

Department of Veterans Affairs

User Guide Veteran Health Identification Card (VHIC) 4.2



February 2014

Version 2.0

Revision History

Date	Version	Description	Author
05/07/2012	0.1	Initial Creation	S. Schaubach
08/07/2012	0.2	Added Proofing	T. Keyzman
10/24/2012	0.3	Updated after review with the Business team	T. Keyzman
11/21/2012	0.4	Updates per Anomaly log	T. Keyzman
12/28/12	0.5	Updated screen shots	T. Keyzman
01/24/2013	0.6	Updated after review with the Business team	T. Keyzman
01/28/13	1.0	Technical edit and review Fixed the formatting and numbering in many places...	I. Levine
04/29/2013	1.1	Updated based on testing results	T. Keyzman
05/15/2013	1.1	Updated MVI search instructions	T. Keyzman
05/16/2013	1.2	Updated Proofing section	J. Awe
06/04/13		Tech edit. Converted to 508 compliant pdf and posted to TSPR.	I. Levine
06/20/13	1.3	Added information from Provisioning & Proofing training	T. Keyzman
06/21/13	1.4	Updated proofing information	J. Awe
06/24/13	1.5	Updated Provisioning url	T. Keyzman
06/25/13	1.6	Added Help Desk Tier 1 email	T. Keyzman
07/18/13	1.7	Changed VIC to VHIC	T. Keyzman
07/26/13		Updated Proofing information re: State of Issuance K. Solomon	K. Solomon
08/14/13	1.7.3	Fixed formatting, numbering and replaced images.	T. Keyzman
08/19/13	1.7.4	Version update	T. Keyzman
08/21/13		Added alt text to all screenshots. Converted to 508 compliant PDF and posted to VIC TSPR.	Irene Levine
10/21/13	1.7.5	Updated Step 5, "Capture Veteran Image, provisioning section, SSOI section, and added BOS	T. Keyzman

Date	Version	Description	Author
01/17/14	1.7.6	Updated SSOi section	T.Keyzman
01/24/14	1.7.7	Updated to address Product Support team comments	T.Keyzman
01/31/14	1.7.8	Updated to address additional Product Support team comments, added Appendix H	T.Keyzman
02/04//2014	1.7.9	Updated to address additional Product Support team comments.	T.Keyzman
02/10/2014	1.7.10	Updated to address CBO comments	T.Keyzman
02/12/2014	2.0	Technical edit, converted to 508 and posted to TSPR.	Irene Levine

Table of Contents

1. What is Veteran Health Identification Card (VHIC) System.....	5
2. Webcam.....	5
3. Roles.....	15
VHIC Read-Only User	15
VHIC Auditor	15
VHIC Associate.....	15
VHIC Supervisor	15
VHIC Technical Administrator – Tier 3	15
VHIC Program Administrator	15
4. Provisioning Service	15
5. Accessing VHIC Application using Single Sign On Internal (SSOi) Service.....	16
6. Accessing VHIC Application from a Browser	18
7. PIV Card Login for Step-Up Authentication.....	20
9 Creating a Veteran Health Identification Card (VHIC)	21
Card Request: Step 1 - Search for a Veteran.....	23
Card Request: Step 2 – Select Veteran	25
Card Request: Step 3 – Verify Identity Attributes	28
Card Request: Step 4 – Proof Veteran	30
Proofing Process: Step 1 - User Profile.....	31
Proofing Process: Step 2 - Address Verification	32
Proofing Process: Step 3 – Primary Identification	34
Proofing Process: Step 4 - Secondary Identification.....	36
Proofing Process: Step 5 – Submit Proof.....	39
Card Request: Step 5 - Capture Veteran Image.....	40
Card Request: Step 6 - Save Card Request.....	44
10. Reporting Capabilities	Error! Bookmark not defined.
Report Page.....	46
Veteran/Direct Record Search.....	48
Card Request Totals Report.....	51
Card Status Report	51
Multiple Requests Report.....	54
Card History.....	55
Auditing	57
11. Getting Help	59
APPENDIX A: MVI Probabilistic Search.....	60
APPENDIX B: ACCEPTABLE IDENTITY DOCUMENTS	61
APPENDIX C: ADDRESS CONFIRMATION DOCUMENT CRITERIA	62
APPENDIX D: PROVISIONING	63
APPENDIX E: SSOi.....	80
APPENDIX F: VA Service Desk Manager (SDM).....	87
APPENDIX G: Set up Adobe Flash Player	89
APPENDIX H: Guidelines for Scanning Barcode	93

1. What is Veteran Health Identification Card (VHIC) System

The VHIC System is a web-based application for the issuance of the Veterans Identification Card (VHIC). This system is used by VHIC end users at VA medical facilities throughout the United States.

To receive a Veteran Health Identification Card (VHIC), the Veteran must meet the following eligibility criteria:

- Be eligible for VA medical benefits
- Be enrolled in the VA Healthcare system
- Be Level 2 proofed at a VA medial facility
- Veterans Identity must be recognized in the Master Veteran Index (MVI), which is managed by the Identity and Access Management of the VA

Each day the card requests are transmitted from the VHIC system to a vendor to print and mail the cards to the Veterans or to the requesting facility. Typically, the cards are received in 7-10 business days from date of request.

To ensure the VHIC is received at the appropriate address, the VHIC Associate verifies that the current address is used and the Print Vendor verifies that the address is valid. If the U.S. Postal Service cannot deliver the card, it is returned to the requesting facility.

Note: The level 2 proofing process is a method to verify the identity of Veterans. VA requires Veterans to provide approved identification documents to access Personal Identifiable Information (PII), Personal Health Information (PHI) and request a Veterans Health Identification Card (VHIC).

2. Webcam

The Logitech Webcam Pro 9000 webcam works well with VHIC 4.2. Other cameras that can transmit their image to a computer or computer network via USB, FireWire or similar cable will work with VHIC 4.2 also.

The primary technical specifications for the Logitech Webcam Pro 9000 are listed below. Other cameras used instead of the Logitech Webcam Pro 9000 must have comparable specifications.

Logitech Webcam Pro 9000 Technical Specifications

- Carl Zeiss® optics with autofocus
- Native 2-MP HD sensor
- High-definition video (up to 1600 X 1200*)
- 720p widescreen mode with recommended system
- Up to 8-megapixel photos (enhanced from native 2 MP sensor)
- Hi-Speed USB 2.0 certified

- Logitech® webcam software (including Logitech® Video Effects™: fun filters, avatars, video masks, and face accessories)
- Universal clip fits notebooks, LCD or CRT monitors

The following information will discuss the installation and use of the camera software to help facilitate the picture taking process. If you do not have the actual installation disk, you can download the software from the webcam manufacturer website.

The download page should auto-detect your operating system and the version you need. Click the 'Download Software' button. Once the download is complete and with the camera disconnected from your system, run the installation of the software. It will direct you to connect the camera during the installation process.

Instructions provided below are for **Logitech Webcam Pro 9000**.

Link to download software:

<http://www.logitech.com/en-hk/support/3056?section=downloads&osid=14&bit=64>

***Note:** Users may be directed to uncheck the Logitech Motion Detection option.

QuickCam® Pro 9000

[Support](#)[Downloads](#)[Troubleshooting](#)[Support Community](#)[Contact Us](#)

M/N: V-UBM46,UBM46

Windows 7

Logitech Webcam
Software

lws251.exe

[Download Now](#)

Selected Software:

Title: Logitech Webcam Software

Software Version: 2.51.828.0

Post Date: 8-OCT-2012

Platform: Windows 7

File Size: 73 Mb

Description

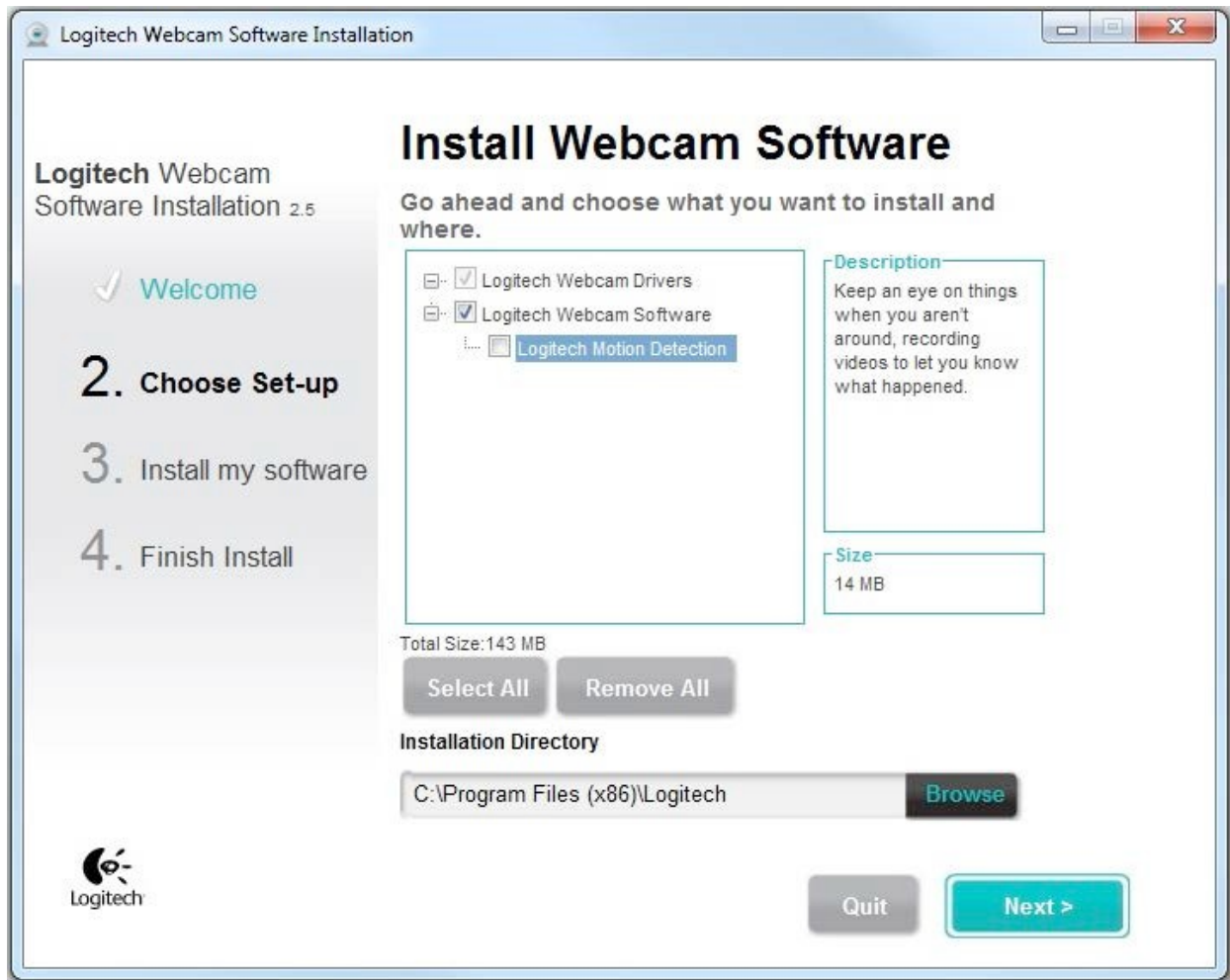
Logitech Webcam Software lets you capture your own photos and videos (720p/1080p mode with some cameras), upload them to Facebook with one-click, adjust your camera settings, activate motion detection, and use face-tracking with your preferred video-calling software.

Why Update?

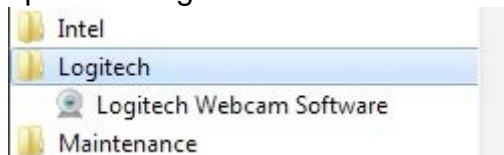
- Windows 8 support has been added.
Note: If you want to take advantage of the new Windows 8 interface, look for the Logitech Camera Controller available at the Windows 8 Store. (This feature only works with these webcams: C170, C270, C310, C525, C615 and C920.)
- This version of LWS no longer supports Video Effects.

Download Instructions

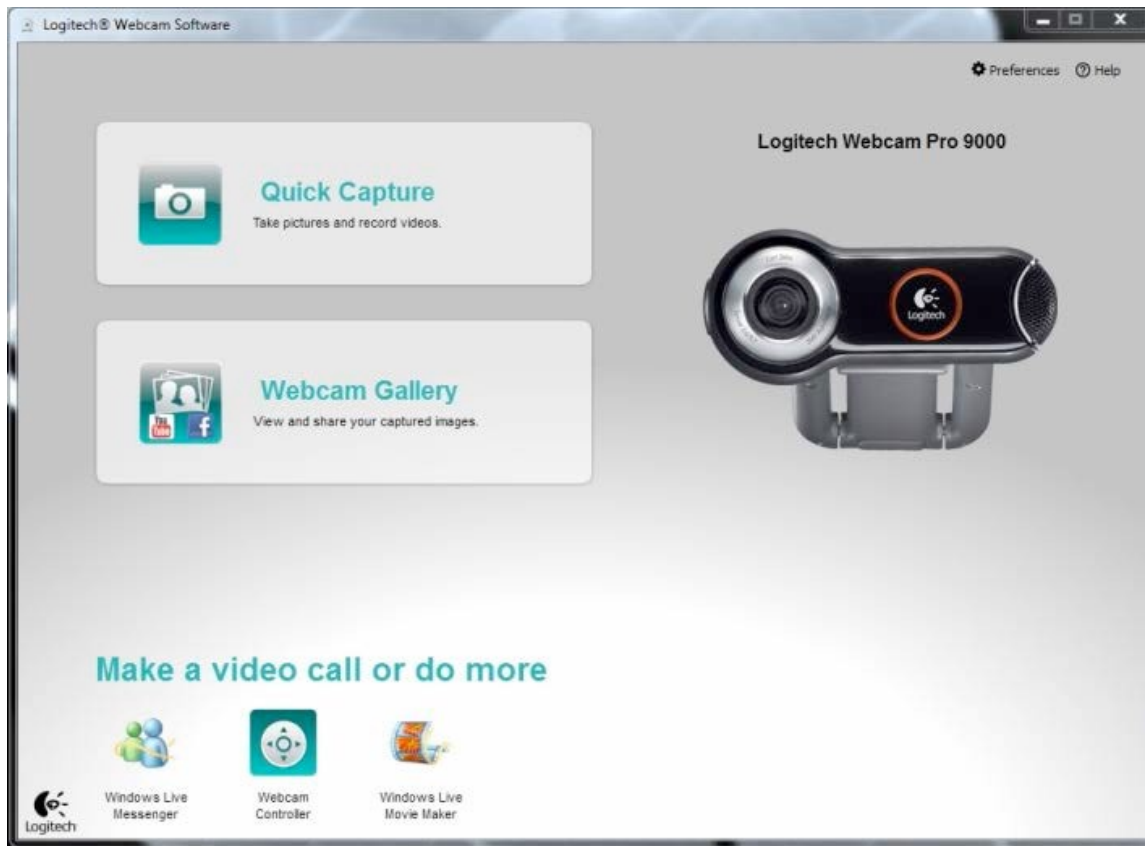
1. Select your operating system from the drop-down menu on the left. To determine your operating system:
 - Windows — Click **Start > Run**, or in the "Search" box, type `winver.exe` and press **Enter**.
 - Mac — Open the Apple menu and click **About This Mac**.
2. Select the software you want to download.
3. Select the installation type or file. ([Do I need the 32 or 64-bit version?](#))
4. Click **Download Software**.



