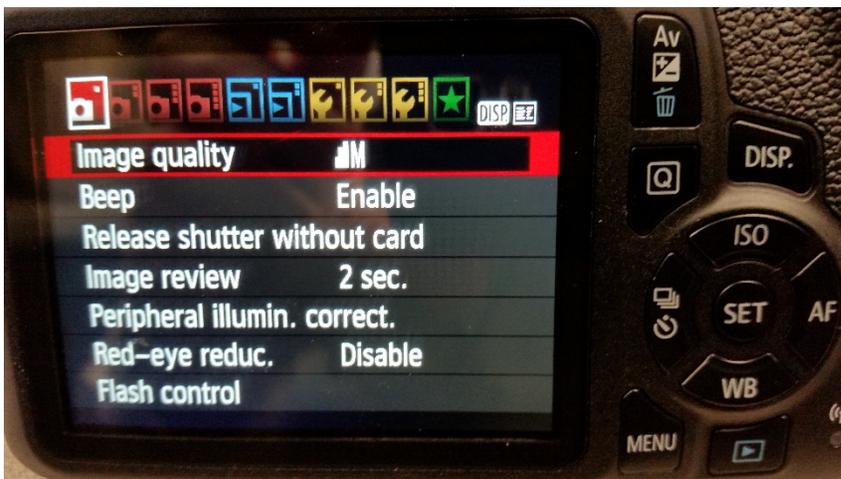


Figure 11: Correct Camera Image Quality Setting

- 4. Check camera power settings
  - a. Press the **MENU** button on camera.
  - b. Scroll right with the AF button to select first tab with wrench icon and press the **SET** button.



- c. Use the WB button to scroll down and select **Auto Power Off**.

- d. Use the AF button to change to **disable**.
  - e. Press the **SET** button.
5. Press the **MENU** button to exit. The view finder should be dark again.

## 1.7 USB Cables

Each USB cable is labeled with the component it belongs to and its connection placement in the hub or Laptop. Do not remove the cable labels, as this station may be packed up and moved to another location, and the labels will be needed when setting the station up at a new location.

1. Plug the cable labeled H1 into the flatbed document scanner.



Figure 12: H1 USB Cable and Flatbed Scanner

2. Plug the cable labeled H2 into the left side of the camera. Use the Camera Extension cable (labeled Camera Ext) if needed. If not needed, place the Camera Ext cable back in the case for future shipping.

**NOTE:** This extension cable may **ONLY** be used with the camera. Do not use with any other peripheral.



Figure 13: H2 USB Cable, Camera Extension Cable, and Camera on Tripod

3. Plug all cables into the Hub as shown below.



Figure 14: Peripheral Connections to the Hub

- Once complete, the Hub should look like Figure 15: Hub Connections.



Figure 15: Hub Connections

- Plug the other end of the H8 cord into the right side of the Laptop.



Figure 16: Right Side of Laptop Showing Hub Cable Connection

- Plug the fingerprint scanner labeled LR1 into the Laptop as shown in Figure 17: Fingerprint Scanner Connection.

**NOTE:** The port labeled **PTR** is for local printers only. Please do not plug **anything** into this port at this time. If your agency participates in the Local Printing service, more instruction will be provided separately to you. For now, this is only the CU set up.

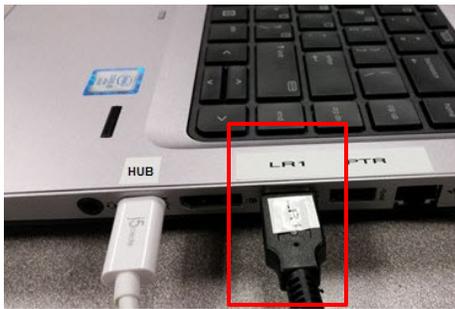


Figure 17: Fingerprint Scanner Connection

7. Plug the CAT6 network cable into laptop, and the other end into the active network jack in the wall, or follow your agency-provided network connection instructions if using another type of network connection such as Wi-Fi.



Figure 18: CAT6 Network Cable Connection

8. Turn the flatbed scanner over, and unlock the scanner by pushing the lock switch toward the unlock position.



Figure 19: Bottom of Flatbed Scanner

9. Turn the power on for the camera, and ensure the camera is in Program mode (turn the dial on the top to 'P').



Figure 20: Program Mode on Camera

10. Remove the lens cap on the camera and place to the side. Put the lens cap back on the camera at the end of the day.
11. Position the backdrop on a wall behind the seat the Applicant will be occupying when the enrollment photo is taken. The backdrop should be a minimum of four feet (4 ft) from the camera. Ensure the backdrop is stretched tight to eliminate wrinkles and fold marks that may distort the photo optimization and final image.
12. Place the fingerprint scanner cleaning cloth in a convenient location close to the CU.

## 1.8 Power on the Laptop

1. Open the Laptop cover and turn the power on.
2. Login to the Laptop using provided Local Administrator username and password.

**Local Admin Login:** CU-USX-ADMIN

**Default Local Admin Password:** KW, 3UZ5;wtA2nv

**IMPORTANT NOTE:** You MUST change the Local Admin password. Follow Agency standards for developing a strong admin password. Since your agency is responsible for managing the laptop and the users on the laptop, it is the agency's responsibility to maintain this information.

**NOTE:** The CU will only allow a max of three failed attempts to enter the password. After three unsuccessful attempts, the laptop log on is locked for 30 minutes.

3. User is prompted to change the local administrator password. Change it now to a strong password that follows Windows 10 and your agency's guidelines for passwords.
4. Windows 10 automatically detects the devices as they are connected to the system.
5. Open USAccess System Info (icon on desktop).



Figure 21: USAccess System Information Icon

6. Record System ID for entering into Site Manager. The System Type says MOBILE\_CU. The Site Code will read 91000 until the MCU System ID is added to your site.

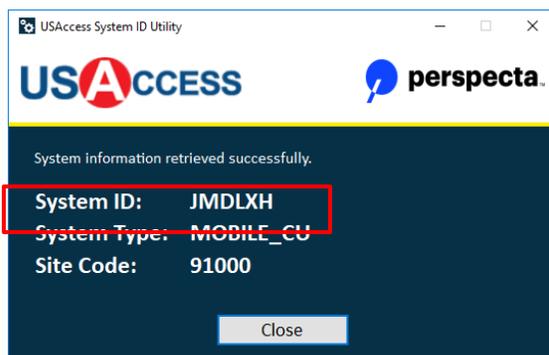


Figure 22: Site Manager System Info

**NOTE:** Give the System ID to your Local or Agency Site Manager and ask them to add the system to your site in the Site Manager portal. Failure to do this will prevent the system from working.

7. Close the System Info Tool.

## 1.9 Enter System ID in Site Manager

At this point, the ASM or LSM must enter the CU System ID into Site Manager before continuing with the test. The person completing this section **MUST** have either the ASM or LSM role for the site.

1. Log into Site Manager and pull up the Site the where the CU is located.
2. Click on **Workstations**.
3. Click **Add Workstation**.
4. Type in **Workstation System ID** and today's date as **Start Date**.
5. Click **Validate**.

**NOTE:** If workstation does not validate, compare the System ID entered in Site Manager with what is displaying on the MCU. If correct, and system will not Validate, call the USAccess Help Desk for assistance.

6. Once successfully validated, click **Add**.
7. Next, for each LCS kit that will no longer be used, set the **End Date** for the appropriate LCS Kit System ID.
8. If your site also uses the Scheduler, and you are prepared to stop using the LCS, click on **Workstation Schedule** for each end dated LCS workstation, and click the checkbox next to **Disable Workstation**, and click the **Update Workstation** button. This removes the LCS workstation from the Scheduler.
9. Define the CU appointment schedule in Site Manager, if it is not going to follow the Site Schedule already defined.
10. Notify the site that the Mobile CU has been added to Site Manager.

## 2.0 Testing the MCU

Test the MCU, by logging into Windows as a user to ensure the CU will work as expected for the everyday users of the system.

### 2.1 Network Test Tool

1. Double click the Network Test Tool icon on the Desktop.



Figure 23: Network Test Tool Icon

- Click the **Network Test** radio button, and click the **Run** button. Check Test Status, all should show “Completed Successfully”

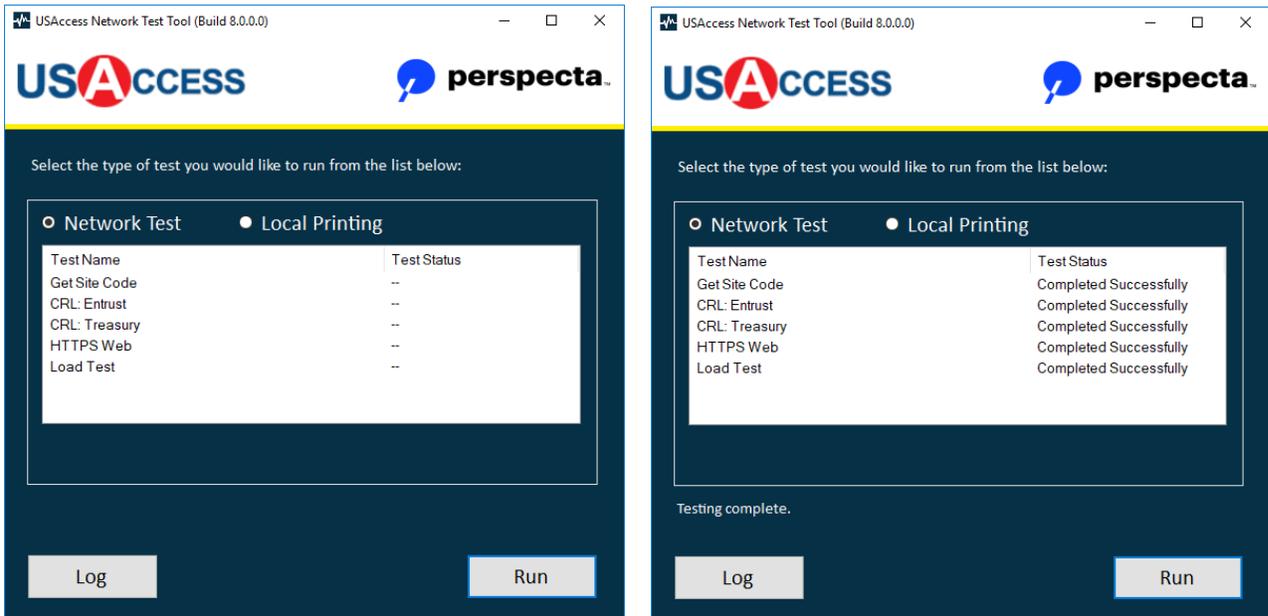


Figure 24: Network Tests

- If any of the tests failed, click the Log button to review any errors that occurred, which will lead you to troubleshooting.

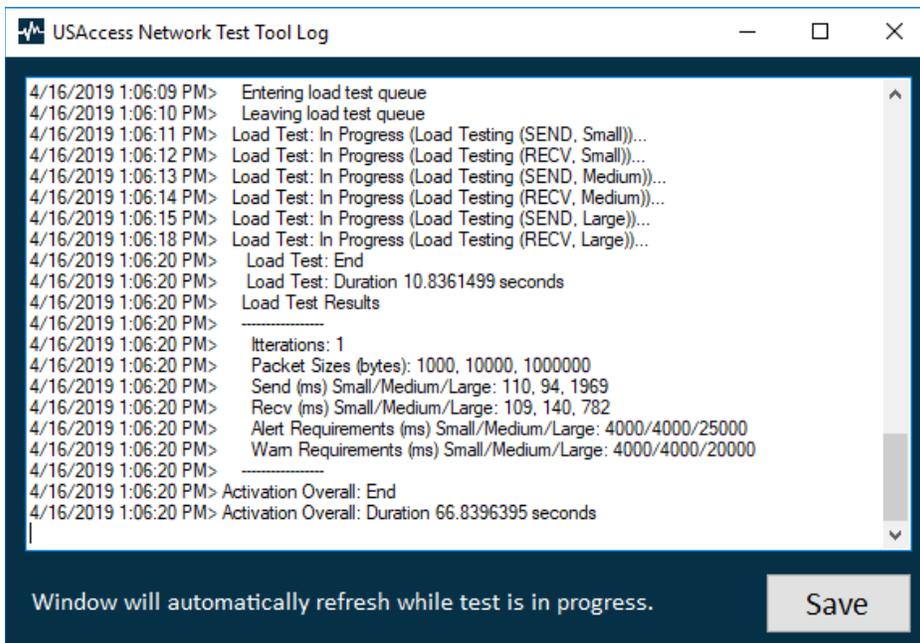


Figure 25: MCU Network Test Log

- Scroll through the log to look for errors. To save the Log click the **Save** button, and save it to the hard drive.
- Close the Network Test Tool.

## 2.2 Testing Enrollment

1. Have Registrar insert PIV credential into one of the card readers.
2. Launch the Assured Identity – USAccess icon.

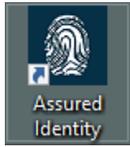


Figure 26: Enrollment Icon

3. The PIV Credential Log In screen displays for Enrollment. Click **Login with a Smart Card**.

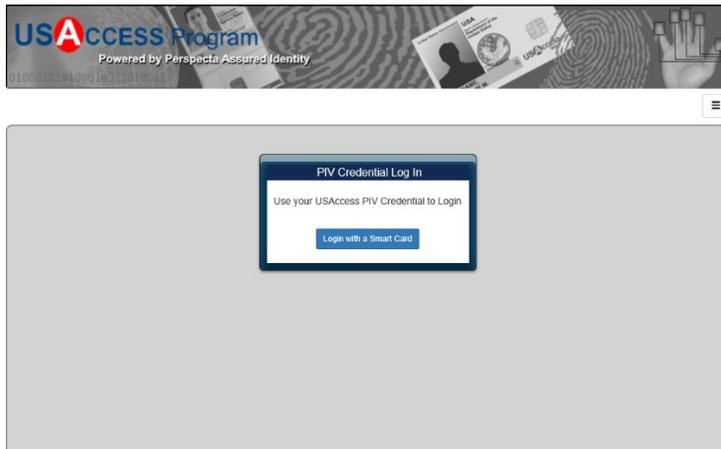


Figure 27: USAccess PIV Card Login Screen

4. Select your Authentication certificate when prompted. (If the “Signature” certificate displays, click **More Choices** and click the Authentication certificate), and click the **OK** button.

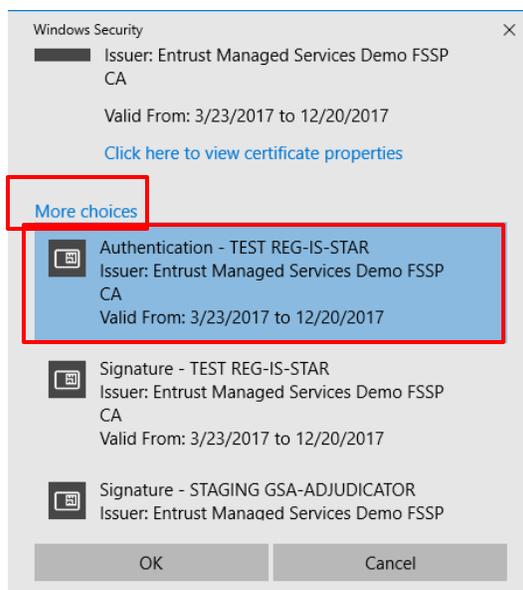


Figure 28: Authentication Certificate for Login

5. When prompted, enter your PIN.

6. The Web Enrollment application opens to the **Search Enrollee** page.

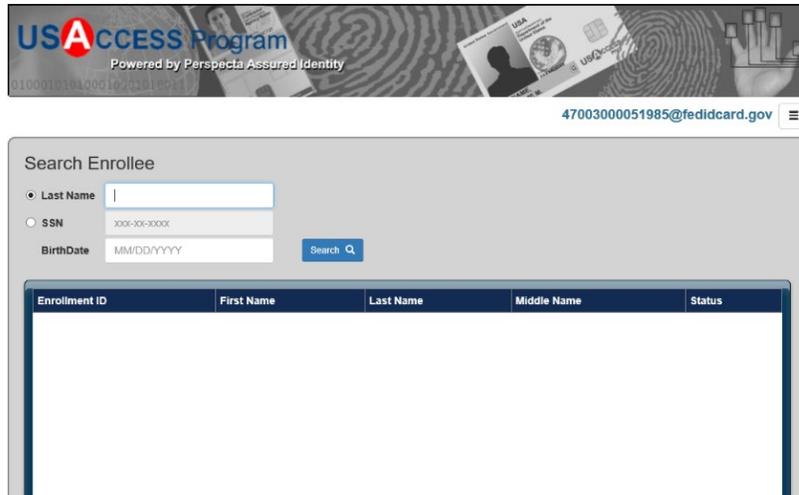


Figure 29: Web Enrollment – Search Enrollee Page

7. Run through a Test Enrollment using one of the following Test cases (do NOT save the enrollment at the end:

Last Name	Date of Birth	Last Name	Date of Birth	Last Name	Date of Birth
CERTIFYSITE-A	01/01/1981	CERTIFYSITE-J	01/01/1981	CERTIFYSITE-S	01/01/1981
CERTIFYSITE-B	01/01/1981	CERTIFYSITE-K	01/01/1981	CERTIFYSITE-T	01/01/1981
CERTIFYSITE-C	01/01/1981	CERTIFYSITE-L	01/01/1981	CERTIFYSITE-U	01/01/1981
CERTIFYSITE-D	01/01/1981	CERTIFYSITE-M	01/01/1981	CERTIFYSITE-V	01/01/1981
CERTIFYSITE-E	01/01/1981	CERTIFYSITE-N	01/01/1981	CERTIFYSITE-X	01/01/1981
CERTIFYSITE-F	01/01/1981	CERTIFYSITE-O	01/01/1981	CERTIFYSITE-Y	01/01/1981
CERTIFYSITE-G	01/01/1981	CERTIFYSITE-P	01/01/1981	CERTIFYSITE-Z	01/01/1981
CERTIFYSITE-H	01/01/1981	CERTIFYSITE-Q	01/01/1981		
CERTIFYSITE-I	01/01/1981	CERTIFYSITE-R	01/01/1981		

8. Place any piece of paper in the flatbed scanner and scan it, give it a fake number, and select a document type.
9. Take anyone’s picture. The photo capture will attempt to optimize the image and will require a subject when the photo is taken or it will not allow you to continue. Multiple attempts may be necessary when setting up the camera.
10. Take all rolls and slaps of yourself or another person.
11. Verify prints, click **Next** to go to the Save page, then CANCEL the enrollment.
12. Close the portal.

## 2.3 Testing Activation

Run through an actual Activation of a new card, or a Card Update, using Unattended Activation.

