

USAACCESS Program

Registrar Quick Reference Guide

Version 4.3

May 2019



This page intentionally left blank.

Table of Contents

Table of Contents	i
About this Guide	iii
Page Elements	iii
Key Information.....	iii
Procedures.....	iii
Registrar Job Aid List	iv
The Credentialing Unit Workstation	1
Credentialing Center Operations	3
Site-specific Orientation	3
Attendance.....	3
Daily Setup.....	3
Handling USAccess Credentials.....	5
Damaged and Defective USAccess Credentials	5
Appointment Management Procedures	6
Checking Appointments In and Out.....	9
Cancelling Appointments	10
Resources for Registrars and Activators	11
USAccess Help Desk.....	11
TRACKS Web Site.....	12
TRACKS Log In Process	12
TRACKS Web Site Features	14
Applicant Enrollment Procedures	17
Log in to Assured Identity	17
Search for Applicant’s Record	20
Capture Biographic Information	21
Scan Identity Documents.....	23
Capture a Photo.....	27
Capture Fingerprints	29
Rolled Fingerprints.....	29
Slap Fingerprints.....	31
Primary and Secondary Fingerprints	32
Complete the Enrollment Process	33
Fingerprint Capture Exceptions	35
Amputee.....	35
Extra Fingers	38
No Fingerprints Captured	38
Fingerprint Verification Failures	41
Fingers with Long Fingernails.....	43
Re-enrollment and Reissuance	44
Re-Enrollment Procedure	44

Table of Contents

- Activation Procedures..... 46**
 - Unattended Activation..... 46
 - Attended PIV USAccess Credential Activation with Fingerprints 46
 - Searching for the Applicant..... 49
 - Initiating Credential Activation 51
 - Verifying the Applicant’s Fingerprint against the Database 53
 - Completing the Information Gathering Screen 54
 - Agreeing to the Acknowledgement of Responsibilities..... 56
 - Digitally Signing the Acknowledgement of Responsibilities 56
 - Completing the USAccess Credential Activation 57
 - Attended USAccess Credential Activation without Fingerprints 58
 - Activation Errors and Error Messages 59
 - Fingerprint Verification Errors 59
 - Card Activation Error Messages 60
 - PIN Reset..... 63
- Appendix A – Enrollment Process Flow..... 67**
- Appendix B – Terms and Acronyms 69**
- Appendix C – Definitions 71**
- Appendix D – Homeland Security Presidential Directive 12 73**

About this Guide

Page Elements

The names of Web pages, menu options, fields, and buttons are shown in bold text. For example, “On the **Login** page, enter the User ID in the **User ID** field.” A list of acronyms used in this document can be found in Appendix A, and a list of Figures is located in Appendix D.

Key Information

Key information is emphasized with a graphic adjacent to the information presented in a shaded area. This User Guide uses three types of key information emphasis:



Tip

A Tip provides you with a helpful tip or shortcut.



Key Point

A Key Point gives you information that aids in your understanding of the task or concept presented.



Watch Out!

A Watch Out! Warns about some feature of the software or an action that may cause problematic results or a breach of security.

Procedures

Procedures are written in numbered steps, including the details necessary to complete each task. Screen shots and notes are included as needed.

Registrar Job Aid List

This guide contains some of the content for the following Registrar Job Aids. The entire list of Job Aids is also available on TRACKs, which is discussed later in this guide:

- Enrollment Procedures
- Acceptable Forms of Identification
- Fingerprinting Guide
- Registrar Daily Checklist
- Attended Credential Activities Guide
- Unattended Credential Activities Guide
- Identity Documents Mismatch
- PIV Process Flow Diagram

This page intentionally left blank.

The Credentialing Unit Workstation

USAccess Credentialing Centers may be configured as Fixed Credentialing Unit (FCU) or Mobile Credentialing Unit (MCU) workstations. All Credentialing Units consist of these elements:

- | | |
|------------------------------|-----------------|
| Laptop with mouse | Digital camera |
| Flatbed scanner | Camera tripod |
| Fingerprint capture device | Numeric keypad |
| Two Omnikey card readers | USB Hub |
| Photo backdrop (blue screen) | Surge protector |

- Supplied by the site:
 - Worktable
 - 2 chairs

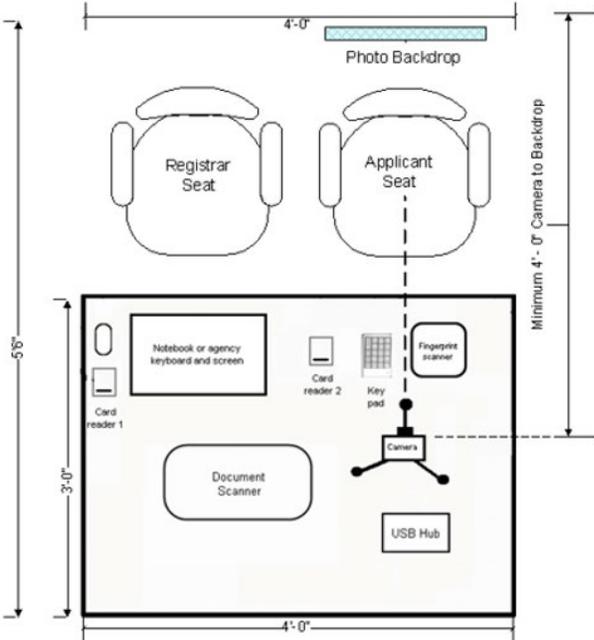
Fixed Credentialing Units include all items listed above and a hardware VPN router. FCUs are managed by USAccess, so all software and application updates are pushed to the FCUs remotely and without the need for on-site support. FCU hardware cannot be moved or altered in anyway without advanced approval from the MSO.

Mobile Credentialing Units include all items listed above and come in a locked Pelican case. MCUs are managed by your agency, and are designed to operate on your agency approved network connection. Software and application changes will be updated by a site POC and/or local IT administrator. MCUs are designed to be mobile and connect to any agency approved network connection. No advanced notice is required to move a Mobile CU.



The following schematic illustrates the minimum footprint at a USAccess Credentialing Center.

USAccess Program CU Setup



Credentialing Center Operations

In your role as Registrar, you are responsible for many of the daily procedures that contribute to the management of your Credentialing Center. Each Agency and site has its own policies. You need to learn about the unique aspects of your center and responsibilities there prior to reporting for duty.

Site-specific Orientation

Your supervisor defines the following:

- Hours of operation
- Methods for documenting your time (time cards)
- Policies regarding breaks, lunch, etc.
- Center points of contact (POCs)
- Policies for handling USAccess Credentials including destruction of USAccess Credentials
- Referral telephone numbers

If you have any questions, be sure to contact your supervisor for clarification. It is your responsibility to ask for more clarification when needed.

Attendance

Registrars and Activators have the responsibility to ensure that the Credentialing Center is open and ready to receive Applicants during the hours of operation. USAccess recommends that you should arrive approximately 15 minutes before the stated opening time so that you have time to open the Center and check that all of the systems are functional using the Registrar's Daily Checklist.

If you are unable to come to work for any reason, contact your supervisor as far ahead as possible so that alternate arrangements can be made. Your supervisor may have the ability to arrange for a replacement Registrar or Activator to cover for you and will need some time to make the necessary arrangements.

If your supervisor is unable to arrange for another Registrar or Activator to take your place, he or she should arrange to have your Site Manager block the schedule if you use the GSA Online Scheduling System. It is the site's responsibility to contact and cancel any appointments that cannot be accommodated. Once appointments are cancelled, Applicants receive an e-mail advising them of the cancellation and requesting that they reschedule an appointment using the Assured Identity Scheduler System.

Daily Setup

When you arrive, unlock the Credentialing Center door and perform the activities necessary to set up the center. These activities include:

- Ensuring that Welcome signage and any explanatory handouts provided by your Agency Lead are in place. Since there is no designated person to greet Applicants, the signage and handouts play a vital role in alerting the Applicants to center operations.

- Following the steps in the Registrar's Daily Checklist to check the Credentialing Unit and perform the equipment and application daily test.
- Check the lighting to make sure that the room lights are working properly and close/open the window blinds as appropriate. The digital camera is set to function properly without flash in lighting conditions that are normally found in an office environment.
- Ensure camera and chair are in proper places. The camera and Applicants chair are stationary and may be inadvertently moved during the day. However, tape lines may be in place to indicate where the camera and chair must reside in order to capture an acceptable photo.

At the end of the day, you must:

- Log off the Assured Identity Application.
- Cancel all no-shows in the Assured Identity Scheduler (if your site uses the Scheduler.)
- Close the Assured Identity Scheduler (If your site uses it.)
- Close all open Windows on the Credentialing Units (CUs), and Light Activation (LA) workstations.
- Log out of Credentialing Unit(s).
- Remove your PIV credential if still in the reader.
- Press Ctrl+Alt+Del and click the Lock Computer button on the pop-up window.
- Do NOT turn off the Fixed CUs (those connected to a VPN router). The Fixed CUs need to be on for remote maintenance to occur in the evenings and on weekends.
- Lock up any credentials ready for pickup.
- Lock the door when you leave.

Handling USAccess Credentials

USAccess Credential handling is site and agency specific. There are several situations in which you may be asked to handle USAccess Credentials. These include:

- Receiving the Credential from the shipper and storing before activation.
- Handing out Credentials for activation.
- Collecting damaged, defective, or expired Credentials.

Again, procedures for receiving, storing, and destroying Credentials, and handing them out for activation are site specific. Your agency provides you with proper procedures should you need to perform these tasks.

Damaged and Defective USAccess Credentials

USAccess Credentials may be damaged during the activation process or in rare situations, arrive defective from the manufacturer. It may be impossible to determine if a Credential's failure to activate is due to damage or defect. Defective Credentials are replaced by the manufacturer without cost to the USAccess Program.

With a card that will not activate, call the USAccess Help Desk and follow the directions given to you.

Appointment Management Procedures

Assured Identity Scheduler, also known as AI Scheduler, is a Web portal that serves as an appointment book, allowing Registrars and Activators to manage appointments scheduled online by Applicants. These tasks include:

- Checking appointments in and out
- Cancelling appointments

Appointments in the AI Scheduler are scheduled every 15-30 minutes (depending on the site's request) for a specific workstation. Applicants are asked to arrive early for their appointments and set aside an adequate amount of time in their personal schedule for their enrollment or activation (approximately 15 minutes). Use your own judgment and flexibility when working with people who arrive late and attempt to fit them in if possible. You may need to take people out of turn.

If there are multiple workstations in your center, it may also be possible to use a different Credentialing Unit for enrollment or activation after checking the Applicant into the AI Scheduler.

The AI Scheduler can be accessed through the desktop icon, or through a browser at <https://portal.usaccess.gsa.gov/aisso>



AI Scheduler

Desktop Shortcut to AI Scheduler

Registrars and Activators who are assigned those roles can log in to the AI Scheduler using their PIV credential. If you cannot login, first check with your Role Administrator to ensure you were assigned the correct roles, then if so, contact the USAccess Help Desk to request login credentials for the scheduler. Follow these steps to log in:

1. Log in to the Credentialing Unit.
2. Select the **AI Scheduler** desktop icon.

The PIV Credential Login screen displays in your browser.

PIV Credential Log In

Use your USAccess PIV Credential to Login

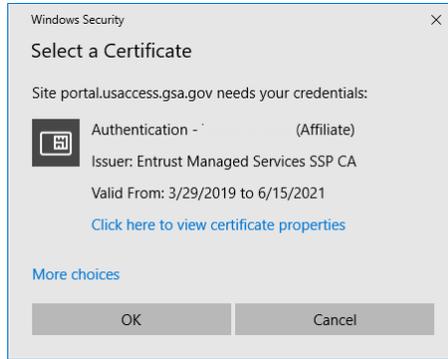
Login with a Smart Card

WARNING! THIS SYSTEM IS FOR AUTHORIZED USE ONLY!

This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY". This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

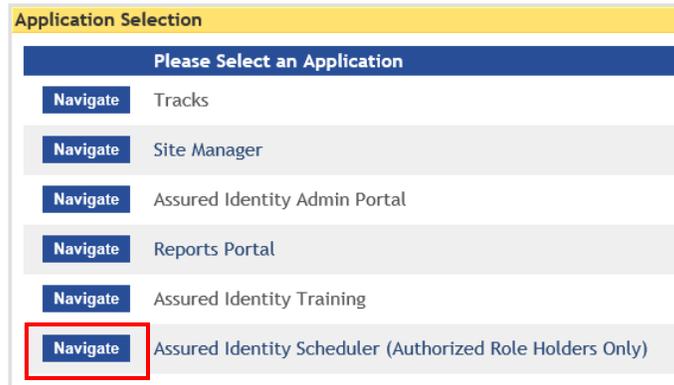
PIV Credential Login

3. Click the **Login with a Smart Card** button.
4. Select the Authentication certificate when prompted.



Authentication Certificate

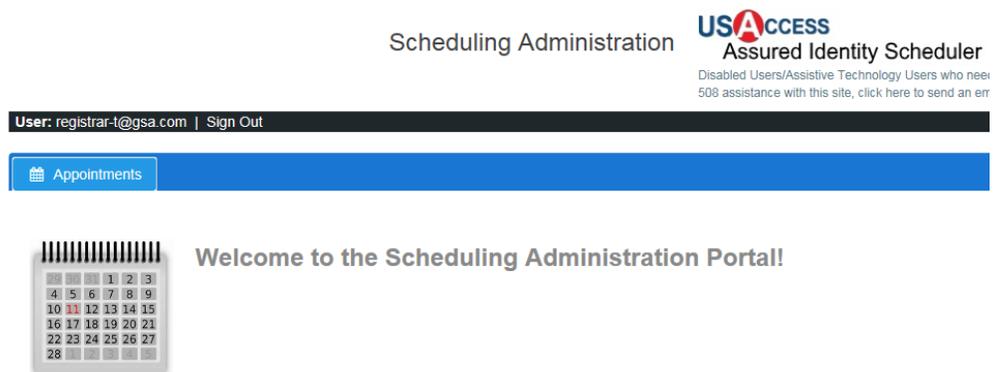
The **Application Selection** screen displays.



Application Selection

5. Click the **Navigate** button next to *Assured Identity Scheduler (Authorized Role Holders Only)*.

The **Assured Identity Scheduler** screen displays.



Assured Identity Scheduler Welcome Screen

6. Click the *Appointments* tab. The *Appointments* tab displays.

Appointments

Site: [Dropdown]
 Last Name: [Text Field] First Name: [Text Field]
 Start: 04/23/2019 07:54 AM [Calendar Icon] End: [Calendar Icon]
 Show Cancelled - No: [Toggle Switch]
 Search [Clear]

Site Code	Activity	Asset(s)	Start	In	Out	Duration	Applicant	Phone
No records found								

1 10

+ Make New Appointment Cancel Selected

AI Scheduler Appointments Tab

7. In the **Site** field, type in the Site code, the City you are located in, or any part of your address, and select your site from the list provided.

Appointments

Site: test [Dropdown]
 Last Name: Greg Test 16 Scheduler, VIRGINIA, 20175-4103
 Start: Shared - Mercury Highway Test Site, Bldg 1002, Las Vegas, NV -DOE, NEVADA, 89023
 Show Canc: Sync Test A Scheduler, VIRGINIA, 20175-4103
 Search [Clear]
 VACO PCIF (TEST ONLY) , DISTRICT OF COLUMBIA, 20420-0001

Site Code	Activity	Asset(s)	Start	In	Out	Duration	Applicant	Phone
No records found								

1 10

+ Make New Appointment Cancel Selected

AI Scheduler Site Search

8. Click the **Search** button to locate your appointments. *The list of appointments displays.*

Appointments

Site: Sync Test A Scheduler, VIRGINIA, 20175-4103 [Dropdown]
 Last Name: [Text Field] First Name: [Text Field]
 Start: [Calendar Icon] End: [Calendar Icon]
 Show Cancelled - No: [Toggle Switch]
 Search [Clear]

Site Code	Activity	Asset(s)	Start	In	Out	Duration	Applicant	Phone	
<input type="checkbox"/>	192899	enrollment: Enroll	fcuwrk-192899: F	Apr 17, 2019 10:00 AM ED	<input type="checkbox"/> No	<input type="checkbox"/> No	15:00	greg seventeen	3015551212
<input type="checkbox"/>	192899	enrollment: Enroll	fcuwrk-192899: F	Jun 12, 2019 12:00 PM ED	<input type="checkbox"/> No	<input type="checkbox"/> No	15:00	greg twel	3015551212

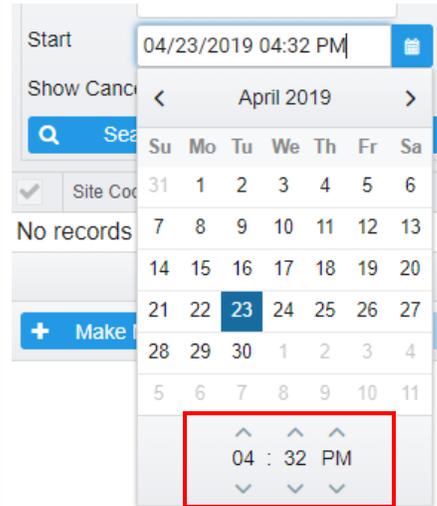
1 10

+ Make New Appointment Cancel Selected

The **Appointments** screen provides a view of all appointments scheduled. Appointments listed can be ordered by any of the column headers. Click on the column header you want to sort by. You can also resize any of the columns by clicking on the column separator and dragging it to the position you want, just like in an Excel spreadsheet.