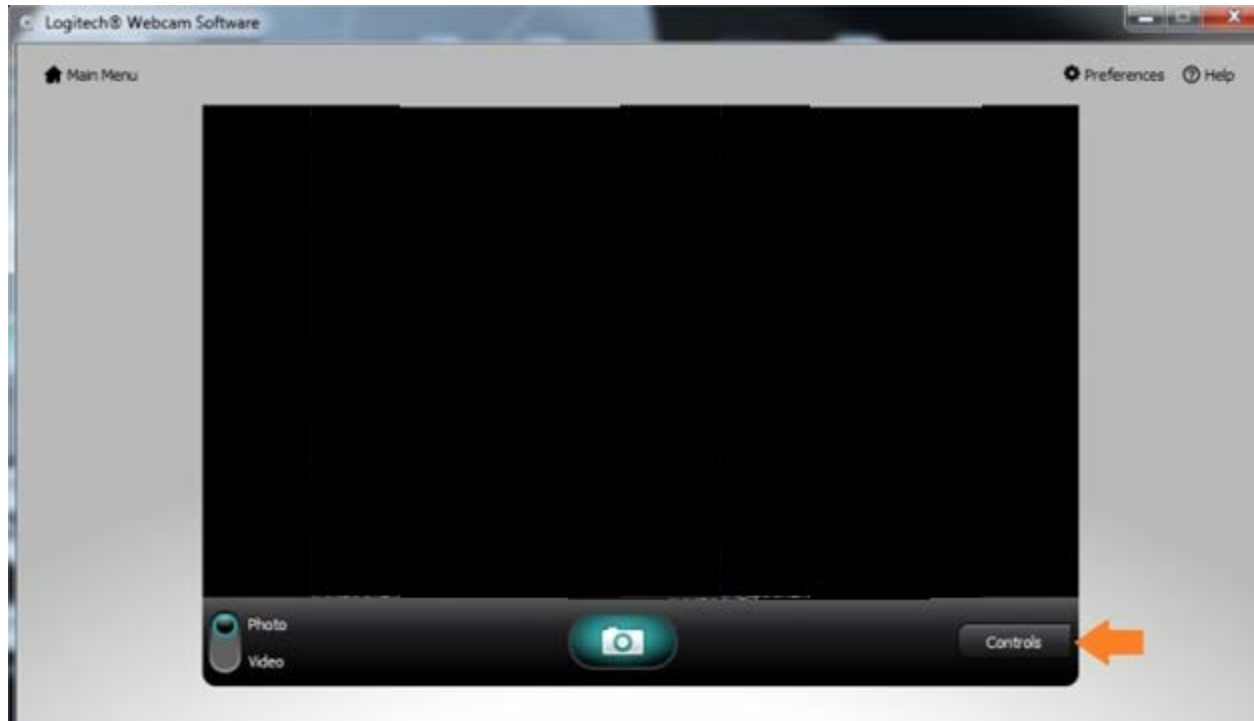
Once installation is complete you can adjust and save your basic camera settings in one of two ways. If you do not currently have the software open, you will want to locate and open the Logitech Webcam Software.



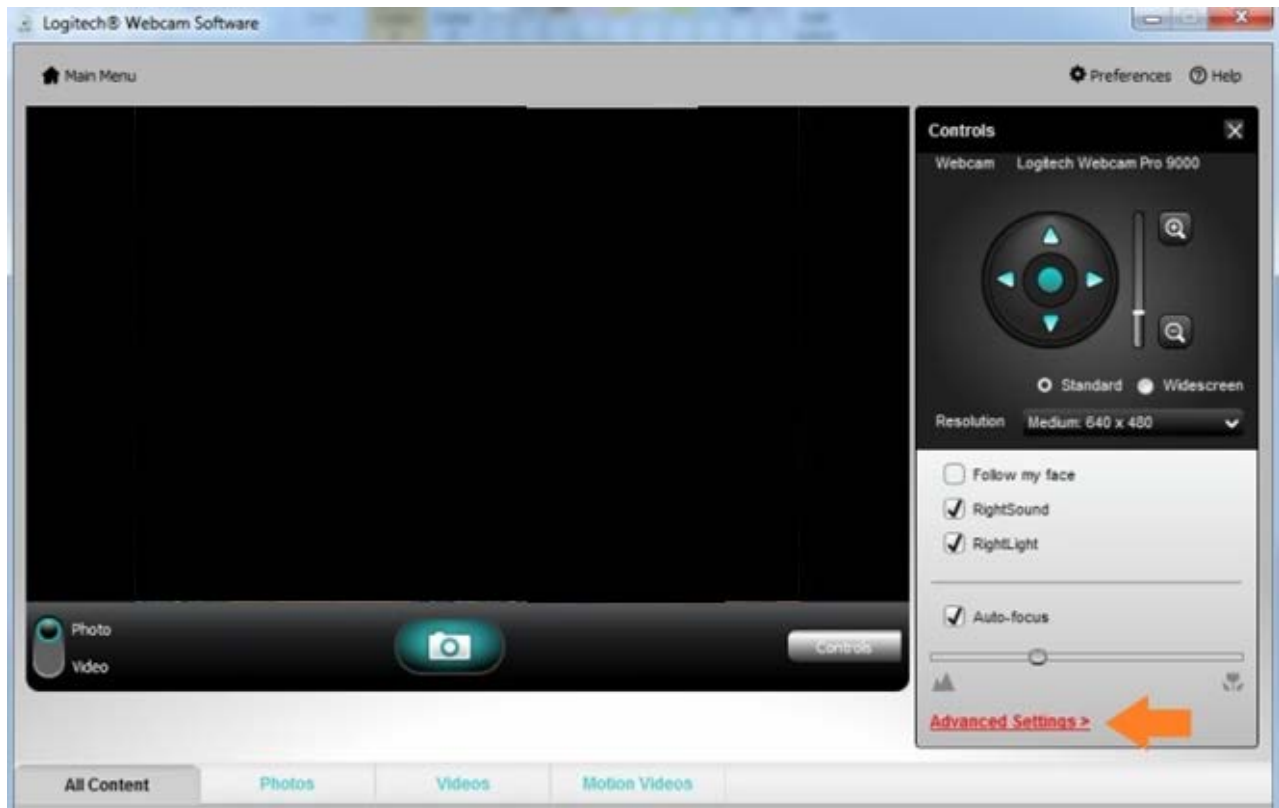
You should see the following screen or something similar:



Clicking on **Quick Capture** will open up a new screen and activate the camera. If the additional options panel is not displayed initially, you will want to click on the **Controls** button in the lower right of the camera window. This will open up additional functionality.

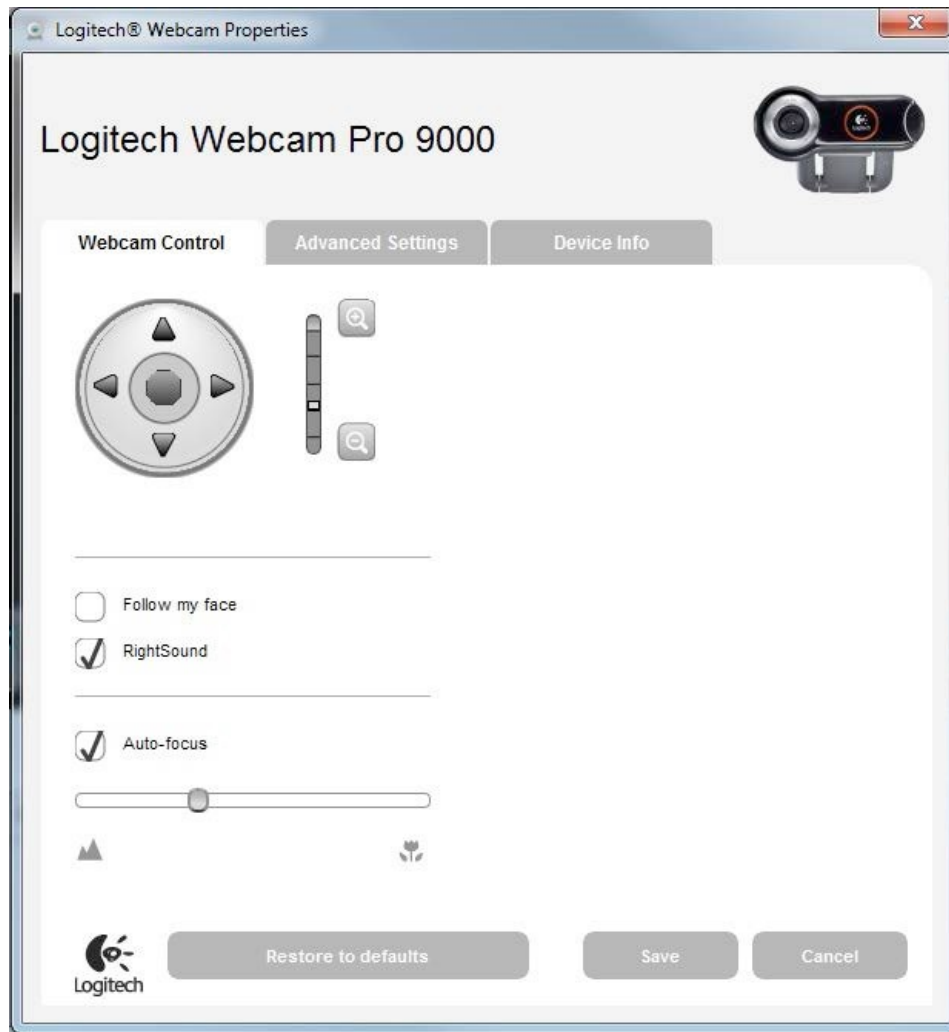


Once you open up the additional panel, click on the **Advanced Settings** link at the bottom of the new panel.



From here, click on the **Webcam Control** tab. Your camera should already be in its permanent location. From here, adjust your zoom and up/down/left/right positioning to the desired settings. Click **Save**.

You will want to leave **Follow my face** unchecked as this has a tendency to zoom in too close to the individual.



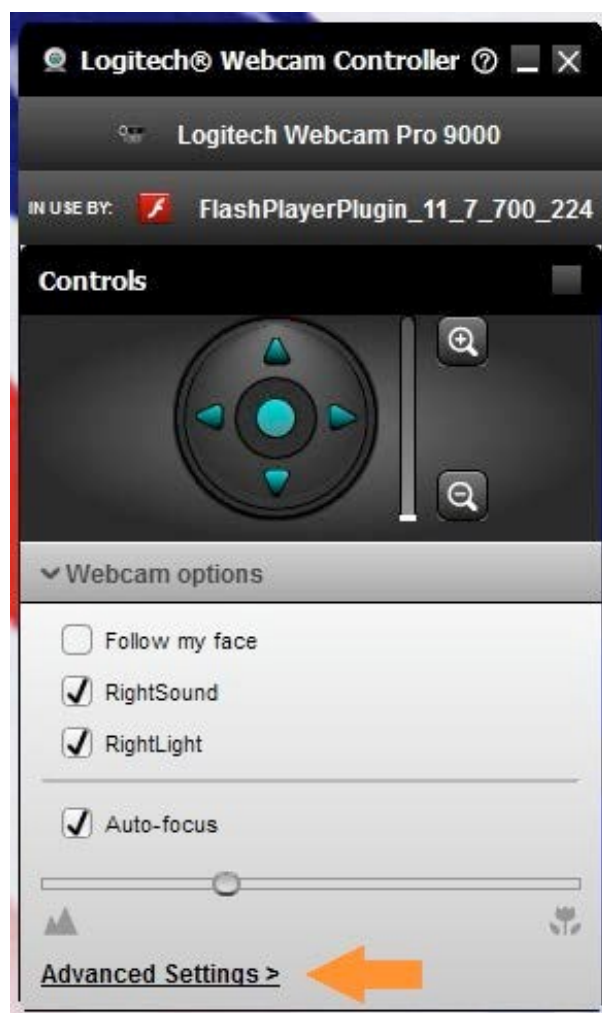
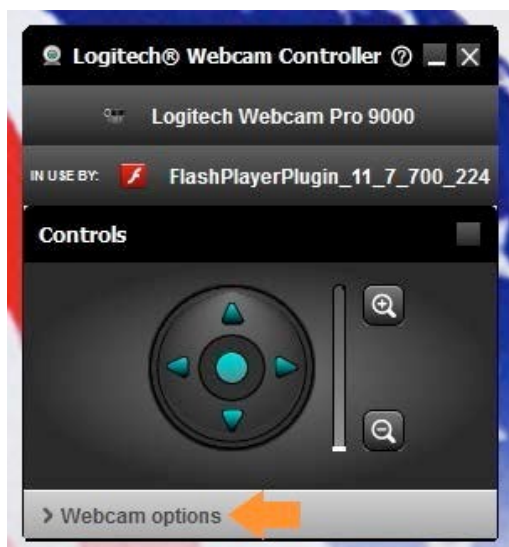
These saved settings should then come in to play when accessing the camera portion of the VHIC application. You also have the option of adjusting your settings within VHIC itself.

***IMPORTANT:** After installation of the software and during the initial encounter of the camera within VHIC – the user will be presented with a pop up request over top of the mini camera console. It will state: “Next time you start video, do you want your webcam controller to automatically launch?”

Click **Yes** so that the console is available for any minor positioning adjustments that may be needed during the picture taking process. It will always be available by accessing it from its desktop icon or folder location, but this saves time and ensures that it is readily accessible to the user when needed.



From the mini console, the user has the ability to access the same window to adjust and save settings as shown earlier. Simply click on **Webcam options** which will drop down some additional controls. From here, click on **Advanced Settings** to bring up the camera settings page.



3. Roles

These are the roles available within the system.

VHIC Read-Only User

The VHIC Read-Only User role shall be assigned to users with read-only access to the VHIC System.

VHIC Auditor

The VHIC Auditor role shall be assigned to users with read-only access to the VHIC System. The VHIC Auditor has access to Auditing reports.

VHIC Associate

The VHIC Associate role shall be assigned to individuals responsible for processing card requests and resolving card request issues.

VHIC Supervisor

The VHIC Supervisor shall automatically inherit all access and privileges given to the VHIC Associate. The VHIC Supervisor role is allowed to submit a request for user access to the VHIC application.

VHIC Technical Administrator – Tier 3

VHIC Technical Administrator (Tier 3) automatically inherits all access and privileges given to the VHIC Associate. The VHIC Technical Administrator (Tier 3) has access to the Administration page.

VHIC Program Administrator

The VHIC Administrator role shall be assigned to individuals responsible for the creation and maintenance of all other VHIC accounts/roles. The VHIC Administrator shall automatically inherit privileges given to the VHIC Supervisor.

4. Provisioning Service

The Provisioning Service is an integral component of the Identity and Access Management (IAM) solution, which institutes an automated, streamlined approval workflow process to augment the existing identity life cycle model of the VA. Provisioning encompasses various aspects of user access management, including initial assignment of user entitlements, subsequent modification of those entitlements, and removal of entitlements. It provides ability to automate processes, rules and procedures for approving, granting, and removing system access.

All VHIC Users must be provisioned to access the VHIC application. To provision a User, an access request should be submitted from the Provisioning Service interface.

Access the Provisioning Service through a browser using the following link:

<https://provapp.iam.va.gov/iam/im/prov/>.

All access requests should be approved by VHIC Program.

The VHIC Associates should contact their VHIC Supervisors to request access to the VHIC application.

VHIC User Provisioning Steps and additional Provisioning Service Information can be found in Appendix D.

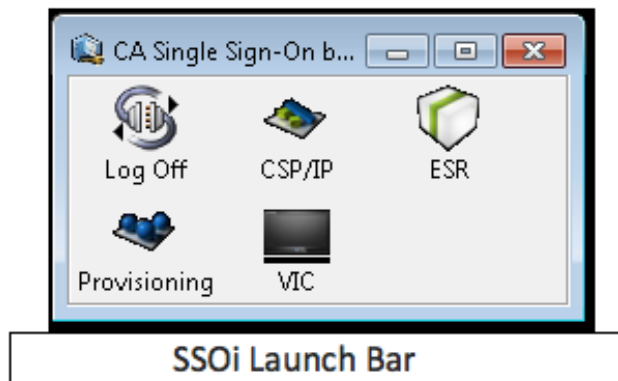
5. Accessing VHIC Application using Single Sign On Internal (SSOi) Service

This section demonstrates the **step-by-step process** for accessing VHIC application using SSOi:

1. Log on to a VA desktop using:
 - Your username and password credentials (Do NOT enter domain name)
 - Or a PIV Card and PIN authentication.
2. Launch the SSOi Launch Bar from the Program menu.
 - Click on Start
 - Click on All Programs
 - Click on CA
 - Click on Single Sign-On
 - Click on Single Sign-On launch bar



3. You will be presented with one or more icons representing the integrated applications to choose from.
4. Select VIC application from the SSOi launch bar.



When initiating the integrated application session via the SSOi Service (applications integrated with CA SSO) for the first time, you will be prompted to enter application credentials. See Appendix E for more information.

When the application password is changed for the applications integrated with CA SSO, you will be prompted to enter new application credentials.

6. Accessing VHIC Application from a Browser

This section demonstrates the **step-by-step process** for accessing VHIC application from a browser:

1. Log on to the VA desktop using your username and password or PIV Card and PIN authentication.

Note: Do NOT enter the domain name when you sign using your credentials

2. Open a web browser and enter the URL for an SSOi Service integrated application.

Enter the URL below to login to the VHIC application:

<https://vic.iam.va.gov/VIC/faces/index.jsf>



Note: URL is case-sensitive and 'VIC' must be capitalized

3. Following SSOi centralized page will be displayed that will allow users to either ID/Password or PIV/PIN
4. The SSOi Service will automatically log you in to the application

If you are prompted to enter your user credentials, enter your username and password. **DO NOT** enter the domain name in the Username field.