1. Open the Unattended Activation Program. Click the **Activation** icon on the workstation Desktop as shown in Figure 30: Activation Icon

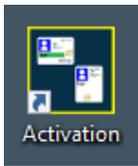


Figure 30: Activation Icon

2. The Activation screen displays. Click the **PIV Unattended Activation** icon.



Figure 31: PIV and PIV-I Activation Options

The **Welcome to USAccess Card Management** screen displays as shown in Figure 32: Welcome Screen.

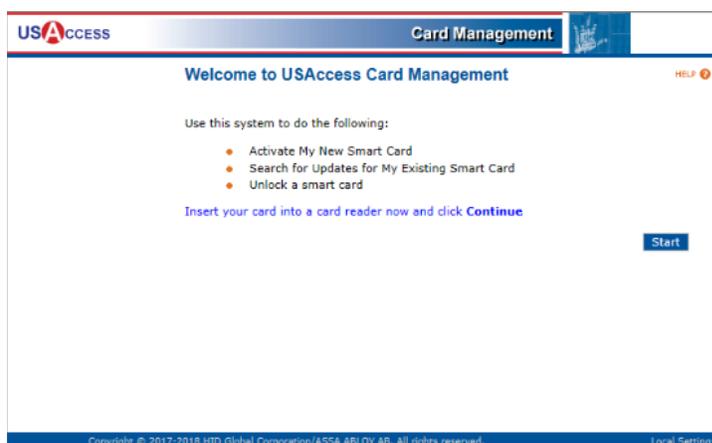


Figure 32: Welcome Screen

3. Insert your credential in the card reader and click the **Start** button.

4. Enter your PIN number when prompted, and click the **Continue** button.
5. The *Card Updates Detected* screen displays. If there is an update pending, continue with the card update. Otherwise, click the **Done** button.



**Figure 33: Card Updates Detected**

The MCU has successfully connected to the CMS server. This means that an employee or contractor should be able to perform Unattended Activation and post-issuance maintenance activities, and a person assigned the Activator role can assist an employee or contractor to perform Attended Activation or post-issuance functions.

6. Close the browser windows.
7. Log off as Administrator.

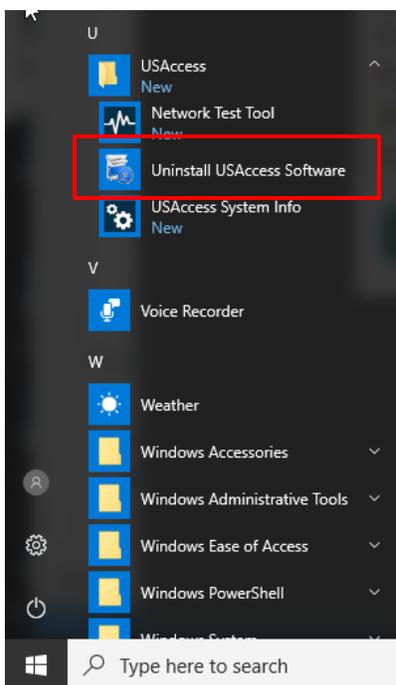
**The MCU is ready for use at this time. Do not proceed further unless needed for Local Print, agency configuration, or troubleshooting.**

## 3.0 Software Uninstall

**The Mobile CU was shipped with the Mobile CU software already installed and configured for use. This section is ONLY needed if you are troubleshooting, or need to uninstall the software for agency configuration reasons.**

**NOTE:** The Mobile CU Installer only recognizes and uninstalls/installs applications that the Mobile CU installer initially installed. **DO NOT uninstall any components of the CU software through the Control Panel unless instructed to do so by the Help Desk. Use the steps shown below to uninstall individual components of the CU package.**

1. Disconnect the Hub and finger print scanner from the CU. If you have a local printer, turn off the power.
1. Restart the computer. Login to the laptop with Administrative Rights.
2. Click **Start, USAccess**, and click **Uninstall USAccess Software**.



**Figure 34: CU Software Uninstaller**

3. Place checkmarks next to the items to remove (or click **Select All** to mark all items).

**NOTE:** If your agency has installed Local Print, you will see the Card Printer on this screen.

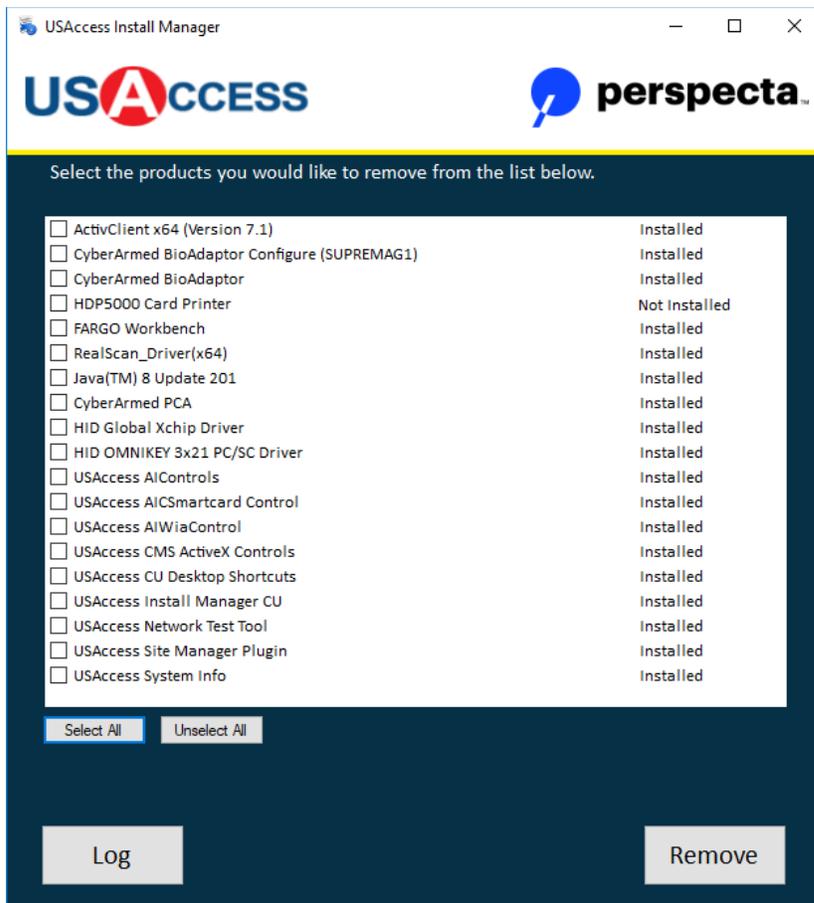
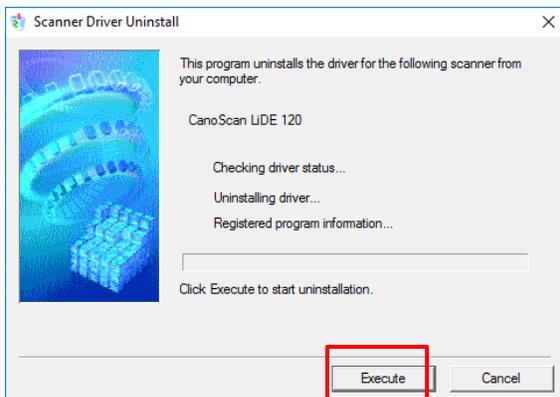


Figure 35: List of Installed Applications

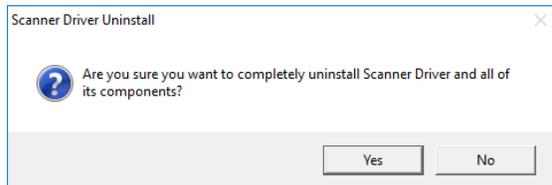
4. Click the **Remove** button to begin the uninstall process. If you chose to remove the flatbed scanner drivers, the *Scanner Driver Uninstaller* window displays as shown in Figure 36: Scanner Driver



Uninstaller. Click the **Execute** button.

Figure 36: Scanner Driver Uninstaller

5. A message box displays asking if you are sure you want to uninstall. Click the **Yes** button.



6. The scanner uninstall completes. Click the **Complete** button as shown in Figure 37: Canon Scanner Uninstall Complete.

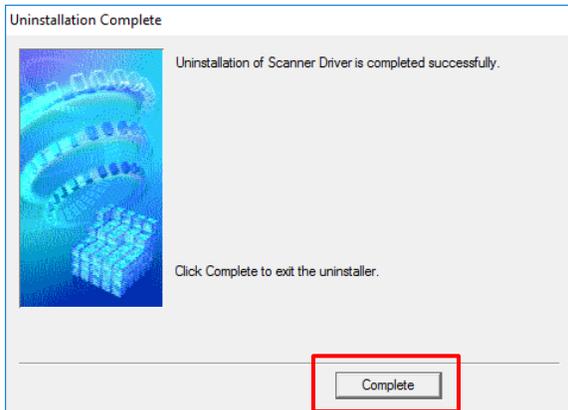


Figure 37: Canon Scanner Uninstall Complete

7. When the Uninstaller finishes, the *USAccess Installer* window displays as shown in
8. Figure 38: Uninstall Complete reporting on the uninstall status of each application package.

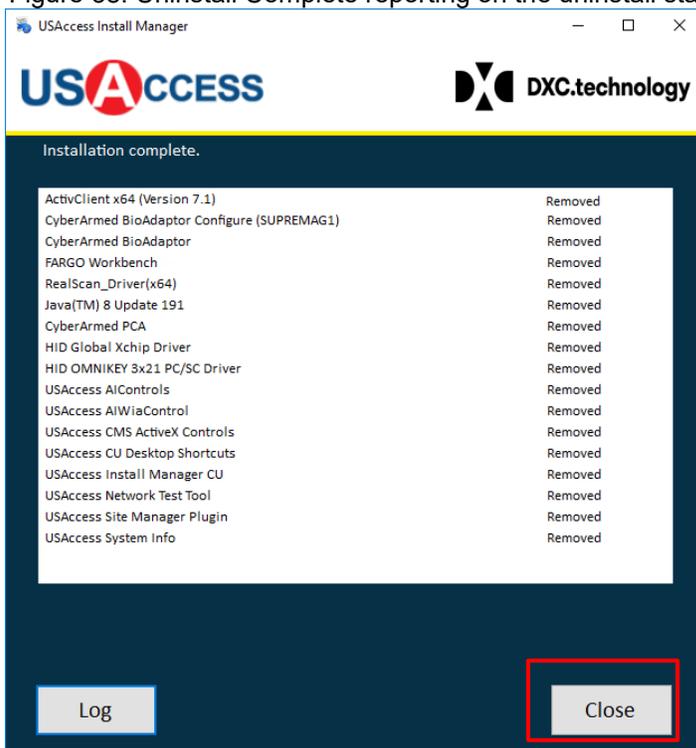


Figure 38: Uninstall Complete

9. Click the **Close** button. **The un-install of the Mobile CU USAccess software is complete.**

**NOTE:** If you intend to re-install the software, you must reboot the CU before re-installing.

## 4.0 Software Re-Install

**The Mobile CU was shipped with the Mobile CU software already installed and configured for use. This section is ONLY needed if you have re-imaged the laptop, or uninstalled the USAccess CU software on the laptop, and need to reinstall.**

**MCU software v2.1.0 is required for Mobile CU Kits to complete Activations/Updates/Rekeys once USAccess Software Release 15.6 moves to production on June 1, 2019.**

### 4.1 Mobile CU Prerequisites

Below is the list of pre-requisites for the Mobile CU:

- Perspecta-provided Mobile CU laptop
- Windows 10 64-bit
- MS Visual C++ Runtime (2010)
- MS Visual C++ Runtime (2008)
- .NET 4.6.2 (normally installed by Windows 10)

**NOTE:** Visual C++ Runtime (2010) and (2008), and .NET 4.6.2 can be found in the \MCUInstaller\Preinstall folder.

### 4.2 Software Being Installed

- ActivClient v7.1.0.153
- ActivClient Hotfix (7.1.0.244)
- CanoScan IJ Scan Utility v1.1.11.1
- CanoScan LiDE 120 Scanner Driver x64 v1.01
- CyberArmed BioAdaptor v1.6.567
- CyberArmed BioAdaptorConfigure Utility (SUPREMAG1) v1.1.1
- CyberArmed PCA v1.5.12.1922
- Fargo Workbench v3.2.0
- HDP5000 Card Printer v2.7.0.3.2 (only if site has a printer)
- HID\_Global\_xchip\_driver\_ru\_x64\_1.2.26.140
- HID Omnikey Smartcard Driver x64 v1.2.24.27
- Java 8 update 201
- RealScan\_Driver(x64) v1.3.0.0
- USAccess AICSmartcardControl 1.0.0
- USAccess AIControlsDeployment v1.3.0
- USAccess AIWiaControl v1.1.0
- USAccess CMS 5.0.0 ActiveX Controls
- USAccess CU Desktop Shortcuts v3.0.0
- USAccess Install Manager CU v6.0.0
- USAccess Network Test Tool v8.0.0

- USAccess Site Manager Plugin v3.0.2
- USAccess System Info v6.0.0

### 4.3 Software Install

The software install must run with Administrator rights.

**NOTE:** The latest MCU software is available on the USAccess SFTP server. Access to the SFTP server is controlled by your Agency Lead. Contact your agency lead for the software zip file.

1. Unzip the **MCUInstaller v2.1.0.zip** file onto the hard drive of the CU in a folder of your choice.

**NOTE:** Do not install from mapped network drives, flash drives, a server, or any other remote location not local to the machine. Doing so can cause issues with the installation.

2. Navigate to **MCUInstaller** and double click the **MCUInstaller.exe** file. The USAccess Install Manager displays.

**IMPORTANT NOTE:** If your site does NOT have an approved Local Printer, you must **UNCHECK the HDP5000 Card Printer**, otherwise the install will fail when it cannot detect the Printer. Leave the box checked if you have an approved HDP5000 printer.

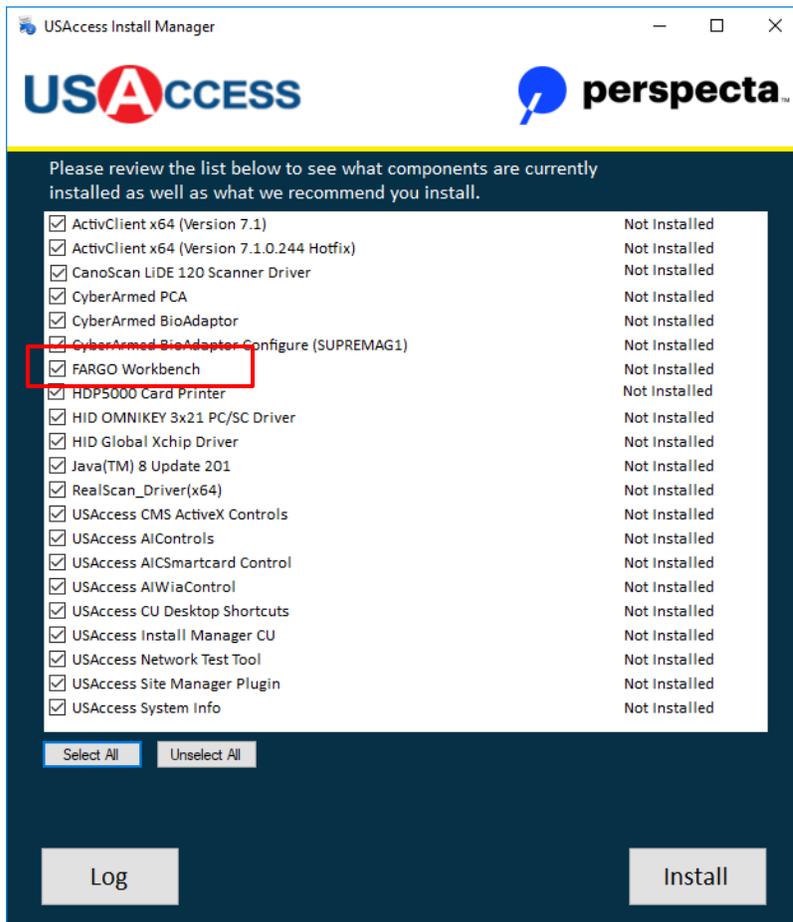


Figure 39: Mobile CU Software Installer

3. Click the **Install** button.

If an item fails to install, the installer lists the status as 'Failed'. There are many reasons the installation could fail, but common reasons are:

- a. Insufficient Privileges: Installation requires local administrative rights on the workstation.
- b. Package Already Installed: The software item may already be installed without using the Install Manager. If already installed, the installer lists 'failed' as the result because it cannot install the package.

**NOTE:** Some applications, like ActivClient, fail if another version is already installed, but other applications like Java only fail if the specific version is already installed.

- 4. If you chose to install the Card Printer, you are prompted to turn it on and connect it to the Mobile CU. Otherwise, wait for the install to complete.



Figure 40: Turn On and Connect Card Printer

- 5. If the install completed successfully, click the **Close** button.



Figure 41: Mobile CU Install Complete

- 6. If there were any failures, click the **Log** button to determine the reason for the failure.

## 4.4 Software Re-Install Configuration

Some manual installation is required after re-installing the software. Follow these directions after running the Mobile CU Installer.

### 4.4.1 Configure Suprema Fingerprint Reader

1. Plug in the Suprema fingerprint reader to port LR1 on the laptop.
2. Navigate to **C:\Programs Files (86)\CyberArmed\PCA**, right click **BioConfigure.exe**, and click **Run as administrator**.