To search for a specific person’s appointment, enter a full Last Name or First Name in the field provided. Partial name searches are not allowed at this time (Ex. Enter “Smith” instead of “Smi”).

To change the dates of the appointments displayed, enter Start and End dates and click Search again. The Start and End fields also contain times of the day, to narrow the search.



Checking Appointments In and Out

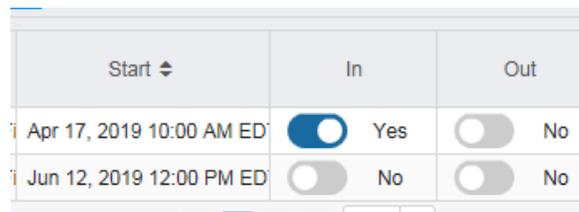
The ideal enrollment appointment should take approximately 15 minutes; however, this is an average. There are situations in which Applicants need additional time because they are experiencing difficulties with fingerprint capture or have questions.

Be sure to answer an Applicant’s questions, even if it takes extra time. Your goal is to complete the enrollment within 15 minutes, but customer service is a priority.

Check Applicants in to the system when they arrive for their appointment, and check them out of the system when their appointment is complete.

Follow these steps to check an Applicant in and out of the system:

1. Click the **In** button that corresponds to the Applicant’s appointment on the **Appointments** screen.



When the Applicant’s appointment is finished:

2. Click the **Out** button that corresponds to the Applicant’s appointment on the **Appointments** screen.

The Applicant has now been checked in and out of the system.



Hint

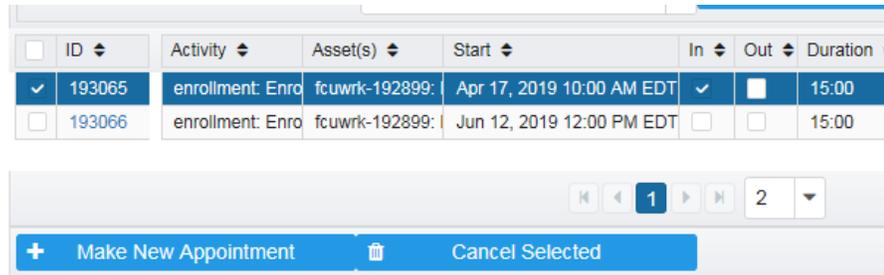
If you check in the wrong Applicant, simply click the **In** or **Out** box to change it back to white. Then click the boxes for the correct Applicant.

Canceling Appointments

When Applicants fail to appear or their appointment cannot be completed once they have arrived, their appointment must be cancelled in the system. When you cancel an appointment, the Applicant receives an email asking them to reschedule the appointment.

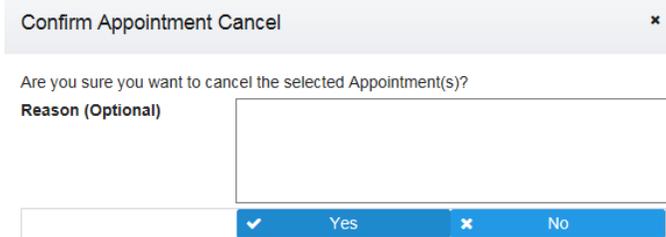
Follow these steps to cancel an Applicant's appointment:

1. Select an appointment by clicking on the box next to the appointment.
2. Click the **Cancel Selected** button.



Cancel Selected Screen

3. The system displays a Confirm Appointment Cancel message.



Cancellation Confirmation

4. Registrars/Activators click **Yes** to cancel, or **No** to keep the appointment. The Reason field is not required, however any comments entered in this field will show in the cancellation email the system sends to the Applicant.
5. The appointment has been cancelled and an e-mail sent to the Applicant that they must reschedule.

Resources for Registrars and Activators

There is a learning curve to becoming a proficient Registrar and Activator. In addition to this manual, there are other resources to guide you when you need help or have questions.

A toll-free number is available to Registrars for technical hardware or software-related questions. Also, a secure website known as TRACKS (Team Registrar and Activator Communication and Knowledge Source) has been made available on the Credentialing Units. Registrars and Activators can get program and status updates, training and job aids, system enhancement announcements, and system issue notifications using the TRACKS tool.

USAccess Help Desk

Perspecta provides the following Help Desk services for the USAccess Program:

- A USAccess Role Holder Help Desk is staffed onsite in Herndon, Virginia, with hours of operation from 7:00 a.m. – 7:00 p.m. Eastern Time, Monday through Friday, excluding federal holidays. The number is 1-866-493-8391, and is for USAccess Role Holders only. Calls outside of these normal business hours are routed to a mobile on-call help desk analyst and answered on a first come, first served basis. If all analysts are busy, callers are given the option of leaving voicemail messages that are responded to in a timely manner. All calls are documented and data is captured regarding the caller, purpose of call, actions taken, and resolution.
- An Automated Call Distribution (ACD) system is available to receive, process, log, and handle all calls that are routed to the system from the USAccess Program toll-free telephone number. Ongoing support of the ACD includes maintaining the ability to separately identify/handle USAccess Program calls so that callers receive customized responses when calling the Help Desk. In addition, ACD messages are updated and maintained as required to ensure appropriate handling of the USAccess Program Help Desk callers to provide improved customer service and response to these callers.
- The USAccess Role Holder Help Desk also responds to e-mail inquiries from Role Holders. All e-mail inquiries are logged as an incident and responded to within two business days. E-mail the Help Desk at usaccess.helpdesk@perspecta.com.

*The 866-493-8391 phone number and the usaccess.helpdesk@Perspecta.com email address should **never** be given to Applicants for assistance. They are for Role Holders only. Applicants needing further assistance should be directed to the MSO Help Desk at 877-572-4773 or hspd12@gsa.gov.*

TRACKS Web Site

TRACKS (Team Registrar and Activator Communication and Knowledge Source) is a secure Web site accessible to Registrars and Activators from a work or home computer. The site contains Advisories, Training Information, Job Aids and Tips, Frequently Asked Questions, and a Contact Us feature and requires use of your PIV credential to log in to the Web site.



TRACKS Desktop Icon

The TRACKS web site URL is accessible at: <https://portal.usaccess.gsa.gov/aisso>

TRACKS Log In Process

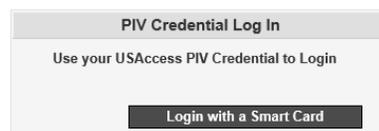
The TRACKS Web site requires you to verify your identity by logging in to the portal. To log in, you must use your USAccess Credential and enter your PIN, similar to how you log in to the Enrollment application.

NOTE: Your PIV card and PIN have a password associated with the UPN (User Principal Name). This password is not necessarily used for system access, but it does need to be updated every 90 days for smart card log-in to function properly. The system does not notify you when this UPN password is set to expire, so be mindful of the 90 day expiration. Please see the Guidance for Resetting UPN Password Guide for further instruction.

Follow these steps to log in to TRACKS using your USAccess Credential:

1. Click on the TRACKS icon on your desktop, or go to the Single Sign on URL at: <https://portal.usaccess.gsa.gov/aisso>

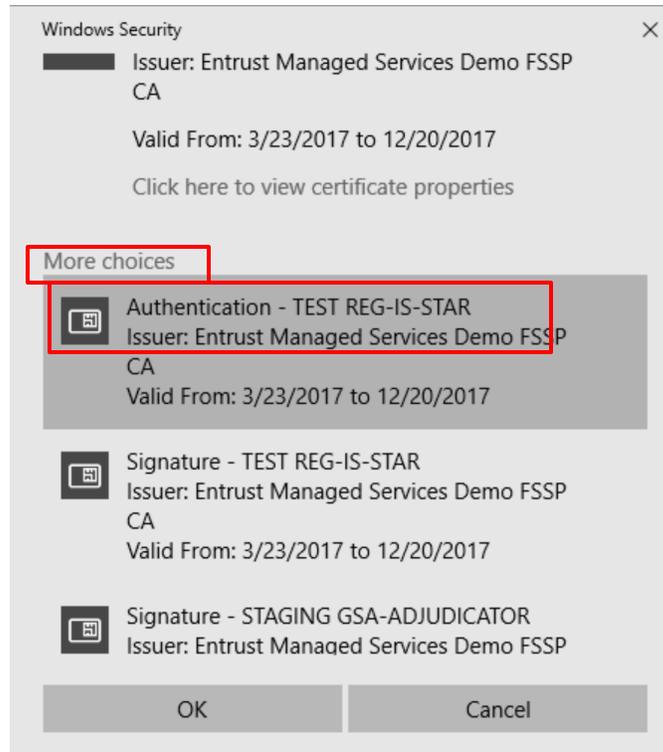
*The PIV Credential Log In screen displays. Click **Login with a Smart Card**.*



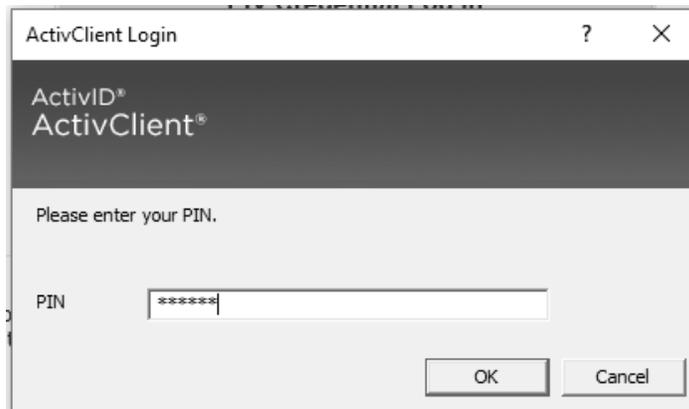
WARNING! THIS SYSTEM IS FOR AUTHORIZED USE ONLY!
This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY". This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

USAccess PIV Card Login Screen

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

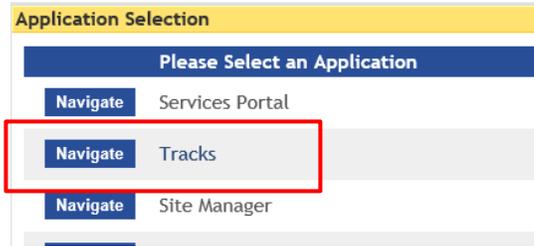


2. Enter your Credential PIN, and then click the **OK** button.
 Note that if you are attempting to log in to TRACKS from your desktop computer using your USAccess Credential and PIN, you must have a card reader and the ActivClient Middleware installed on that PC.



ActivClient Login Window

3. From the menu presented, click the **Navigate** button next to **Tracks**.



Registrar Menu

TRACKS Web Site Features

The **Home** page has Advisories that announce any planned system maintenance or program updates, and report any issues with the service that may impact Registrars' and Activators' ability to conduct enrollment or activations. Check the Web site in the morning and as needed during the day.



TRACKS Home Page

The **Training** page lists items like the Registrar Refresher Training presentations. You can use the drop-down list to display presentations for your specific system type.

TRACKS Training Page

The **Job Aids** page contains quick reference guides to aid you in performing specific tasks. Use the drop-down list to display guides for your specific system type. Registrars can print these documents from any workstation with an Internet connection, card reader, and printer capabilities.

Job Aids Page

The **Frequently Asked Questions** page is updated with questions and comments from the field. When Registrars have time between appointments, they can look for new questions and answers on this page. Before you call the Help Desk or send a question in via the Contact Us form, please check the FAQs to see if your question has been answered.

Frequently Asked Questions Page

The **Contact Us** form is for Registrars and Activators with questions, suggestions, or comments. Enter the information requested, choose a topic from the **Select Nature of Request** drop-down box, and click **Submit**. The USAccess support staff tries to answer these messages within 24 hours. This is NOT A REPLACEMENT FOR THE HELP DESK and if a Registrar or Activator is having CU, LCS, or LA issues, or an issue using the Enrollment, Activation or scheduling applications, they should contact the USAccess Help Desk for the most immediate support. The Contact Us feature can be used if Registrars or Activators have an issue that is not resolved by FAQs, or if they have general questions about the program.

Contact Us Page

Applicant Enrollment Procedures

The following table lists the enrollment process tasks Registrars perform. The same tasks are in the Enrollment Procedures job aid. Keep this list near the enrollment workstation to guide you through the enrollment procedure.

Enrollment Tasks Performed by Registrar

Enrollment Tasks	
1.	Greet and welcome Applicant.
2.	Ensure Applicant has the appropriate source identity documentation. Check photos against the Applicant's face.
3.	Check-in Applicant using AI Scheduler on the Manage Appointments screen.
4.	Open the Web Enrollment Portal using the Assured Identity desktop icon; search for Applicant's record.
5.	Review with the applicant the data entered by the Sponsor and ask if it is correct. If NOT correct, refer them back to their Sponsor.
6.	Complete the remaining fields on the Biographic Data page and ensure all data is correct by verifying with applicant.
7.	Scan the primary form of ID using the flatbed scanner. Remember to scan both front and back.
8.	Scan the remaining source identity documents (front and back) using the flatbed scanner.
9.	Capture Applicant's photo.
10.	Capture rolled fingerprints
11.	Capture slap fingerprints. Ensure number of slap prints equals number of rolled prints.
12.	Verify Applicant's primary and secondary fingerprints.
13.	On the Enrollment Status screen, verify Registered status.
14.	Save Applicant's record.
15.	Enter your PIN, if prompted, to digitally sign the enrollment record.
16.	Let Applicant know about e-mail notification sent out when credential is inventoried.
17.	Check out Applicant on AI Scheduler.
18.	Return all identity documents to Applicant.

Log in to Assured Identity

Your Credentialing Unit desktop has a shortcut to the Assured Identity Enrollment application. This is the software application that guides you through enrollment and collects the Applicant's data.

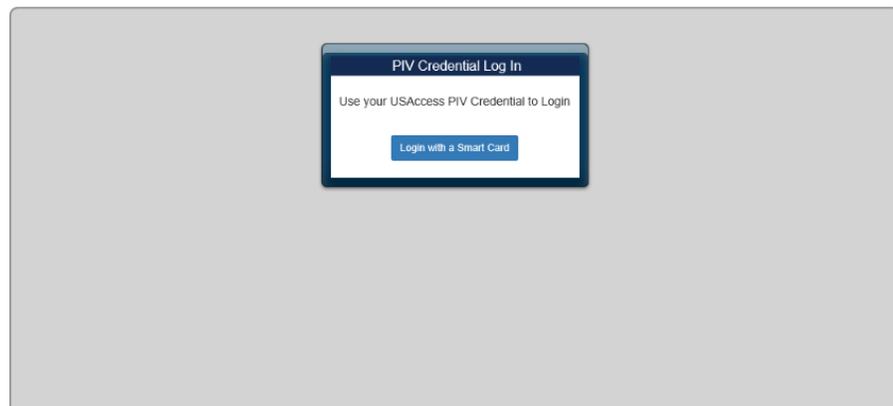


Assured
Identity

Assured Identity Shortcut

You must use your PIV credential to log on to the USAccess Credentialing Unit. Follow these steps to access the Assured Identity Enrollment Application:

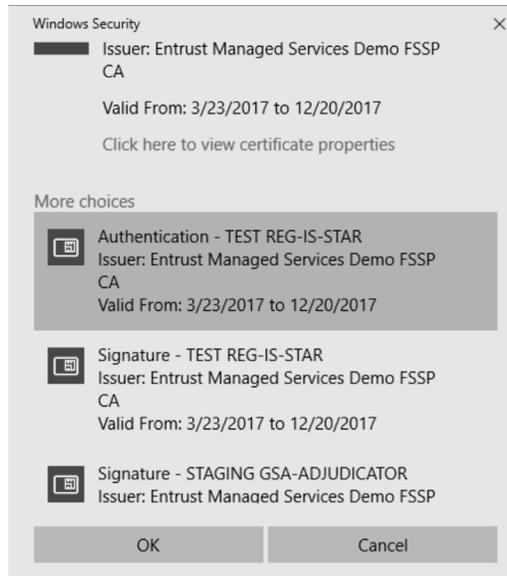
1. Double click the Assured Identity shortcut on your desktop.
2. The PIV Credential Log In screen displays for Enrollment. Click **Login with a Smart Card**.