VA Identity and Access Management System (IAM)

Select Login Methods to access /CentralLogin/VIC/redirect.asp

User ID and Password Authentication	HSPD-12 PIV Card Authentication	Windows Authentication
<p>Please enter your VA Active Directory User ID and Password below then click Login</p> <p>User ID <input type="text"/></p> <p>Password <input type="password"/></p> <p>Login </p>	<p>If you are a VA employee, you may use any approved HSPD-12 PIV Card to log into IAM. Please insert your VA PIV card into your card reader and click Login</p> <p>Login</p> <p></p>	<p>This option allows users to use their current Windows session to authenticate to their application. Click Login to seamlessly authenticate.</p> <p>Note: This option can only be used if you are logged onto a VA issued computer.</p> <p>Login</p>

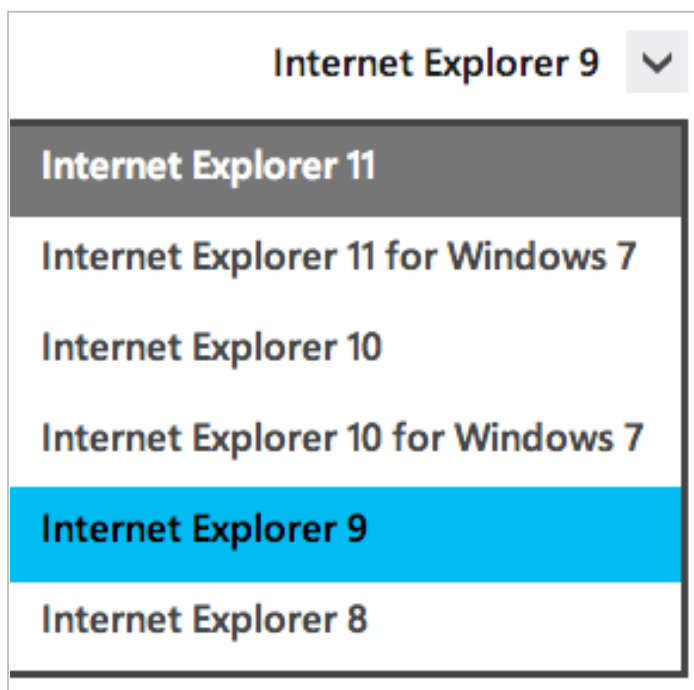
If you get redirected to the VA Home page, please contact your VHIC Supervisor and request to be provisioned to the VHIC application.

Please do not use the 'Refresh' button at the top of your browser window if you mistype the VHIC URL. The 'Refresh' button will redirect you to the VA website. Please re-enter the VHIC URL and try again.

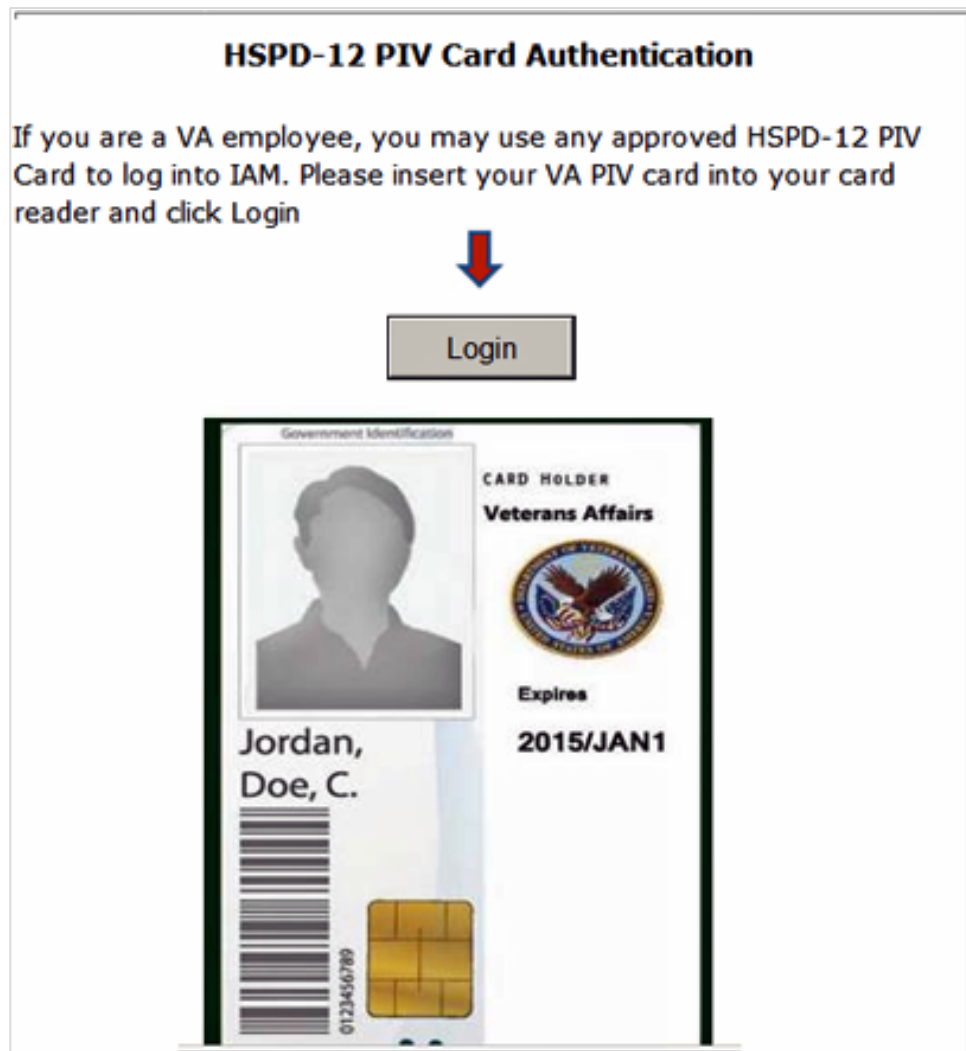
After successfully signing onto VHIC, it is recommended that you add the VHIC URL to your Favorites using the instructions provided at the link below, which are for Internet Explorer 9:

<http://windows.microsoft.com/en-us/internet-explorer/add-view-organize-favorites#ie=ie-9>

Click on drop-down arrow to view instructions for other IE versions:



1. PIV Card Login for Step-Up Authentication



- ☐ This is the process through which you log on to sensitive applications using PIV card integration with the SSOi Service.
- ☐ This function allows you to provide a higher level of credentials for sensitive applications, such as administrative functions, if you have logged in to the desktop with lower-level credentials.

This section demonstrates the **step-by-step process** for using the PIV-SSOi service:

1. You are already logged on to the desktop using your username and password.
2. Insert a PIV card into the card reader.
3. Navigate to the URL for the SSOi Service integrated application.
4. SSOi centralized page will be displayed that will allow users to enter either ID/Password or PIV/PIN.
5. Click on Logon button in HSPD – 12 PIV CARD Authentication section.
6. Enter PIN number.
7. After you enter your correct PIN, you gain access to the application.

Password Change: Every 90 days the application will prompt you to change your password.

Additional SSOi Information can be found in Appendix E.

9 Creating a Veteran Health Identification Card (VHIC)


This section will walk the VHIC user through the process of creating a card for a Veteran.

The VHIC application provides context-sensitive help to assist the user throughout the issuance of the card request.

Please click on the question mark to invoke the context-sensitive help.



Please see the context-sensitive help example below:

Card Status	Pending
Card	
No Br	
	<p>The military branch of service information is retrieved from the ES. If this information is not available in ES, the message "No Branch of Service is available" is displayed. If the Veteran would like BoS to be displayed on their card, their ES information must be updated. The missing military branch of service information does not prevent the user from proceeding with the card request.</p> <p><i>User Guide: Branch of Service (BoS)</i></p>
	<input type="button" value="Submit Card Request"/>

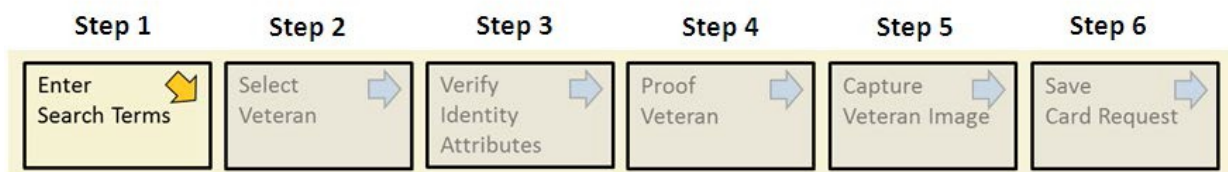
The first screen in VHIC is the “Home” screen. It contains two blocks, “Card Requests” and “Card Reports.” To begin the card request process, the VHIC user selects “Card Request” by clicking on the block. The user may also begin the card request process by clicking on the words “Card Request” in the upper left hand corner of the screen.



Card Request Navigation Bar

The card issuance process follows numbered Steps 1-6. Each step must be completed before you will be allowed to proceed to the next step.

Search for Veteran
Select Correct Veteran
Verify Identity Attributes
Proof Veteran
Capture Veteran Image
Save Card Request



Note: The appearance of the step block will change to indicate the step you are currently working by appearing to be the brightest. See the illustration below.



Card Request: Step 1 - Search for a Veteran

The first step in the card request process is to perform a probabilistic search for the Veteran in Master Veteran Index (MVI) database. See Appendix A – MVI Probabilistic Search for more details.

Search Guidelines and Notes:

When searching for a Veteran the following rules apply:

- Include the full last name in all searches.
- Enter the entire field value. For example, the whole first name as presented must be entered and not just the first initial.
- Wildcards (such as “*”) are not allowed in the search.
- If the SSN is used as a search trait, you must enter it as nine digits with no punctuation.
- Enter a minimum of three search traits.

- f. The full Veteran name is considered one search trait.
- g. The Veteran address is considered one search trait. If the address is used as a search trait, provide the Street address, City, State and Zip.

It is highly recommended to use as much data as is available to ensure optimum results are achieved. Matching success is dependent on what traits are provided.

The recommended search traits combinations:

- ☐ Full Veteran
Name SSN
DOB
Gender
- ☐ Full Veteran
Name SSN
Address

After the information has been entered into the required fields, the user may click on the Search button in the lower right hand corner of the box containing the search criteria.

Step 1 Enter Search Terms → **Step 2** Select Veteran → **Step 3** Verify Identity Attributes → **Step 4** Proof Veteran → **Step 5** Capture Veteran Image → **Step 6** Save Card Request

Veteran Search Criteria

Name

* Last Name: DEFOSSE
First Name: SAUL
Middle Name: WALLACE

Person

Date of Birth: 19281202 (DOB format YYYYMMDD)
Gender: Male
Home Phone:

Address

Street Address:
City:
State:
Zip Code:

Identification

SSN: 019234339 (format: #####-####)

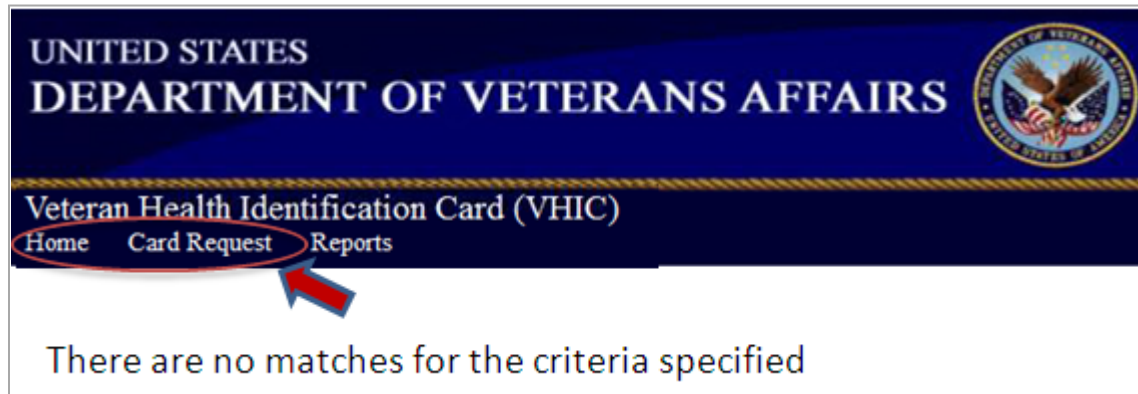
Clear Search

*For optimal results, Last Name, First Name, DOB and SSN are all required. At a minimum, please supply the Veteran's Last Name, plus values from at least two of the other three sections (Person, Address, Identification)

If the Veteran is not found in the MVI database, the following message is returned:

“There are no matches for the criteria specified”.

If this occurs, the user will not be able to proceed with the card request. To resolve: The user should verify the Veteran is indeed enrolled, then return to Step 1 Enter Search Terms to begin another search. If the Veteran is not enrolled, the user must redirect the individual to go through the registration process.



Card Request: Step 2 – Select Veteran

If the search was successful and a possible match is found in the system, the Step 2 – “Select Veteran” screen is displayed

Step 2, “Select Veteran” block at the top of the screen is now active and appears the brightest. All other blocks remain dimmed.

The screen displays the possible Veteran matches based on the information the user entered in the Step 1, “Enter Search Terms” screen. If the Veteran already has a VHIC the Veteran’s photo is included in the search results.

It is very important to select or identify the correct Veteran record.

If you are **NOT** certain that the Veteran before you and the Veteran, whose information is displayed on the screen are the same, click on ‘Veteran Not Listed’ button. You will be redirected to the Search/Home Page.

Step 1
Enter
Search Terms

Step 2
Select
Veteran

Step 3
Verify Identity
Attributes

Step 4
Proof
Veteran

Step 5
Capture
Veteran Image

Step 6
Save
Card Request

Picture	Full Name	SSN	DOB	Gender
Veteran Image	ROY, ROBERT	XXX-XX-6200	1/15/1954	MALE
<div><div>?</div><div>Veteran Not Listed</div></div>				

If you **ARE certain** that the Veteran before you and the Veteran, whose information is displayed on the screen are the same, click on the hyperlinked Veteran Full Name to advance to the next step.

Clicking the hyperlinked Veteran Full Name results in a behind-the-scenes query to the MVI service to populate all information for the selected Veteran.

Picture	Full Name	SSN	DOB	Gender
Veteran Image	ROY, ROBERT	XXX-XX-6200	1/15/1954	MALE

? Veteran Not Listed

If the selected Veteran is not eligible for a VHIC, the screen will display the following message: "The Veteran is not eligible for a VHIC." The user cannot proceed with the card request.

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

Veteran Health Identification Card (VHIC)

Home Card Request Reports

The Veteran is not eligible for a VHIC

Note: Please allow up to 2 days for the eligibility status change to be reflected in VHIC. Please inform the Veteran.

The VHIC user may either select **Home** or **Card Request** in the upper left hand corner of the screen to begin another search.

Card Request: Step 3 – Verify Identity Attributes

Step 3, “Verify Identity Attributes” block at the top of the screen is brightened. All other blocks remain dimmed. The purpose of this screen is to compare system data to identification documents presented by the Veteran.

The screen displays the information retrieved from the Master Veteran Index (MVI) and the Enrollment System (ES) for the selected Veteran. Take this opportunity to check and make sure Veterans have the identification documents in their possession that are required for the proofing process.

If the user discovers that the Veteran does not have the documents needed to complete the proofing process or the information displayed on the screen does not match the information on the identification documents, the user should click the “No” button in the lower right hand corner of the Veteran Identity Confirmation box.

The user will be returned to the Step 1 screen. The user should advise Veterans to update their identity and/or address before the card request process can be completed.

If the information on the screen is a correct match, the user selects “Yes” in the lower right hand corner of the Veteran Identify Confirmation box to advance.

Step 1 Enter Search Terms

Step 2 Select Veteran

Step 3 Verify Identity Attributes

Step 4 Proof Veteran

Step 5 Capture Veteran Image

Step 6 Save Card Request

Veteran Identity Confirmation

First Name SONNY

Last Name DAY

Street 123 HAPPY TRAILS

City CITYVILLE

State VA

Zip Code 23606

Date of Birth 8/19/1946

Does the veteran's information as displayed on the screen match the information on the identification documents presented by the veteran?

No Yes

If the information displayed on the screen is **WRONG** or **MISSING** the user cannot proceed with the card request and must select “No” in the lower right hand corner of the Veteran Identify Confirmation box to advance.

Note: Please allow up to 2 days for the address changes made in ES to be reflected in VHIC. Please inform the Veteran.

If a Level 2 proofing record exists for the Veteran, the application displays the Veteran / Card Details screen to initiate photo capture. Please refer to step 6 – Capture Veteran Image.

If a Level 1 proofing record exists, then the VHIC system redirects the VHIC user to the Identity Proofing system to retrieve the Veteran’s existing Level 1 proofing record for upgrade to Level 2.

If no proofing record for the Veteran is found, the VHIC system redirects the VHIC user to the Identity Proofing system to proof the Veteran.

Card Request: Step 4 – Proof Veteran

Step 4 – Proof Veteran block at the top of the screen is now active and appears the brightest. All other blocks remain dimmed. The Identify Proofing Portal box is displayed on the screen. Follow the instructions on the screen.

Proofing Process

The Veteran must present certain documentation in order to request a VHIC. This documentation consists of a primary and secondary identification credential as well as proof of current address postmarked within the past 30 days.

As depicted below, the proofing process proceeds along the following path:

- ☐ User Profile
- ☐ Address Verification
- ☐ Primary Identification
- ☐ Secondary Identification
- ☐ Submit Proof



The proofing process follows numbered Steps 1-5. Each step must be completed before you are allowed to proceed to the next step.