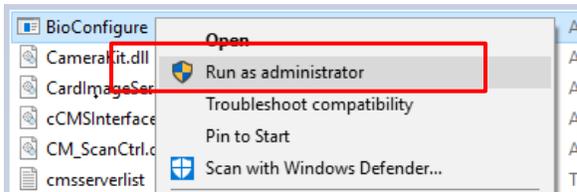


Figure 42: BioConfigure - Run administrator

3. In the Biometric Reader drop down box, select SUPREMAG1 and click the **Update Configuration** button.

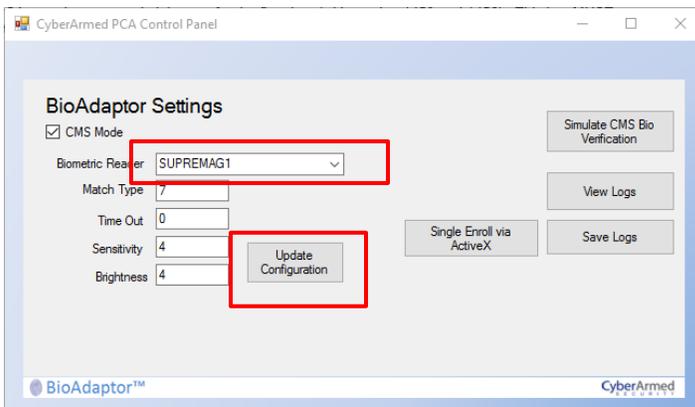
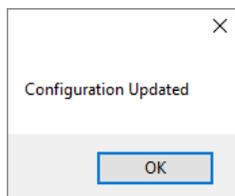


Figure 43: CyberArmed PCA Control Panel

4. Click the **OK** button.



5. Confirm the Suprema Fingerprint device is properly connected to the hub.

6. Select **Simulate CMS Bio Verification**.

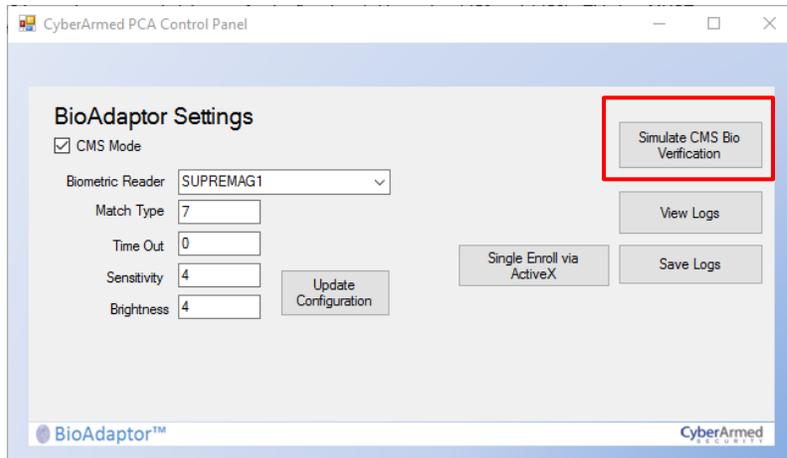


Figure 44: Simulate CMS Bio Verification

7. The Biometric Verification window opens. Place the right index finger on the device.

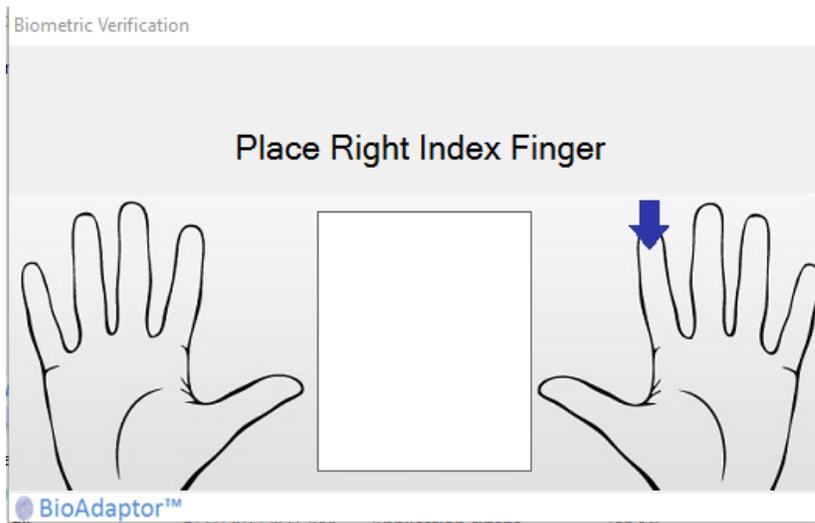
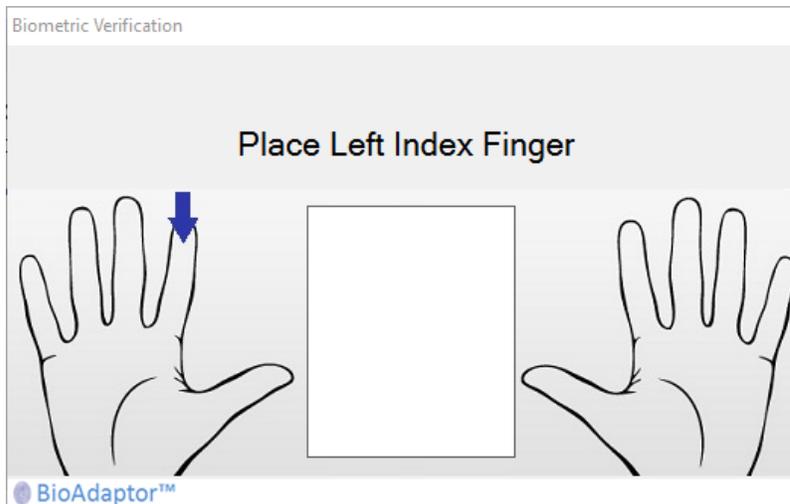


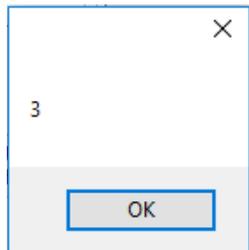
Figure 45: Biometric Verification Window

- 8. Capture and remove finger 3 times. Wait for glowing light before placing finger each time.
- 9. The application prompts for the next finger to verify.

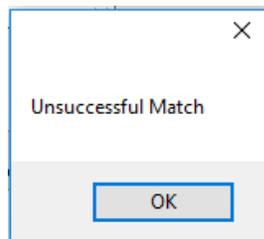


10. Repeat "Capture and remove finger" 3 times.

11. After capture a window pops with "3" up click the **OK** button.



12. Another window pops up displaying "Unsuccessful Match" click the **OK** button.



13. Close all windows.

14. Use Suprema cleaning cloth to wipe fingerprints from the glass.

## 5.0 Manual Configuration after Re-Image

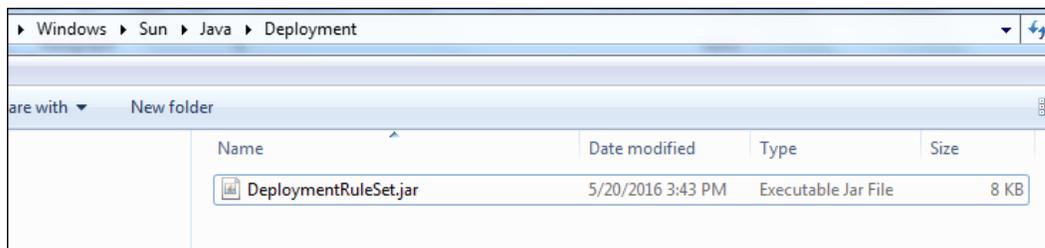
**This section is ONLY needed if you have completely re-imaged the Mobile CU laptop.** If you have completely re-imaged the laptop due to your agency configuration requirements, or in an effort to troubleshoot laptop issues, the following additional manual configuration must be completed after re-installing the Mobile CU software as detailed in section 4.0 above.

### 5.1 Java 8 Configuration

#### 5.1.1 DeploymentRuleSet.jar File

The DeploymentRuleSet.jar file must be copied to the correct folder on the workstation to prevent Java out of date messages and Java pop-up messages from displaying.

1. Browse to **C:\Windows**.
2. Right click on the directory and click **New, Folder**.
3. Type **Sun** and hit **Enter**. Click the Sun folder.
4. Right click and click **New, Folder**.
5. Type **Java** and hit Enter. Click the Java folder.
6. Right click and click **New, Folder**.
7. Type **Deployment** and hit Enter. Click the Deployment folder.
8. Browse to CD-ROM or local folder  
**MCUInstaller\Install\common\USAccess\Manual\Java\DeploymentRuleSet**
9. Copy the file **DeploymentRuleSet.jar** to C:\Windows\Sun\Java\Deployment.



**Figure 46: DeploymentRuleSet.jar Copied**

(There should be no other files in this folder)

10. To verify that the DeploymentRuleSet.jar is installed correctly, perform these steps.
  - a. Launch the Windows Control Panel.
  - b. Inside the Control Panel, open the Java Control Panel.
  - c. Select the Security tab.

- d. A new label displays titled 'View the active Deployment Rule Set'.

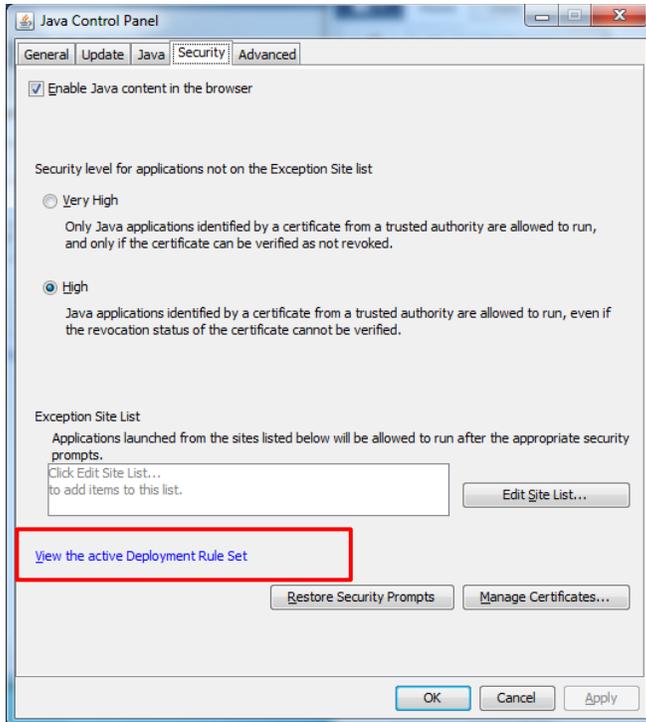


Figure 47: Java Control Panel with New Link

- e. Click on the new label titled **View the active Deployment Rule Set**. A popup window displays showing the rule set.
- f. Check the **Timestamp** for May 20, 2016.

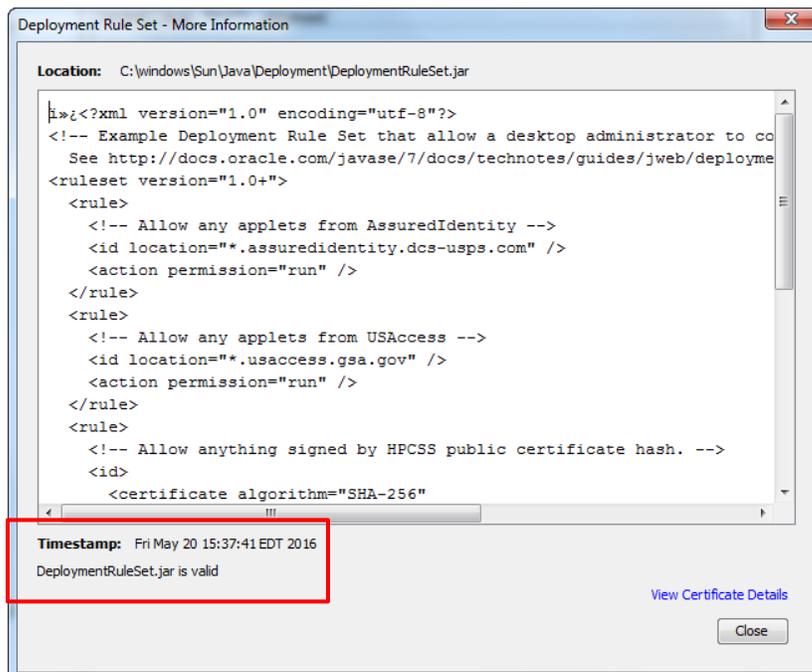


Figure 48: Java Deployment Rule Set

- g. Click the **Close** button to close the Deployment Rule Set popup.

- h. Click the **OK** button to close the Java Control Panel.

## 5.1.2 Disable Java Auto Update (optional)

Java is set to automatically update which can cause issues with the Mobile CU. To disable this automatic polling function from Java follow these steps to disable the Auto Update feature on Java. **NOTE:** These steps will not prevent Java from updating if the update is being pushed from your agency's network or domain, it only stops the search for updates from the Java product itself. Contact your agency network administrator should the machine need to be added to an exemption list for Java pushes.

1. Browse to **\\MCUInstaller\Install\common\USAccess\Manual\Java\DisableAutoUpdate**.
2. Double click on **Disable\_Java\_Update.reg**.

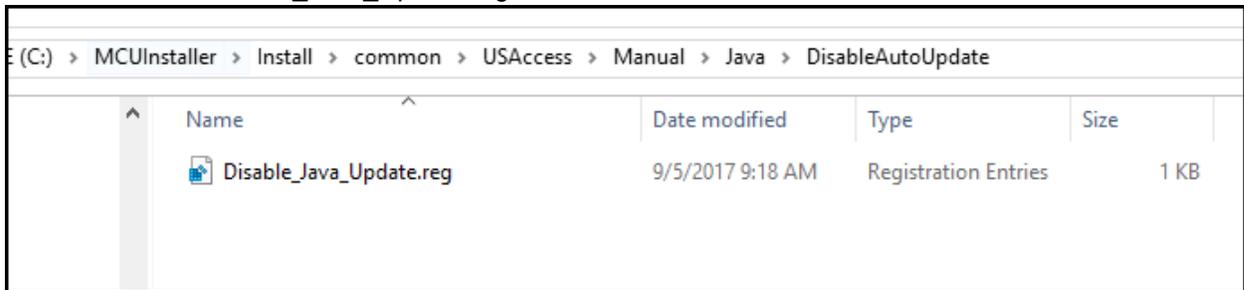
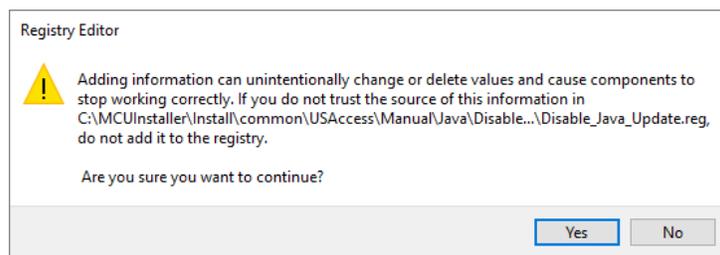
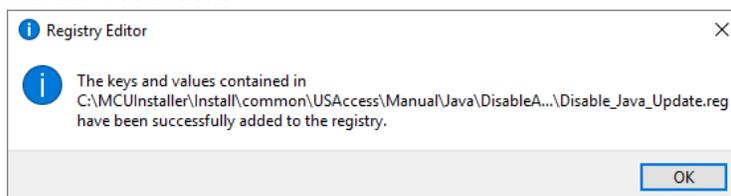


Figure 49: Disable Java Auto Update

3. When prompted, click the **Yes** button.



4. Click the **OK** button.



**NOTE:** These actions require you to be logged onto the system with *Administrative* privileges.

## 5.2 Install Certificates

1. Launch the Microsoft Management Console (MMC). In the bottom left corner of your screen, type **mmc.exe** in the **Type here to search** field, and hit the **Enter** key.

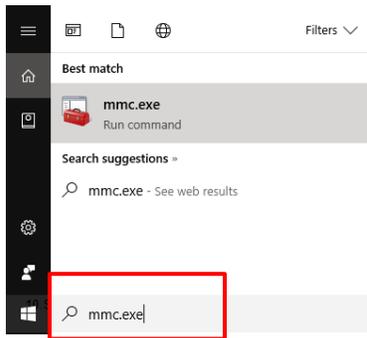


Figure 50: Launch MMC

**NOTE:** A User Account Control box may display. If so, click the **Yes** button to allow the application to run.

2. Click **File, Add/Remove Snap-in...**

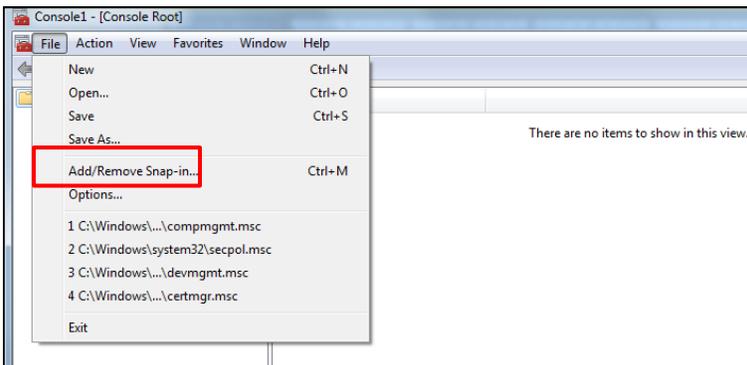


Figure 51: Add/Remove Snap-in

3. In the left pane, select **Certificates** and click the **Add** button.

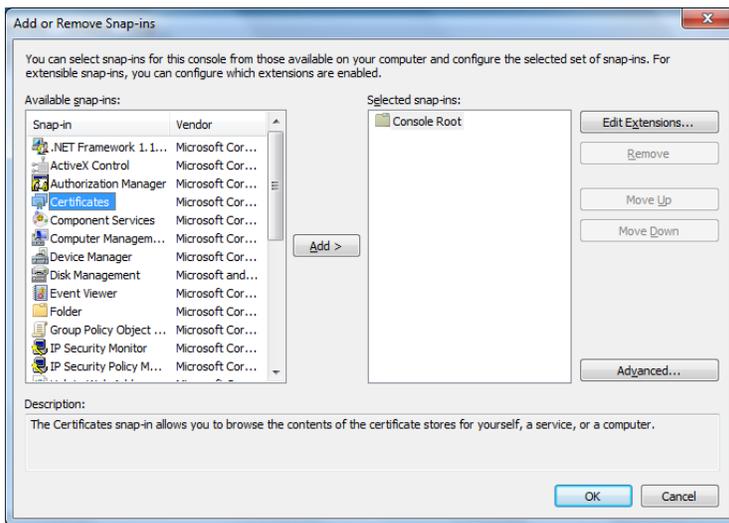


Figure 52: Add Certificates

4. Mark the **Computer account** item and click the **Next** button.

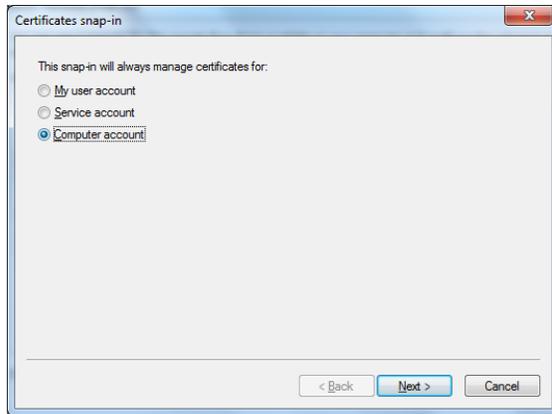


Figure 53: Computer Account

5. Click the **Finish** button.

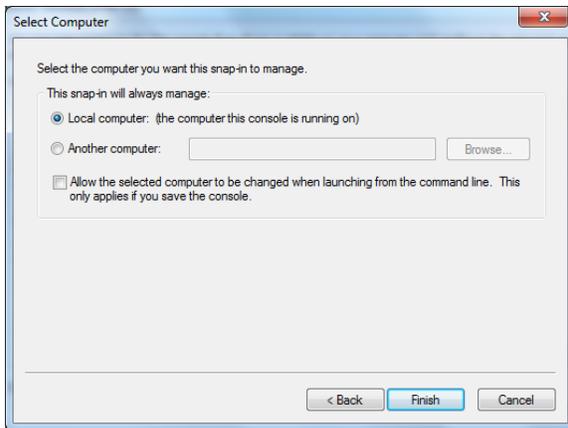


Figure 54: Complete Certificate Snap-in

6. Click the **OK** button.

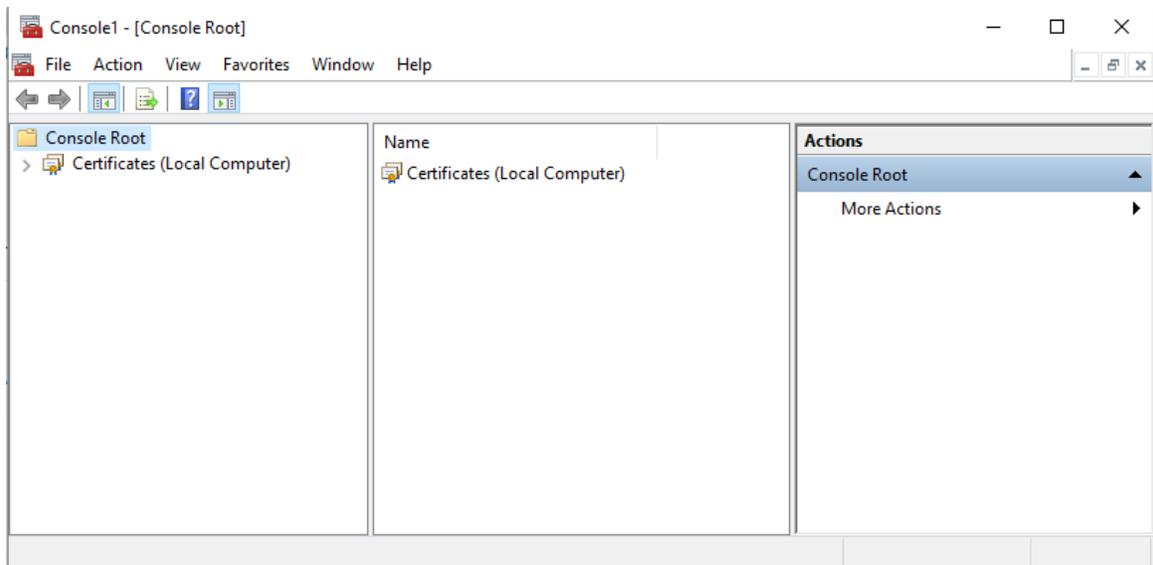


Figure 55: Certificate Snap-in Added

7. Expand the left pane to **Certificates (Local Computer) \Trusted Root Certification Authorities\Certificates**.
8. Right click on Certificates and choose **All Tasks, Import...**