3. Insert your USAccess Credential into the card reader and click **Login with a Smart Card**.

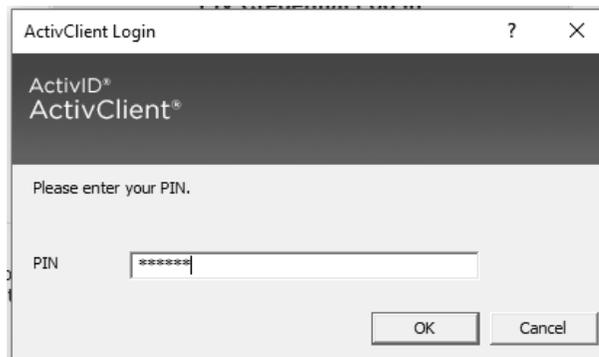
*The Select a Certificate window displays. Select the PIV AUTH Certificate and click OK. If PIV AUTH Certificate is not displayed select **More Choices**. Select the correct certificate (on the CU it will be the Authentication certificate) from the list and click OK.*

The system authenticates the certificates on your Credential and then confirms that you are a trusted Registrar.



Select a Certificate Window

- After the Certificate has been authenticated, the **ActivClient Login** window displays and you are asked to enter your Personal Identification Number (PIN). This is the PIN you created when you activated your USAccess Credential.



ActivClient Login Window

- Enter your **PIN** and select the **OK** button.



Watch Out!

The system only allows six attempts to enter the correct PIN. With each incorrect entry, the system displays the message **Incorrect PIN. Attempts remaining: [5]**. Once the six attempts are exhausted, the Registrar's USAccess Credential is locked.

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

47003000051985@fedidcard.gov 

Search Enrollee

Last Name

SSN

BirthDate

Enrollment ID	First Name	Last Name	Middle Name	Status

Web Enrollment Search Enrollee Screen



Key Point

Do not remove your Credential from the card reader during enrollment. The system cancels the enrollment and closes the Assured Identity application.



Watch Out!

Note that there are no partial saves in the enrollment procedures. To save all data and images entered, you must complete the entire enrollment process.

If you try to exit before completing the enrollment process, a pop-up message displays asking, **Are you sure you want to exit record without saving? Yes/No**. These are your options:

- Clicking **Yes** closes the record and lose all data entered.
- Clicking **No** returns the Registrar to the current screen to continue the enrollment process.

Search for Applicant's Record

Use the **Enrollee Search** screen to search for an Applicant's record.

To search for an Applicant, do the following:

1. Enter the Applicant's last name and date of birth in the search fields:
 - Last Name
 - Birth Date

Alternatively, you can enter an Applicant's Social Security Number and Date of Birth.

- SSN
- Birth Date

- Click the **Search** button.
The search results display.

The screenshot shows a 'Search Enrollee' form with the following fields: Last Name (practice), SSN (xxx-xx-xxxx), and BirthDate (01/02/1981). A 'Search Q' button is present. Below the form is a table with the following data:

	Enrollment ID	First Name	Last Name	Middle Name	Status
Select	3000055373	CLARA	PRACTICE	NMN	NEW

Enrollee Search Results

Notice that the Applicant's Status indicates **NEW**.

- Click the **Select** button next to the Applicant's info.
*The **Biographic Data** page displays.*

Capture Biographic Information

The **Biographic Data** screen contains all information that was entered by the Sponsor. Notice that some of the fields cannot be edited. If the information in these fields is incorrect, the Applicant must contact their Sponsor to have any errors corrected.

The screenshot shows the 'Biographic Data' screen with the following information:

- Biographic Tab:** First Name (JD), Middle Name (NMN), Last Name (LCLPRINT-G), Suffix, Birth Date (01/02/1981), SSN (xxx-xx-1654), Foreign ID, Citizenship (USA), Race (WHITE), Gender (MALE), Hair Color (GREY), Eye Color (BROWN), Weight, Height (0 ft. 0 in.), Personal Email (INPUT@INPUT.COM), Other Email (INPUT@INPUT.COM), Home Phone, Mobile Phone.
- Address History Tab:**

Start Date	End Date	Address Date	City	State	Zip	Country
01/01/0001	Current					

© 2007 - 2017 DXC Technology. All rights reserved. Version: 1.0.0.11

Biographic Data Screen

Show the applicant the screen and ask the Applicant to verify that each item of their information is correct.

If name, birth date or social security number is not correct, explain that only the Sponsor can update the data fields and the Applicant will not be able to complete the enrollment until the Sponsor corrects the biographic data. Use language similar to this:

“We will not be able to continue your enrollment at this time because the name your Sponsor has entered is either inaccurate or does not match your source identity documents.

As you can see, the required fields are inactive and the system does not allow me to update your information. Only your Sponsor can make the changes that are required. The system is set up this way because HSPD-12 makes sure that there is a separation of duties between the person enrolling you and the person sponsoring your Credential.

It is up to you to contact your Sponsor and request that your information be corrected or updated. When your Sponsor makes these changes, you will receive an e-mail with instructions to reschedule your enrollment appointment. Do you have any questions about how to contact your Sponsor?”

4. Complete all fields marked with an asterisk.
5. Enter aliases the Applicant may have, by clicking on the *Alias* tab. Ask the Applicant if there are other names they have legally used or been known by.. Do not include nicknames.



Key Point

Ask the Applicant to verify that each field in the **Biographic Data** screen is correct.

6. Click the **Next** button.
The Document Collection screen displays.

Document Collection Screen – Document 1

Scan Identity Documents

There are three objectives to successfully completing the document collection portion of the Enrollment process:

- Capture at least two documents (at least one must be a primary document) in the corresponding document window.
- Determine if a document requires more validation by a Security Officer.
- Determine if a linking document is required.

Linking Documents

Although the Applicant is required to provide two identity documents, the document collection screen can display up to three documents, accommodating a linking document if necessary.

When a linking document is presented, you must scan the document in the **Document 3 Image/Linking Document** section.

Linking documents are required when documents with different names are offered as primary and secondary source identity documentation.



Key Point

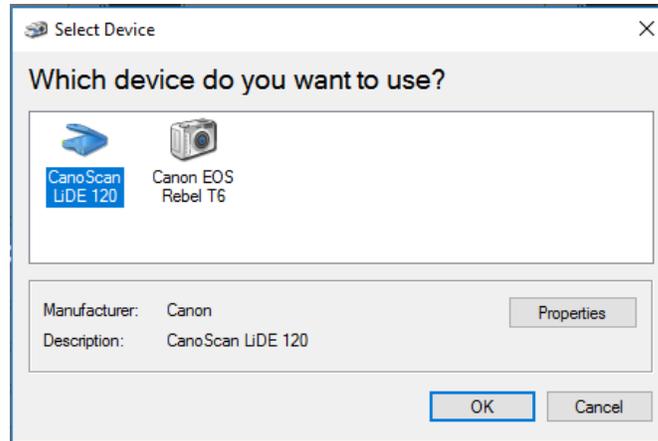
The only time identity source documents with different names can be accepted is when an official linking document such as a marriage certificate, certified copy of birth certificate, or court record can be provided linking the two names.

The linking document must have both the former and current legal names on it and both the primary and secondary documents must be valid and not expired.

For example, a married woman may use both a current driver's license, with her married name, and a certified copy of her birth certificate, with her maiden name, as primary and secondary sources of identification as long as she brings a linking document, her marriage license, with both her maiden name and married name on it.

Follow these steps to begin scanning identity documents:

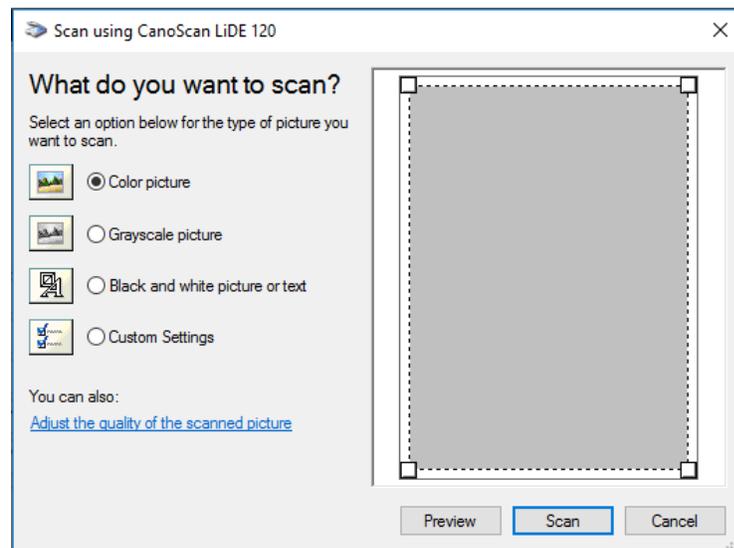
1. After verifying that the **Front** tab is selected under **Primary Document**, click the **Scan** button under the **Primary Document** section.
*The **Select Device** dialog box displays.*



Select Device Dialog Box

2. From the Select Device dialog box, select the Canon scanner.
3. Place the primary identity document to be scanned face down on the scanner bed.
4. Click the **OK** button.

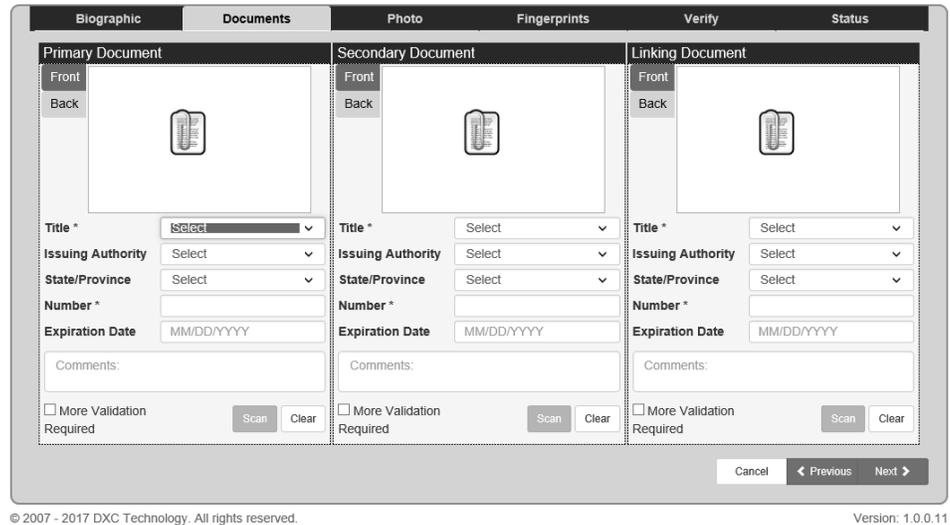
*The **Scanner Control and Preview** dialog box displays.*



Scanner Control and Preview Dialog Box

5. In the **Image Scanning** window, select an option for the type of picture you want to scan (Color picture, Grayscale picture, Black and white picture or text, or Custom Settings).
If you are scanning a paper document with a raised seal, such as a birth certificate, select **Grayscale**. Otherwise, leave the default set to **Color picture**.
6. Click the **Preview** button.
The scanned image displays in the preview window.
7. Crop the image if necessary to remove excess spacing around image.
8. If the image is upside-down or if there is a problem with the image, adjust the document on the scanner and click the Preview button again.

9. If the image quality is acceptable, click the **Scan** button.
*The **Document Collection** screen displays.*



Primary Document Collection

Notice that the Applicant's document appears in the **Primary Document** section.

Click the magnifying glass icon  in the lower right corner of the **Document Image** section for an expanded view of the image; click **X** to close window.

10. Flip the document over on the scanner, select the **Back** tab, and repeat the scanning process for the back of the document.
- Enter data in the **Primary Document** fields using the dropdown lists. In the Title field pulldown below each scanning window, the interface displays only those documents that are acceptable in that given window. For example, under the Primary Document window, only documents that are acceptable as primary identification are listed. Listed below are a list of the document Titles for each document:

Primary Docs:

- ALIEN REGISTRATION RECEIPT CARD I-551
- DRIVER'S LICENSE
- EMPLOYMENT AUTH. CARD I-766
- MILITARY ID CARD
- MILITARY DEPENDENT ID CARD
- PASSPORT
- US PASSPORT CARD
- PIV CARD
- PERMANENT RESIDENT CARD

Secondary Docs:

- ALIEN REGISTRATION RECEIPT CARD I-551
- BIRTH CERTIFICATE
- CERTIFICATION OF BIRTH ABROAD
- CANADIAN DRIVER'S LICENSE
- US CITIZEN ID CARD

- CERTIFICATE OF NATURALIZATION N550 N570
- DRIVER'S LICENSE
- EMPLOYMENT AUTH. CARD I-766
- EMPLOYMENT AUTH. DOC. - DHS
- EMPLOYMENT AUTH. CARD I-688A
- EMPLOYMENT AUTH.DOC.-DHS I-688B
- ID CARD
- ID CARD - RESIDENT CITIZEN I-179
- MILITARY ID CARD
- MILITARY DEPENDENT ID CARD
- USCG MERCHANT MARINER CARD
- NATIVE AMERICAN TRIBAL DOC.
- PASSPORT
- US PASSPORT CARD
- PIV CARD
- PERMANENT RESIDENT CARD
- RE-ENTRY PERMIT I-327
- REFUGEE TRAVEL DOCUMENT I-571
- SOCIAL SECURITY CARD
- TEMPORARY RESIDENT CARD I-688
- CERTIFICATE OF US CITIZENSHIP N560 N561
- VOTER REGISTRATION CARD

Linking Docs:

- BIRTH CERTIFICATE
- COURT ORDER
- DIVORCE DECREE
- MARRIAGE LICENSE
- OTHER

11. The required **Document Information** fields for each identity document are:

- Title
- Number



Watch Out!

Be sure that the correct side of the document is scanned under the **Front** and **Back** tabs.



Hint

Click the **Clear** button to remove a Document Image and the Document Information below it.

Completed Document Collection Screen

12. Scan remaining document(s) as applicable. After all identity documents are scanned, click the **Next** button to proceed to the next screen.
The **Photo Capture Screen** displays.



Hint

If any required fields on the **Document Collection** screen are missing data, the system prompts you to enter the data before you can move on to the next task.

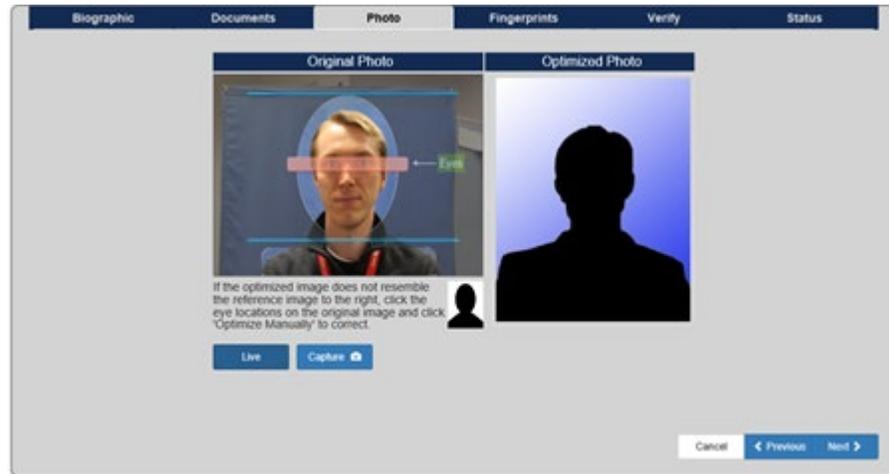
Photo Capture Screen

Capture a Photo

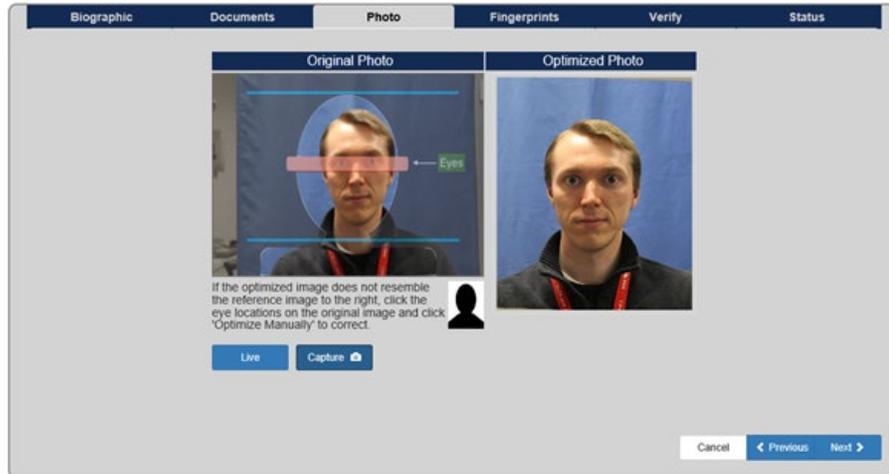
The Applicant should be sitting in front of a blue screen for their photo. They should be sitting up straight and looking straight at the camera while you take the photo. They must have a neutral facial expression for the photo, where all facial muscles are in a relaxed state. No part of the face can be hidden or otherwise obscured by hair, or any type of head covering. You may need to raise or lower the camera tripod if your subject is either very tall or very small in stature.