Note: The appearance of the step blocks change to indicate the step you are currently working by appearing to be the brightest.

Proofing Process: Step 1 - User Profile

The first step in the Veteran proofing process is to verify the information in the User Profile screen.

The User Profile screen is pre-populated with the data the VHIC user reviewed earlier except the 'Phone Number' field. If the Veteran's phone number is available, it can be entered in the Phone Number field.

The 'Proofing Location' that is pre-populated should match the location where the Veteran is being proofed. If the Proofing Location does not match the user's location or is not pre-populated, the VHIC user must to populate the '**Proofing Location**'. Click the arrow to the right of the field, and then select a location from the drop-down list. Once the information is verified by the VHIC User, the user selects the "Next" button, located in the lower right hand corner of the screen, to continue.

If the VHIC User selects the 'Cancel' button, the process will be stopped and the user will be redirected to the VHIC Home/Search screen.

Step 1 **Step 2** **Step 3** **Step 4** **Step 5**

User Profile Address Verification Primary Identification Secondary Identification Submit Proof

VHIC Identity Proofing (Step 1): User Profile

* - Required

** - Enter the first few characters of a proofing station number in the proofing station filter to shorten the number of proofing stations listed. Please note that special characters and regular expressions are not supported by the filter.

* First Name KENNETH

* Last Name FERGUSON

* Date of Birth Month 03 Day 21 Year 1963

Phone Number

* Street Address 33 SULLEY CIRCLE

* City ARCADIA

* State CA

* Country USA

* Postal Code 91077

* Affiliation Veteran

** Proofing Station # Filter (Not Required)

* Proofing Location 508: ATLANTA VAMC

Back Next Cancel

Proofing Process: Step 2 - Address Verification

Step 2, “Address Verification” block at the top of the screen is now active and appears the brightest. All other blocks remain dimmed.

The screenshot shows a web interface for the 'Address Verification' step. At the top, there are five step indicators: Step 1 (User Profile), Step 2 (Address Verification, highlighted with a yellow star), Step 3 (Primary Identification), Step 4 (Secondary Identification), and Step 5 (Submit Proof). Below the indicators, a legend states '* = Required'. The main form area contains the following fields: 'Address Validation Type' (a dropdown menu with a red arrow pointing to it), 'Postmark Date' (with sub-fields for Month, Day, and Year, and a checkbox for 'N/A'), 'Street Address', 'City', 'State', 'Country', and 'Postal Code'. On the right side, there is a label 'Person being proofed:'. At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a red circle and a red arrow pointing down to it), and 'Cancel'.

The purpose of this screen is to verify the Veteran’s current address. The information pre-populated on the screen must match the Veteran’s current address.

If a Veteran is getting a replacement card and his current address does not match the information displayed on the screen, the card request process stops. The Veteran’s ES record must be updated before a card request can be re-initiated.

1. Click the dropdown arrow to the right of **Address Validation Type** for a list of document types a Veteran may use for address verification.

Veterans are allowed to use the following documents/artifacts to validate their address (Appendix C):

- Primary ID
- Secondary ID
- Phone bill
- Electric bill
- Fossil fuel (oil, gas, propane) bill
- Credit card statement
- Checking/Savings account statement
- Local personal property tax bill
- Mortgage/Rent payment voucher
- VBA corporate data

2. The VHIC User must then inspect the document or artifact presented by the Veteran and confirm that the address on the artifact matches the address on the screen. If the Veteran is using any document other than the Primary/Secondary ID for Address Verification, the document provided must be postmarked within the **last 30 days** to be valid.

Note: The check box labeled '**N/A**', located next to the '**Postmark Date**' field, should only be checked when a Veteran uses an unexpired Primary or Secondary ID.

3. The VHIC user inspects the document presented by the Veteran to ensure that the document type is listed in the drop-down list.
4. Once the address information is verified as being correct, the user clicks on "Next" in lower right hand corner of the screen to proceed.

Step 1 User Profile Step 2 Address Verification Step 3 Primary Identification Step 4 Secondary Identification Step 5 Submit Proof

* = Required

Person being proofed: ELDON ONISHEA

* Address Validation Type: Electric bill from a local electrical service provider

Postmark Date: Month 07 Day 11 Year 2013 ☐ N/A

Street Address: 5243 W 11TH ST

City: GREELEY

State: CO

Country: USA

Postal Code: 80634

Back Next Cancel

Proofing Process: Step 3 – Primary Identification

Step 3, “Primary Identification” block at the top of the screen is brightened. All other blocks remain dimmed.

The screenshot shows a web interface for the proofing process. At the top, there are five steps: Step 1 User Profile, Step 2 Address Verification, Step 3 Primary Identification, Step 4 Secondary Identification, and Step 5 Submit Proof. Step 3 is highlighted with a red circle and a yellow arrow. Below the steps, there is a form with several required fields marked with an asterisk (*). The fields are: ID Type (a dropdown menu with a red arrow pointing to it), Country of Issuance (a dropdown menu), State of Issuance (a dropdown menu), Identification Number (a text input field), Expiration Date (Month, Day, and Year dropdown menus, followed by a checkbox for N/A), and Information Provided/Verified By (a dropdown menu). At the bottom right, there are three buttons: Back, Next (circled in red with a red arrow pointing to it), and Cancel.

The VHIC user inspects the documents presented by the Veteran to ensure that the documents can be used for identity verification purpose. The document type must be listed in the **ID Type** drop-down list. **The expired documents cannot be used for proofing purpose.**

The following lists the identity documents that are acceptable for the purpose of in-person identity proofing with the Primary ID.

Primary Identification Documents (Appendix B)

(Must be a government issued Photo ID)

- State-Issued Driver's license
- U.S. Passport or U.S. Passport Card (unexpired)
- Foreign passport with Form I-94 or Form I-94A (unexpired)
- U.S. Military card
- Military dependent's ID card
- U.S. Coast Guard Merchant Mariner Card
- Foreign passport that contains a temporary I-551 stamp
- Permanent Resident Card or Alien Registration Receipt Card (Form I-551)
- Federal, state, or local government issued ID card with a photograph
- Employment Authorization Document that contains a photograph (Form I-766)
- Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A
- School ID with photograph

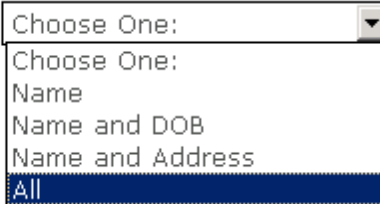
***For persons under age 18 who are unable to present a document listed above:**

- School record or report card, clinic, doctor, or hospital record
1. Click the dropdown arrow to the right of **ID Type** to display the list of document verification options that the Veteran may use.
 2. Click the dropdown arrow to the right of **State Issuance** to display the list of State abbreviations.
 - Select the appropriate two-letter State abbreviation for documents issued by a state.
 3. The VHIC user enters information from primary identity proofing document. All fields on this screen are required.

Note: The check box labeled '**N/A**' should stay unchecked unless the Primary identity proofing document doesn't have an expiration date.

4. The Information Provided/Verified By is the information provided by the Veteran being proofed.

* **Information Provided/Verified By**



The image shows a dropdown menu with the following options: 'Choose One:', 'Name', 'Name and DOB', 'Name and Address', and 'All'. The 'All' option is currently selected and highlighted in blue.

5. The VHIC User selects one of the four options, which corresponds to what the identification physically conveys.

For Example,

- ☐ Name (*Name Only: SSN Card*)
- ☐ Name and DOB (*Name & DOB: Birth Certificate, Passport**)
- ☐ Name and Address (*Voter registration, Utility Bill or Other appendix E document*)
- ☐ All (*Name, DOB and Address: Passport*, State Issued DL*)

*US Passport instructs holder to pencil in address. This may be only valid for the Name and DOB.

6. Once all fields are completed, the VHIC user clicks "Next "in the lower right hand corner of the screen to proceed.

* = Required

Person being proofed:

* ID Type

* Country of Issuance

* State of Issuance

* Identification Number

* Expiration Date Month Day Year ☐ N/A

* Information Provided/Verified By

Back Next Cancel

7. Click Next

Proofing Process: Step 4 - Secondary Identification

Step 4, "Secondary Identification" block at the top of the screen is brightened. All other blocks remain dimmed.

1. The VHIC user enters information from secondary identity proofing document. All fields on this screen are required.

Note: See step-by-step instructions in Step 3 Primary Identification. The check box labeled '**N/A**' should stay unchecked unless the Secondary identity proofing document doesn't have an expiration date, such as Social Security.

The following lists the identity documents that are acceptable for the purpose of in-person identity proofing with a Secondary ID.

Note: An artifact from the Primary ID list can be used to fulfill the Secondary ID requirement.

Secondary Identification Documents (Appendix B)

(Non-Picture ID and/or Acceptable Picture ID not issued by Federal or State government)

- Social Security Card
- Original or certified Birth Certificate
- Certification of Birth Abroad Issued by the Department of State (Form FS-545)
- Certification of Report of Birth issued by the Department of State (Form DS-1350)
- Voter's Registration Card
- Native American Tribal Document
- U.S. Citizen ID Card (Form I-197)
- Identification Card for Use of Resident Citizen in the United States (Form I-179)
- Employment Authorization document issued by the Department of Homeland Security
- Canadian Driver's License

Once all fields are completed, the VHIC user clicks on the “**Next**” button in the lower right hand corner of the screen to proceed.

* = Required

Person being proofed: BFSTCDCOKRP BLSTCDCOKRP

* ID Type: Military ID Card

* Country of Issuance: UNITED STATES

* State of Issuance: LA

* Identification Number: 26756765765

Expiration Date: Month [] Day [] Year [] ☒ N/A

* Information Provided/Verified By: Name and Address

Back Next Cancel

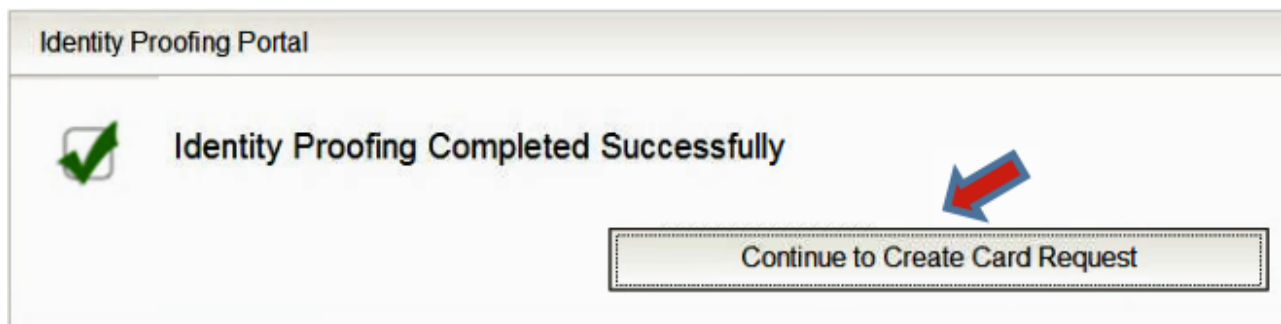
8. The VHIC User selects one of the four options, which corresponds to what the identification physically conveys.

For Example,

- ☐ Name (*Name Only: SSN Card*)
- ☐ Name and DOB (*Name & DOB: Birth Certificate, Passport**)
- ☐ Name and Address (*Voter registration, Utility Bill or Other appendix E document*)
- ☐ All (*Name, DOB and Address: Passport*, State Issued DL*)

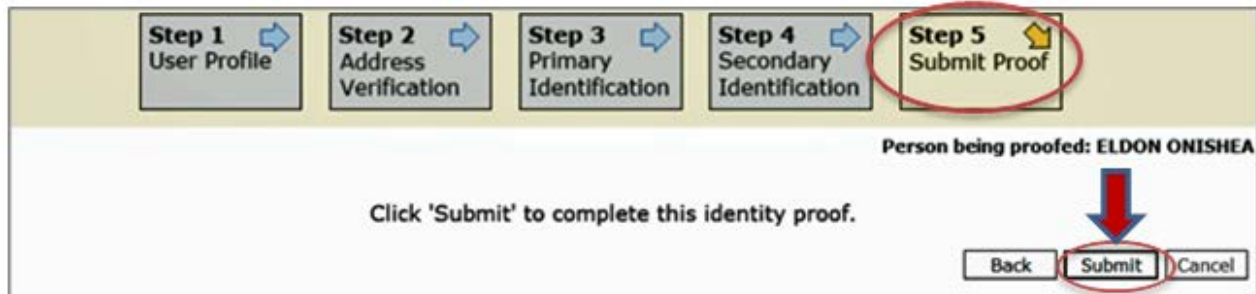
*US Passport instructs holder to pencil in address. This may be only valid for the Name and DOB.

The message “Proofing has been completed successfully” will be displayed. The user has to click on “Continue to Create Card Request” to return to the VHIC application and continue with the card request.



Proofing Process: Step 5 – Submit Proof

Step 5, “Submit Proof” block at the top of the screen is brightened. All other blocks remain dimmed.



Step 1 User Profile Step 2 Address Verification Step 3 Primary Identification Step 4 Secondary Identification Step 5 Submit Proof

Person being proofed: ELDON ONISHEA

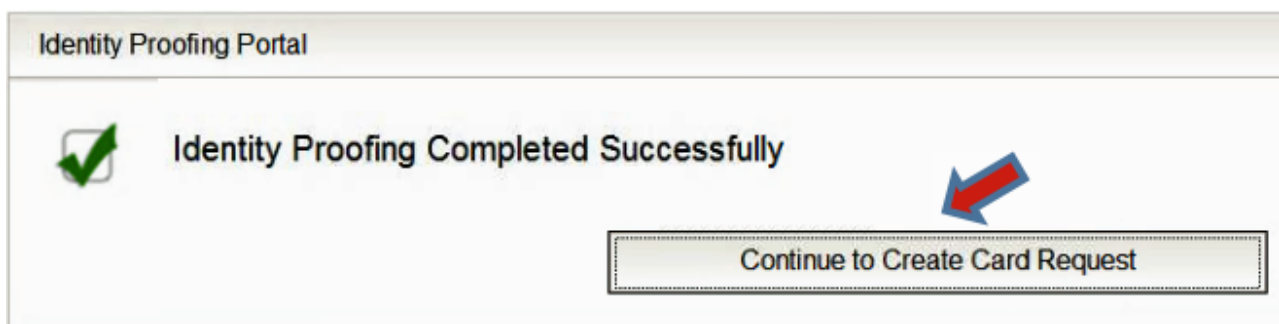
Click 'Submit' to complete this identity proof.

Back Submit Cancel

To continue, click on Submit.

User clicks on the “Submit” button in the lower right hand corner of the screen to proceed.

If the proofing process is successful, the screen will display the following message, **“Proofing Complete”**. The system will advance automatically to the next screen in the proofing process, which tells the user that the proofing was successful. The user clicks on the “Continue to Create Card Request” bar, and then the screen indicates, “Identify Proofing Completed Successfully” to proceed.



Identity Proofing Portal

Identity Proofing Completed Successfully

Continue to Create Card Request

Card Request: Step 5 - Capture Veteran Image

Step 5, “Capture Veteran Image” block at the top of the screen is brightened. All other blocks remain dimmed.

Capture Veteran Image

Be sure the location is bright and without glare. If the lights are too dim, you may need an extra lamp for additional lighting.

Before taking a photo, please review the guidelines below to ensure that the Veteran photo meets all the requirements:

- Face must be straight forward
- No closed eyes
- No dark glasses (can't see eyes)
- Tinted glasses OK (can see eyes)
- Not more than one face in image
- No open mouth
- Face cannot touch edge of photo (hair can, but not face)

Position the Veteran so that his/her image is within the outlined image area shown on the screen. Once the Veteran is positioned correctly within frame, click “Capture”.

Note: Please refer to the Appendix G for instructions how to set up Adobe Flash Player.

Veteran Health Identification Card (VHIC)
Home Card Request Reports Logged in as: VHAI5WKEY

Step 1 Enter Search Terms Step 2 Select Veteran Step 3 Verify Identity Attributes Step 4 Proof Veteran Step 5 Capture Veteran Image Step 6 Save Card Request

VA U.S. Department of Veterans Affairs

Barcode

Face must be straight forward
No closed eyes
No dark glasses (cannot see eyes)
Tinted glasses OK (can see eyes)
Not more than one face in image
No open mouth
Face cannot touch edge of photo (hair can, but not face)

Capture

To finalize the image capture process, click "Accept".

To retake the image click "Reset".

Veteran Health Identification Card (VHIC)
Home Card Request Reports Logged in as: VHAISWKEY

Step 1 Enter Search Terms Step 2 Select Veteran Step 3 Verify Identity Attributes Step 4 Proof Veteran Step 5 Capture Veteran Image Step 6 Save Card Request

VA U.S. Department of Veterans Affairs

U.S. Department of Veterans Affairs

Reset Accept

- Face must be straight forward
- No closed eyes
- No dark glasses (cannot see eyes)
- Tinted glasses OK (can see eyes)
- Not more than one face in image
- No open mouth
- Face cannot touch edge of photo (hair can, but not face)


Branch of Service (BOS)

The military branch of service the Veteran served can be populated on the face of the card.