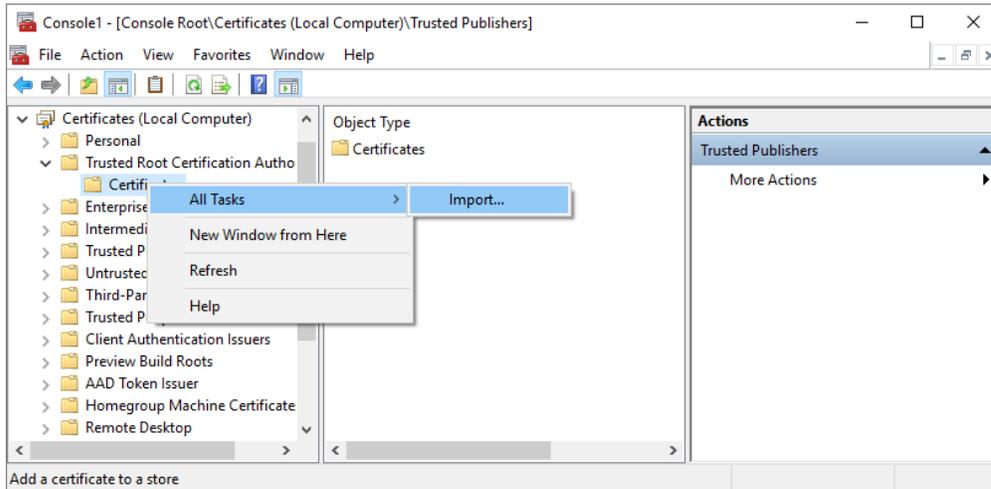


Figure 56: Import Certificates

9. The Certificate Import Wizard window displays. Click the **Next** button.
10. Click the **Browse** button, and navigate to **MCUInstaller\Install\common\USAccess\Manual\Certificates** folder.
11. Click **Entrust Managed Services NFI Root CA.cer** and click the **Open** button.

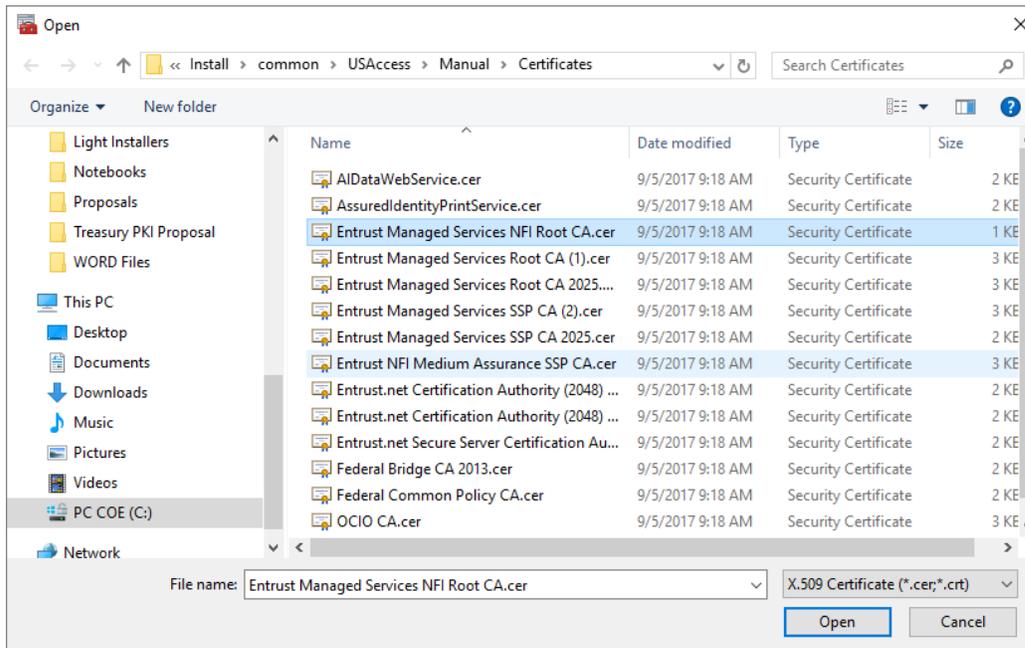


Figure 57: Mobile CU Certificates

12. Click the **Next** button.
13. Click the **Next** button.
14. Click the **Finish** button.

15. When prompted the import was successful, click the **OK** button.

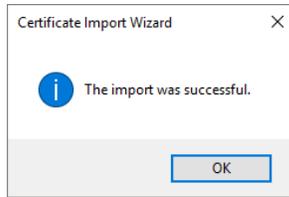


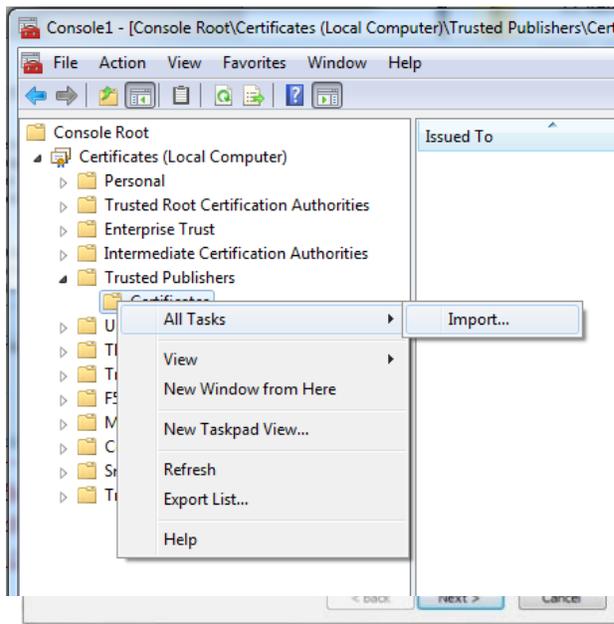
Figure 58: Successful Certificate Import

16. Repeat steps 8 through 15 above for the following certificates:

- a. **Entrust Managed Services Root CA (1).cer**
- b. **Entrust Managed Services Root CA 2025.cer**
- c. **Entrust Managed Services SSP CA (2).cer**
- d. **Entrust Managed Services SSP CA 2025.cer**
- e. **Entrust NFI Medium Assurance SSP CA.cer**
- f. **Entrust.net Certification Authority (2048) (1).cer**
- g. **Entrust.net Certification Authority (2048) (2).cer**
- h. **Entrust.net Secure Server Certification Authority.cer**
- i. **Federal Common Policy CA.cer**
- j. **OCIO CA.cer**
- k. **US Treasury Root CA.cer**

17. Expand the left pane to **Certificates (Local Computer) \Trusted Publishers\Certificates**.

18. Right click on Certificates and choose **All Tasks, Import...**



19. The Certificate Import Wizard window displays. Click the **Next** button.

20. Browse to ...\\Certificates folder, click **AssuredIdentityPrintService.cer** and click the **Open** button.

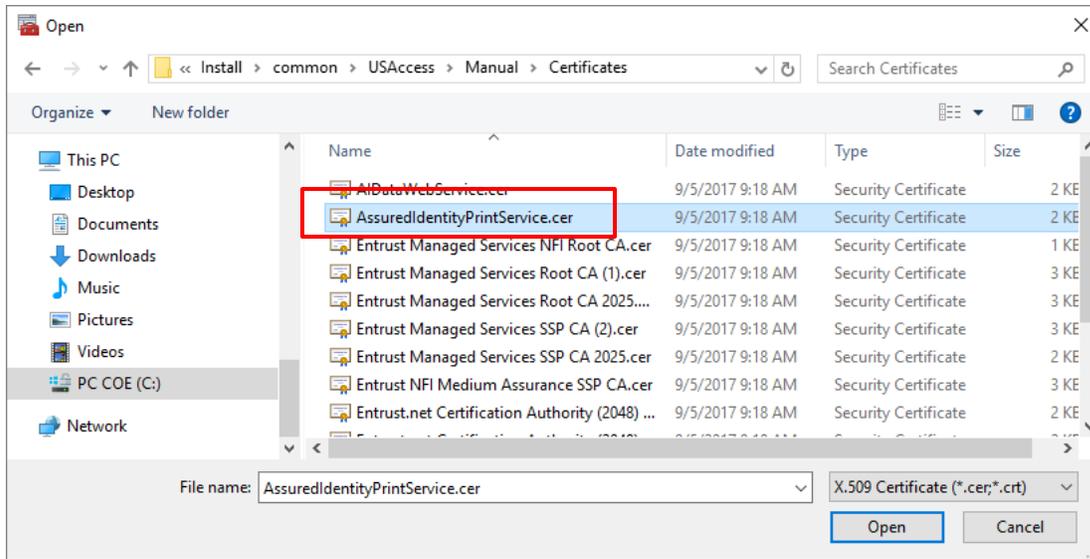


Figure 59: AssuredIdentityPrintService Certificate

21. When the File to Import window displays, leave the default file name and click the **Next** button.

22. Click the **Next** button.

23. Click the **Finish** button.

24. When prompted the import was successful, click the **OK** button.

25. Click the red **X** in the upper right corner to exit the console and click the **No** button when prompted to save.

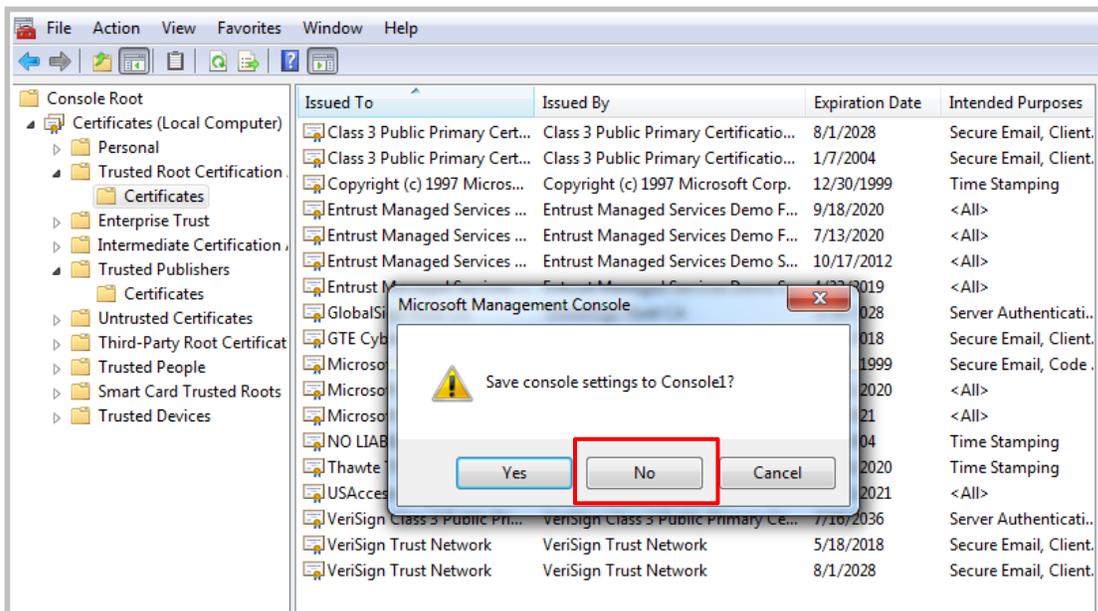


Figure 60: MMC Save Settings

26. IF you have an approved HDP5000 Local Printer, return to section 6.0 MCU Local Printer Setup, to configure the printer, then continue with section 5.3.

## 5.3 Add USAccess Portals as Trusted Sites

The Card Management System (CMS) portal uses ActiveX and Java, and the USGCB configuration prevents ActiveX and Java from running on any site not configured to be included in the 'trusted' domain. This configuration can be pushed down via a policy setting or can be configured as a local group policy. The steps below are for configuring a local group policy.

**NOTE:** You must be logged on as a local administrator to perform this action.

1. Launch the Group Policy Editor (GPE). In the **Type here to search** box at the bottom left, type **gpedit.msc** and hit the **Enter** key.

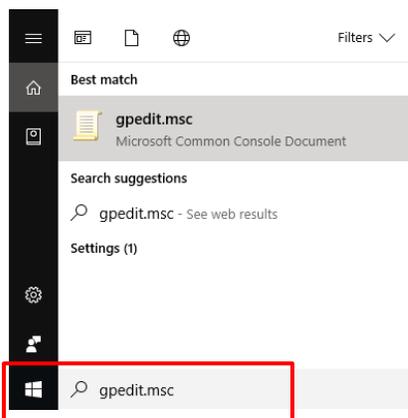


Figure 61: Group Policy Editor Launch

**NOTE:** A User Account Control box may display. If so, click the **Yes** button to allow the application to run.

2. The GPE window displays as shown in Figure 62: Microsoft Group Policy Editor.

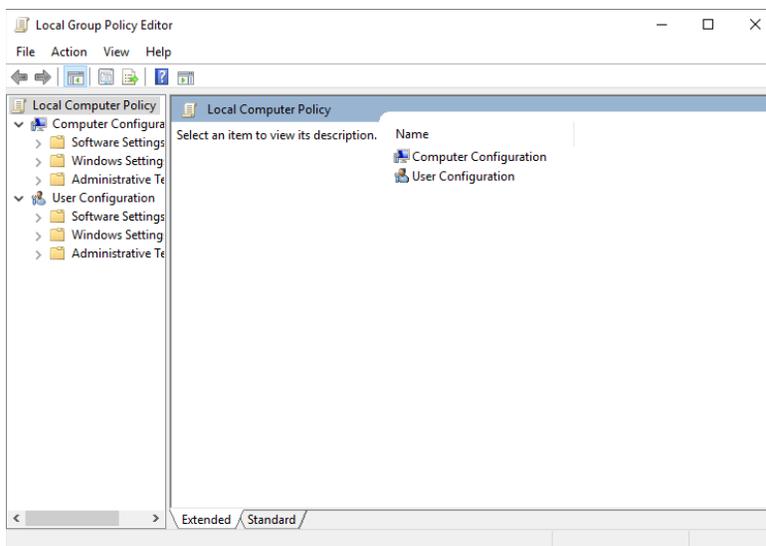


Figure 62: Microsoft Group Policy Editor

3. In the left pane, expand the tree to **Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page**.
4. Click the *Security Page* folder.

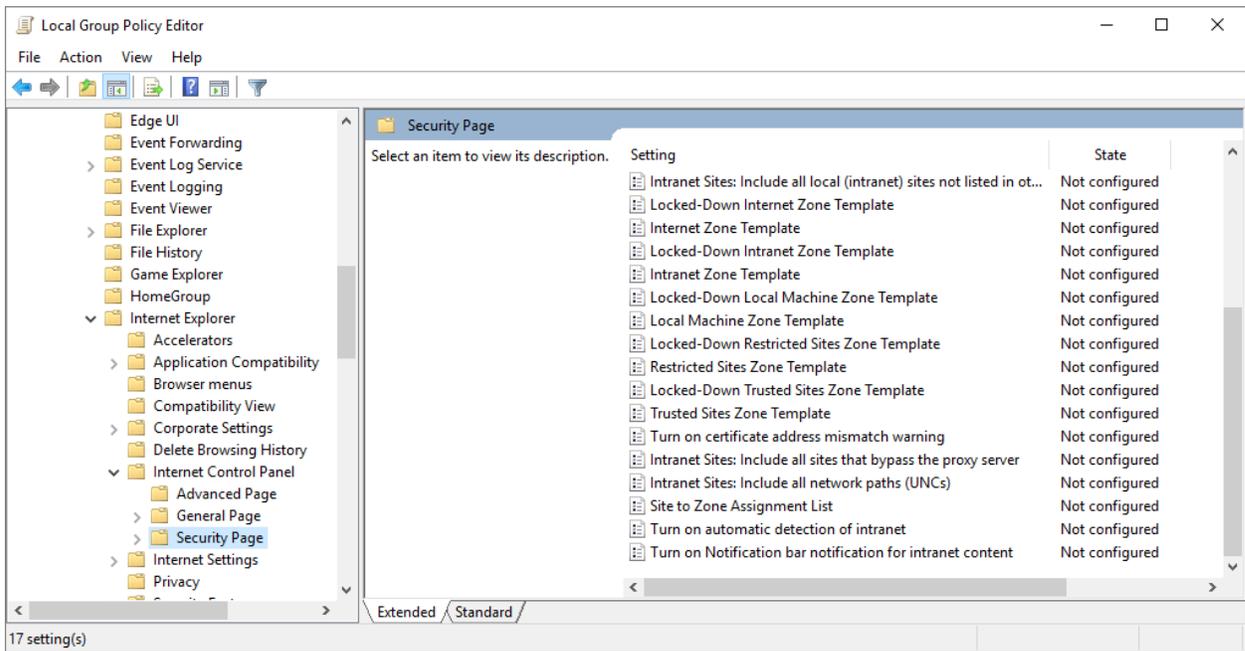


Figure 63: GPE Security Page

- In the right pane, double click on **Site to Zone Assignment List**.
- Click the **Enabled** radio button.