To capture a photo image of the Applicant, do the following:

1. Position the Applicant in front of the camera. Tell the Applicant to have a plain expression for the photo.
2. Click the **Live** button. On the photo capture page, Registrars will see real time/live preview of the Applicant in the Original photo image screen.
3. Line up the Applicant's eyes with the pink bar in the middle of the screen.



4. Click **Capture**. The photo takes on the second camera click and the system automatically optimizes the photo.



Key Point

USAccess photos must be in front of the blue background. The blue background must be visible in the photo that prints on the credential. If you have difficulty placing the photo background, please contact the agency HSPD-12 POC or the GSA MSO. Contact numbers for the GSA MSO are located under **Contact Us**, on the USAccess Website, <http://www.fedidcard.gov>.



Watch Out!

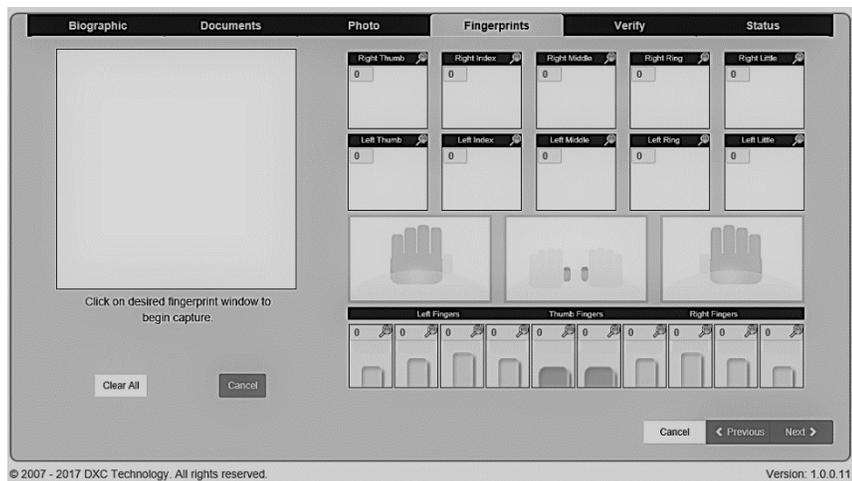
USAccess Enrollment photos are captured using normal room lighting, no flash. If the flash flips up on the camera, push it closed and take the photo again without the flash.

Hint

You may need to take more than one picture if the photo does not meet guidelines listed above. Take additional pictures by clicking the **Live** then **Capture** buttons again. Please note that this will replace the original picture.

- If there are no error messages and the photo image resembles the referenced (silhouetted) image, click the **Next** button to proceed to the next screen.

The **Fingerprint Capture** screen displays.



Fingerprint Capture Screen

Capture Fingerprints

The **Fingerprint Capture** screen has the ability to capture slap and rolled fingerprint images.

The images required on this screen are:

- 10 Rolled fingerprints
- Segmented Left Slaps (automatically populated after Left Slap completed)
- Two Thumb Slaps
- Segmented Right Slaps (automatically populated after Right Slap completed)

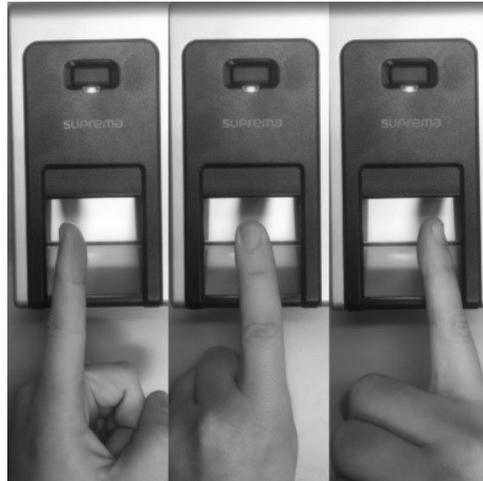
Rolled Fingerprints

Rolled fingerprints are obtained when the Applicant rolls their fingers on the scanner to capture a “wrap-around” image of the fingerprints.

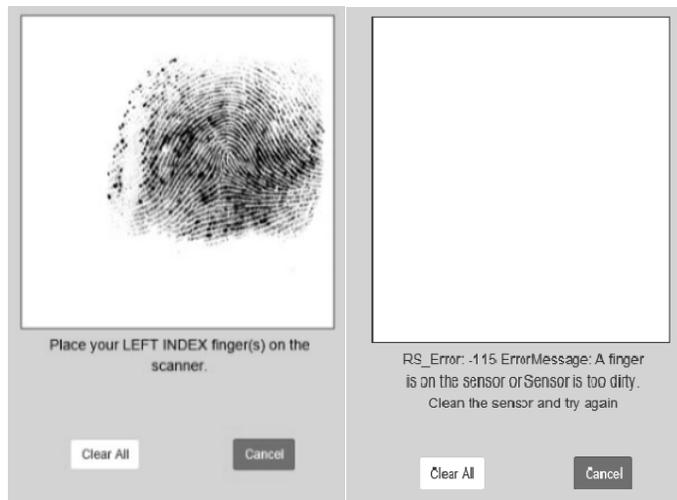
Follow these steps to capture rolled fingerprints

- Click the image box or title bar above the thumb or finger to be printed.

2. Based on your selection in step 1, have the Applicant start by placing the nail side of the finger upon the platen.
3. The scanner will beep once the finger has been placed on the platen. Instruct them to roll their finger or thumb slowly across the platen until it faces the opposite direction. (Essentially side to side).



The scanner beeps, indicating the print has been captured successfully. *The fingerprint displays in the **Capture Window** as it is being captured.* The scanner will present a message below the capture window if the finger position needs to be adjusted on the platen or if the platen is dirty and needs to be cleaned



Capture Window – Clean Sensor Error Message

The Applicant may have to try step 3 a few times to acquire the proper technique for rolling a quality print. View the image in the **Capture Window** and note the quality score in the image box.

A score below 60 displays in red and must be recaptured.

4. If the fingerprint is poor quality, click the image box or title bar to delete the print and ask the Applicant to roll the print again.



Hint

You can click the  in the upper right corner of each rolled image to open a window for an expanded view. Click the X to close the window.

Coach the Applicant to assist them in acquiring an acceptable print. You may also have to assist the Applicant to roll their fingers.

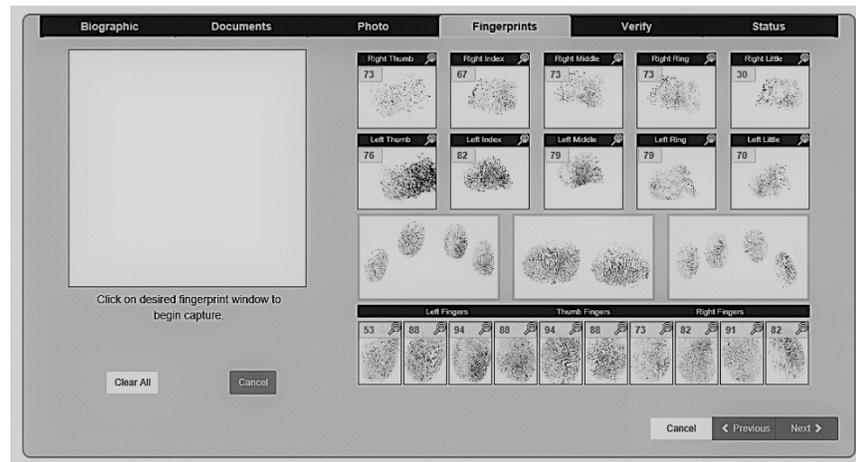
Generally, the weight of the finger is the maximum pressure needed to clearly capture a fingerprint. Different levels of pressure may be needed depending on how light or dark the image is. In order to take advantage of the natural movement of the forearm, the hand should be rotated from the more difficult position to the easiest position.

5. Repeat steps 1 through 5 until all fingerprints are processed.

Slap Fingerprints

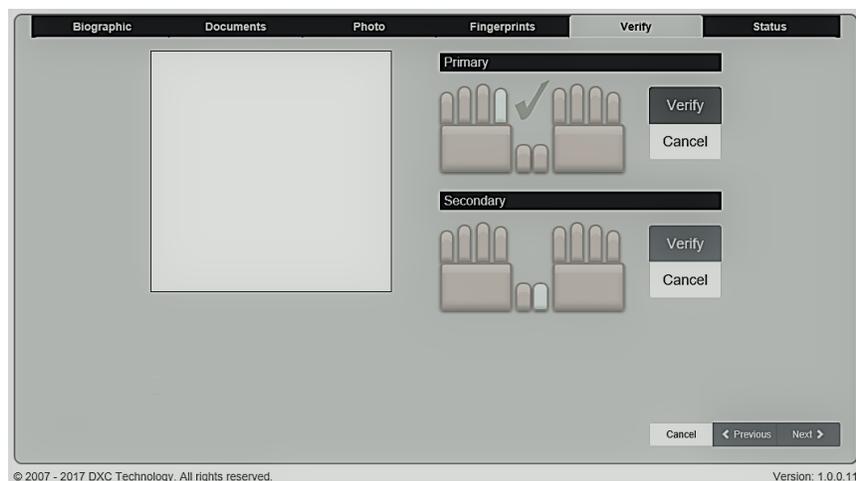
Slap fingerprints can be obtained by placing fingers flat on the scanner without rolling any of the fingers. Follow these steps to obtain slap fingerprints:

1. Click the **image box** or **title bar** above the set of fingerprints to be captured (Left Slap, Two Thumbs, or Right Slap).
2. Click in the **Left Slap** image box.
3. Ask the Applicant to place their left index and middle fingers (as directed beneath the capture window) on the platen. After the Index and middle finger have been captured have the Applicant place the ring and little finger on the platen. All four fingers will display in the left slap box after the slaps are completed.
4. Ask the Applicant to press firmly, but not too hard.
When the scanner beeps the slap is captured.
The fingerprints display in the Capture Window as they are being captured.
5. View the image in the **Capture Window** and note the quality score in the image box. An acceptable score is 60 or higher.
If the score is below 60, click the image box or title bar to delete the prints and capture the prints again.
6. Repeat the same process with both thumbs and the four fingers on the right hand.



Completed Ten Print Capture Screen

7. Click the **Next** button to proceed to the next screen.
*The **Finger Verification** screen displays.*



Fingerprint Verification Screen

Primary and Secondary Fingerprints

Once all fingerprints have been captured, the system requires the Applicant to verify the two primary fingerprints - normally the right and left index fingers. The **Fingerprint Verification** screen is used to validate the Primary and Secondary Fingerprint templates that were generated from the fingerprint capture.

Follow these steps to verify the Primary and Secondary fingerprints:

1. Click the Verify button in the Primary Fingerprint section.
2. Have the Applicant press their primary finger, as indicated on the screen, on the **Fingerprint Reader**.

The image displays in the **Fingerprint Capture** window.

Once the system validates the fingerprint, it sounds a beep and displays a green checkmark indicating the fingerprint was verified.

If the system is having difficulty processing the fingerprint, it displays various messages in the **Fingerprint Capture** window to facilitate a clear reading.

3. Click the **Verify** button in the Secondary Fingerprint section.
4. Have the Applicant press their secondary finger, as indicated on the screen, on the **Fingerprint Reader**. The image displays in the **Fingerprint Capture** window. Once the system has validated the fingerprint, it displays a green checkmark indicating the **Secondary Finger Verified**.
5. Click the **Next** button to proceed to the next screen.

The **Enrollment Status** screen displays.

Enrollment Status Screen

Complete the Enrollment Process

The final step in the enrollment process involves reviewing the information on the **Enrollment Status** screen.

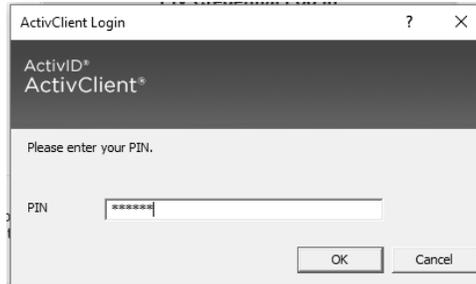
To complete the enrollment process, do the following:

1. Review contents of the **Enrollment Status** screen to compare and verify that the name and photo on the screen match the enrollee.

Green ✓ marks in the **Registration Status** section indicate that all steps have been completed. A red X marks any part of the enrollment that was not completed. Use the **Previous** button to return the section that is incomplete. Complete the section and use the **Next** button to return to the **Enrollment Status Screen**.

2. Enter any appropriate comments in the Enrollment Status Comments field.
3. Click the **Save** button.

The **ActivClient Login** window displays.

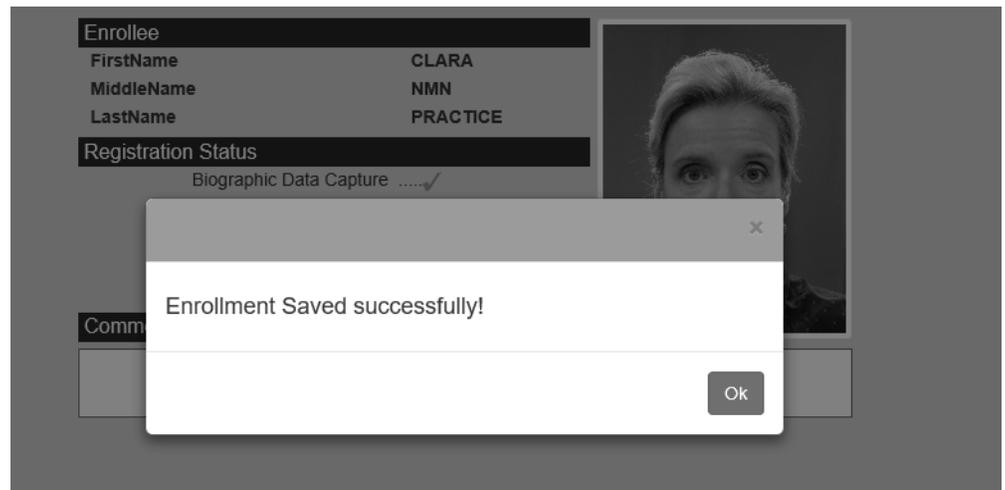


ActivClient Login Window

You must verify your identity to save the changes and digitally sign the record.

4. Enter your PIN in the ActivClient dialog box.
5. Click the **OK** button.
6. Enrollment Saved Successfully displays.
7. Click the **OK** button.

A blank **Enrollee Search** screen displays.



Enrollment of the Applicant is complete. At this point, the Registrar can continue to enroll the next Applicant or click the **Logoff** button to log off from the system.



Key Point

Fluctuations in network connectivity may cause an error message when you try to save the record. If this happens, try to save it again. Occasionally, you may have to cancel the record and begin again.



Watch Out!

Remember, there are no partial saves in the enrollment procedures. When you save and digitally sign the record, you can no longer access this record. You cannot go back and change data, recapture a photo or recapture fingerprints. The data is sent to the Identity Management System. No data remains behind on the enrollment workstation computer.

Fingerprint Capture Exceptions

There are several scenarios in which an Applicant's fingerprints may be difficult to capture. This is called a Failure to Enroll (FTE). When the system detects problems with capturing fingerprints, the **Fingerprint Verification** screen requests the Registrar to identify the problem and provide any applicable comments.

Special fingerprinting situations may involve poor quality fingerprints and amputees.

Amputee

When an Applicant is missing fingers, the system requests identification of the existing fingers. In this example, an Applicant is missing the right middle finger.

Follow these steps to process fingerprints for an amputee:

1. On the **Ten Print Capture** screen, capture individual fingerprint rolls as you normally would, skipping over the missing finger(s).



Key Point

For fingerprint rolls, the system does not request identification of the existing fingers. For slaps, the system requests identification of the existing fingers as soon as it recognizes an incomplete slap.