The military branch of service information is retrieved from the ES. If this information is not available in ES, the message “No Branch of Service is available” will be displayed on the screen.

Veteran Card Details

	Card Number	
	EDIPI	2013070902
	VISN	7
	Facility	508
	Date of Birth	3/25/1948
ASHLEY WECK 23551 AVENIDA LA CAZA UNIT 132 COTO DE CAZA, CA 92679 USA	Card Status	Pending
	Card Request Date	07/15/2013 15:22
	No Branch of Service is available	
	<input type="button" value="Submit Card Request"/>	

The Veteran's ES record must be updated before the military branch of service can be printed on the face of the card.

The missing military branch of service information does not prevent the user from proceeding with the card request.

The Veteran has the option to decline displaying the military branch of service on the VHIC card.

If the Veteran declines display of the branch of service on the face of the card the VHIC User selects “Veteran Declines Branch of Service Logo” and proceeds with the card request.

Veteran Card Details

Card Preview: SAUL WALLACE DEFOSSÉ
236 TIMBER WAY
MONROE, LA 71203 USA

Card Information:
Card Number: 2013070903
EDIPI: 7
VISN: OHIO: DAYTON
Date of Birth: 12/2/1928

Card Status: Pending
Card Request Date: 07/15/2013 13:03

Branch of Service:
☐ Army
☒ Veteran Declines Branch of Service Logo

Submit Card Request

If multiple BOS are available the VHIC User has to verify with the Veteran, which branch of service should be displayed on the face of the card.

The user selects the branch of service specified by the Veteran and proceeds with the card request.

Veteran Card Details

Card Preview: STERLING L. SORRELL
14164 LAKEPOINT DR
WILLIS, TX 77318 USA

Card Information:
Card Number: 5441
EDIPI: 2013070905
VISN: 7
Facility: 508
Date of Birth: 12/8/1913

Card Status: Pending
Card Request Date: 07/22/2013 16:01

Branch of Service:
☒ Air Force
☐ Army
☐ Veteran Declines Branch of Service Logo

Submit Card Request

Card Request: Step 6 - Save Card Request

Step 6, “Save Card Request” block at the top of the screen is brightened. All other blocks remain dimmed.

On the “Veteran Card Details screen, the VHIC user has an opportunity to verify that the picture is acceptable and that all pertinent information correctly appears on the card.

Once the VHIC user is satisfied with the card’s completeness and accuracy, click “Submit Card Request” button in the lower right hand corner of the screen to complete the card issuance process. Note: The *Card Status/Card Request Date* area is now green and a *Card Number* generated.

The screenshot displays the 'Veteran Card Details' interface. On the left, there is a preview of the Veteran Health Identification Card (VHIC) for Ashley Weck, including the VA logo, a placeholder for the 'Veteran Photo', a barcode, and the address: 23551 AVENIDA LA CAZA UNIT 132, COTO DE CAZA, CA 92679 USA. To the right of the preview, a table lists the card details:

Card Number	2013070902
EDIP	
VSN	7
Facility	508
Date of Birth	3/25/1948

Below this table, a green box highlights the 'Card Status' as 'Pending' and the 'Card Request Date' as '07/15/2013 15:22'. A large red arrow points down to a 'Submit Card Request' button located in the bottom right corner of the screen.

The system will indicate the request has been sent successfully. The Veteran can expect to receive the VHIC in 7-10 business days at the verified address.

Upon clicking the button labeled “**OK**” on the message pop-up window, the system will return to the Search/Home Page.

10. Reporting Capabilities

This section provides general instructions for generating the reports.

The first screen in VHIC is the “Home” screen. It contains two blocks, “Card Requests” and “Reports.” To create a report, the VHIC User selects “Reports” by clicking on the block.



Report Page

The report page provides access to all reports available in the VHIC application. The VHIC user selects the desired report by clicking on the appropriate tab. The selected report tab is highlighted in blue.

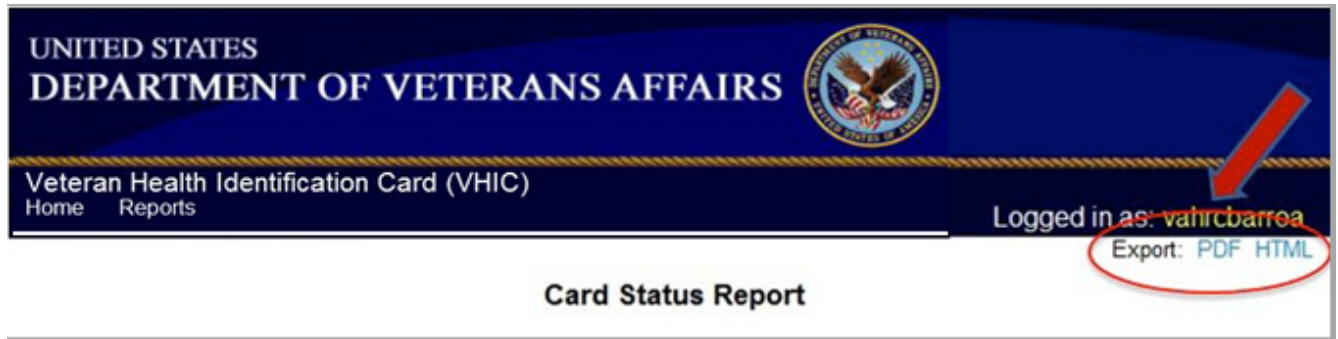
Click on the 'Card' or 'Print Services' tab to display additional reports.



Once the report type has been selected, the user can provide additional search criteria. The additional search criteria may differ from one report to another.

- ☐ Electronic Data Exchange Person Identification (EDIPI) is a unique number assigned to a record in the United States Department of Defense's Defense Enrollment and Eligibility Reporting System (DEERS) database.
- ☐ Integration Control number (ICN) is a unique identifier assigned to patients when they are added to the Master Veteran Index (MVI).
- ☐ CARD ID is the unique identifier assigned to a card request. Each Veteran may have one or more of these.
- ☐ PERSON ID is the unique auto-generated identifier assigned to a Veteran record. There will only be one of these for each Veteran.
- ☐ Veterans Integrated Service Network (VISN) is a network of hospitals that include clinics and nursing homes.
- Site is the VA Facility where the card was requested
- Workstation is the IP address of the VHIC user workstation.

All reports can be exported in HTML and PDF format.



- ☐ The report in HTML format is displayed in the browser and provides a printer-friendly version of the report.
- ☐ The report in PDF format can be saved on your computer or printed out. The PDF format is a printer-friendly format.

Veteran/Direct Record Search

The user can select the Veteran report by clicking on the 'Veteran' tab.

To perform a direct record search of the VHIC database, the VHIC user has to enter either the Veteran's: *Last Name, ICN, EDIPI, Card ID or Person ID*, and then click the "Query" button.



The screenshot shows a web application interface for searching the VHIC database. At the top, there are four tabs: 'Veteran', 'Card', 'Print Services', and 'Auditing'. The 'Veteran' tab is currently selected, indicated by a red arrow pointing to it. Below the tabs, there is a form with several input fields: 'Last Name', 'First Name', 'DOB' (with a calendar icon), 'Last 4 of SSN', 'ICN', 'EDIPI', 'Card ID', and 'Person ID'. A 'Query' button is located at the bottom right of the form.

The Veteran report will be displayed. See a sample report below.

Click on Veteran's Name or ICN to view Veteran demographic information and card request status.

Veteran Search Results										
Name	Date of Birth	ICN	EDIPI	Service Connected	POW	PH	MH	VHA Enrolled	#CardRequests	#CardsMailed
HARRISON J CHOCHREK JR	07/26/1925	1008532446V876394	2013070901	Y	U	U	N	Y	1	1

Veteran Report

Full Name	Date of Birth	Date of Death	ICN	EDIPI
HARRISON J CHOCHREK JR	07/26/1925		1008532446V876394	2013070901

Service Connected	Prisoner of War	Purple Heart	Medal of Honor	VHA Enrolled
Y	Unknown	Unknown	Not a recipient.	Y

Card Number	Card Status	Print Release Status	Total Card Requests
5435	Processing	Mailed	1

Permanent Address			
1003 GOTHAM DRIVE			
SAINT JAMES		NY	11780

Address Start Date	Address End Date
12/23/2013	

Veteran Photo



Person ID
22356
Last Update
12/23/2013
Updated By
vaausiam-victest31
Member Benefit Plan



The Veteran Report provides an easy way to track the card request status. Please see the table below for more details.

If the card status is mailed and the Veteran has not received the card, you may verify if the Veteran address is valid at the URL below:

<https://tools.usps.com/go/ZipLookupAction!input.action>

If the U.S. Postal Service cannot deliver the card, it is returned to the requesting facility.

Card Status	Print Release Status	Veteran will receive the card in (days)	Comments
Processing	Printing	5-7	Request entered, waiting to be sent to print site.
Processing	Sent	5-7	Request sent to print site.
Processing	Received	5-7	Request received by print site.
Active	Mailed	3-5	Card mailed to Veteran and ready for use.

Veteran Report				
Full Name	Date of Birth	Date of Death	ICN	EDIPI
HARRISON J CHOCHREK JR	07/26/1925		1008532446V876394	2013070901
Service Connected	Prisoner of War	Purple Heart	Medal of Honor	VHA Enrolled
Y	Unknown	Unknown	Not a recipient.	Y
Card Number	Card Status	Print Release Status	Total Card Requests	
5435	Processing 	Mailed 	1	

Card Request Totals Report

The user can select the Card Request Totals report by clicking on the “Card” tab, and then on “Request Totals” tab.

Once the report type has been selected, the user can specify the report criteria by selecting VISN and/or Site. The desired date range for the report can be specified through entry of *Start Date* and *End Date* in the fields provided.

Once the desired report criteria are provided, the user will click on “Query” button to create a report. The system will display the report.

The screenshot displays the Veteran Health Identification Card (VHIC) system interface. At the top, there is a navigation bar with tabs for "Home", "Card Request", and "Reports". Below this, a secondary navigation bar contains tabs for "Veteran", "Card", "Print Services", and "Auditing". The "Card" tab is selected. Under the "Card" tab, there are four sub-tabs: "Request Totals", "Status", "Multiple Requests", and "History". The "Request Totals" sub-tab is selected. The main area of the interface contains the following fields and controls:

- VISN:** A dropdown menu with a downward arrow.
- Site:** A dropdown menu with a downward arrow.
- Start Date:** A text field containing "10/1/2013" and a calendar icon.
- End Date:** A text field containing "11/5/2013" and a calendar icon.
- Query Button:** A button labeled "Query" is located at the bottom right, circled in red. A large blue arrow points down towards it.

Card Status Report

The user can select the Card Status report by clicking on the “Card” tab, and then on “Status” tab.

Once the report type has been selected, the user can specify the report criteria by selecting VISN/Site.

The desired date range for the report can be specified through entry of *Start Date* and *End Date* in the fields provided. Once the desired report criteria are provided, the user will click on “Query” button to create a report.

Note: National report option is only available to VHIC Administrator/VHIC Technical Administrator Tier 3

When selecting Print Release Status, there will be nine Release Statuses to choose from, please see the table below for details.

Status Code/Reason Code Description:

Release Status	Release Status Description
Cancelled	Request is cancelled
Error	Request error: data integrity
Hold	Request is on-hold
Ineligible	Request ineligible for card; phone and data stored.
Mailed	Request processed, card has been mailed
Printing	Card Print Site prints the card
Received	Request has been received by Card Print Site
Rejected	Request rejected by Card Print Site
Sent	Request has been sent to Card Print Site

The Card Status report is provided for four card request statuses listed below. No selection is required.

Status	Status Description
Active	The card is active
Inactive	The card is deactivated
Processing	The Print Facility is processing the card request.
Request	The card is sent to the Print Facility

The screenshot shows the 'Veteran Health Identification Card (VHIC)' system interface. At the top, there are navigation tabs: 'Home', 'Card Request', and 'Reports'. Below these, there are sub-tabs: 'Veteran', 'Card', 'Print Services', and 'Auditing'. Under the 'Card' tab, there are further sub-tabs: 'Request Totals', 'Status', 'Multiple Requests', and 'History'. The 'Status' sub-tab is selected. Below the sub-tabs, there are input fields for 'National' (checkbox), 'VISN' (dropdown), and 'Facility' (dropdown). There are also radio buttons for 'Card Status' (selected) and 'Print Release Status'. Below these are date pickers for 'Start Date' (10/1/2013) and 'End Date' (11/5/2013). A large blue arrow points down to a 'Query' button, which is circled in red.

Note: Depending on your browser, the Print Release Status report selection box may be still visible when the Card Status report is selected. The selection made in this box will be ignored, and the Card Status report will be created. The system will display the report. See a sample report below

Card Status Report							
VISN	VISN #	Facility	Facility #	# Active	# Inactive	# Processing	# Requested
VA Southeast Network	7	Atlanta (Decatur)	508	0	1	8	0

Multiple Requests Report

The user can select the Multiple Card Requests report by clicking on the “Card”, and then on the “Multiple Requests” tab.

This report provides information on cards that have been requested on more than one occasion for the same Veteran.

Once the report type has been selected, the user can specify the report criteria by selecting National/VISN/Facility and Cards Requested or Cards Mailed. The desired date range for the report can be specified through entry of *Start Date* and *End Date* in the fields provided.

The user can also specify the maximum of Card Requests to search for. The results returned will be equal to or greater than the maximum of Card Requests entered.

Once the desired report criteria are provided, the user will click on “Query” button to create a report.

The screenshot shows the Veteran Health Identification Card (VHIC) system interface. At the top, there is a navigation bar with links for Home, Card Request, and Reports. The user is logged in as 'User'. Below the navigation bar, there are tabs for Veteran, Card, Print Services, and Auditing. The 'Card' tab is selected. Under the 'Card' tab, there are sub-tabs for Request Totals, Status, Multiple Requests, and History. The 'Multiple Requests' sub-tab is selected. The main form area contains the following fields and controls:

- Card Requests: A text input field with the value '2'.
- VISN: A dropdown menu.
- Facility: A dropdown menu.
- Radio buttons for 'Cards Requested' (selected) and 'Cards Mailed'.
- Start Date: A date input field with the value '12/1/2013' and a calendar icon.
- End Date: A date input field with the value '1/30/2014' and a calendar icon.
- A large blue arrow pointing down to a 'Query' button, which is circled in red.

The system will display the report. See a sample report below.

Multiple Card Requests Report			
VISN	VISN #	# Veterans	Cards Requested
VA Southeast Network	7	1	3

Card History

The user can select the Card History report by clicking on the 'Card History' tab. Once the report type has been selected, the user can specify the report criteria by entering Card and/or Person ID. The Person ID is the unique auto-generated identifier assigned to a Veteran record. There will only be one of these for each Veteran. Once the desired report criteria are provided, the user will click on "Query" button to create a report.

The screenshot shows the 'Veteran Health Identification Card (VHIC)' system interface. At the top, there are navigation tabs: 'Home', 'Card Request', and 'Reports'. Below these, there are sub-tabs: 'Veteran', 'Card', 'Print Services', and 'Auditing'. The 'Card' tab is selected. Under the 'Card' tab, there are four buttons: 'Request Totals', 'Status', 'Multiple Requests', and 'History'. The 'History' button is highlighted. Below these buttons, there are two input fields: 'Card ID' and 'Person ID'. To the right of these fields is a large blue arrow pointing down to a button labeled 'Query', which is circled in red.

The system will display the report. See a sample report below.

Card History Report									Export:
Card ID	Person ID	VISN	VHIC Station IP Address	Request Date	Issuer	Card Status Code	Print Release Code	Reason Code	
5494	22395	7	10.234.203.178	07/22/2013	vhaiswcustom	P	P	4	
5494	22395	7	10.234.203.178	07/22/2013	vhaiswcustom	P	S	4	

Status Code/Reason Code Description:

Status Code	Status Code Description
R	Request
P	Processing
A	Active
I	Inactive

Reason Code	Reason Code Description
1	Lost or Damaged
2	Being Misused
3	Expired
4	Replaced

Note: Please refer to the table on p. 53 for Print Release Code description.

VHIC Card History Report in PDF Format:

VHIC Card History

Veteran ID: ANY Card ID: 5434

Veteran: **HARRISON J CHOCHREK** Person ID: **22355**

Gender	DOB	Service	POW	Purple Hrt.	Med.	VHA	Cntr
M	07/26/1925	Y	U	U	N	Y	1

Card ID: **5434**

Veteran Photo

Card Issuer	Card Type	Manufacturer	Last Changed Date	Last Changed By		
vaausiam-victest31	PLAIN	PLAIN				
Issue Date	VISN	Site	VHIC Station IP Address	Current Status	Current Reason	Current Print Release
11/06/2013	7	508	10.234.200.209	P	4	P

Status	Prt Release	Batch	Message	Status Change Date	Changed By
P	P		New Request	11/06/13 01:12:11	vaausiam-victest31

Auditing

The Auditing Report provides information on all user's activity in the system. The report can be used for fraud detection and prevention or for tracking the user's activities. The Auditing report tracks the user activities listed below.