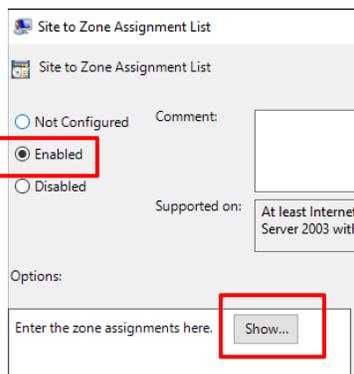


Figure 64: Site to Zone Assignment List

- Click the **Show** button.
- In the Value name column enter **\*.usaccess.gsa.gov**

9. In the **Value** column enter **2**.

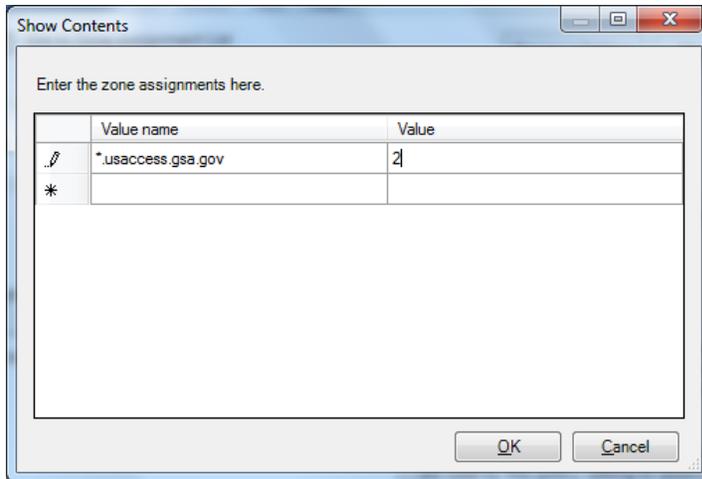


Figure 65: Zone Assignment

10. Click the **OK** button to close the **Show Contents** window.

**NOTE:** As an alternative to using **\*.usaccess.gsa.gov**, the individual USAccess portals can be explicitly configured as trusted sites. In order to do this, repeat steps 7, 8 and 9 and substitute the URL name in step 7 with the following explicit values:

portal.usaccess.gsa.gov  
 issuance.usaccess.gsa.gov  
 services.usaccess.gsa.gov  
 ack.usaccess.gsa.gov  
 extenroll.usaccess.gsa.gov  
 nonpiv-issuance.usaccess.gsa.gov

11. Click the **OK** button to close the Site to Zone Assignment List window.
12. Leave the Group Policy Editor (GPE) open for the next two sections, if you are completing them, otherwise, close the GPE.

## 5.4 Configure ActivClient for Certificate Deletion on Card Removal (Optional)

A Mobile CU is expected to be used to activate many credentials. Each time a credential is read by the CU, the certificates on the credential are loaded into the Windows certificate store. This can create a condition where the Windows certificate store is loaded with many user certificates, which may have an impact on performance, and be annoying to the Registrar/Activator. ActivClient can be configured to remove certificates from Windows when a credential is removed from the card reader. To set this configuration in ActivClient version 7.1, perform the following steps:

1. Open Group Policy Editor (**gpedit**) if not already open from the previous section.
2. In the left pane, expand the tree to **Local Computer Policy\Computer Configuration\Administrative Templates\HID Global\ActivClient\Certificate Availability**.

- On the right side, right click on **Remove certificates from Microsoft Windows on smart card....**

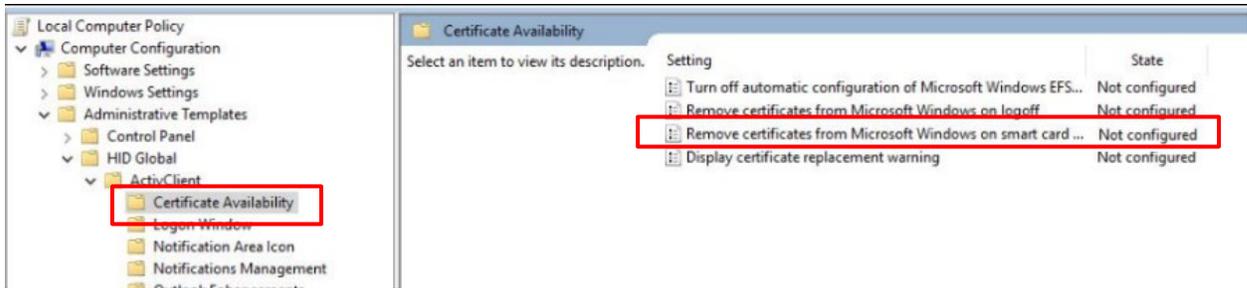
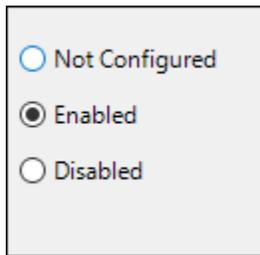


Figure 66: GPE ActivClient Certificate Availability

- Click the radio button for **Enabled**.



- Click the **OK** button. “Remove certificates...” now says Enabled.



- Close the GPE or leave open if configuring section 5.5.

## 5.5 Configure ActivClient to Disable the Card Blocked Message (Optional)

By default, ActivClient displays the following message when a smart card’s Card Manager is blocked: “Your smart card’s Card Manager is blocked; please contact the person or organization who gave you this card.” This is an intended state for USAccess credentials that are not yet activated. ActivClient can be configured to disable this error message. To set this configuration in ActivClient version 7.1, perform the following steps.

- Open Group Policy Editor (**gpedit**) if not already open from the previous section.
- In the left pane, expand the tree to **Local Computer Policy\Computer Configuration\Administrative Templates\HID Global\ActivClient\Notifications Management**.
- On the right side, right click on **Hide Blocked Card Manager message when a smart card wit....**

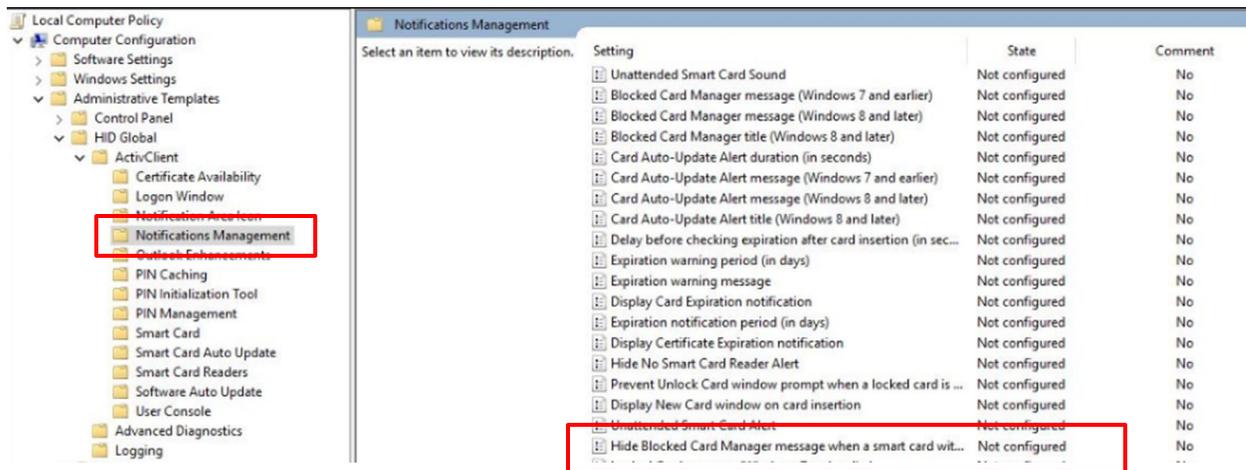
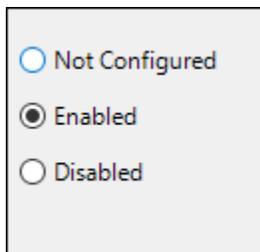


Figure 67: GPE ActivClient Notifications Management

- Click the radio button for **Enabled**.



- Click the **OK** button. “Hide Blocked Card...” now says Enabled.



- Close the Group Policy Editor.

## 5.6 Enable Transport Layer Security (TLS)

**NOTE:** The installer must perform this action first with local administrator rights, and then on every User Account that will be using the software. The installer must log on (or have the user log on) under each User Account and set this configuration. This is a browser configuration that needs to be updated every time a new User Account is added to this computer.

The USGCB specification requires that PIV-certified encryption be enabled.

- Launch Internet Explorer.
- Click **Tools, Internet Options**.
- Click the *Advanced* tab as shown in Figure 68: Advanced Tab in Internet Tools.

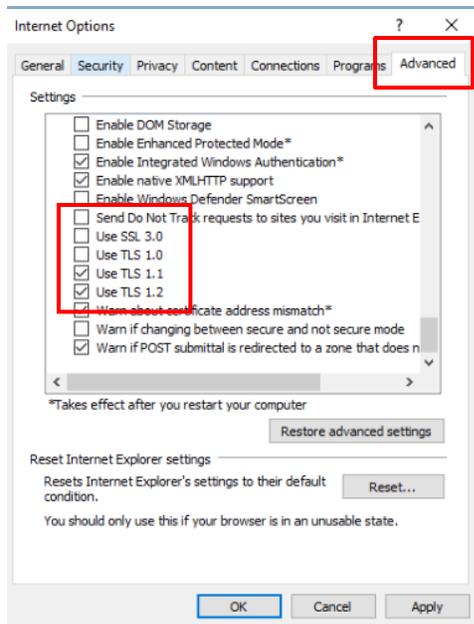


Figure 68: Advanced Tab in Internet Tools

4. Scroll down to the bottom under Security and check the box next to **Use TLS 1.1** and **Use TLS 1.2**.
5. Uncheck the boxes next to **Use SSL 3.0**.

**NOTE:** USAccess recommends **deselecting these options** due to security risks. They are not needed by USAccess and may cause issues if selected.

6. Click the **Apply** button.
7. Click the **OK** button.
8. Close Internet Explorer.

## 5.7 Allow Pop-ups from the CMS Portal

**NOTE:** The installer must perform this action first with local administrator rights, and then on **every** User Account that will be using the software. The installer must log on (or have the user log on) under each User Account and set this configuration. This is a browser configuration that needs to be updated **every time** a new User Account is added to this computer.

During an activation process, the Card Acknowledgment page (also referred to as the Privacy Statement) displays in a new Internet Explorer browser window. The Internet Explorer pop-up blocker needs to be configured to allow pop-up windows from the USAccess application. To allow pop-ups from USAccess sites, perform the following steps:

1. Launch Internet Explorer.
2. Click **Tools, Internet Options**.
3. Select the *Privacy* tab.

- In the Pop-up Blocker section, click the **Settings** button.

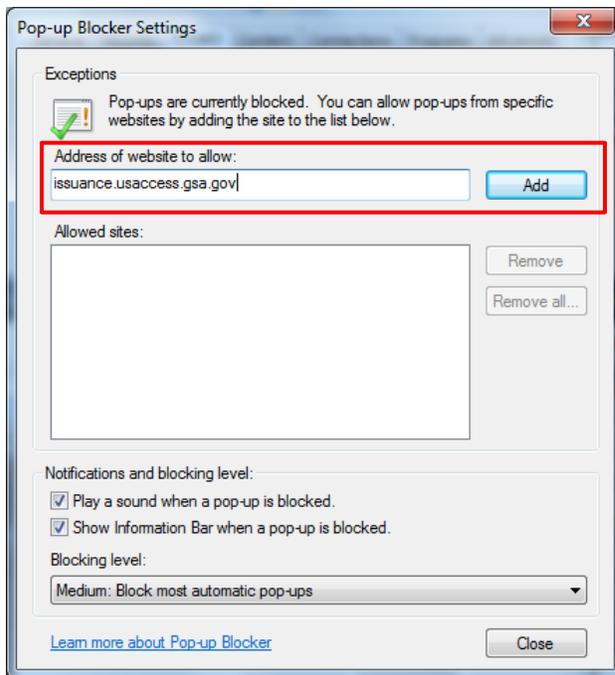


Figure 69: Pop-up Blocker Settings

- In the Address of website to allow: field, type **issuance.usaccess.gsa.gov**.
- Click the **Add** button.
- In the Address of the website to allow: field, type **nonpiv-issuance.usaccess.gsa.gov**.
- Click the **Add** button.
- Click the **Close** button.
- Click the **OK** button to close Internet Options.
- Close Internet Explorer.

The Mobile CU is now configured to work. Run through the Network Test Tool, a test enrollment, and an activation activity as described in section 2.0 Testing the MCU.

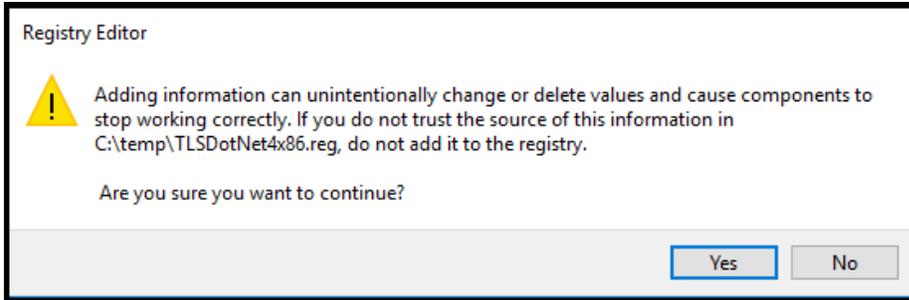
## 5.8 TLS Registry Updates

The following changes are required on all USAccess Mobile Credentialing Units (MCUs in order to disable TLS 1.0.

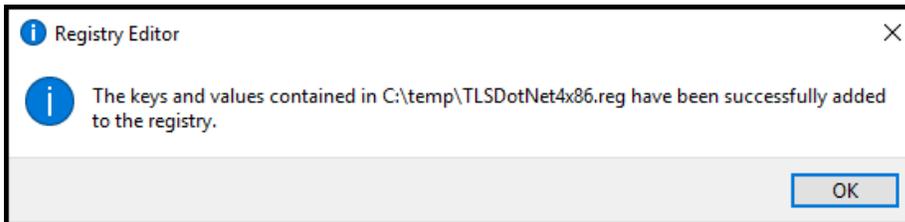
### 5.8.1 Registry Instructions for 64-bit Windows

- Navigate to **\\MCUInstaller\Install\common\USAccess\Manual\TLSDotNet4\_Updates**.
- Double click **TLSDotNet4x86.reg** to insert the entries into the Windows Registry.
- Click **Yes** when asked 'Do you want to allow this app to make changes to your device?'

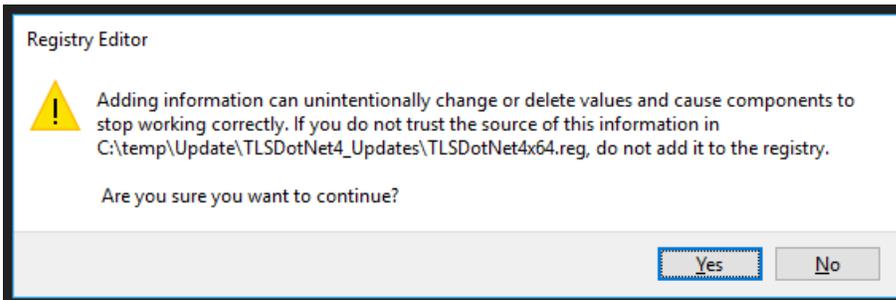
- Click **Yes** when asked 'Are you sure you want to continue?' by the Registry Editor message box.



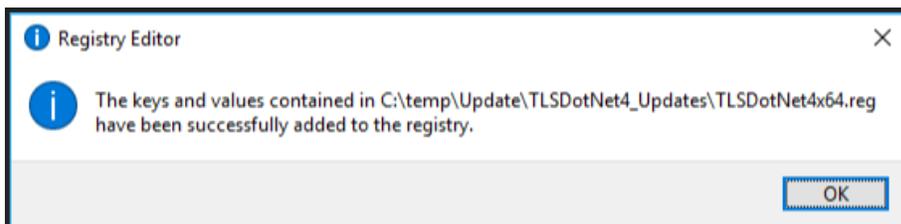
- Click **Ok** to complete the registry entry install.



- Double click **TLSDotNet4x64.reg** to insert the entries into the Windows Registry.
- Click **Yes** when asked 'Do you want to allow this app to make changes to your device?'
- Click **Yes** when asked 'Are you sure you want to continue?' by the Registry Editor message box.



- Click **Ok** to complete the registry entry install.

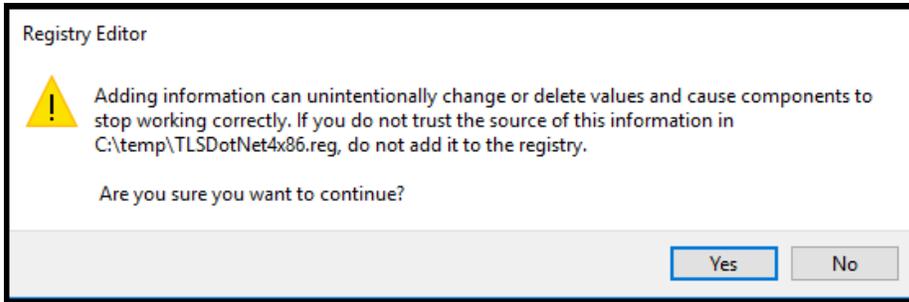


- Skip to the section labeled **TLS 1.2 Hotfix MSI**

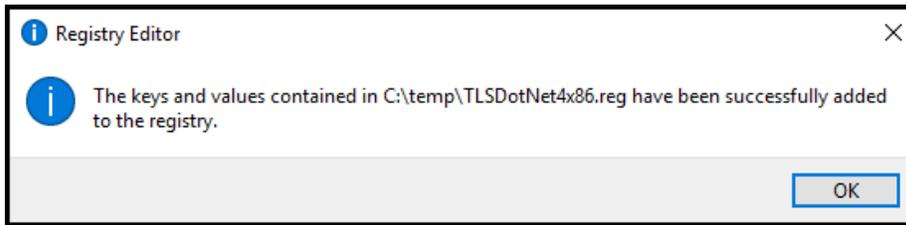
## 5.8.1 Registry Instructions for 32-bit Windows

- Navigate to **\MCUIInstaller\Install\common\USAccess\Manual\TLSDotNet4\_Updates**.
- Double click **TLSDotNet4x86.reg** to insert the entries into the Windows Registry.
- Click **Yes** when asked 'Do you want to allow this app to make changes to your device?'

4. Click **Yes** when asked 'Are you sure you want to continue?' by the Registry Editor message box.



5. Click **Ok** to complete the registry entry install.



## 6.0 MCU Local Printer Setup

If your site has an approved USAccess Local Printer, follow these steps to install it on the MCU. If you do not currently use a local printer, this section is not needed for your MCU.