2. Proceed to capture the Left Slap, Two Thumb Slap, and Right Slap. *When you capture the Right Slap (with the missing middle finger), the system detects the missing finger and the **Missing Finger Detected** dialog box displays.*



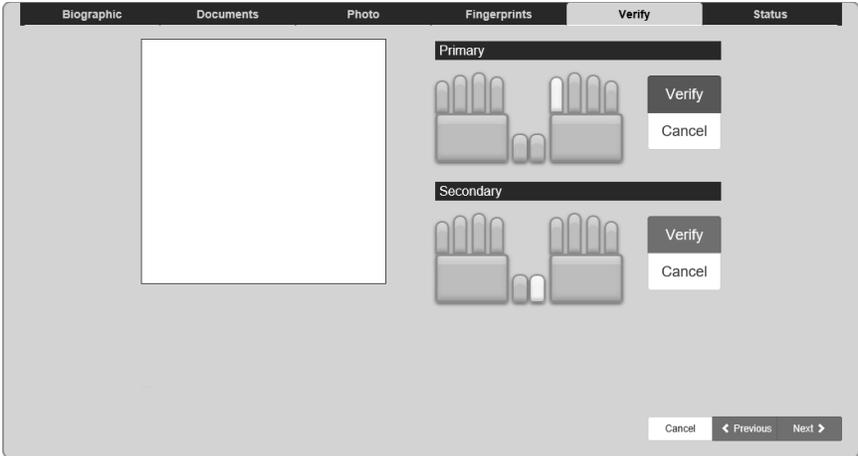
Missing Finger Detected Dialog Box

3. In the **Missing Finger Detected** dialog box, select the finger that is **present**. The system then prompts to retake the slap with the existing finger. **NOTE:** The system is asking you to verify the finger that is present in the slap, therefore in this example the right index finger would be selected.



Missing Finger Detected – Identifying Existing Fingers

- 4. You will then be prompted to place the existing finger on the scanner again. The scanner will beep when the slap has been successfully captured.
- 5. Click the **OK** button.
*The **Fingerprint Verification** screen displays.*



Fingerprint Verification Screen

In this example, the Primary Fingerprint is the right index finger. The Secondary Fingerprint is the right thumb.

Follow these steps to verify the Primary and Secondary fingerprints:

6. Click the Verify button in the Primary Fingerprint section.
7. Have the Applicant press their primary finger on the **Fingerprint Reader**.

*The image displays in the **Fingerprint Capture** window.*

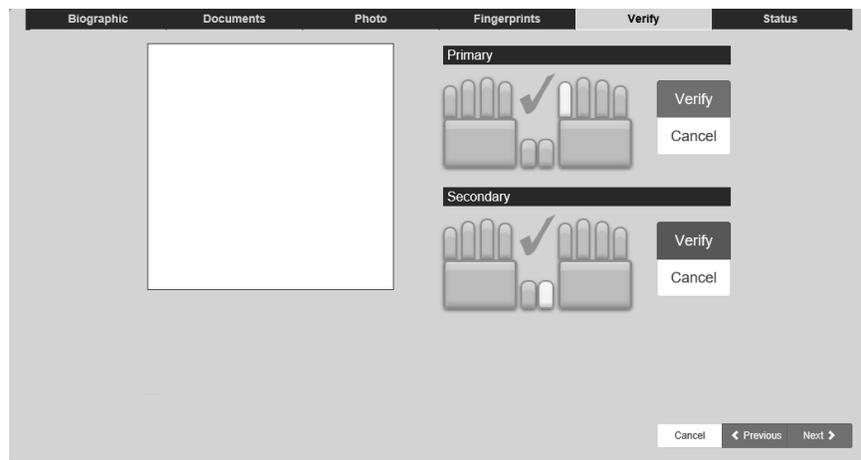
Once the system validates the fingerprint, it displays the message **Primary Finger Verified**.

If the system is having difficulty processing the fingerprint, it displays various messages in the **Fingerprint Capture** window to facilitate a clear reading (e.g., press harder, move left, move up).

8. Click the Verify button in the Secondary Fingerprint section.
9. Have the Applicant press their secondary finger on the **Fingerprint Reader**.

*The image displays in the **Fingerprint Capture** window.*

Once the system has validated the fingerprint, it displays the message **Secondary Finger Verified**.



Fingerprint Verification Screen – Fingerprints Verified

10. Click the **Next** button to proceed to the next screen.
*The **Enrollment Status** screen displays, indicating the steps have been completed.*

Enrollee	
FirstName	CLARA
MiddleName	MARY
LastName	PRACTICE
Registration Status	
Biographic Data Capture	✓
Document Collection	✓
Photo Capture	✓
Fingerprint (10 Print) Capture	✓
Fingerprint Verification	✓
Comments	

Enrollment Status Screen – Steps Completed

11. Click the **Save** button on the **Enrollment Status** screen.
*The **ActivClient Login** window displays.*

ActivClient Login Window

12. Enter your PIN and Click the **OK** button.
*The system returns you to the **Enrollee Search** screen.*
The enrollment process is complete.

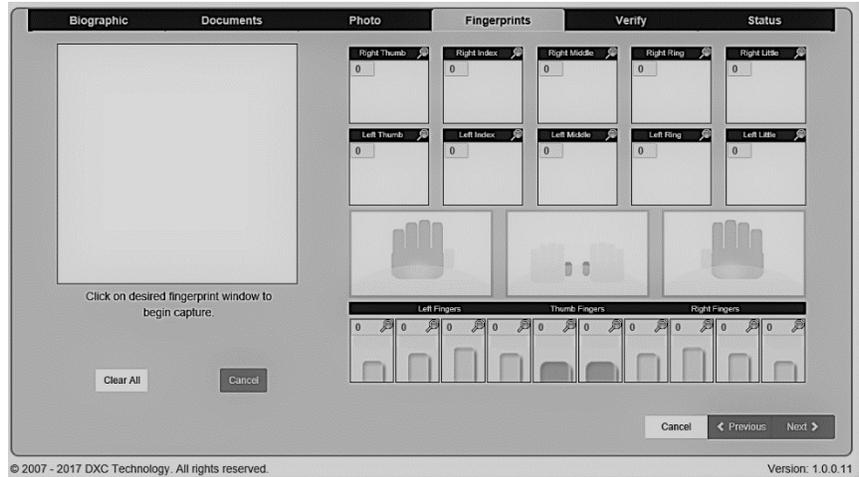
Extra Fingers

If an Applicant has more than ten fingers, the fingerprints from the thumbs and the next four fingers should be captured. Any additional fingers would be considered extra fingers and can be disregarded for the purpose of fingerprinting.

No Fingerprints Captured

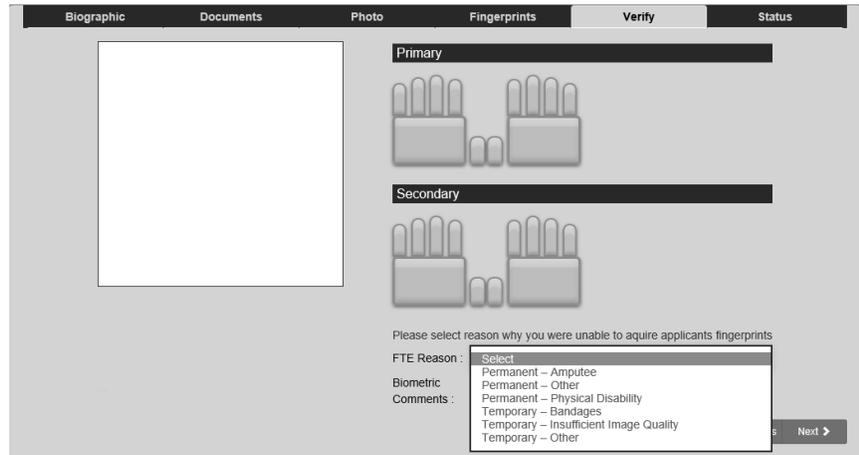
With an Applicant physically incapable of providing any fingerprints, completely skip the fingerprint capture steps.

1. On the **Ten Print Capture** screen, click the **Next** button.



Ten Print Capture – No Prints Captured

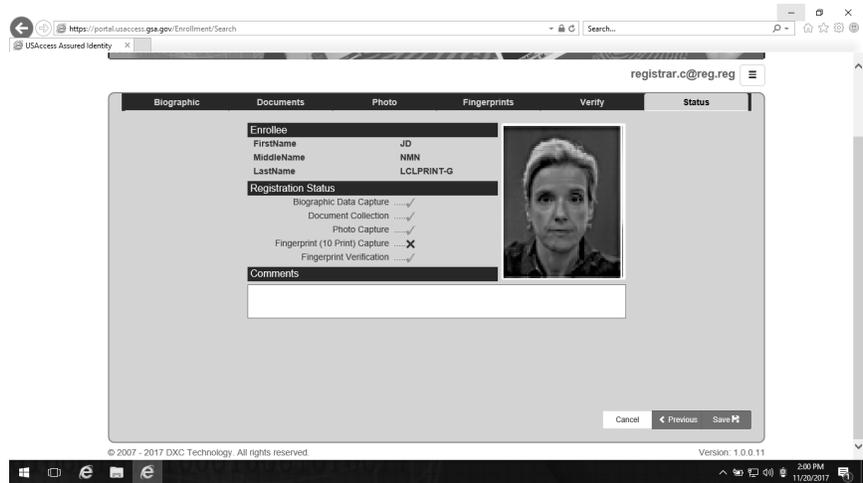
2. If there were no prints captured, the **Fingerprint Verification** page displays with the message: *Please select reason why you were unable to acquire applicants fingerprints*
3. In the Reason Field, select appropriate reason from the dropdown list. The following image shows a list of the FTE Reason Codes.



Fingerprint Verification Screen

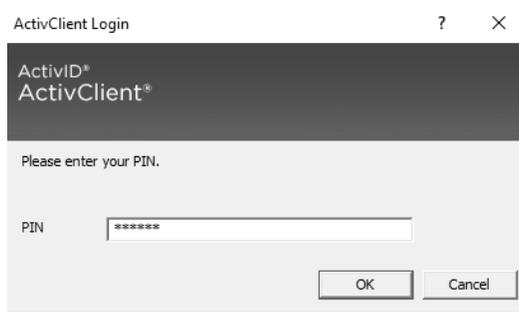
Note that you must provide a reason for the lack of fingerprints.

4. Enter appropriate comments in the Comments field. Comments may be required for some selections.
5. Click the **Next** button.
*The **Enrollment Status** screen displays, indicating fingerprints were not captured.*



Enrollment Status Screen –Steps Completed

6. Click the **Save** button on the **Enrollment Status** screen.
*The **ActivClient Login** window displays.*



ActivClient Login Window

7. Enter your PIN and click the **OK** button.
*The system returns you to the **Enrollee Search** screen.*
The enrollment process is complete.



Key Point

It is important for the Registrar to indicate the correct FTE reason. Reasons for not capturing fingerprints are divided into two categories: permanent or temporary FTE reasons.

- Permanent — amputee
- Permanent — physical disability
- Permanent — other
- Temporary — bandages
- Temporary — insufficient image quality
- Temporary — other

Permanent FTE reasons include things like amputations or curled hands/fingers (physical disability) that cannot be straightened to fit on the platen. Fingers that have been damaged and have severe scarring would be an example of the Permanent – other reason and would require a comment describing the reason.

Temporary FTE reasons include things like poor image quality and bandaged hands or fingers. Fingers or hands that have rashes or cuts for example would be considered Temporary – other and would require a comment describing the reason.

Fingerprint Verification Failures

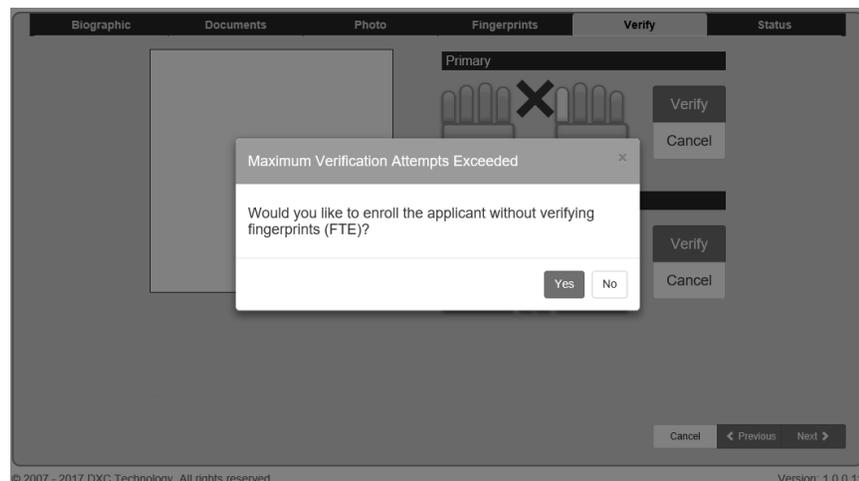
Occasionally fingerprints cannot be verified even after many attempts. This occurs when the quality of the slap fingerprints is not sufficient to create verifiable fingerprint templates. When fingerprint verification fails, the slaps should be recaptured and an attempt should be made to verify the fingerprints again. When fingerprint verification fails after print recapture three times, the record is marked as *Failure to Enroll* and a reason for the inability to verify prints must be indicated before the record can be saved.

In this example, the following message appears when 10 attempts are made to verify the primary and/or secondary finger:

Exceeded maximum number of attempts to verify. Would you like to enroll the applicant without verifying fingerprints (FTE)?

If “Yes” please select the correct reason code from the list provided.

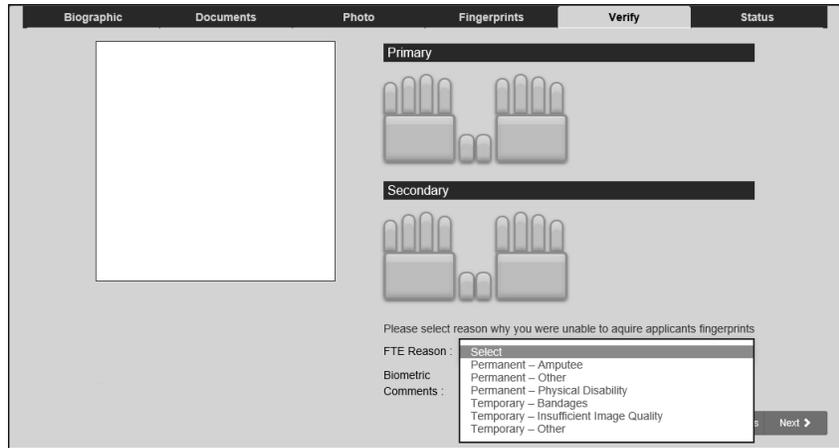
If “No” please return to the previous form to re-capture slaps.



Fingerprint Verification Screen – Maximum Attempts Exceeded

1. If high quality rolls and slaps cannot be captured, please troubleshoot the issue:
 - Be sure equipment is working properly.
 - Clean the fingerprint scanner platen.
 - Be sure to try all tips and techniques to get good fingerprint scores.
2. If there is difficulty verifying an Applicant's prints, click **No** on the above message and, once back in the **Ten Print Capture** screen, click in the **Left Slap**, **Two Thumb Slap**, and **Right Slap** boxes to clear only the slaps.
3. Capture the fingerprint slaps again. Click Next to move to the Fingerprint Verification screen.
4. Try to verify the Primary and Secondary prints again.
5. If one or both of the fingerprints cannot be verified after 10 attempts and the above error message displays, click **No** on the message and repeat steps 1 through 4 again up to three times.

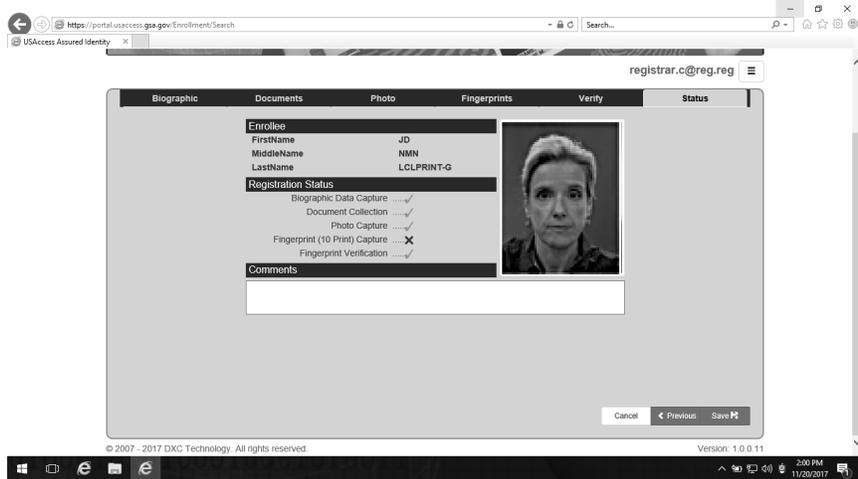
6. After three unsuccessful attempts at recapturing and verifying the fingerprints, when the above error message displays, this time click **Yes** on the error message. *The **Fingerprint Verification** screen displays indicating Fingerprints Not Enrolled.*



Fingerprint Verification Screen

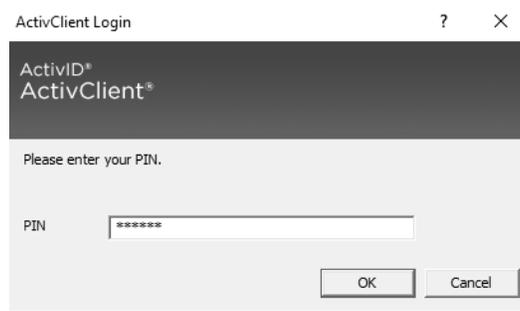
Note that you must provide a reason for fingerprints not enrolled.