User Activity	Activity Description
MVI_SEARCH	A search is performed on the MVI webservice for the parameters provided.
MVI_GETIDS	A search is performed on the MVI webservice for the various identification numbers stored in that system for the
ESR_GETSUMMARY	A search is performed on the ESR webservice that provides information relating to the veteran specified.
PROOFING_WS	A search is performed on the Proofing webservice that provides proofing information on the veteran specified.
CARD REQUEST	A new record is created in the tbl_person_card table for the person_id specified in vet_id and the person_card_id specified in card_id.
PERSON CREATED	A new record is created in the tbl_person table with the person_id specified in vet_id.
rptCardCounts	The card count report is run with the parameters provided.
rptCardStatuses	The Card Status report is run with the parameters specified.
rptPersonMultiples	The Person Multiples report is run with the parameters specified.
rptPerson	The Veteran Report is run with the parameters specified.
rptCardHistory	The Card History Report is run with the parameters specified.
rptAuditing	The Auditing Report is run with the parameters specified.

The user can select the Auditing report by clicking on the 'Auditing' tab. Once the report type has been selected, the user can specify the report criteria by entering Login and providing the desired date range through entry of *Start Date* and *End Date*. Once the desired report criteria are provided, the user will click on "Query" button to create a report.

Veteran Health Identification Card (VHIC)
 Home Card Request Reports

Veteran Card Print Services **Auditing**

Login
 Start Date
 End Date

Auditing Report
Export: [PDF](#)

Previous
1-20 of 119
Next 20

Date Time	Login	Action	Person ID	EDIPI	Card ID	Query String
12/20/2013 02:18:06	vaausiam-victest31	MVI_SEARCH				lastName=WECK, DOB=19480325, SSN=037314148, firstName=ASHLEY
12/20/2013 02:18:22	vaausiam-victest31	MVI_GETIDS				icn=1008532456V343881
12/20/2013 02:18:27	vaausiam-victest31	ESR_GETSUMMARY				vpid=0000001008532456V343881000000
12/20/2013 02:18:42	vaausiam-victest31	PROOFING_WS				cspid=null, fname=ASHLEY, lname=WECK, dob=03/25/1948, postalAddress=23551 AVENIDA LA CAZA UNIT 132, city=COTO DE CAZA, state=CA, country=USA, postalCode=92679
12/20/2013 02:20:32	VAAUSIAM-VICTEST31	PERSON CREATED	22355	2013070902		
12/20/2013 02:20:32	vaausiam-victest31	CARD REQUEST	22355	2013070902	5434	

11. Getting Help

If you need assistance with the **VHIC Application** the VA National Help Desk is your first point of contact. The VA National Help Desk is available 24/7, although after-hours calls must be 'high priority' calls if assistance cannot wait until next day. You can reach the Help Desk by calling 1-888-596-4357.

If you need assistance with accessing VHIC application or provisioning VHIC users (**SSOi or Provisioning services**) please contact the AcS Help Desk.

The AcS Help Desk solution is integrated with the National Help Desk (NSD) in Philadelphia. The VA Service Desk Manager (SDM) solution is used to record and assign tickets. AcS has stood up a Tier 2 Help Desk with designated hours of operation (M-F; 8AM-5PM EST), a toll free telephone number, and Email address to offer limited support of all AcS services. The following contact information for the AcS Help Desk is provided:

Internal AcS Help Desk:

Tier 1- NSD (855) 673-4357, Option 4; NSDTUSCALOOSAUSD@va.gov

Additional SDM Information can be found in Appendix F.

APPENDIX A: MVI Probabilistic Search

The VA has upgraded to an Enterprise Probabilistic matching algorithm from the former Deterministic (exact) matching. The change in matching algorithms was made because the probabilistic method allows for a greater chance of getting a correct match. For example, if a search supplies a first name of “Joe” instead of “Joseph,” the match might return both records, as both are probable matches. In Deterministic matching, only the “Joe” record would return (missing a possible “Joseph” match) as the values in a deterministic search must match exactly to what is in an existing record, or no match will be found. Probabilistic matching has a greater possibility of detecting potential matches and therefore helping prevent potential duplicate records being added to the system for a person who already exists.

Table 1 Identity Management Service Attended Search Criteria

			Identity Management Service Attended Search Criteria										
			Patient - Probabilistic - Attended (Search Threshold and Above)										
			Searches for the Provision of Healthcare										
			Scenario Number										
	Person Id Traits / Criteria	Max Score	1	2	3		4	5	6		7	8	9
1	Name	6.22											
a	First Name		X	X	X		X	X	X		X	X	X
b	Middle Name		X'	X'	X'		X'	X'	X'		X'	X'	X'
c	Last Name	3.95	R	R	R		R	R	R		R	R	R
2	Social Security Number (SSN)	5.77	X				X	X	X				
3	Date Of Birth (DOB)	4.01					X				X	X	X
4	Gender	0.25	X	X	X						X		
5	Home Address (Street, City, St. , Zip)	4.10		X				X				X	
6	Home Phone				X				X				X
	Place of Birth (POB - City & State												
	Mother's Maiden Name (MMN)												
	Aggregate Score w/Exact Matches		12.24	10.57	10.57		16.00	16.09	16.09		10.48	14.33	14.33

Results	Persons returned from search based on the criteria supplied
R	Denotes required search criteria
X	Denotes required for optimized results
X'	Denotes recommended if available for optimized results
blank	Denotes optional search criteria
10.2	Search threshold / results below threshold will not be provided
10	Maximum number of results / None will be returned if results are more than 10

APPENDIX B: ACCEPTABLE IDENTITY DOCUMENTS

The following documents are designated as acceptable for the purpose of in-person identity proofing.

COLUMN A Government Issued Photo ID	COLUMN B Non-Picture ID and/or Acceptable Picture ID not issued by Federal or State Government
<ul style="list-style-type: none"> • Driver's license • U.S. Passport or U.S. Passport Card (unexpired) • Foreign passport with Form I-94 or Form I-94A (unexpired) • U.S. Military card • Military dependent's ID card • U.S. Coast Guard Merchant Mariner Card • Foreign passport that contains a temporary I-551 stamp • Permanent Resident Card or Alien Registration Receipt Card (Form I-551) • Federal, state, or local government issued ID card with a photograph • Employment Authorization Document that contains a photograph (Form I-766) • Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A • School ID with photograph <p>For persons under age 18 who are unable to present a document listed above:</p> <ul style="list-style-type: none"> • School record or report card • Clinic, doctor, or hospital record 	<ul style="list-style-type: none"> • Social Security Card • Original or certified Birth Certificate • Certification of Birth Abroad Issued by the Department of State (Form FS-545) • Certification of Report of Birth issued by the Department of State (Form DS-1350) • Voter's Registration Card • Native American Tribal Document • U.S. Citizen ID Card (Form I-197) • Identification Card for Use of Resident Citizen in the United States (Form I-179) • Employment Authorization document issued by the Department of Homeland Security • Canadian Driver's License

APPENDIX C: ADDRESS CONFIRMATION DOCUMENT CRITERIA

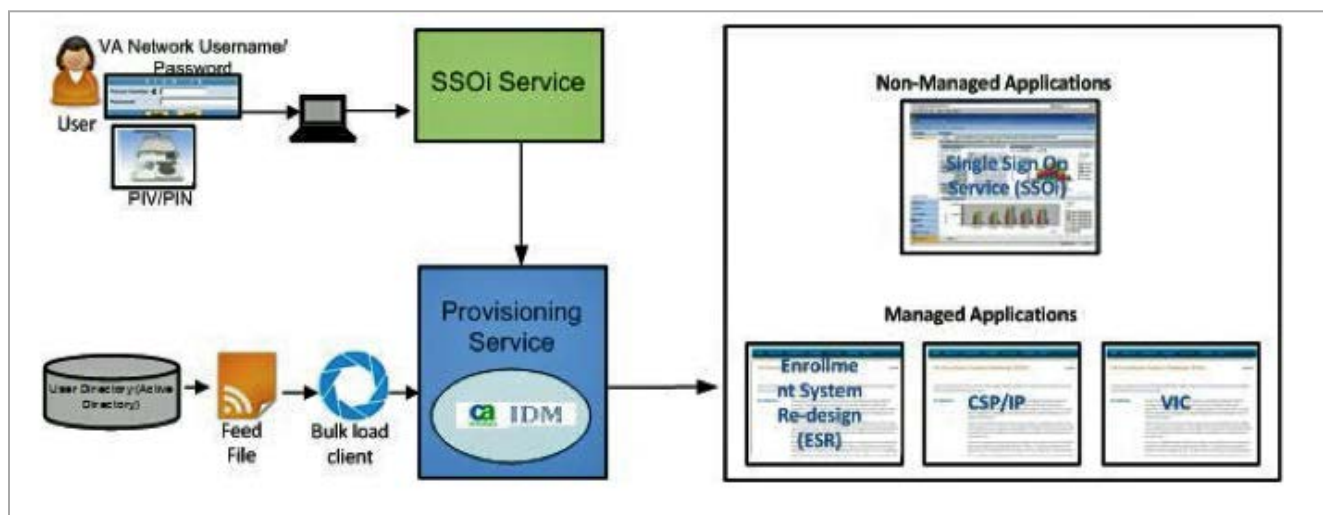
The following documents are designated as acceptable for identifying the current mailing address. The applicants name must be the addressee on the document, and the document must be dated within the last 30 days.

Acceptable Documents to Verify Mailing Addresses
<ol style="list-style-type: none">1. Primary Identification2. Secondary Identification3. Phone bill from local phone service provider4. Electric bill from a local electrical service provider5. Fossil fuel (oil, gas, propane) bill from a local service provider6. Credit card statement7. Checking or savings account statement8. Local personal property tax bill9. Mortgage or rent payment voucher10. Veterans Benefits Administration (VBA) corporate data reflecting correct mailing address as verified by applicant

APPENDIX D: PROVISIONING

The Provisioning Service provides an automated workflow process to provision user accounts.

It automates request, creation, termination, and modification of access rights across diverse connected applications. The access to the VHIC application is provided in the Provisioning system.



User Types within the Provisioning Service

- ☐ Privileged Users – Responsible for control and maintenance of the solution.
- ☐ User Administrators – Responsible for workflow approvals, delegation, running audit reports, and user access management.
- ☐ User – Capable of requesting and tracking access for integrated VA applications

Accessing the Provisioning Service

This is the process by which you access the Provisioning Service to provision a VHIC user.

1. Access the Provisioning Service through a browser using the following link:
<https://provapp.iam.va.gov/iam/im/prov/>.
2. Login to Provisioning Service using your existing VA credentials.

Steps to Provisioning a VHIC User

There are two steps* that be completed to enable a user to log into the VHIC application and complete the proofing process.

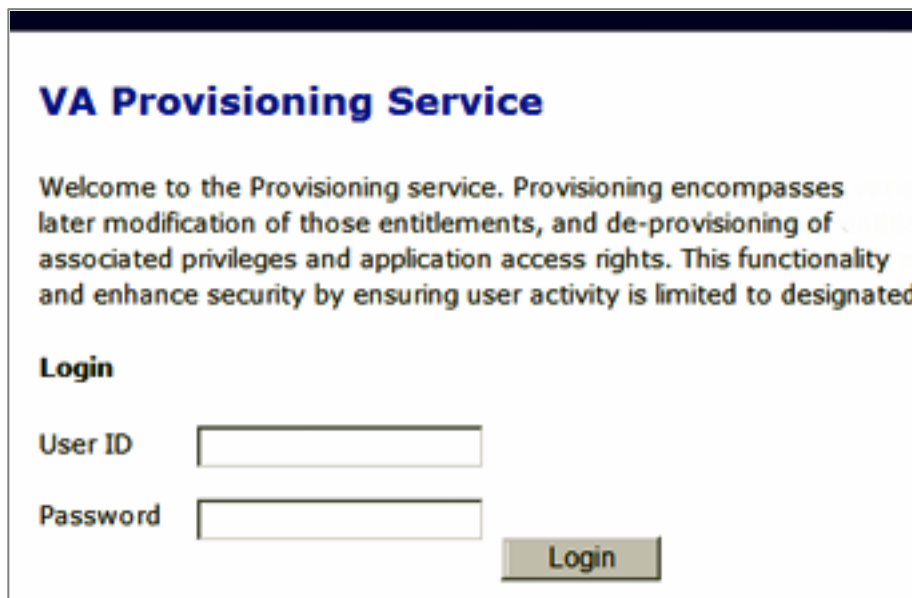
1. Provision User as VIC Identity Proofer
2. Provision User as VHIC User

* - These two steps apply only for those that need to ID Proof a Veteran. If their role does not require ID proofing a Veteran, then only step 2 applies for granting access.

These two steps are completed in the Provisioning Service and are detailed in the following sections.

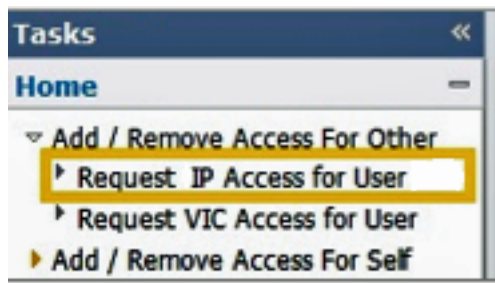
Provision User as VIC Identity Proofer

1. Login to Provisioning Service
 - a) Log in to VA Provisioning Service
<https://provapp.iam.va.gov/iam/im/prov/>
 - b) Use your existing VA credentials to login.



The screenshot shows the 'VA Provisioning Service' login interface. At the top, the title 'VA Provisioning Service' is displayed in blue. Below it, a welcome message states: 'Welcome to the Provisioning service. Provisioning encompasses later modification of those entitlements, and de-provisioning of associated privileges and application access rights. This functionality and enhance security by ensuring user activity is limited to designated'. Under the heading 'Login', there are two input fields: 'User ID' and 'Password'. To the right of the 'Password' field is a 'Login' button.

2. Determine if the user already has the VIC Identity Proofer role.
 - a) Click on the little triangle that is *Add/Remove Access For Other (top left of the provisioning window)*
 - b) Select *Request IP Access for User*



- c) Search for the specified user you would like to add. You also have the option to search by first name or last name as well as User ID (the user's VA login ID).
- d) Input the necessary info and click on search (make sure you input the correct info for the right option you chose to search by)

- e) If you search by User ID, you should see the user returned and the radio button already selected.
- f) If you searched by any other means and have multiple results, you will want to select the proper user by clicking on the checkbox to the left of the correct person

Select	Last Name
<input checked="" type="radio"/>	yourUserID

3. Update User Profile

- a) Once you have found the right user, clicked the radio button, and clicked the **Select** button in the lower right corner of your screen
- b) You will now be taken to the IP Profile page allowing you to make sure that you have the correct person.
- c) Enter the *Justification*.
- d) Clicks Next, (bottom right of your screen) to either verify if the user is already setup. If the user is setup, the VIC Identity Proofer check box will be checked. If they are not setup, the check boxes will be unchecked.
- e) If they have the VIC Identity Proofer checked, then click **Cancel** and move to the next step for requesting VHIC access.

<input type="checkbox"/> Select	▲ Name
<input checked="" type="checkbox"/>	VIC Identity Proofer

Request CSP-IP Access for User: Profile

1 Profile

• = Required

User ID

First Name

Last Name

Email

Job Title

Employee Type

Office Location

Business Phone

• Justification

test

4. If a user does not have access to IP (as noted above, the below screen shot is what you will see. Please follow the below steps to provide a user with access to the IP Admin role and VIC Identity Proofer role.
 - a) Click on the **Add a provisioning role button**
 - b) This will take you to the screen to select the appropriate role. Simply hit **Search** (leaving just the asterisk (*)).
 - c) Click in the check-box *VIC Identity Proofer* role, and click **Select**

Name	Description	Comments	Department
No results.			

Click on the add button to search for CSP-IP roles for which you can request access.