**Do not connect your USAccess Local Printer until instructed below.**

### 6.1 Site Requirements

There are two keys provided to the locked card hopper. One should be with the Print Operator; the agency decides where second key goes.

**NOTE:** Never allow the print operator to have both keys.

Maintain a secure lockable cabinet or safe large enough to hold blank card stock and the locked card hopper from the printer.

The site should have ample electrical outlets and sufficient power to run the number of kits and printers you plan to operate.

Site should have enough space to comfortably hold the MCU, Printer, Print Operator, and Applicant. If Activation and/or Enrollment are taking place in the same room, additional space will be required.

### 6.2 Printer Unpack and Set Up

The following graphic shows Fargo 5000 printer once it is all set up.



Figure 70: Fargo 5000 Card Printer

#### 6.2.1 Unpacking the Printer

Printers purchased through the USAccess program are shipped in a Pelican case. Figure 71: Fargo 5000 Printer in Pelican Case shows the printer parts in a case.



Figure 71: Fargo 5000 Printer in Pelican Case

6. Unpack the printer and all parts and place them on a table. Determine the setup location of the printer. Ensure there is adequate space for all printer parts (printer, lamination module and card hoppers) next to the MCU it will be attached to.
7. **NOTE:** Do not attach the power supply cords to the printer and lamination module until instructed to do so.
8. Remove the Cleaning Kit and store it where it can be easily accessed by the Print Operator in the future. This kit is not needed until after the first 1,000 cards have been printed.

## 6.2.2 Assembling the Printer

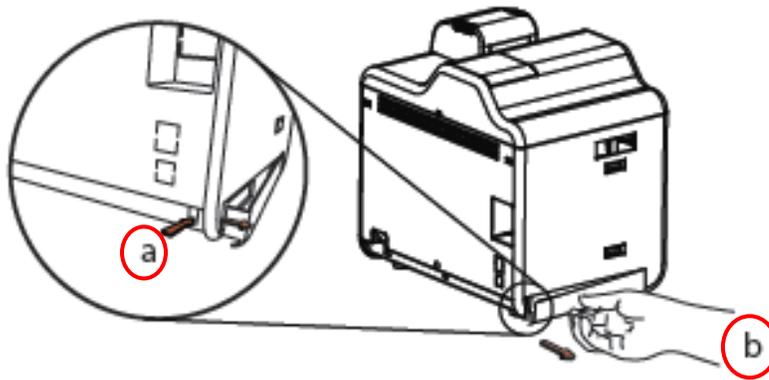
9. Set up the Printer next to the MCU.



Figure 72: Printer

10. Prepare the printer for adding the Flipper Module:
  - a. Release the latch on the upgrade cover by pulling out the pin shown in the figure below.

- b. Pull on the bottom of the upgrade cover to remove from the printer.



- 11. Using the Upgrade Tool provided (shown in the upper right corner in the figure below), remove and **save** the two screws from the bottom of the dual-sided printing module.

**NOTE:** The screw driver tool is packed in one of the plastic bags containing printer documentation.

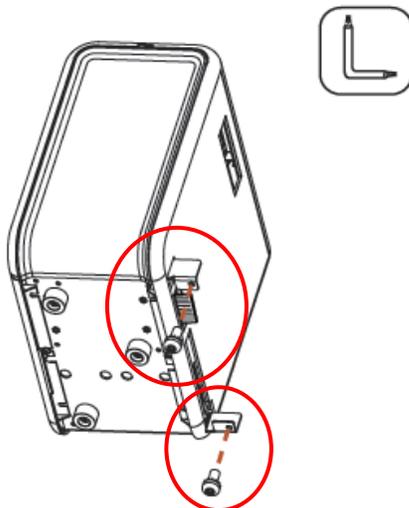


Figure 73: Dual Sided Printing Module

12. The Flipper Module has two L-shaped mounting tabs on the bottom, a circuit board connector and an internal USB cable, that fit into the corresponding slots on the Printer.

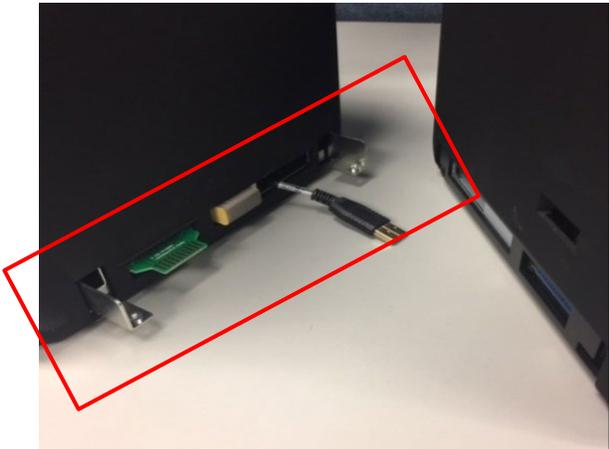


Figure 74: Flipper to Printer Connections

13. Connect the USB cable first.



Figure 75: USB Connected to Printer Module

14. Align the L-shaped tabs and circuit board to the printer, and gently slide the Flipper Module into the Printer, until they click in place.

**Note:** To avoid breaking the circuit board and to ensure a proper connection, apply minimal force.

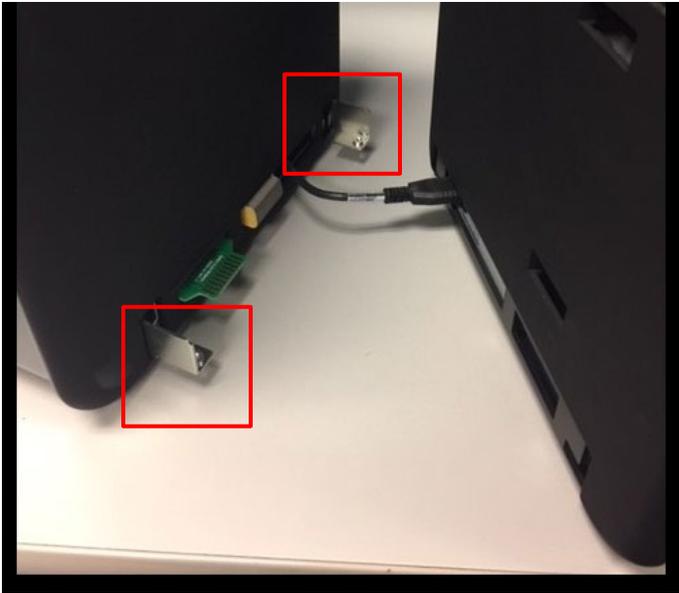


Figure 76: Connect Flipper to Printer

15. Once the two modules are connected, tip the whole printer on its back.



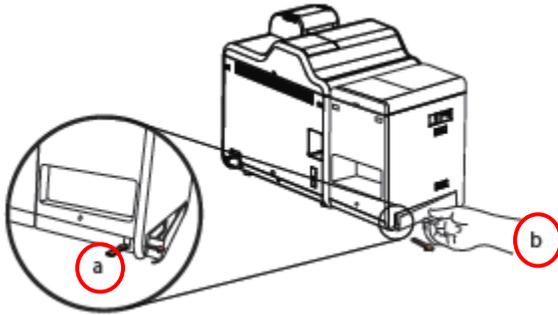
16. Using the Upgrade Tool and the two screws provided, secure the Flipper Module to the Printer. The two screws go into the holes on the left top and bottom side of the Printer.



Figure 77: Screws for the Printer

17. Prepare the Flipper Module for upgrade:

- a. Release the latch on the upgrade cover.
- b. Pull on the bottom of the upgrade cover to remove from the Flipper Module.



18. Using the tool provided, remove and save the two screws from the bottom of the Lamination Module.

19. The Lamination Module has two L-shaped mounting tabs on the bottom and a circuit board connector that fit into the corresponding slots on the Flipper Module. Align the tabs and circuit board to the slots, and gently slide the Lamination Module into the Flipper Module.

**NOTE:** To avoid breaking the circuit board and to ensure a proper connection, apply minimal force.



Figure 78: Lamination Module Connection

20. Tip the whole printer on to its back in order to secure with screws.



Figure 79: Printer Tipped Over

21. Using the Upgrade Tool and the two screws provided, secure the Lamination Module to the Flipper Module. The two screws go into the holes on the left top and bottom side of the Flipper Module.



Figure 80: Lamination Screw Placement

22. Stand the entire printer back upright on the table.

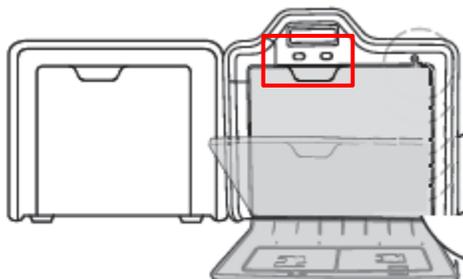
## 6.3 Installing the Cartridges

For a demonstration of how to do this in video, go to <https://www.youtube.com/watch?v=EptcV7iNuzo> for a video on how to change the different consumables.

### 6.3.1 Installing the Printer Film

Turn the power off on the printer before attempting to install any cartridges.

1. Push the door release on the printer front cover to open the printer.



2. Remove the HDP film cartridge by pressing down on the blue handle on the right and pulling the cartridge out.

**NOTE:** This cartridge has blue and orange rolls on the ends of the film.



3. Load Printer Ribbon into the ribbon cartridge. Note that the ribbon rolls are color coded. Start by placing the blue ribbon roll into the blue end of the cartridge and push gently until it clicks into place. Role the ribbon over the top and secure the orange roll into the orange end of the cartridge pushing gently until it clicks into place.



4. Check to make sure you rolled the ribbon over the correct side of the cartridge. To do this, the ribbon must be rolled over the small image of the ribbon on the cartridge with an up/down arrow, as shown below on the left. On the right below you can see another image of the ribbon with an X through it, showing the side of the cartridge that must not be covered by the ribbon.



5. Before placing the cartridge back in the printer, turn cartridge so the blue roller is on top, and tighten the top roller (as shown below) clockwise until taut.



6. Insert the cartridge back into the right side of the printer (match the orange and blue colors), until you hear it click into place.



### 6.3.2 Installing the Transfer Film

1. Remove the HDP film cartridge by pressing down on the blue handle on the left and pulling the cartridge out.

**NOTE:** This cartridge has green and yellow rolls on the ends of the film.



2. Load the Transfer Film into the cartridge. Note that the film rolls are color coded. Start by placing the yellow film roll into the yellow end of the cartridge and push gently until it clicks in place. Role the film over the top.



3. With the film in one hand, turn the cartridge on its side, and secure the green roll into the green end of the cartridge, pushing gently until it clicks in place.



4. Tighten the green roll by the ends, until you feel resistance.



5. Ensure you have the transfer film rolled over the correct side of the cartridge by checking to see that the film is not rolled over the image with the X through it as shown below.



6. Before placing the cartridge back in the printer, turn cartridge so the green roller is on top, and tighten the top roller (as shown below) counter-clockwise until taut.



7. Insert the HDP Film cartridge into the printer until it clicks.



8. Close printer front cover.

### 6.3.3 Installing the Laminate

Ensure the power is off to the Lamination module before inserting the lamination cartridges.

1. Pull open the Lamination module cover.

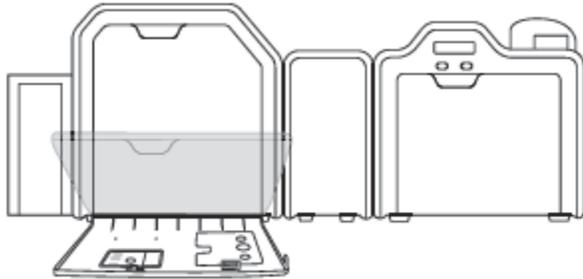


Figure 81: Open Lamination Module Cover

2. Store the upgrade tool in the empty space under cartridge 1.



Figure 82: Store Upgrade Tool

3. Pull out the laminate cartridges labeled 1 and 2.



- a. Laminate Cartridge 1 is to laminate the front of the card and has a square hole for the chip.
- b. Laminate Cartridge 2 is to laminate the back of the card and is perforated to only laminate half the card.
- c. Label Cartridge 1 as “Front of Card” and Cartridge 2 as “Back of Card” for future laminate replacements.

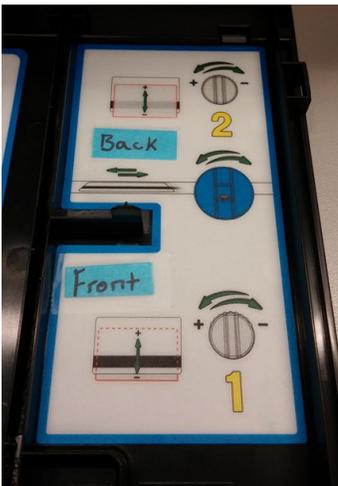
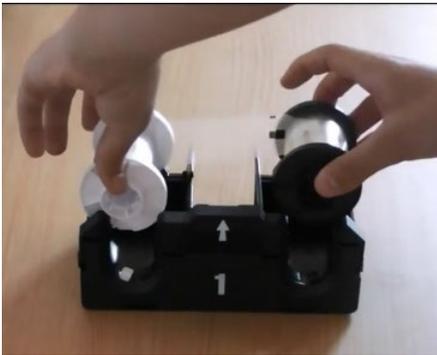


Figure 83: Label Laminate Cartridges

4. Beginning with Cartridge 1, load the laminate. With the “1” facing you, place the white roller in the left side of the cartridge and the black roller in the right side of the cartridge.



5. Gently press down on each side until they click in place.

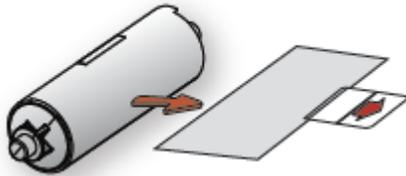
6. Tighten the Lamination roll by the black roll until you feel resistance.



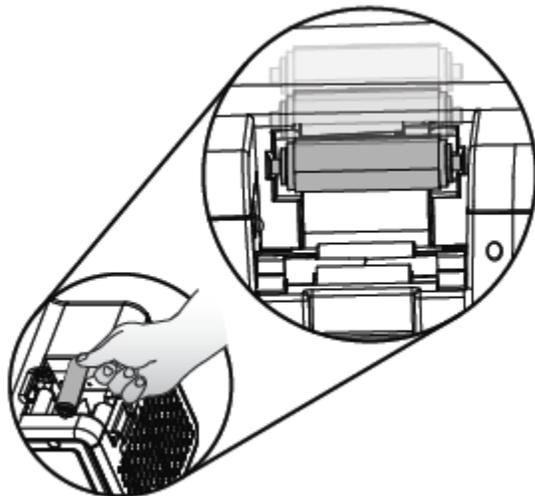
7. Repeat this process with Cartridge 2.
8. Insert the laminate cartridges back into the lamination module, pushing gently until they click in place.
9. Close the lamination module front cover.

### 6.3.4 Installing the Cleaner Roll

1. Locate the Cleaner Roll. A new roll comes with each printer ribbon.
2. Remove the protective sleeve from the card-cleaning roller.



3. Insert the card-cleaning roller into the card input area.



## 6.4 Card Input Cartridge and Output Hopper

**NOTE:** Be very careful to touch only the edges of the cards while loading and unloading the cards. NEVER touch the front or back of the cards.

1. Locate the locked Card Input Cartridge. Use the key to open the input cartridge.



Figure 84: Card Input Cartridge

2. Load cards face down with the chip pointing away from you into the card input cartridge.

**NOTE:** The card cartridge holds a maximum of 200 cards. Do not load more than 200 card into the cartridge; the suggested maximum to avoid possible card jams, is actually 150.

3. Lock the input cartridge and store the key in a safe place.
4. Place card input cartridge onto printer and push until it clicks.



Figure 85: Card Input Cartridge in Place

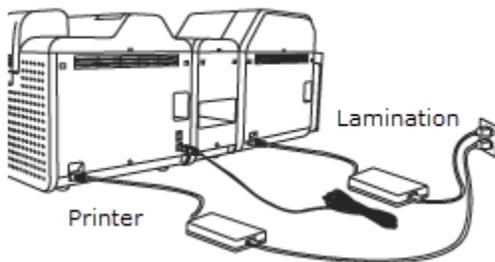
5. Locate the Card Output Hopper. Place card output hopper onto output side (left) of the lamination module and push down until it clicks.



Figure 86: Card Output Hopper

## 6.5 Connect the Printing Unit

The lamination module requires a separate power strip from the MCU and printer. The separate power strip is used because there is no power button on the lamination module and the printer will not recognize the lamination module unless it is powered on when the printer is powered on. To turn the lamination module off, you must turn off power at the power strip. The lamination module must be powered on before the printer.



1. Connect the Lamination module power supply to the lamination module and the printer power strip.  
**CAUTION:** Connect the Lamination module power before the Printer power.
2. Connect the Printer power supply to the printer and plug it into the surge protector for the MCU.
3. Connect the USB cable to the back of the printer.
4. Connect the other end of the USB to the PTR port on the MCU. Label the cord and port for future installations.

**NOTE:** Do NOT plug the printer USB cable into the hub. The printer USB must be plugged into the PTR port on the laptop and must be plugged into the same port each time.

**NOTE2:** If the printer is plugged into a different port from initial installation, the MCU may install a second printer showing two printers in the Device and Printers list.

## 6.6 Installing the printer on the MCU

1. Login to the laptop with Administrative Rights.
2. Right click the **Start** button and select **Control Panel**.

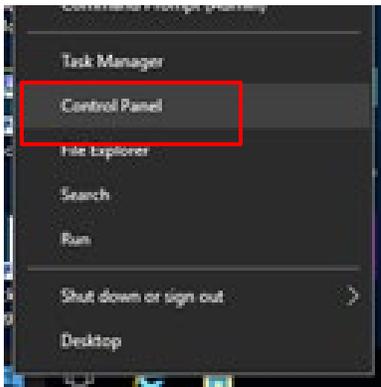
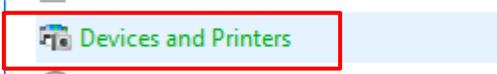


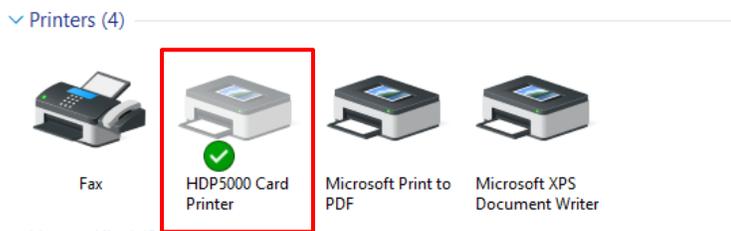
Figure 87: Windows Control Panel

- From Control Panel select **View devices and printers**.



- If there is already an HDP5000 printer icon or multiple HDP5000 printer icons, delete them.