7. In the Reason field, select TEMPORARY INSUFFICIENT IMAGE QUALITY from the dropdown list.
 8. Click the **Next** button.
- The **Enrollment Status** screen displays, indicating all steps have been completed.*



Enrollment Status Screen –Steps Completed

9. Click the **Save** button on the **Enrollment Status** screen.
*The **ActivClient Login** window displays.*



ActivClient Login Window

10. Enter your PIN and Click the **OK** button.
 11. Enrollment Saved Successfully displays.
 12. Click the **OK** button.
*The system returns you to the **Enrollee Search** screen.*
- The enrollment process is complete.

Fingers with Long Fingernails

Occasionally, you may encounter an Applicant with long fingernails which interferes with the fingerprint capture process.

1. Attempt capture of rolls and slaps.
2. If prints are unattainable on the scanner because of fingernail length or curvature, the Applicant must make another appointment when his or her fingers can fit on the platen.

Re-enrollment and Reissuance

Re-enrollment of the Applicant is required when information printed on the Credential changes, when the Credential expires, or when the last enrollment exceeds the valid enrollment period of 12 years.

The Sponsor must request the Credential be reissued. This action allows the record to become available for editing by the Registrar.

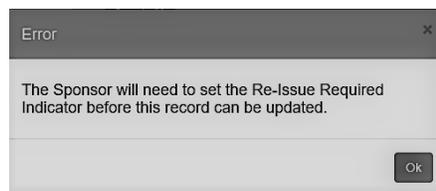
1. The Applicant's record is returned with a status of **REG** in the Enrollee Search Results.

The screenshot shows a 'Search Enrollee' form with the following fields: Last Name (lclprint-f), SSN (xxx-xx-xxxx), and BirthDate (01/02/1981). A 'Search' button is present. Below the form is a table with the following data:

	Enrollment ID	First Name	Last Name	Middle Name	Status
Select	3000051368	JD	LCLPRINT-F	NMN	REG

Enrollee Search Screen Showing Registered Status

2. Click the **Select** button for the Applicant.
If the Sponsor has not requested the Credential be reissued an error message displays indicating the Sponsor needs to set the Re-Issue Required Indicator before the record can be updated.



No Re-Issuance Error Message

Re-Enrollment Procedure

You most likely do not know the reason for the re-issuance; therefore, it is critically important to proceed with the enrollment as if this were the first enrollment for the Applicant.

1. Open the Applicant's record and proceed with the enrollment.

2. Pay particular attention to the Biographic Data screen. Ask the Applicant if the data is correct. Ask about each block individually, especially the physical data information. Make sure eye and hair color are correct as the Applicant states them to be. If you disagree with their choice, you can place a note in the Comments section of the record, but do not argue with the Applicant over their answers.
3. Scrutinize source identity documents as if this were an initial enrollment to identity proof the Applicant. Clear the previous documents and scan the documents presented by the applicant. When conducting a re-enrollment, documents may also be marked for more validation if the registrar deems this necessary.
4. Capture a new photo. Use correct technique to capture a good quality photo.
5. Capture new roll and slap fingerprints.
6. Verify the fingerprints and save the record.

Activation Procedures

Unattended Activation

Applicants can activate their own Credentials by following the steps outlined in the Unattended Credential Activities Guide if they have the one-time password included in their Credential Ready for Pick-up e-mail. Instructions can also be followed on the activation workstation once the Applicant clicks the Unattended Activation icon and starts the Unattended Activation process.

If the Applicant does not have the one-time password, if he or she was enrolled without fingerprint biometrics, or if he or she has difficulty activating the Credential during Unattended Activation, the Activator should assist the Applicant by activating the Credential using Attended Activation.



Key Point

Every credentialing center should have a copy of the Unattended Credential Activities Guide available at the activation workstation for the Applicants to follow.



Watch Out!

USAccess issues both PIV and PIV-I credentials. The PIV and PIV-I activation processes are identical; however, PIV and PIV-I credentials are activated by different card management systems or CMS. The Activation icon on the CU desktop contains links to both PIV and PIV-I attended and unattended activation CMS. Use the correct activation link for the credential type. Graphics are provided to help you select the correct CMS activation link.

Attended PIV USAccess Credential Activation with Fingerprints

This section outlines the steps an Activator follows to activate a USAccess Credential for an Applicant. All system information is read-only at this point. The Activator's responsibility is to verify that the system information matches the Applicant present to receive the USAccess Credential.

The Applicant and USAccess Credential are present and, because the Applicant has viable fingerprints physically available, they are authenticated as part of the procedure.

Steps include:

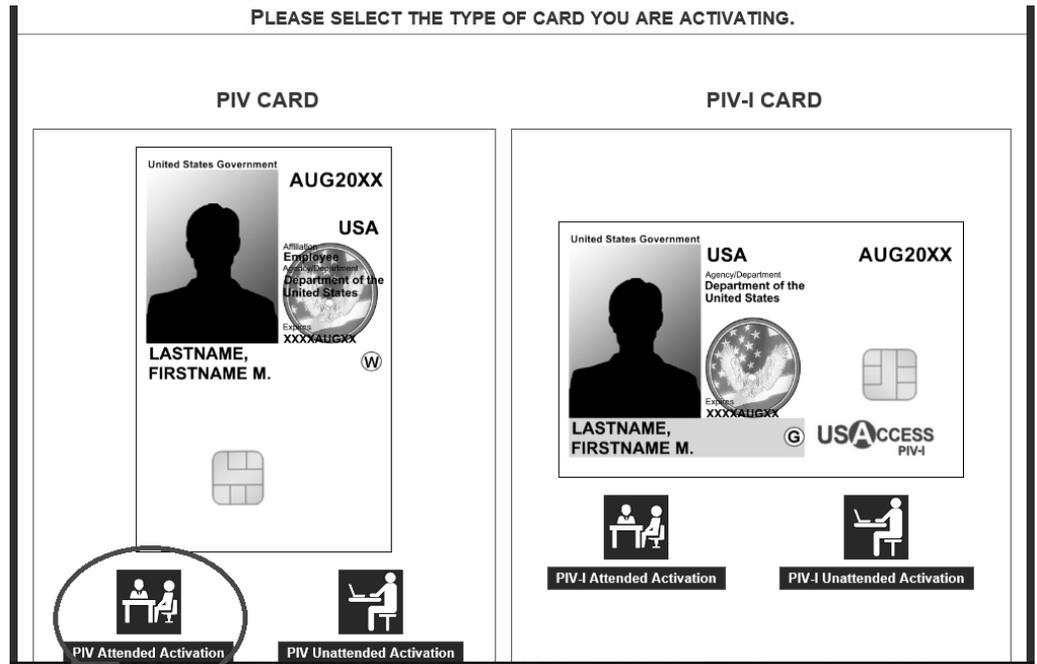
- Ask the Applicant for two forms of ID. Verify the applicant's identity by comparing the applicant, their photo ID, and the photo on the credential you are issuing to that applicant.
- Logging in to the PIV Attended Activation application
- Searching for the Applicant
- Verify the applicant's record matches the applicant in front of you
- Personalizing the USAccess Credential

This procedure begins at the Credentialing Unit Desktop
Follow these steps to log in to Attended Activation:

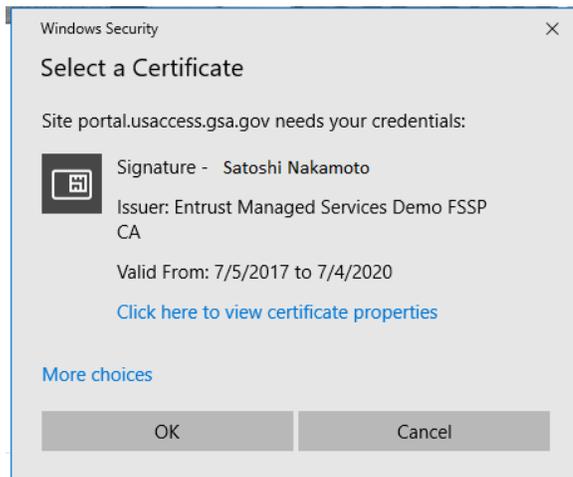
1. Double Click the **Activation** icon on the Desktop.



2. Insert your USAccess Credential into either of the card readers to begin the login process.
3. Double-click the **PIV Attended Activation** Icon at the lower left

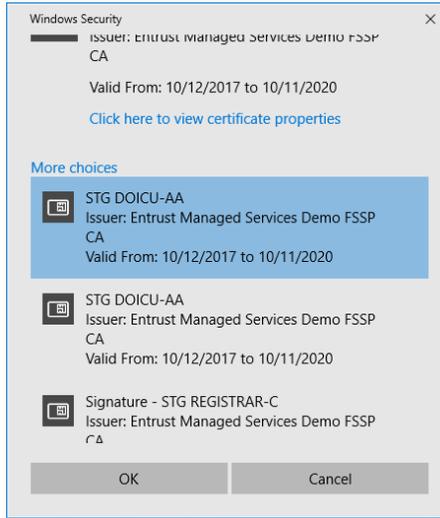


The **Select a Certificate** window displays.



Choose a digital certificate Window

- If your Authentication certificate is displayed, click **OK**. If your Authentication certificate is not displayed, select your certificate from the **More choices** menu.



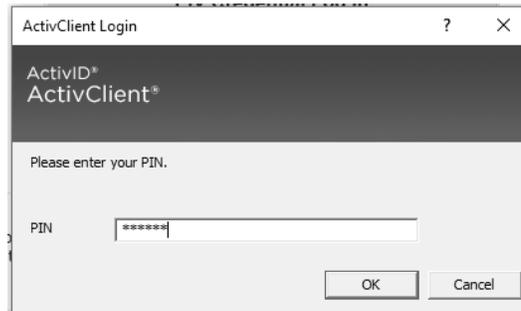
- Click the **OK** button.

*The **ActivClient Login** window displays.*



Watch Out!

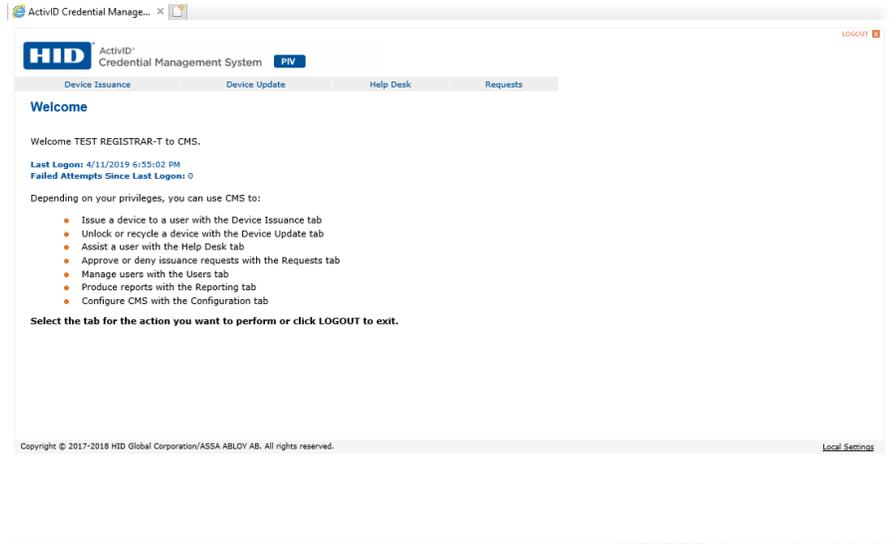
If your USAccess Credential is not inserted in the reader **before** you open PIV Attended Activation the application will not open. Insert your Credential in the card reader and wait for the lights to stop blinking. Then, click the **PIV Attended Activation** icon to open the application



ActivClient Login Window

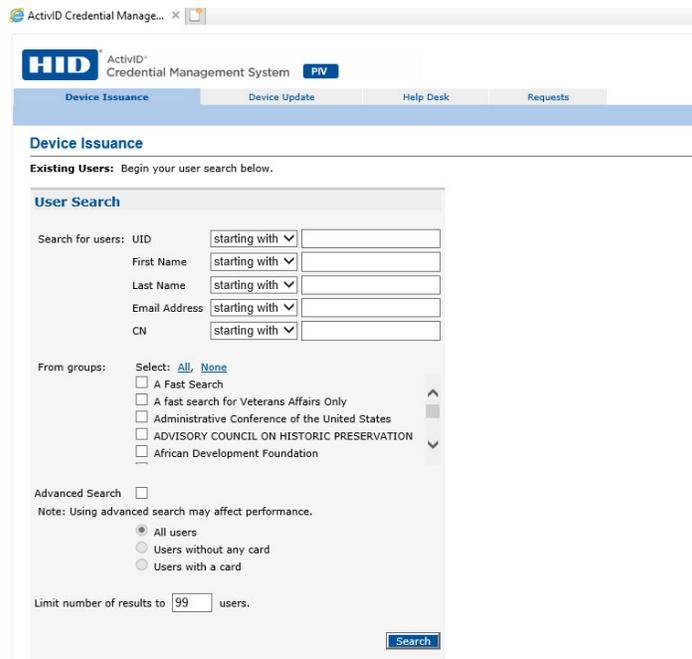
- Enter your PIN and click the **OK** button.

*The **Welcome** screen displays.*



Attended Activation Welcome Screen

7. Click the **Device Issuance** tab at the top of the **Welcome** screen. *The Device Issuance – User Search screen displays.*



Device Issuance – User Search Screen

Searching for the Applicant

The **Card Issuance** screen contains **User Search** fields to help narrow down the Applicant search.

Follow these steps to select the criteria for your Applicant search and begin the USAccess Credential activation process.

1. In the **Search for users** section, search for the Applicant using one or more of the following options: User ID, First Name, Last Name, Email Address, or cn.

Search for Users Section

2. Use the drop-down list next to any search option to select starting with or matching.
3. Enter the Applicant’s information in the fields provided.
4. In the From groups section, select the Applicant’s agency/department.



Hint

Review the Applicant’s Credential to determine their agency/department affiliation. If in doubt, you may ask the Applicant to indicate the sub agency with which they are affiliated. Look for the full name of the agency as well as the acronym. Alternately, you may use the **A Fast Search** option to search for the Applicant through all agencies at the same time.

From Groups Section - Agency/Department Affiliation

5. In the Advanced Search section, All Users is the default option. Select the Advanced Search check box to optionally search for users without any card or users with a card.
6. If necessary, enter a limit (up to 99) for the number of desired results in the **Limit number of results to** section.

- Click the **Search** button.
*The list of users meeting the search criteria displays at the bottom of the **User Search** screen.
 If there is only one match, the system displays the **Issuance to [Applicant's Name]** screen, where you can review the Applicant's information.*

Appalachian Regional Commission
 Arctic Research Commission

Advanced Search
 Note: Using advanced search may affect performance.

All users
 Users without any card
 Users with a card

Limit number of results to users.

Search

Search returned 4 users:

UID ▲ ▾	First Name ▲ ▾	Last Name ▲ ▾	Email Address ▲ ▾
47001000123583	TEST	CMSTESTA	ULTIMATEES.TER1234567890@GMAIL.COM
47001000123584	TEST	CMSTESTB	
47001000123743	TEST	CMSTESTAA	
47001000123744	TEST	CMSTESTBB	CMSTESTBB@AA.BB

Search Results below the User Search fields

- Select the Applicant's User Identification (**UID**) link
*The **Issuance to [Applicant's Name]** screen for the selected user displays.*

Initiating Credential Activation

Issuance to TED SMITHSONIAN

1. Review the user information below.

UID: 33001000122023
 First Name: TED
 Last Name: SMITHSONIAN
 Email Address: TEST@TOM.COM
 Photo:

2. Perform the custom operations.

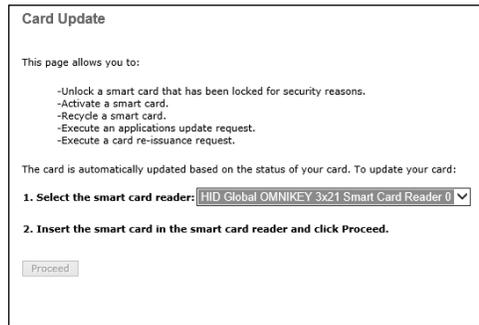
Click Next when ready: [Next](#)

Copyright © 2017-2018 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

Issuance to [Applicant's Name] Screen

Follow the step-by-step instructions on the **Issuance to [Applicant's Name]** screen.