[Add a provisioning role](#)

[Return to Search](#)

Select a IP Role

Search for a provisioning role

Search for a provisioning role

where

+

Name

▼

=

*

+

Search

Clear

Search Results

1-1 of 1

Select	▲ Name	▼ Description
<input type="checkbox"/>	VIC Identity Proofer	VIC person, authorized to perform in-person Identity proofing

1-1 of 1

Select

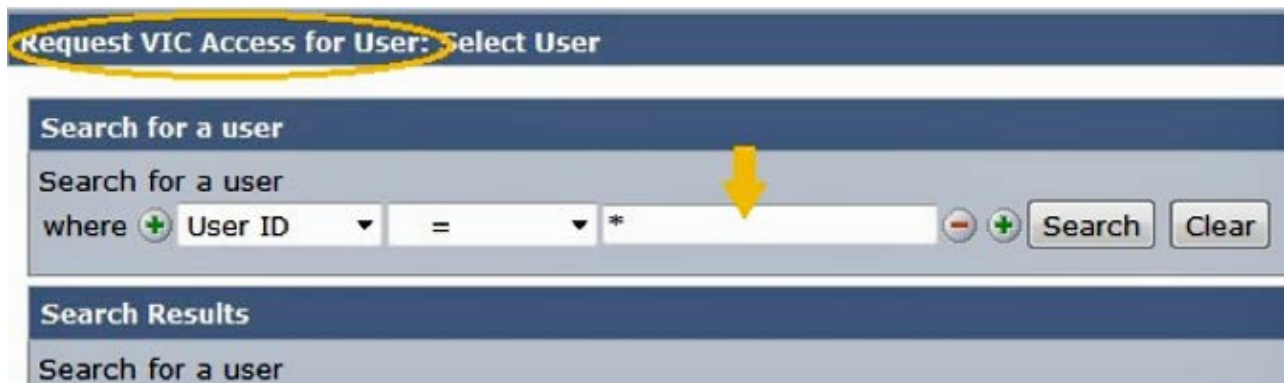
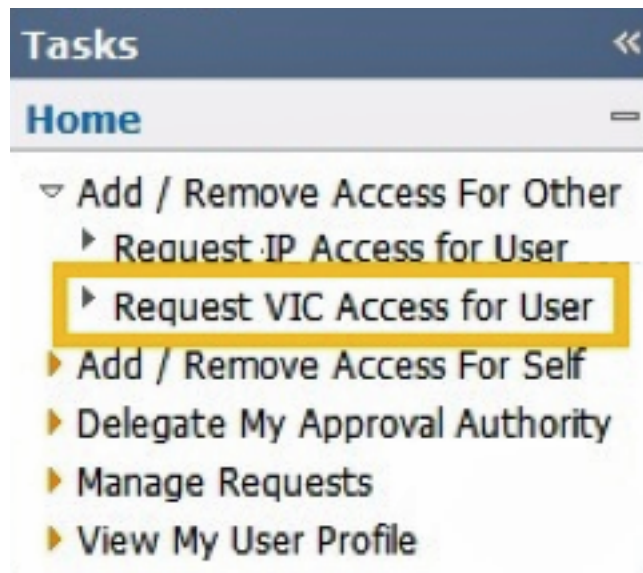
Cancel

FYI: Once you complete the above tasks this will require two approvals (from VHIC Program Approver and VHIC OI&T Approver), before the user's access can be finalized.

Provision User as VIC User

1. Set up the user's VIC Role.
 - a) Click on the *Add/Remove Access For Others*
 - b) Select *Request VIC Access for User* and search for them via User ID, first name, last name, or any combination.

- c) Once the correct user is located, click the **Select** button to continue on to set up the VIC user profile.



2. Fill in the User Profile screen
- a) At this point, the VA VIC Role, VA VIC Facility, and VA VISN must be selected.
- *NOTE: if the proper combination of Facility and VISN are not selected, this can trickle down and cause errors. They currently do not 'feed' off of each other.
- b) A note must be added in the *Justification* box.

Request VIC Access for User: Profile

1

Profile

• = Required

User ID

First Name

Last Name

Email

• VA VIC Role

• VA VIC Facility

• VA VISN

• Justification

c) Once complete, click on **Finish** (in the lower right hand corner of your screen)

You have now successfully “Provisioned” a user. There are a few approvals that need to occur prior to a user being able to access VHIC. So please recommend the user to wait for these emails, prior login to VHIC.

Role Modification by User (User and Privileged User)

User Types within the Provisioning Service

- a. After you have signed up for access using the Provisioning Service, you have the ability to update or modify the roles using the service.
- b. To modify a role, you must access the Provisioning Service and select roles within applications you want to add or remove.
- c. You may have various roles available to you depending on your duties.
- d. As your duties change, the need to change your role will arise.
- e. Requests are sent to provisioning Privileged Users for approval.

This section demonstrates the **step-by-step process** for requesting access to Provisioning applications:

1. Navigate to the IAM Provisioning Service using the SSOi Service or provisioning system link: <https://provapp.iam.va.gov/iam/im/prov/>.
2. Arrive at the End User Provisioning Service Home.
3. Click the **Add / Remove Access for Self** link for the appropriate application to be taken to the request page.
4. Arrive at the Search page, enter search criteria, and then click **Search**.
5. Find the appropriate role and select or clear its checkbox, and then click **Finish**.
6. Confirm the roles and finish the request.

User Role Modification – Screen Shots

1. Navigate to the Provisioning home page.
2. Click the link for the appropriate application to be taken to the request page
3. Ensure all of the required information is correct, and then click **Roles**.

Request CSPIP Access: Profile

1 Profile 2 Roles

• = Required

User ID

• First Name

• Last Name

Email

4. Enter search criteria and click **Search**.

Select Provisioning Role

Search for a provisioning role

Search for a provisioning role where =

Search Results

Search for a provisioning role

5. Find the appropriate role, select or clear the corresponding checkbox, and then click **Select**.

Search Results

1-1 of 1

Select	Name	Description	Comments	Department
<input type="checkbox"/>	CSP-IP Admin			

1-1 of 1

Select Cancel

6. Click **Finish**.

Please use this task for requesting access for only CSP-IP application.

<input checked="" type="checkbox"/> Member	Name	Description	Comments	Department
<input checked="" type="checkbox"/>	CSP-IP Admin			
<input checked="" type="checkbox"/>	ESR Administrator	ESR Administrator		
<input checked="" type="checkbox"/>	SSOi Admin	SSOi Admin		

Click on the add button to search for CSP-IP roles for which you can request access.

Add a provisioning role

No admin

Back Finish Cancel

View Submitted Tasks

This is the process by which you can view the tasks you have submitted through the Provisioning Service. After you submit a request, you can view that request as a submitted task. This function allows you to track your requests.

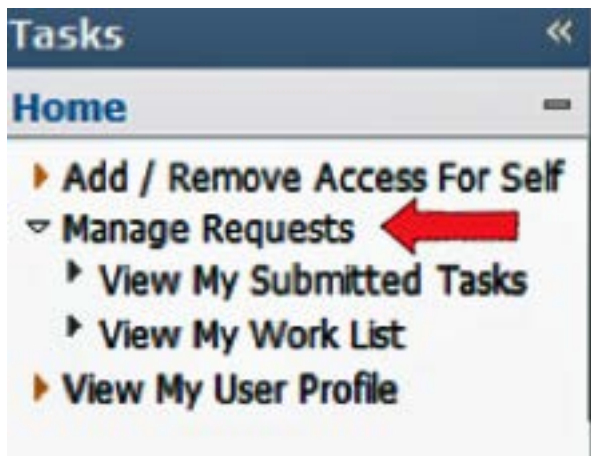
This section demonstrates the **step-by-step process** for viewing submitted tasks:

Navigate to the IAM Provisioning Service using the SSOi Service or provisioning system link: <https://provapp.iam.va.gov/iam/im/prov/>.

1. Arrive at the End or Privileged User Provisioning Service Home.
2. Click **Manage Requests** and then **View My Submitted Tasks**.
3. Select search criteria.
4. Click **Search**.

View Submitted Tasks – Screen Shots

1. Navigate to the Provisioning home page.
2. Arrive at the End or Privileged User Provisioning Service Home.
3. Click **View My Submitted Tasks**.



1. Select search criteria.
2. Click **Search**.

A screenshot of the 'View My Submitted Tasks' search interface. The interface is divided into two main sections. On the left is a sidebar with a 'Tasks' menu and a 'Home' link. The main section on the right is titled 'View My Submitted Tasks' and contains a search form. The search form has a title 'Search for submitted tasks:' and several search criteria options, each with a checkbox and a text input field. The criteria are: 'Approval tasks performed by' (with a 'Validate' button), 'Where task name equals' (with a dropdown menu), 'Where task status equals' (with a dropdown menu), 'Where task priority equals' (with a dropdown menu set to 'Low'), and 'Submitted between' (with two date input fields set to '7/2/13'). There are also checkboxes for 'Show unsubmitted tasks', 'Show approval tasks', and 'Search archive of submitted tasks'. At the bottom of the search form, there is a text input field for 'and return at most' (set to '1000') followed by the word 'rows'. A red arrow points to the 'Search' button at the bottom right of the search form.

View My Work List by Privileged User

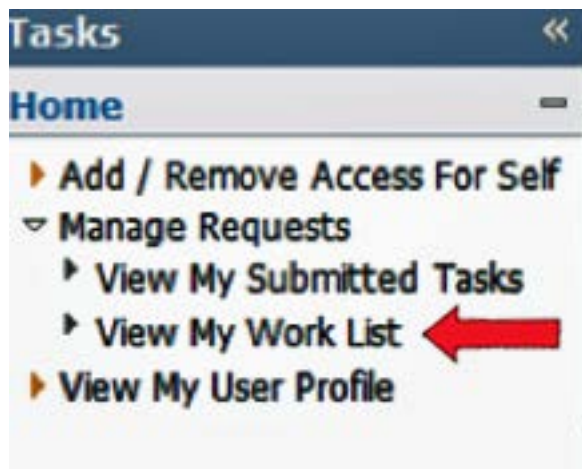
Provisioning Privileged Users receive many access requests from internal users. The View My Work List function displays all of these requests. This function helps provisioning Privileged Users organize and manage the requests they receive. Using this list, the provisioning Privileged User can accept or reject a user access request.

This section demonstrates the **step-by-step process** for viewing tasks:

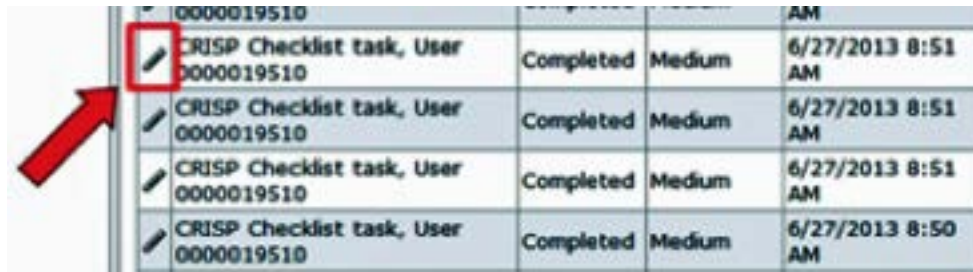
1. Navigate to the IAM Provisioning Service using the SSOi Service or provisioning system link: <https://provapp.iam.va.gov/iam/im/prov/>.
2. Arrive at the End User Provisioning Service Home.
3. Click **View My Work List**.
4. Click the pencil icon to view a task.
5. The Event Detail displays for the task.





View My Work List – Screen Shots

1. Navigate to the Provisioning home page.
2. Select **Manage Requests**.
3. Click **View My Work List**.



4. Click the pencil icon to view a task.



	CRISP Checklist task, User 0000019510	Completed	Medium	6/27/2013 8:51 AM
	CRISP Checklist task, User 0000019510	Completed	Medium	6/27/2013 8:51 AM
	CRISP Checklist task, User 0000019510	Completed	Medium	6/27/2013 8:51 AM
	CRISP Checklist task, User 0000019510	Completed	Medium	6/27/2013 8:50 AM

5. Task event details are displayed.

Delegate Approvals by Privileged User

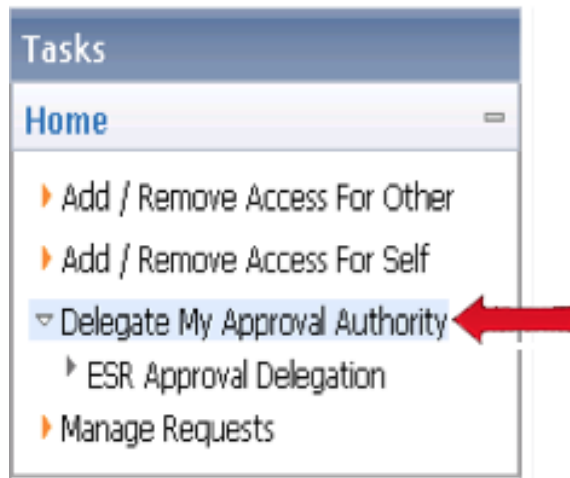
A provisioning Privileged User has the ability to delegate approval authority of provisioning requests to another user. You can delegate only to other provisioning Privileged Users identified as approvers. This feature helps the provisioning Privileged User delegate the approval authority while they are away.

This section demonstrates the step-by-step process for delegating approvals:

1. Navigate to the IAM Provisioning Service using the SSOi Service or provisioning system link: <https://provapp.iam.va.gov/iam/im/prov/>.
2. Arrive at the Provisioning Service Home.
3. Select **Approval Delegation** for the appropriate application.
4. Arrive at the user search page and enter search criteria, and then click **Select**.
5. Click a delegation Item.

Delegate Approvals – Screen Shots

1. Navigate to the Provisioning home page.
2. Arrive at the Provisioning Service Home.
3. Click Approval Delegation for the appropriate application.



4. Enter search criteria and click **Search**.



5. Click a delegation item.

Access Reports by Privileged User

- a. Provisioning Privileged Users have the ability to generate reports using the Compliance Audit and Reporting (CAR) tool.
- b. CAR reports allow Privileged Users to display information based on a defined time frame.

Knowledge Base Articles - Provisioning

Question	Answer
What are the available provisioning reports?	<p>Provisioning User Account Details – Provides user account details such as application access, approved roles, and permissions.</p> <p>Privileged User Account Details – Displays a list of Privileged Users.</p> <p>Provisioning Report – Displays accounts provisioned for an application.</p> <p>De-Provisioning Report - Displays accounts provisioned for an application.</p>
What is the role of the application Privileged User?	The Privileged User can manually provision or modify user accounts for non-managed accounts.
What is the role of the approver?	The approver can approve or deny provisioning requests for access creation, modification, or de-provisioning. They may also delegate alternate approvers for a defined period of time.
What is the role of the provisioning administrator?	The provisioning administrator performs administrator functions for the provisioning service, including systems configuration, workflow management, and so on.
What is the role of the provisioning user?	The provisioning user requests the creation or modification of an existing account to a managed or non-managed application integrated with the provisioning service.
What is a managed application?	A managed application is an application with which the provisioning service provides automated workflow and active connection to provision directly to endpoint applications.
What is a non-managed application?	A non-managed application is an application with which the provisioning service provides semi-automated workflow and does not connect directly to provision users to endpoint applications.
What if a user is unable to view their existing profile information and associated application roles?	Verify that the user has logged in with their own network credentials and that the provisioning service is running. Also make sure that the user is entitled for the application roles. If the issue persists, contact the National Service Desk.

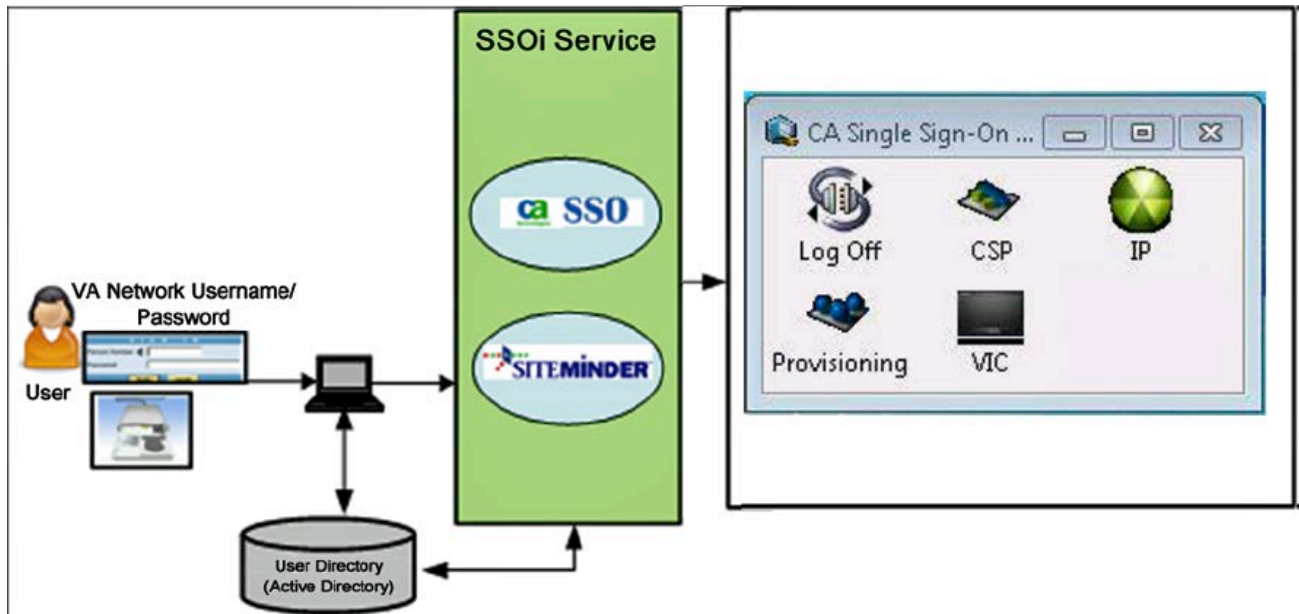
Question	Answer
How do you add users to approver groups so that they can be approvers for a given application?	The user should have rights to manage an approval group and should have a Groups tab. Using the Groups tab, they can search for the user and add them to the approval group. If the user is not entitled to manage approval groups, contact the National Service Desk.
How is the status of an application tracked?	View Submitted Task provides the status of a submitted request and where it is in the workflow (such as whether it is with an approver, whether it was rejected or approved, or whether there was a system failure).
What if the user is unable to see the request access link, delegation link, or reports link?	Verify whether the user has been entitled and provided the appropriate role to be able to see the tasks such as the Request Access link for an application, the Approval Delegation links, or the report links. Contact the National Service Desk to add the appropriate role to the user's profile in the provisioning system.