**NOTE:** If there are no HDP5000 icons proceed to 6.7 Installation and Configuration.



- Right click the HDP5000 Card Printer icon and select **Remove device**. The Remove Device window displays, click the **Yes** button.

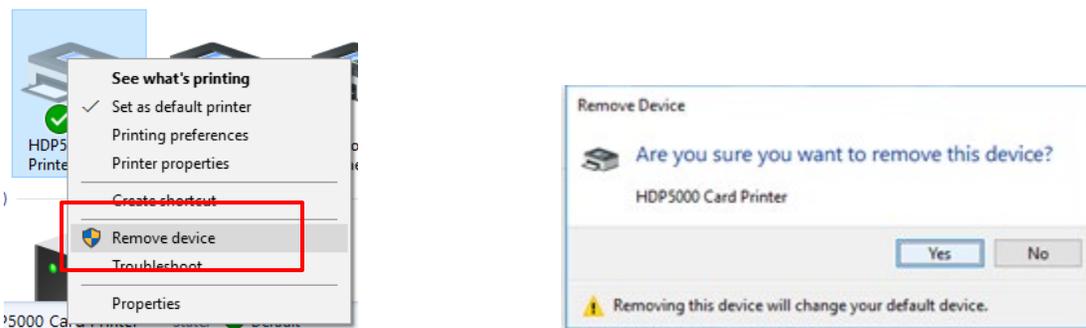


Figure 88: Delete Existing HDP5000 Printers

## 6.7 Installation and Configuration

2. Plug your USAccess local Printer into the port labeled PTR on the laptop.

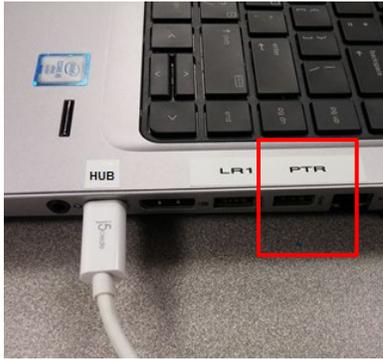
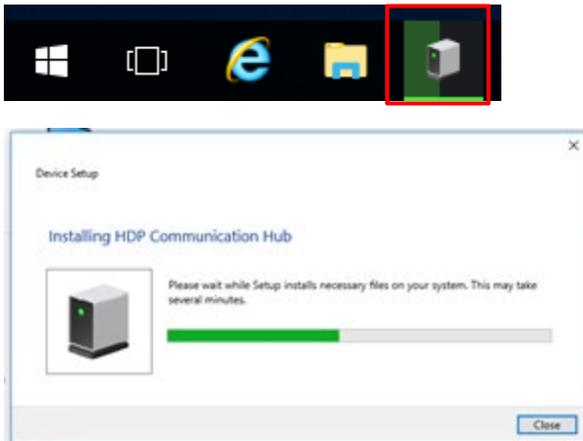
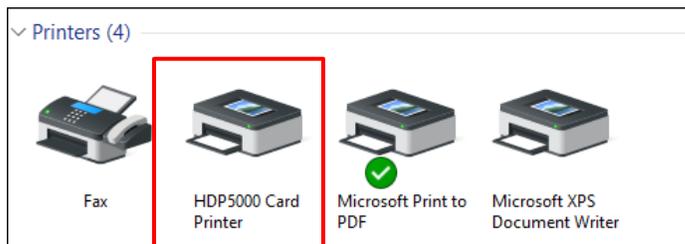


Figure 89: Printer Port

2. The installation icon displays in the taskbar. Click the installation icon for more details and wait for installation to complete.



3. You should now see the HDP5000 printer icon appear in the Devices and printers window.



4. Right click the HDP5000 printer and select **“Set as default printer”**.

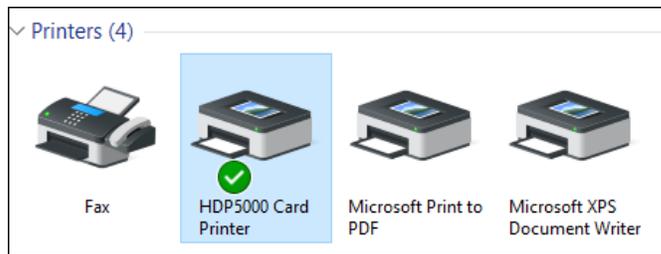
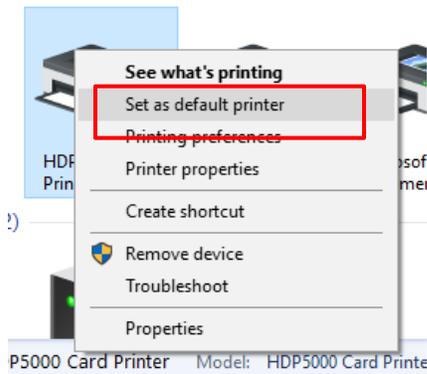


Figure 90: Set As Default Printer

## 6.2 Printer Configuration

1. Right click the HDP5000 printer and select **Printer Properties**.

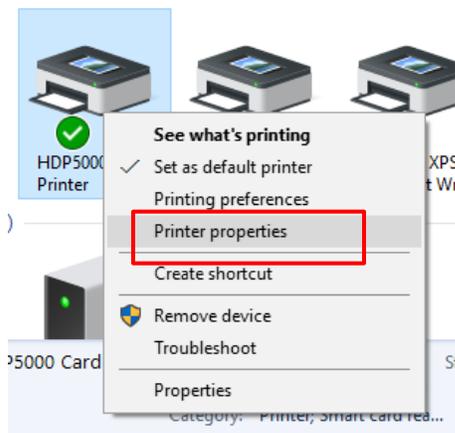


Figure 91: Printer Properties

2. Click on the *Security* tab.

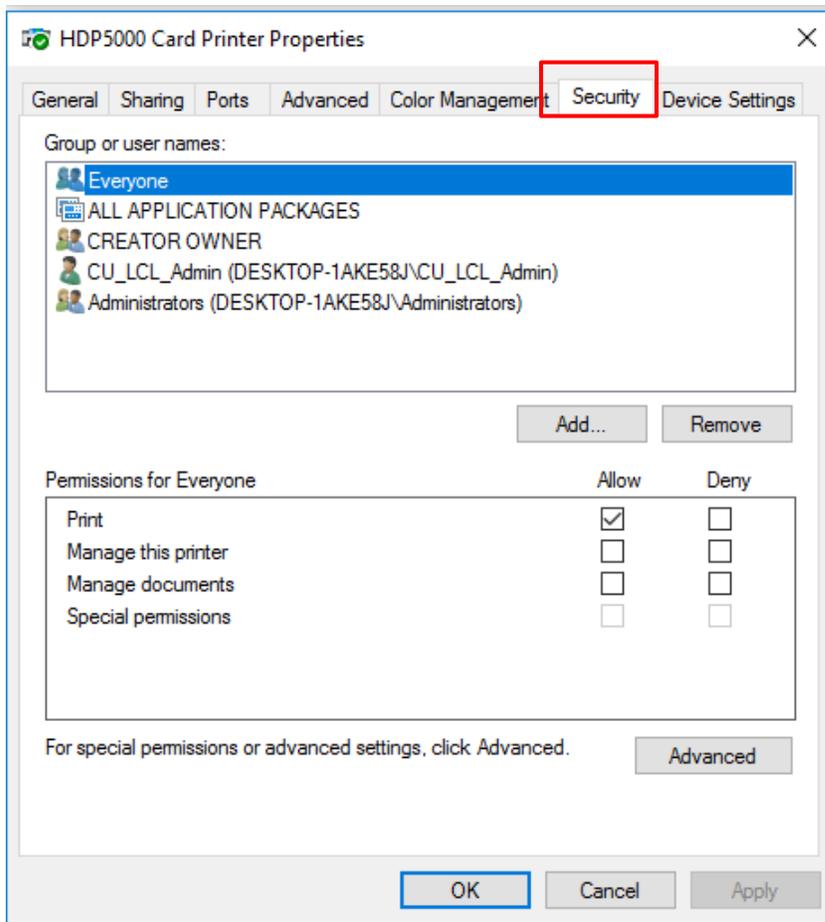


Figure 92: Printer Configuration Security Tab

- From the **Group or user names** section, select **Everyone**.
- In permissions for Everyone check the Allow box for **Manage this printer** and **Manage documents**.
- Click the **OK** button.

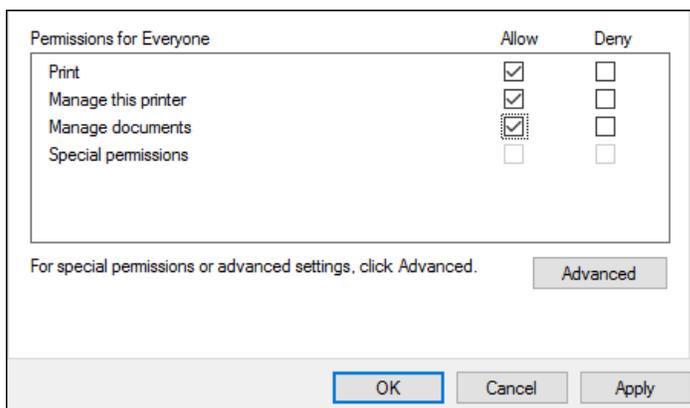


Figure 93: Printer - Everyone Rights

- Right click the HDP5000 and select **Printing preferences**.

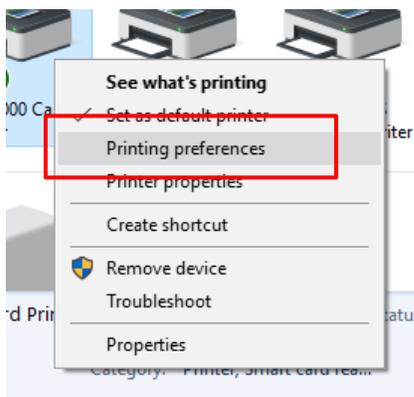


Figure 94: HDP5000 Printing Preferences

7. If not already displaying, click the *Card tab*. From the *Card tab*, select **ToolBox**.

Figure 95: Printing Preferences - Card Tab

8. In Toolbox, select the *Advanced Settings tab*.

- a. Change **Print Top of Form** setting. Take Default setting and then subtract 25, insert sum into Current field. Note: Numbers can be set to negatives.
- b. Change **Transfer TOF** setting. Take the Default setting and then add 25, insert total into Current field

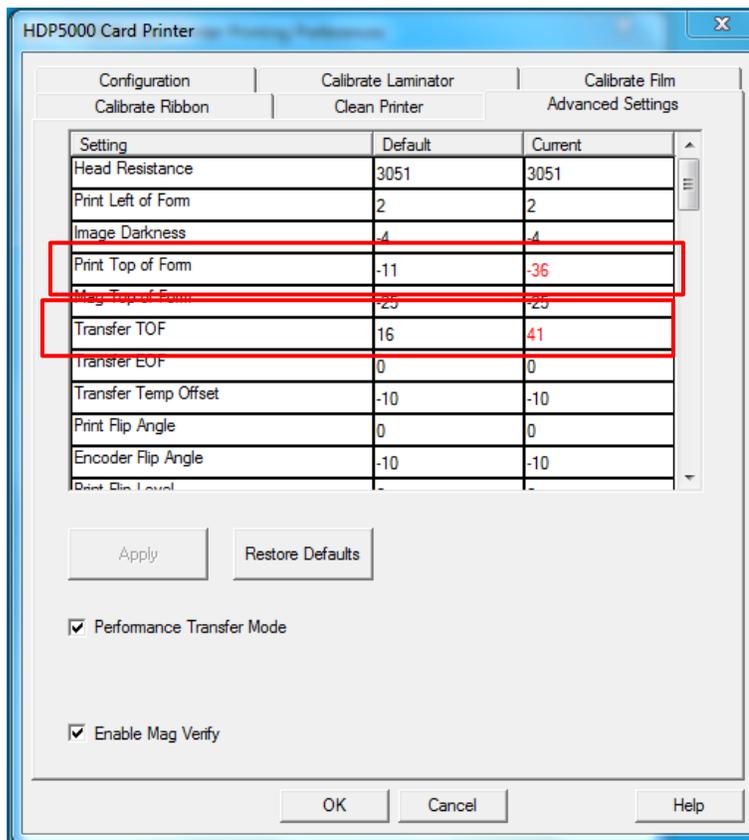


Figure 96: Advanced Setting Tab

9. Click the **OK** button to close Toolbox.

10. The system returns to the **Printing Preferences** page.

11. Select the *Device option* tab.

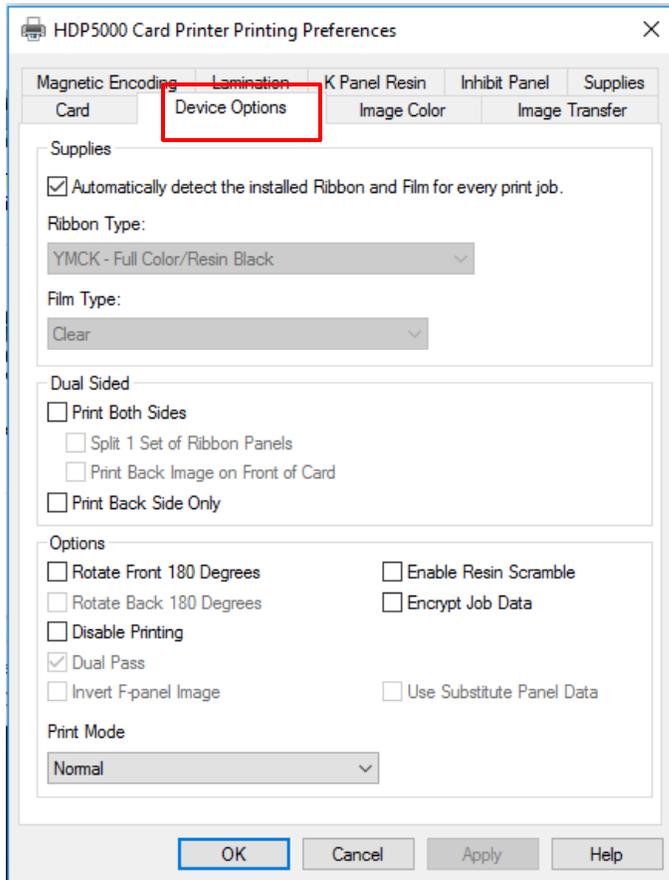


Figure 97: Device Options Tab

12. In the **Dual Sided** section check the box for **Print Both Sides** and click **Apply**.

**NOTE:** If the “Split 1 Set of Ribbon Panels” is checked, UNCHECK it. Do NOT check this box as it can make the font on the back of the card blurry.



13. Select the *Lamination* tab.

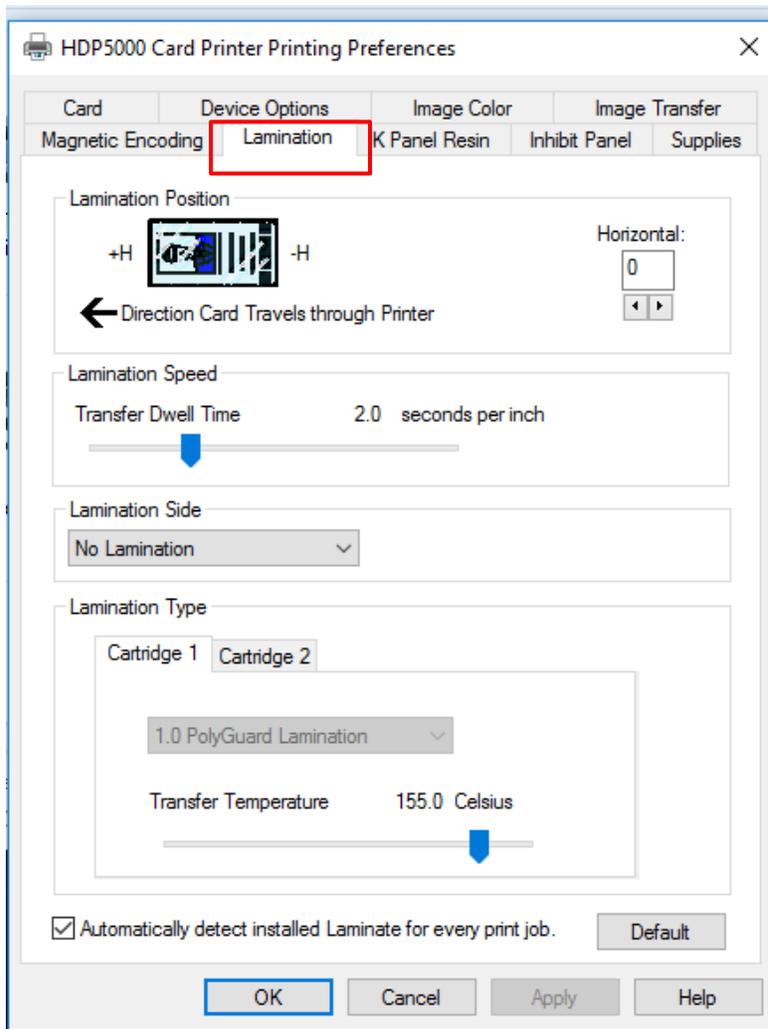
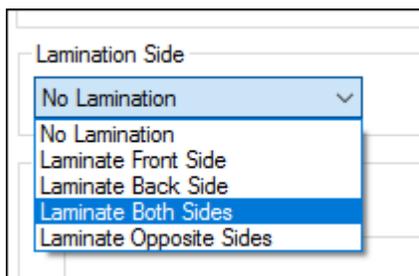


Figure 98: Lamination Tab

14. Use the dropdown in the **Lamination Side** section and select **Laminate Both Sides**.



15. Click the **OK** button.

## 6.3 Configure Local Print Utility

Configure the Local Print Utility next.

1. Click **Start, All Programs, Personal Credential Assistant, Local Print Utility**.

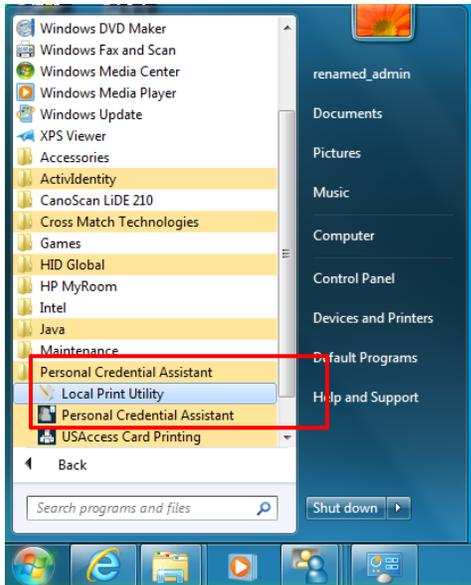


Figure 99: Local Print Utility

2. The Print Utility application opens up. Press the **Get Printer Information** button. (This is also where you find your consumable levels.)