9. Review the Applicant's information and digital photograph to verify identity. Verify that the record, the applicant in front of you, their photo ID and the credential you are issuing match.
10. Click the Next button.
11. The system verifies your site code. If correct, you are prompted to proceed.
12. From the **Choose the smart card reader for issuance** drop-down list, select the smart card reader that is not holding a Credential

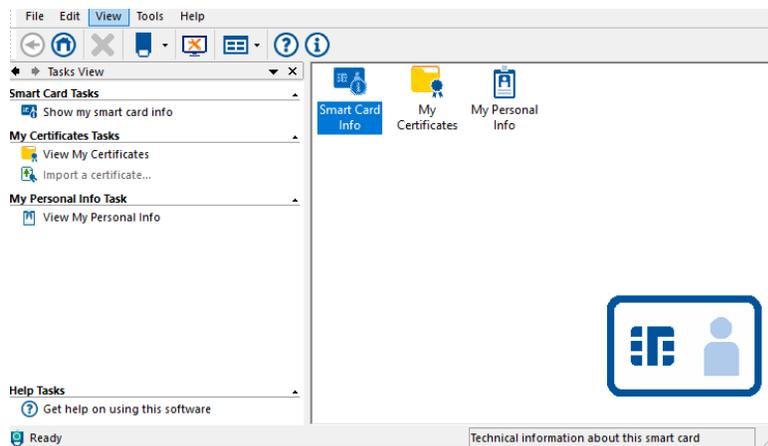


Smart Card Reader Drop-down List

Choosing the Empty Card Reader

You can determine the name of the empty smart card reader by accessing the ActivClient User Console program. Locate **ActiveID ActivClient** in the **Windows Start Menu** list at the lower-left corner of your monitor.

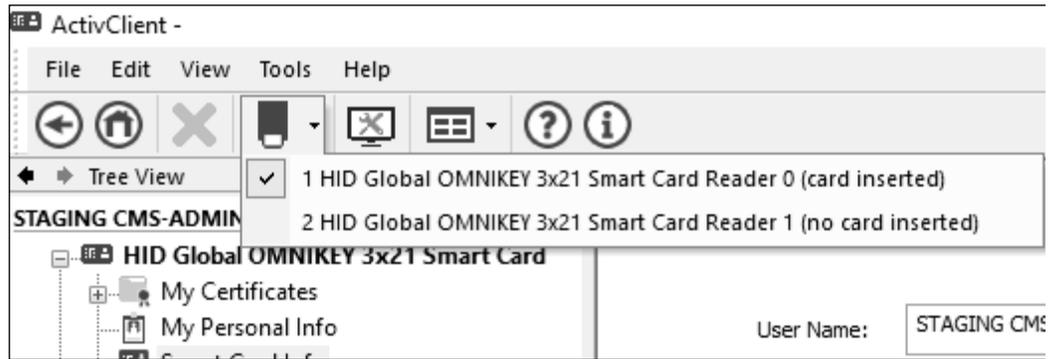
1. Click **ActiveID ActivClient** Then click User Console
*The **ActivClient User Console** window will open.*



ActivClient Menu

2. Select the card reader icon located in the task bar.

A drop down menu will show the card readers labeled 0 or 1 and will show if a card is inserted into a reader



ActivClient Smart Card Info Window

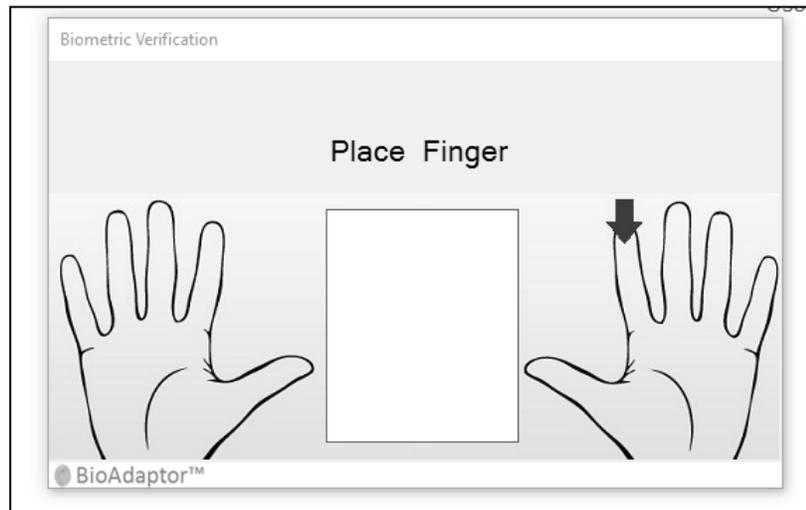
3. Make note of which OMNIKEY reader is displaying (**no card inserted**).



Hint

If the card readers at the Credentiaing Unit workstation have not previously been labeled, label them now with a 0 or 1. This allows you to perform the Activation process without stopping to determine the card reader number.

Insert the Applicants USAccess Credential into the reader and click **Next**.
*The system indicates that biometric authentication is in progress and the **Fingerprint Capture** window displays.*



Fingerprint Capture Window

Verifying the Applicant’s Fingerprint against the Database

The system requires biometric authentication of the Applicant.

Note: The system omits this step when fingerprints are not available during enrollment.

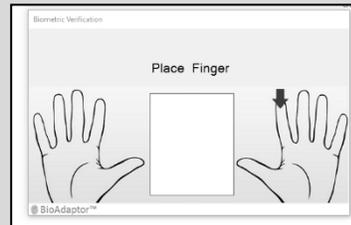
1. Ask the Applicant to place his or her primary finger, which is indicated by the hand diagram, on the fingerprint reader.

The Applicant's fingerprint displays in the Fingerprint Capture window. The scanner will present a message below the capture window if the finger position needs to be adjusted on the platen or if the platen is dirty and needs to be cleaned.



Hint

The primary finger is indicated in the window title bar and in the pictogram of the hand in the window.



Hand Diagram with Primary Finger

When the fingerprint has been verified, the Information Gathering screen displays. Note that the “Biometric authentication succeeded” message also displays.



Information Gathering Screen

Completing the Information Gathering Screen

2. Ask the Applicant to choose a Personal Identification Number (PIN) for the smart card.

The PIN must contain at least six but no more than eight numerals. Predictable sequences of numbers are not allowed.



Watch Out!

DO NOT choose or suggest a PIN for the Applicant. Any action the registrar takes to choose, suggest, or enter a PIN for the Applicant is a security violation.

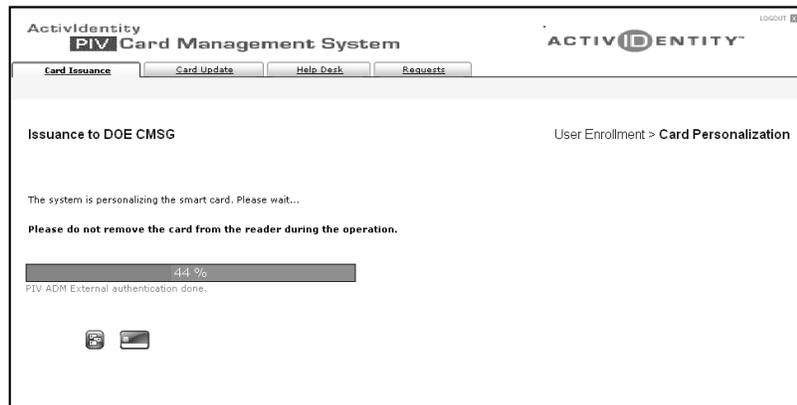
3. Ask the Applicant to enter his or her PIN in the Choose a PIN for the smart card: field.
4. Ask the Applicant to reenter his or her PIN in the Confirm the PIN: field.
5. Click the **Next** to personalize the smart card.

*The **Card Personalization** screen displays. During USAccess Credential personalization, data is read from and written to the Credential. Personalization averages from five to ten minutes depending on your network speed. Note the progress bar indicating the percentage of completion.*



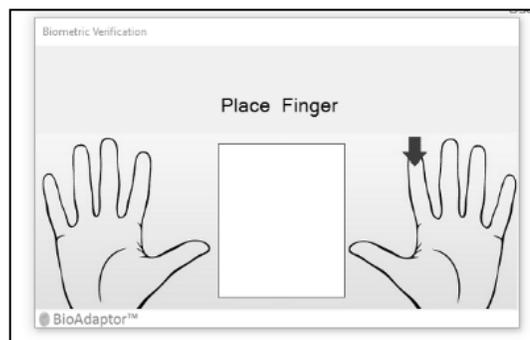
Watch Out!

The system instructs you to not remove the Credential during this process. Do not remove the Applicant's Credential while it is being personalized. Removing the Applicant's card during personalization may damage the chip and render the card unusable. However, it is possible to remove your Credential from the other card reader at this point.



Personalization Message

*The **Fingerprint Capture** window displays at the end of the personalization process.*

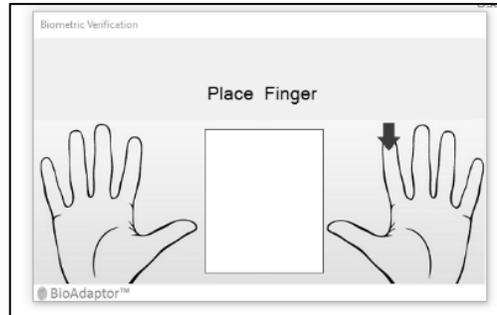


Fingerprint Capture Window

6. Ask the Applicant to place his or her primary finger, which is indicated by the hand diagram, on the fingerprint reader.

Note: The system omits this step when fingerprints are not available.

*The Applicant's fingerprint displays in the **Fingerprint Capture** window*



Hand Diagram with Primary Finger

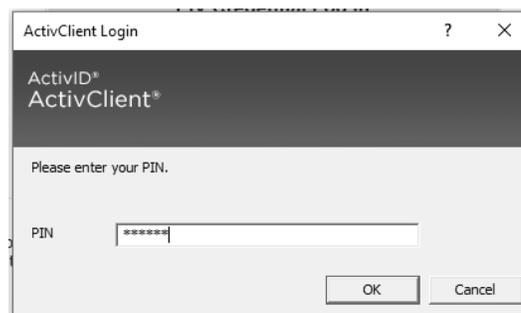
THE CARD HAS BEEN PERSONALIZED. The **Acknowledgment Required:** message displays and you are automatically redirected to the **Privacy Act Statement**.

Agreeing to the Acknowledgement of Responsibilities

As the final step of the activation process, the Applicant must use his or her personalized Credential and PIN to agree to the terms of the **Acknowledgement of Responsibilities**.

1. Remove your USAccess Credential from the reader. Leave the Applicant's Credential in the reader.
2. Ask the Applicant to read the Acknowledgement of Responsibilities.
3. Scroll to the bottom of the screen. Ask the Applicant to click the I Agree button to agree to the terms.

*The **ActivClient Login** window displays.*

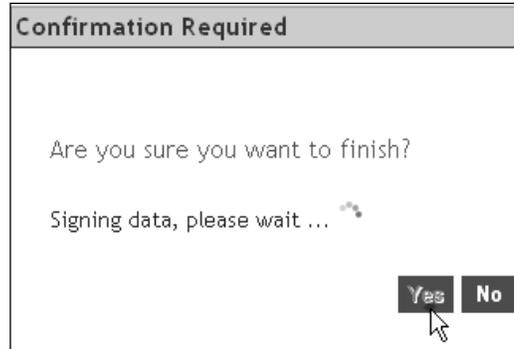


ActivClient Login Window

Digitally Signing the Acknowledgement of Responsibilities

4. Ask the Applicant to enter his or her new PIN.
5. Click the **OK** button.

*The **Confirmation Required** dialog box displays.*



Confirmation Required Dialog Box

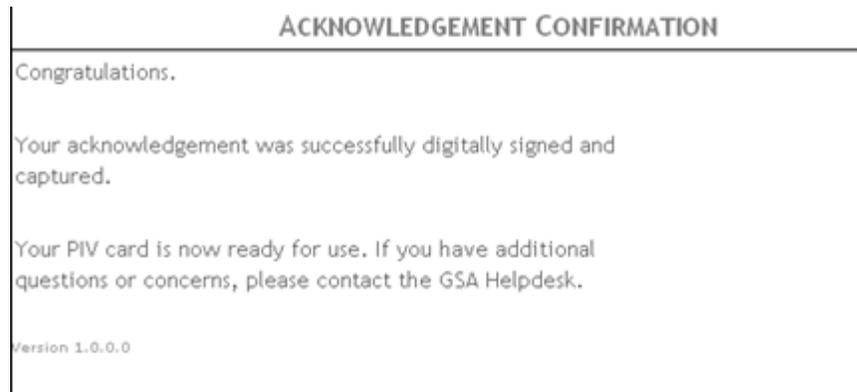


Watch Out!

You may have to scroll the Privacy Act to see the **Confirmation Required** dialog box.

6. Click the **Yes** button.

*The **Acknowledgement Confirmation** screen displays and the Applicant's digital signature has been recorded.*



Acknowledgement Confirmation Screen

Completing the USAccess Credential Activation

7. Ask the Applicant to remove his or her Credential from the card reader. The Credential has been successfully activated and it is now ready for use.

8. If you are conducting another Attended Activation, return your Credential to the card reader and start Attended Activation with the next Applicant.
9. If you are finished with Attended Activation, log out of the PIV Attended Activation program.
10. Click the **LOGOUT** link in the upper right corner of the **PIV Attended Activation Issuance** screen.



Watch Out!

Remember to log out of the system when you are finished with activations. Never walk away from the computer with the application open and logged in with your Credential in the card reader. This is a serious breach of security.

Attended USAccess Credential Activation without Fingerprints

For the most part, the Activation process is the same for an Applicant who was enrolled FTE (without fingerprints) and is unable to provide viable fingerprints during activation. Follow the steps in the **Attended USAccess Credential Activation with Fingerprints** section of this guide to:

- Ask the applicant for two forms of ID. Verify the applicant's identity by comparing the applicant, their photo ID, and the photo on the credential you are issuing to that applicant.
- Launch the PIV Attended Activation
- Search for the Applicant
- Verify the applicant's record matches the applicant in front of you.
- Initiate Credential activation

When you click the **Next** button after inserting the Credential into the card reader, the system skips the primary finger verification against the database and take you directly to the **Information Gathering** screen. A message displays at the top of the screen alerting you that there is **No biometric information** and the system is **Skipping authentication**.

The system then prompts the Applicant to create a credential PIN.



Watch Out!

Chain of Trust Requirements

In most cases you will not know if an applicant is missing fingerprints on their record. If you are performing attended activation and the page displays indicating there is no biometric information in the record, you must verify the applicant's identity. In order to verify their identity, the applicant will need to present 2 valid forms of identification following the same identity proofing requirements needed during Enrollment. The identity documents **DO NOT** have to be the same ones the applicant used during their Enrollment, but they **DO** have to follow the Acceptable Forms of ID list and guidelines.

This same identity proofing process would be required if it is deemed necessary for the Help Desk to remove fingerprints during an activation in which the applicant is unable to verify the existing fingerprint templates.

The purpose of attended activation is to *ensure the applicant's identity is verified* when a fingerprint is not available to establish the chain of trust with the record in the database. If you did not properly verify the applicant's identity, click the back button to go back to the Issuance to Applicant screen. Ask the applicant for two forms of ID. Compare the photo ID with the applicant standing in front of you, the applicant's record on the screen and the photo and information on the card you are about to activate. If all match, click Next and continue with the activation.

Continue with the steps in the **Attended USAccess Credential Activation with Fingerprints** section of this guide to:

- Complete the **Information Gathering Screen** to begin Credential personalization.
- Agree to the Privacy Act Statement and Acknowledgement of Responsibilities
- Digitally sign the USAccess Credential
- Complete the USAccess Credential activation

Note: The system does not ask for verification of the Applicant's fingerprint during Credential personalization.

Activation Errors and Error Messages

Fingerprint Verification Errors

Activation Fails Before or on First Fingerprint Verification

Follow these procedures if Credential activation fails before the first fingerprint verification:

1. Ask the Applicant to remove his or her Credential from the card reader.
2. Try to activate the Credential a second time.

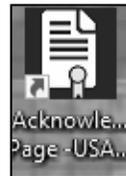
Try all the fingerprint capture techniques: adding moisture, removing moisture, applying more pressure, applying less pressure, etc.

3. Ask the Applicant to remove the Credential from the card reader.
4. Try activating the Credential using Attended Activation.
5. If activation fails again, write down (in its entirety) any error message that displays.
6. Call the Help Desk for assistance at 1-866-493-8391, explain the problem, and state the complete error message displayed in Attended Activation.
7. Ask the Applicant to wait while you follow the Help Desk directions to activate the Credential.

Activation Fails on the Second Fingerprint Verification

Follow these procedures if Credential activation fails on the second fingerprint verification:

1. If using Unattended Activation, write down (in its entirety) and error message that displays.
2. Double click the **Acknowledgement Page** icon on the activation station desktop.



3. Ask the Applicant to digitally sign the Privacy Act Statement.
4. If the statement is successfully signed, the Credential is activated and the person may leave the center with the Credential.
5. If the signing is unsuccessful:
 - a. Try to activate the Credential using Attended Activation. The **Retry the Request** and/or **Recycle the Card** error messages may display. Follow the directions and try to activate the Credential again.
 - b. If the Credential fails the second fingerprint verification again, write down (in its entirety) any error message that displays. Have the Applicant try to sign the Privacy Act again. If the statement is successfully signed, the Credential is activated and the person may leave the center with the Credential.
 - c. If the signing is unsuccessful, call the Help Desk, explain what happened during activation, and state the complete error message. Follow the Help Desk directions.

Card Activation Error Messages

The following error messages may display when performing Attended Activation. Be sure to attempt to perform Attended Activation if Unattended Activation fails because many of the error messages that describe the specific failure only display in Attended Activation.

Where possible, follow the directions in the message. If there are no directions in the message, or the Registrar/Activator is not able to perform the task directed in the message, call the Help Desk. It is critical to have the complete error message available to read to the Help Desk agent.

Retry a Request

1. When the error message directs you to retry a request, open Attended Activation (if it is not already open), and click the Requests tab.
2. A table displays with a link to Retry the request. Click the **Retry** hyperlink.

Recycle a Credential

Recycling a Credential is similar to reformatting a disk. It removes any information placed on the chip when the personalization attempt was made. Recycle a Credential only when directed to do so by the Help Desk or by an error message on the screen.

1. When an error message directs you to recycle a Credential, open Attended Activation (if it is not already open), and click the **Card Update** tab.
2. Insert the Applicant's Credential in the card reader.
3. Select the card reader holding the Credential that needs to be recycled. Click **Proceed**.
4. Follow the directions to recycle the Credential.

Too many users found. Please change your search criteria

Occasionally, the search for an Applicant in Attended Activation results in too many Applicants with the same last name. The system cannot display that many search results and displays this message: "Too many users were found. Please refine your query."

Search for users: UID starting with

First Name starting with

Last Name starting with Anderson

Email Address starting with

cn starting with

From groups: Select: [All](#) , [None](#)

A Fast Search

Administrative Conference of the United States

African Development Foundation

Agriculture

American Battle Monuments Commission

Advanced Search

Note: Using advanced search may affect performance.

All users

Users without any card

Users with a card

Limit number of results to users.

**Too many users were found.
Please refine your query.**

Card Issuance User Search – Too Many Users Found



Hint

When this message displays, use “**cn**” from the **Search for users:** list (“**cn**” stands for “certificate name,” but another way to remember it is “complete name”).

1. Under the **Search for users:** list, select **cn**. Enter the Applicant’s first AND last names, that is, first name followed by a space, then last name. The following example shows Satoshi (space) Nakamoto.

Card Issuance User Search – Search for users: cn

- Next, be sure a group is selected under the **From groups:** list to narrow down the search to just the Applicant’s group. Use **A Fast Search** to shorten the time it takes to search for an Applicant. The search results display all users with the full name you entered. This results in a smaller results return and should not generate the “too many users” error.

PIN Reset

This procedure outlines the steps to reset the PIN on a USAccess Credential. Begin by making sure the Credential is locked. Then, use Attended Activation to unlock the Credential and reset the PIN. The system allows an incorrect PIN to be entered five times before the Credential is locked on the sixth try. USAccess Credential PINs may be reset using Attended Activation.

- Verify the Credential is locked. Ask the Credential holder to use Unattended Activation to lock his or her Credential if it is not yet locked, as PIN resets can only be performed on locked Credentials. Click the **Activations Icon** then click **PIV Unattended Activation** icon at the lower portion of the PIV Window.



PIV Unattended Activation

PIV Unattended Activation Icon

The **Welcome** screen displays.



Welcome to USAccess Card Management Window

2. Click the **Start** button.

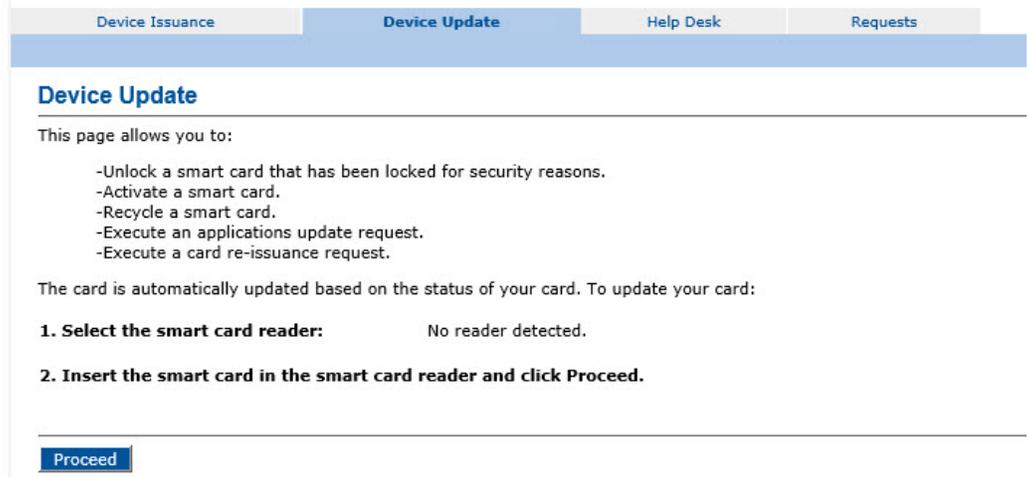
The **Please Identify Yourself** window displays.



Please Identify Yourself Window

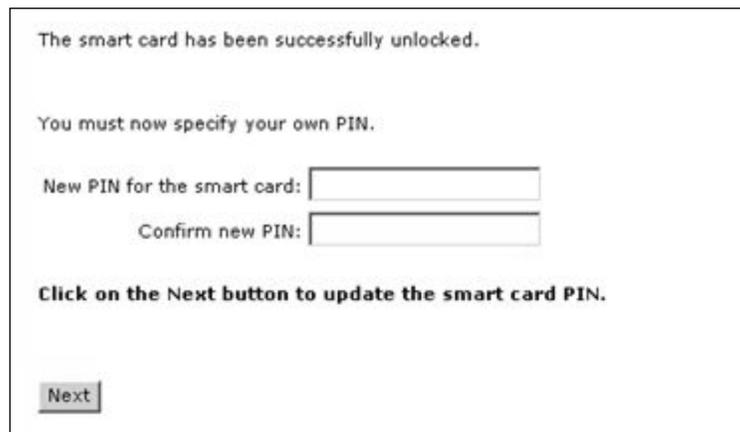
3. Ask the Credential holder to enter an incorrect PIN six times. This message displays when the Credential is locked: "Your card is locked because you entered too many wrong PINs".
4. When the Credential is locked, open **PIV Attended Activation**.
5. Click the **Device Update** tab.

The **Device Update** screen displays.



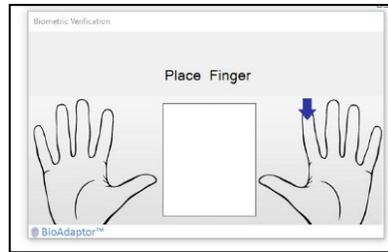
Device Update screen

6. Put the Credential into the empty card reader.
7. Select the card reader holding the locked Credential from the drop-down list.
8. Click **Proceed**.
The Credential holder's record displays.
9. Click **Next** and wait while the system unlocks the Credential. This should not take more than a few seconds.
*The **Smart Card has been successfully unlocked** screen displays.*



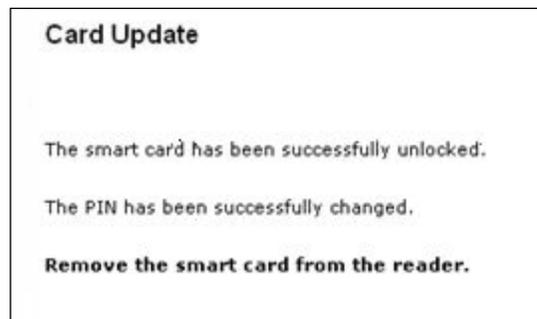
Smart Card has been successfully unlocked screen

10. The Credential has been unlocked and a new PIN is requested. Ask the Credential holder to enter and confirm a new PIN.
11. Click **Next**.
*The **Fingerprint Capture** window displays.*



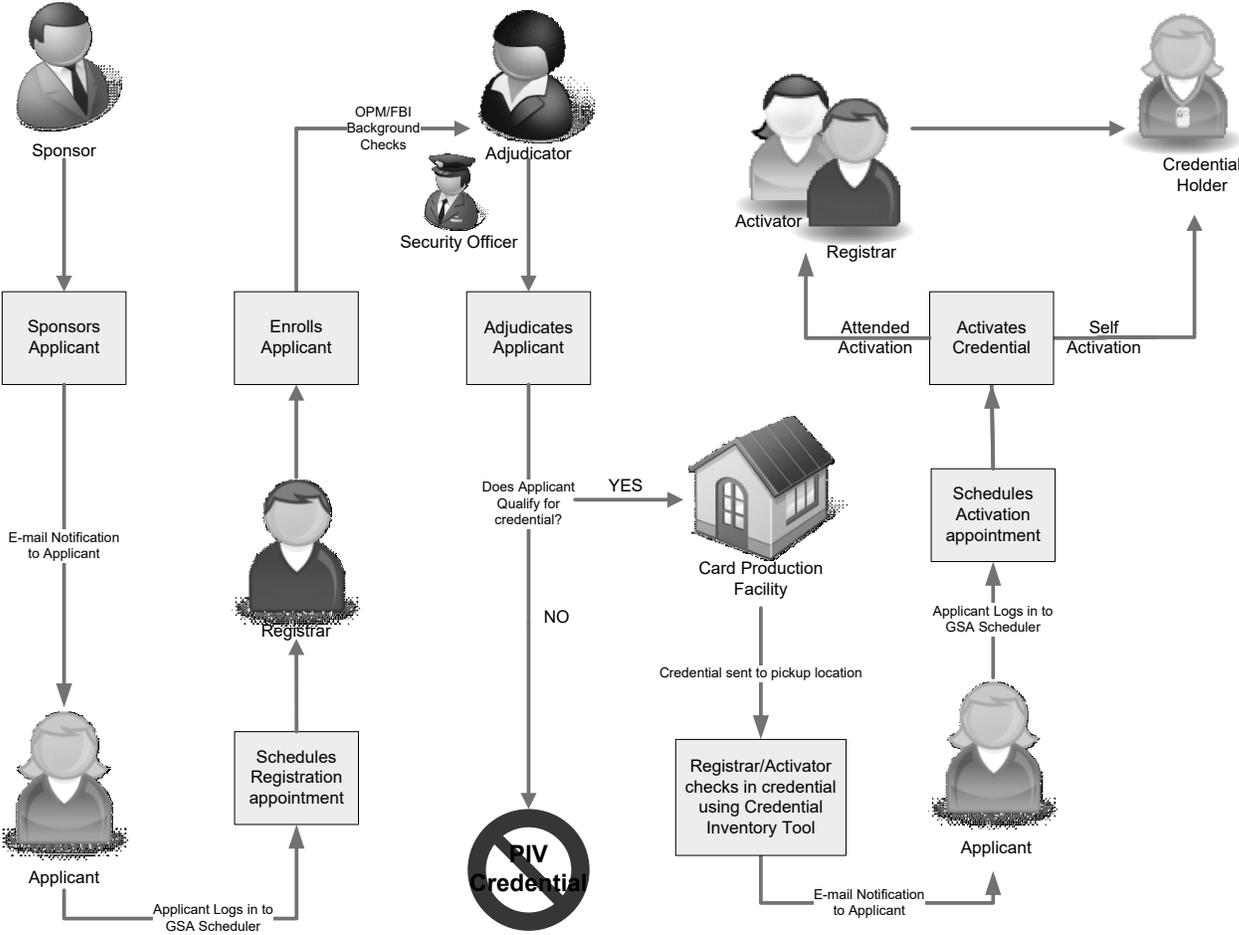
Fingerprint Capture Window

12. Ask the Credential holder to verify his or her fingerprint.
13. The update is complete. Return the Credential to the Credential holder.



Card Update screen - The PIN has been successfully changed

Appendix A – Enrollment Process Flow



This page intentionally left blank.

Appendix B – Terms and Acronyms

Acronym	Definition
C&A	Certification and Accreditation
CA	Certificate Authority
CHUID	Cardholder Unique Identifier
CIT	Credential Inventory Tool
CMS	Card Management System
CU	Credentialing Unit
DAA	Designated Approval Authority
DHS	Department of Homeland Security
e-QIP	Electronic Questionnaire for Investigations Processing
FBI	Federal Bureau of Investigation
FBI FP	FBI National Criminal History Fingerprint
FCU	Fixed Credentialing Unit
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive #12
ICC	Integrated Circuit Chip
IDMS	Identity Management System
LA	Light Activation
LACS	Logical Access Control System
MCU	Mobile Credentialing Unit
MSO	Managed Services Office
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PACS	Physical Access Control System
PCI	PIV Card Issuer
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification – Phase 1

Acronym	Definition
PIV-II	Personal Identity Verification – Phase 2
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
SP	Special Publication
UID	User Identifier (number)
UPN	User Principle Name

Appendix C – Definitions

Access control – the process of granting or denying requests to access physical facilities or areas, or to logical systems (e.g., computer networks or software applications). See also “logical access control system” and “physical access control system.”

Authentication - the process of establishing an individual’s identity and determining whether individual Federal employees or contractors are who they say they are.

Authorization - process of giving individuals access to specific areas or systems based on their rights for access and contingent on successful authentication.

Background Investigation – any one of various Federal investigations conducted by OPM, the FBI, or by Federal departments and agencies with delegated authority to conduct personnel security background investigations.

Biometric – a measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints and facial images. A biometric system uses biometric data for authentication purposes.

Contractor – see “Employee”.

Employee – as defined in Executive Order (EO) 12968, “Employee” means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts on behalf of an agency as determined by the agency head. See also “Employee” as defined in title 5 U.S.C §2105.

e-QIP Tracking Number – Number assigned by e-QIP to each Form SF-85 application. For those Interior bureaus and offices using e-QIP, the tracking number must be written on the fingerprint card when it is submitted to OPM in order to bind the fingerprint card to the proper Applicant.

FBI FP Check – National Criminal History Fingerprint check of the FBI fingerprint files. This check is an integral part of the NACI.

Identity Management System (IDMS) - one or more systems or applications that manage the identity verification, validation, and card issuance process. The IDMS software is used by USAccess Registrars to enroll Applicants.

Identity-proofing – the process of providing identity source documents (e.g., driver’s license, passport, birth certificate, etc.) to a enrollment authority, or the process of verifying an individual’s information that he or she is that individual and no other. FIPS 201-1 requires that one of these documents be an original State or Federal Government-issued photo ID, and the other be from the approved set of identity documents listed on Form I-9.

Logical Access Control System (LACS) – protection mechanisms that limit users’ access to information technology (IT) systems by restricting their form of access to those systems necessary to perform their job function. These LACS may be built into an operating system, application, or an added system.

National Agency Check (NAC) – The NAC is part of every NACI. Standard NACs are Security/Suitability Investigations Index, Defense Clearance and Investigation Index, FBI Name Check, and FBI National Criminal History Check.

National Agency Check with Inquiries (NACI) – the basic and minimum investigation required of all Federal employees and contractors consisting of searches of the OPM Security/ Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division’s name and fingerprint files, and other files or indices when necessary. A NACI also includes written inquiries and searches of records covering specific areas of an individual’s background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

Physical Access Control System (PACS) – protection mechanisms that limit users’ access to physical facilities or areas within a facility necessary to perform their job function. These systems typically involve a combination of hardware and software (e.g., a card reader), and may involve human control (e.g., a security guard).

PIV-II Credential – a government-issued identity Credential, referred to as a smart card, which contains a contact and contact-less chip. The Credential holder's facial image is printed on the Credential along with other identifying information and security features that can be used to authenticate the user for physical access to federally controlled facilities. The Credential may include a PKI certificate, which controls logical access to federally controlled information systems.

Public Key Infrastructure (PKI) – A service that provides cryptographic keys needed to perform digital signature-based identity verification, and to protect communications and storage of sensitive data.

SF-87 - Fingerprint Chart for Federal employee(s) or Applicant for Federal employment.

Submitting Office Identifier (SOI) – Number assigned by OPM to identify office that submitted the NACI request.

Appendix D – Homeland Security Presidential Directive 12



For Immediate Release
Office of the Press Secretary
August 27, 2004

Homeland Security Presidential Directive/Hspd-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard,

the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

###