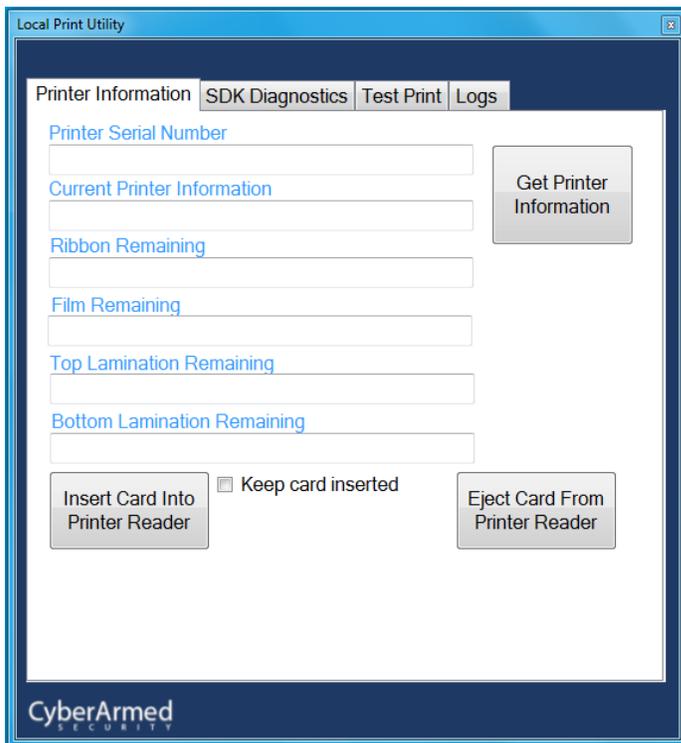


Figure 100: Populate Printer Information

- The printer information populates in the utility. This is where you get your printer serial number to enter into the Site Manager. This **MUST** be in Site Manager before printing can begin.

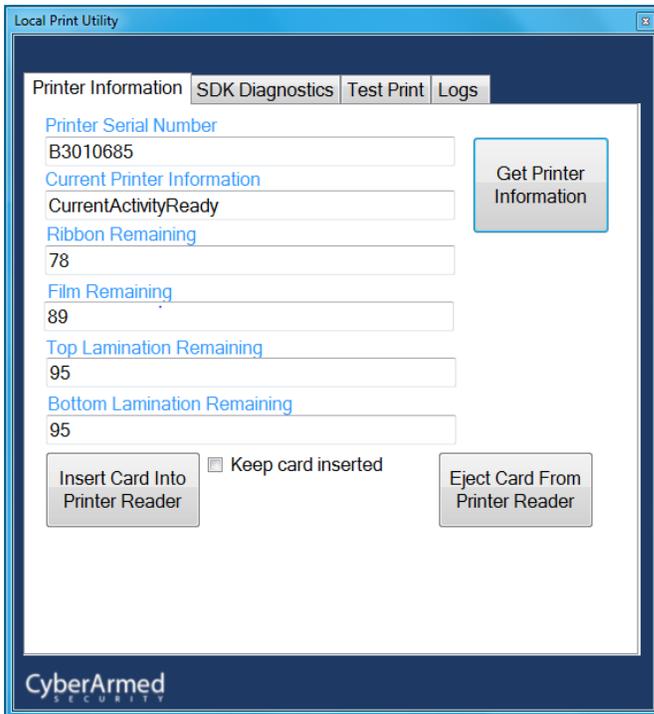


Figure 101: Printer Serial Number and Consumable Levels

- Click the *Test Print* tab.

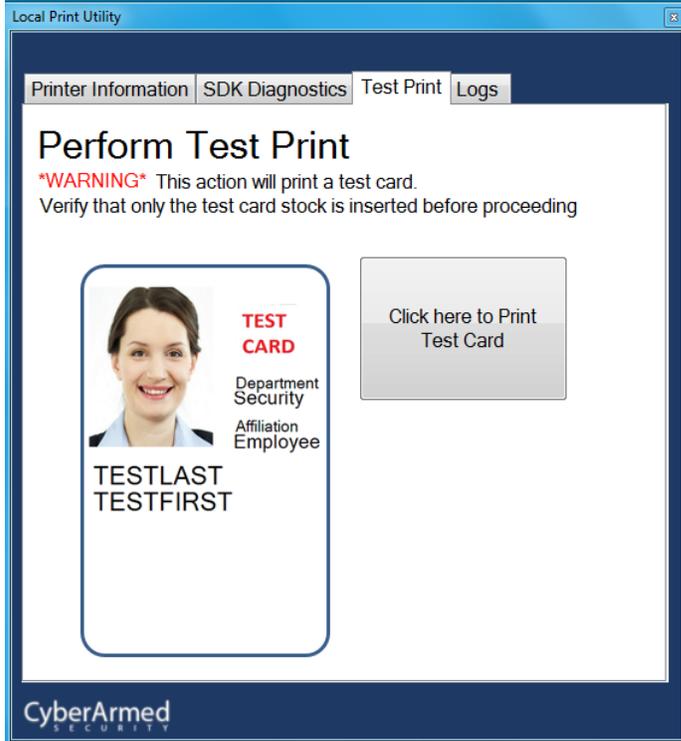


Figure 102: Test Print Tab

- Ensure card stock is properly loaded into the card hopper. See section X for instructions. Then click the **Click here to Print Test Card** button.

6. A warning message displays. Click the **Yes** button if you are ready to proceed. Click the **No** button to cancel the test print.

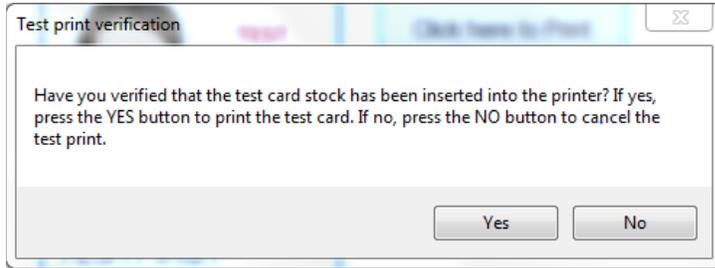


Figure 103: Check Card Stock Verification

7. If you clicked Yes, the test card prints. If you clicked No, the Test Print is cancelled. **NOTE:** There may be a warm up period of several minutes before the test card prints.
8. If anything goes wrong, click the *Logs* tab, and click the **View Logs** button.

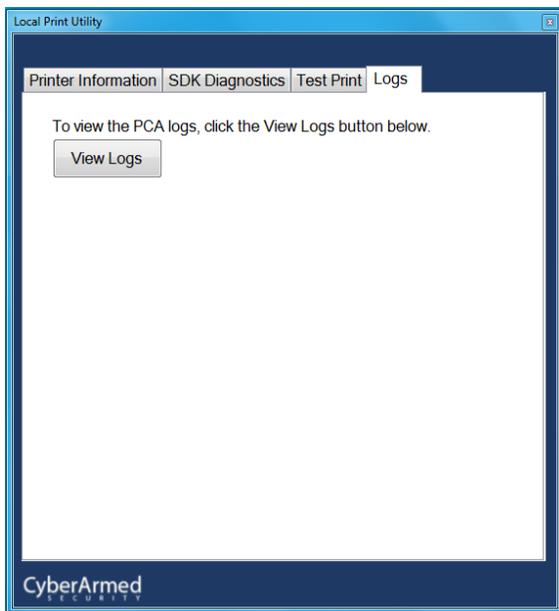


Figure 104: View Logs Button

9. A sample log file is shown below.

```

2016-02-05 17:36:08,161 [1] DEBUG LogFileAppender Initializing MainviewModel class
2016-02-05 17:36:08,179 [1] DEBUG LogFileAppender In the shell constructor
2016-02-05 17:36:08,179 [1] DEBUG LogFileAppender attempting to determine if the theme manager is instal
2016-02-05 17:36:08,179 [1] DEBUG LogFileAppender verifying theme manager library is loaded.
2016-02-05 17:36:08,180 [1] DEBUG LogFileAppender successfully verified theme manager library is loaded.
2016-02-05 17:36:08,180 [1] DEBUG LogFileAppender verifying bioadaptor library is loaded.
2016-02-05 17:36:08,180 [1] DEBUG LogFileAppender successfully verified bioadaptor library is loaded.
2016-02-05 17:36:08,268 [1] DEBUG LogFileAppender
2016-02-05 17:36:08,268 [1] DEBUG LogFileAppender ----- PCA Application startup -----
2016-02-05 17:36:08,268 [1] DEBUG LogFileAppender Initializing the Bootstrapper class
2016-02-05 17:36:08,272 [1] DEBUG LogFileAppender attempting to parse command line parameters.
2016-02-05 17:36:08,272 [1] DEBUG LogFileAppender command line variable is c:\Program Files\CyberArmed\F
2016-02-05 17:36:08,273 [1] DEBUG LogFileAppender running in activation mode. will show the activatin ic
2016-02-05 17:36:08,800 [1] DEBUG LogFileAppender Starting the loading Thread.
2016-02-05 17:36:08,811 [4] DEBUG LogFileAppender In the Bootstrapper Load() method
2016-02-05 17:36:08,836 [4] DEBUG LogFileAppender obtaining workstation id
2016-02-05 17:36:08,837 [4] DEBUG LogFileAppender theme manager configured for site manager support
2016-02-05 17:36:08,837 [4] DEBUG LogFileAppender attempting to initialize the site manager plugin
2016-02-05 17:36:08,837 [4] DEBUG LogFileAppender successfully initialized the site manager plugin
2016-02-05 17:36:08,837 [4] DEBUG LogFileAppender attempting to retrieve the workstation ID
2016-02-05 17:36:08,846 [4] DEBUG SiteManager generating the machine id
2016-02-05 17:36:11,335 [4] DEBUG SiteManager successfully generated the machine id
2016-02-05 17:36:11,335 [1] DEBUG SiteManager retrieving the system id from site manager.
2016-02-05 17:36:32,704 [4] DEBUG SiteManager workstation is active.
2016-02-05 17:36:32,704 [4] DEBUG SiteManager successfully obtained the workstation id
2016-02-05 17:36:32,704 [4] DEBUG SiteManager workstation ID is: QJ3CSA
2016-02-05 17:36:32,704 [4] DEBUG LogFileAppender successfully obtained the workstation ID
2016-02-05 17:36:32,704 [4] DEBUG LogFileAppender setting workstation ID to: QJ3CSA
2016-02-05 17:36:32,705 [4] DEBUG LogFileAppender initializing the biometric reader
2016-02-05 17:36:32,735 [4] DEBUG LogFileAppender initializing the smart card reader service
2016-02-05 17:36:32,766 [4] DEBUG LogFileAppender Attempting to initialize the smartcardreader class
2016-02-05 17:36:32,776 [4] DEBUG LogFileAppender Attempting to initialize the _pivCardReader class
    
```

Figure 105: Sample Log File

10. Your test cards may or may not have a chip on the front. Before printing test cards, check with your Agency Lead and follow established agency procedures.



Figure 106: Successful Test Card Print

## 6.4 Designate Print Operation Role

Designate one or more PIV Credential holders as Print Operator(s) (PO). Request your USAccess Role Administrator assign the role of PO to the person(s) who will be printing cards.

## 6.5 Site Manager Set Up

Before logging into Site Manager, retrieve the Serial Number from the bottom of your printer. You must have the correct serial number to enter into Site Manager. If your MCU that will have the printer attached has not already been added to Site Manager, you will also need the USAccess System ID for the MCU.

This must be complete before attempting to print any cards.

1. Log into Site Manager as an Agency Site Manager (ASM) or Local Site Manager (LSM) at <https://portal.usaccess.gsa.gov/ServicesPortal>.

- If necessary, click your role.

Figure 107: Select Site Manager Role

- Search for and select the site where the printer is located.

Figure 108: Site Search

- Click the **Workstations** link to the left of the site name.

EDIT SITE	WORKSTATIONS	System ID	Site Name	Agency
		10001	GSA, USACCESS STATION 1033A , WASHINGTON , DC 20405	ROB/NCR DIVISION OF SUPPORT SERVICES

Figure 109: Workstations Link

- If your MCU is present, skip to step 8. To add a workstation, click the **Add Workstation** button.

Figure 110: Add Workstation

- Enter the **Workstation System ID** and **Start Date** (today's date or greater). Leave the End Date blank for now, unless you have a specific date the kit will be shutting down. Click the **Validate** button.

Figure 111: Add MCU Workstation Information

- Once validated, click the **Add** button.
- The list of workstations displays.

5BCZZ4	06/03/2017	02/01/2019	Light Credentialing Solution	<a href="#">Edit Workstation</a>	<a href="#">Workstation Schedule</a>	<a href="#">Printers</a>
GHS7M	02/17/2016	02/01/2019	Light Credentialing Solution	<a href="#">Edit Workstation</a>	<a href="#">Workstation Schedule</a>	<a href="#">Printers</a>
RDC5X5	02/05/2019		Mobile CU	<a href="#">Edit Workstation</a>	<a href="#">Workstation Schedule</a>	<a href="#">Printers</a>

Figure 112: Workstation List

- To add a local printer, click the **Printers** button next to the workstation to which the printer is connected.
- The printer list for that workstation displays. From here you can edit the printer, delete the printer, or add a new printer.

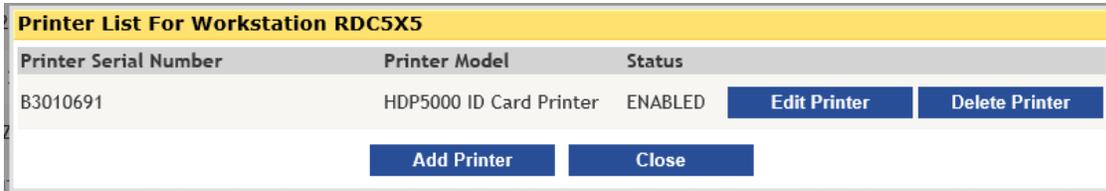


Figure 113: Add Printer to MCU

- Click the **Add Printer** button.
- The Add Printer for Workstation X displays. The **Printer Status** radio button is disabled.

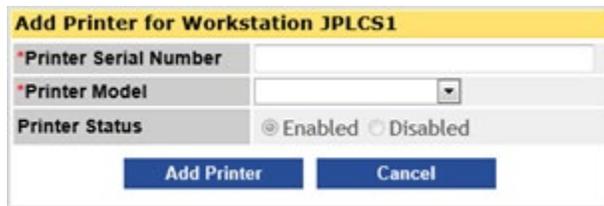


Figure 114: Add Printer Information

- Enter the Serial Number (SN) off the bottom of the printer, in the **Printer Serial Number** field.
- Select the correct model from the drop down box next to **Printer Model**.
- Click the **Add Printer** button.
- Close Site Manager.

## 6.6 Run Local Printing Connection Test

- From the desktop double click the Network Test Tool.



2. Click the **Local Printing** radio button, and click the **Run** button. Check Test Status, all should show “Completed Successfully”.

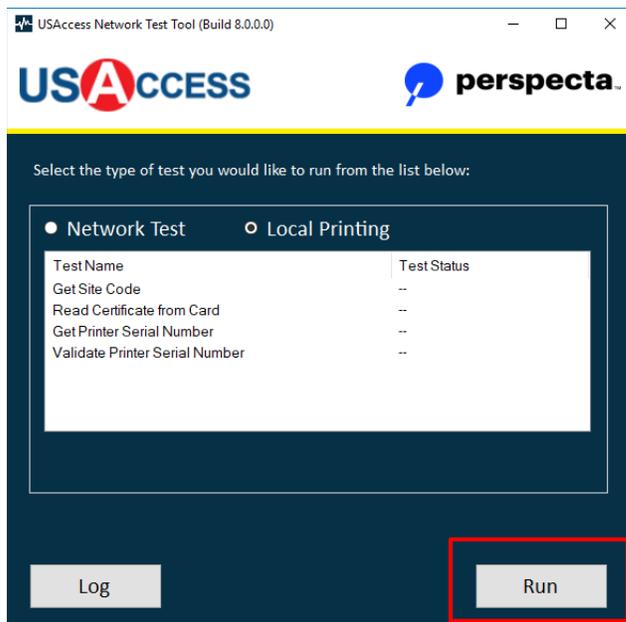


Figure 115: Local Printing Test

3. If any of the tests failed, click the **Log** button to review any errors that occurred, which will lead you to troubleshooting.
4. Close the Network Test Tool.

**Local Print installation is complete.**

## Appendix A – Repacking the CU for Shipment

To pack the Credentialing Unit transport case, follow the steps below. Check off the inventory control sheet as you pack. Below is a picture of an empty case.

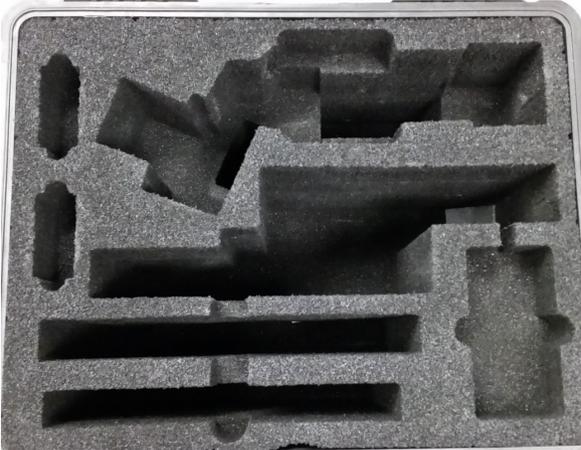


Figure 116: Top Layer of Equipment Packing

1. Pack the following in the box.
  - a. The camera, tripod, camera power supply, and camera USB cable (make sure cap is on camera lens and tripod is loose enough to swivel) go in at the top of the box, camera lens facing toward the left of the case. Make sure that the flash of the camera is pushed down before you place in the case.
  - b. Suprema scanner with attached USB cable (window facing toward the front case with cord in cutout at the rear) and the cleaning cloth
  - c. Insert Laptop (make sure powered off)
  - d. Insert Document Scanner (Lock on bottom of scanner is in “Locked” position)
  - e. Insert two card readers top sides down with bases attached



Figure 117: Equipment Packing

2. Items to be securely packed in the General Accessory section:
  - a. Laptop power supply
  - b. Optical Mouse
  - c. Cleaning cloth
  - d. Cannon Flatbed Scanner USB cable
  - e. Photo backdrop (blue screen)
  - f. Targus USB Keypad
  - g. j5 Create 7 port Powered USB-C Hub w/ power supply and USB-C cable
  - h. APC 8 Outlet Network SurgeArrest 8 Outlet
  - i. Belkin Six foot USB Extension Cable for Digital Camera
  - j. Belkin CAT6 Network Cable 30FT BLU
3. Place the following on top after all equipment is packed
  - a. Inventory Control Sheet (document).
4. Close the lid and lock the four latches.

**NOTE:** The latches are not fully locked until two clicks are heard.



**Figure 118: Closed Latch**

5. Lock the combination on the padlock.
6. Attach the shipping label pouch to a side of the case.