APPENDIX E: SSOi

AcS Single Sign On Internal (SSOi) Service

What is the AcS SSOi Service?

- ☐ It provides Single Sign On (SSO) capability to integrated applications.
- ☐ Upon your successful authentication to the VA desktop, SSOi seamlessly provides you access to a set of applications.



First-Time SSOi Service Access

- This is the process by which you log in to SSOi for the first time to access an integrated application.
- If you are initiating an integrated application session via the SSOi Service (applications integrated with Computer Associates (CA) SSO) for the first time, you will be prompted to enter application credentials. Your credentials are your username and password for each individual application that is integrated with SSO.
Note: If the application is CA SiteMinder enabled, you will not be prompted to enter application credentials the first time.
- It is necessary to enter application credentials for the first time so that they are stored and used for subsequent authentications to integrated applications via the SSOi Service.

How do you log on for the first time?

- You log on to the VA desktop using your Active Directory (AD) credentials or your PIV/PIN.
- Why are you asked to enter a username and password for an application?
- The SSOi Service (applications integrated with CA SSO) requires that you enter a username and password for an application the first time the application is accessed. This information is stored for subsequent authentications.

Are credentials saved after the first logon?

Credentials are stored at the first logon and will not be entered by you to access an application in the future until you change your passwords in the application.

This section demonstrates the step-by-step process for accessing the SSOi Service for the first time:

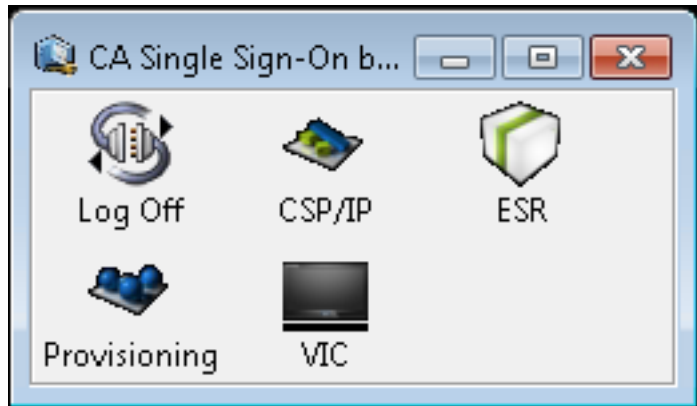
1. Log on to a VA desktop using Windows Active Directory (AD) credentials or a PIV Card and PIN authentication.
2. Open the SSOi Launch Bar by clicking: Start > All Programs > CA> Single Sign-On > Single Sign-On Launch Bar.
3. You will be presented with one or more icons representing the integrated applications to choose from.
4. Select your application from the launch bar.
5. When initiating the integrated application session via the SSOi Service (applications integrated with CA SSO) for the first time, you will be prompted to enter application credentials.
6. When the application password is changed for the applications integrated with CA SSO, you will be prompted to enter new application credentials.

Log Off Using the SSOi Service

- ☐ This is the process through which you log off all application sessions by selecting the **Log Off** icon from the SSOi Launch Bar.
- ☐ This function allows you to log off all applications without having to log off each one separately.

This section demonstrates the **step-by-step process** for logging off using the SSOi service:

1. Open the SSOi Launch Bar.
2. Double-click **Log Off**.
3. The SSOi Service logs you off all active sessions of integrated applications.
4. You are notified that logoff is complete after all applications have been logged off.
5. The SSOi Launch Bar will display the "Log On" icon only.
6. Double-click **Log Off** on the Launch Bar to log off the SSOi Service.



Note: SSOi logoff applies only to the applications that were launched via the SSOi

Access Reports

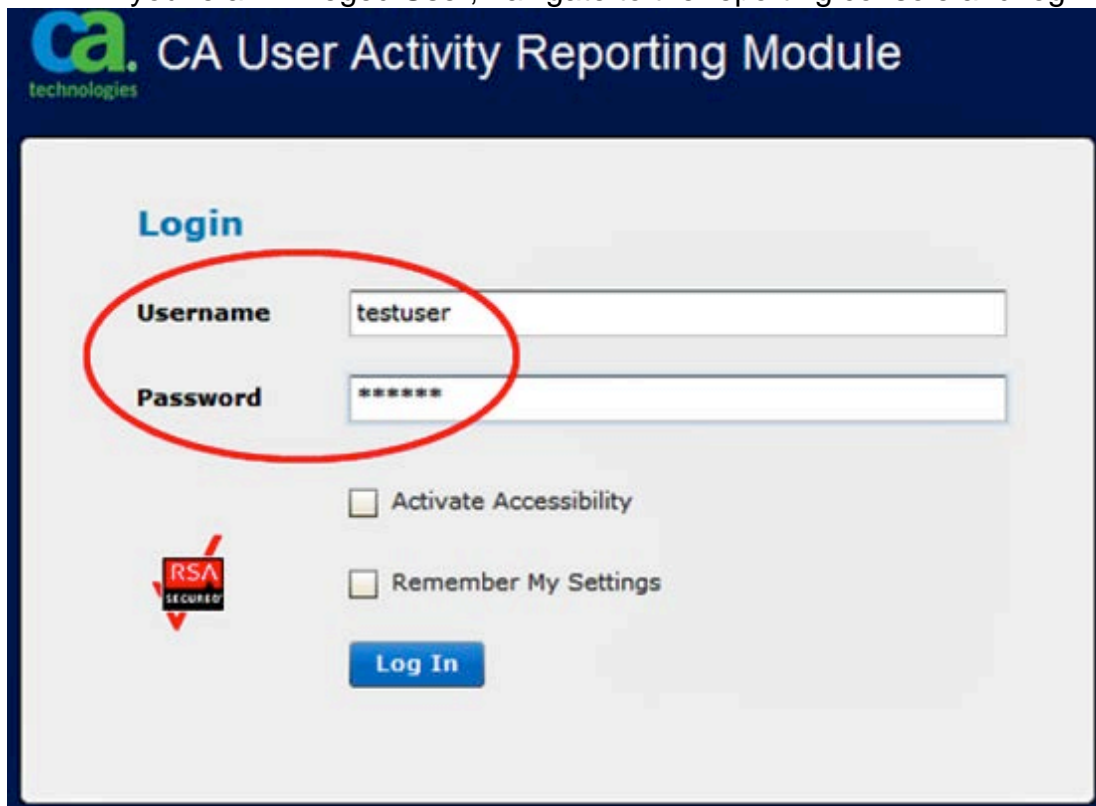
- ☐ SSOi Privileged Users have the ability to generate reports of SSOi-related activities for auditing purposes. A Privileged User is an administrator for utilizing and generating SSOi reports to conduct audits. The user must have a Compliance Audit Reporting (CAR) service account to gain access to the reporting interface.
- ☐ Reports allow Privileged Users to display information based on a defined time frame.

This section demonstrates the **step-by-step process** for accessing reports:

1. Navigate to the Reporting page.
2. Select the type of standard report to run from available options and define available parameters (time period, available attributes).
3. Submit the reporting request to the system.
4. The report is generated and displayed.

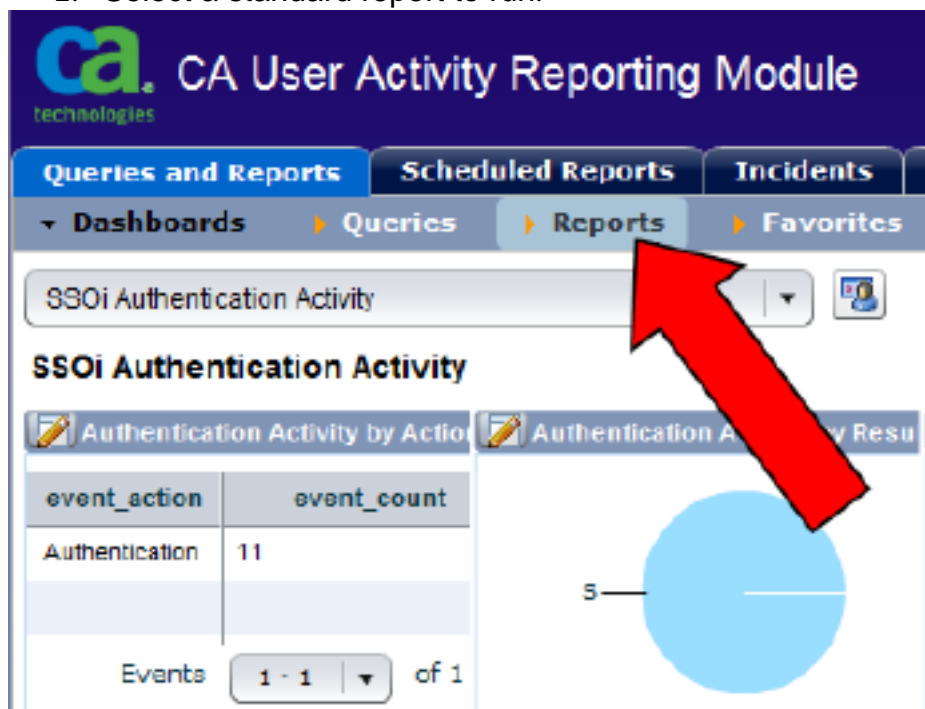
Access Reports – Screen Shots

1. If you're a Privileged User, navigate to the reporting console and log in.



The screenshot shows the login interface for the CA User Activity Reporting Module. The title bar includes the CA Technologies logo and the text "CA User Activity Reporting Module". Below the title, the word "Login" is displayed in blue. A red circle highlights the "Username" and "Password" input fields. The "Username" field contains the text "testuser", and the "Password" field contains six asterisks "*****". To the left of the password field is an "RSA SECURED" logo. Below the input fields are two checkboxes: "Activate Accessibility" and "Remember My Settings", both of which are unchecked. A blue "Log In" button is positioned at the bottom center of the login area.

2. Select a standard report to run.







The screenshot displays the "Reports" section of the CA User Activity Reporting Module. The top navigation bar includes tabs for "Queries and Reports", "Scheduled Reports", and "Incidents". Below this, a sub-navigation bar shows "Dashboards", "Queries", "Reports", and "Favorites". The "Reports" tab is selected, and a red arrow points to it. The main content area shows a dropdown menu with "SSOi Authentication Activity" selected. Below this, the title "SSOi Authentication Activity" is displayed. There are two report options: "Authentication Activity by Action" and "Authentication Activity by Result". The "Authentication Activity by Action" report is selected, showing a table with the following data:

event_action	event_count
Authentication	11

At the bottom of the table, it says "Events 1 - 1 of 1". To the right of the table is a pie chart with a single blue slice labeled "5".

3. Submit the reporting request to the system.
4. The report is generated and displayed.

Details				
<input type="checkbox"/> Show raw events		Match:	<input type="text"/>	<input type="button" value="GO"/>
CA Severity	Date	Performer	Action	Result
 Information	Mon May 20 2013 2:41:37 PM	vaausiam-acstest73	Authentication	S
 Information	Mon May 20 2013 2:40:13 PM	vaausiam-acstest73	Authentication	S
 Information	Mon May 20 2013 2:33:00 PM	vaausiam-acstest73	Authentication	S
 Information	Mon May 20 2013 1:38:17 PM	vaausiam-test9	Authentication	S

Knowledge Base Articles - SSOi

This information will assist you with the topics below.

Question	Answer
How do you log in via a PIV card?	You will be able to authenticate to your desktop using a PIV card. The SSOi application will use your desktop login without prompting you to re-enter credentials. Single sign on using a PIV card uses certificates stored on the smart card.
What types of users have access to reports?	Only Privileged Users for each of the applications have access to report functions using the CAR application.
What information is available for auditing purposes?	The reports provide Privileged Users information on your authentications as well as logon/logoff activities for the SSOi Service.
What if the SSOi Service does not accept an authentication when a valid PIV and PIN are entered?	You must first log in to your desktop with a valid PIV and PIN. If you are able to log in to the desktop, then you should be able to log in to SSOi without any issue unless the SSOi services are down.
What if the first time you log in to an application, you are not asked to enter your user ID and password?	You might have already set your password. The application has been using SiteMinder authentication. If the application is using SiteMinder as the authentication service, then you do not need to enter the user ID and password the first time.
What if every time you choose an application, you are asked to re-enter your user ID and password?	Contact the National Service Desk if the credentials are not being stored by the SSOi Service.
What if the Global Logoff feature is not closing all applications?	Contact the National Service Desk. The tcl script might not have been copied to your desktop.
What if an external user is unable to view the list of applications they can access via SSOi?	SSOi is for users internal to the VA network only.
What if, as a Privileged User, you are unable to run the standard reports?	Check with the National Service Desk to make sure you have been set up to access the CAR Service.
How do you access the SSOi Launch Bar?	Open the Launch Bar by performing the following steps: Click Start . Click All Programs . Click CA .

Question	Answer
	<p>Click Single Sign-On.</p> <p>Click Single Sign-On Launch Bar.</p> <p>The Launch Bar opens.</p>
How do you use your PIV to access an application?	<p>Insert your PIV.</p> <p>Go to the URL for the application.</p> <p>Enter your PIN for PIV when prompted.</p> <p>Note: You can use your PIV and PIN when:</p> <ul style="list-style-type: none"> Logging on to your VA computer, and/or Logging on to an SSOi-enabled application (using either the SSOi client or a browser)
What if the Log Off button is not available on the Launch Bar?	Contact the National Service Desk.
What if I don't see an icon I am authorized for?	Contact the National Service Desk.
What if you receive a message that you are not authenticated?	Contact the National Service Desk.

APPENDIX F: VA Service Desk Manager (SDM)

Provisioning/SSOi Common Tasks Help

Step by step instructions for common provisioning/SSOi tasks are available in VA Service Desk Manager (SDM).

1. Enter `http://vaww.nsd.va.gov/CAisd/pdmweb2.exe` in your browser

The screenshot shows the VA Service Desk Manager (SDM) web application. The header is dark blue with the 'CA Service Desk Manager' logo on the left and user information 'Kindschuh, Jeffrey' with a 'Log Out' link on the right. Below the header, there are two main columns. The left column has a 'Search for a Solution' section with a search bar and a 'Go' button, and a 'Top Solutions' section listing various tasks like 'SDM: How to Create/Modify Contact Records' and 'NT/Windows: Unlock/Reset password for multiple Domains'. The right column has a 'Customer Service' section with links to 'Create a new Request' and 'Service Desk contact information and hours of operation', and a 'Look up my existing tickets' section showing the user's status: 'You have 0 open requests', 'You have 1 closed requests', 'You have 0 open change orders', and 'You have 0 closed change orders'. Below this, there are input fields for 'A request number' and 'OR a change order number', each with a 'Go' button.

2. Enter "AcS: in search box



CA Service Desk Manager

Search for a Solution

Search for a solution using keywords:

[My Bookmarks](#)

[Submit Knowledge](#)

3. Click on



CA Service Desk Manager

Searched for **AcS** in all categories

[Click here to create a new Request](#)

View All	Expand All	Page 1 of 2	1-25 of 28
+	AcS CAR Report Scheduling		
+	VPN user is getting credentials cannot be verified and AcS log shows "External DB account disabled"		
+	VPN user is getting credentials cannot be verified and AcS log shows "External DB password expired" or "External DB user invalid or bad password"; windows password change failed		
+	VPN user is getting credentials cannot be verified and AcS log shows "External DB account locked out".		
+	AcS Access Provisioning Service, Modify a Role, View Submitted Tasks, Request Access for a User, and Privileged User Overview issues		
+	AcS CAR Standard Reporting		
+	AcS Access to CAR		
+	AcS User Activity Reporting Module (UARM) CAR Standard Reporting		
+	VPN: How to access AcS logs for troubleshooting VPN/CAG/RESCUE/One VA VPN access issues/logs.		
+	AcS CAR Managing Alerts		
+	AcS First time access and returning user access		
+	VPN user is getting credentials cannot be verified and AcS log shows "AcS user unknown".		
+	AcS SSODi Access Unable to Login		
+	AcS SSODi Password User ID Reset		
+	AcS Access Reports in CAR (Compliance Audit Reporting)		
+	AcS PIV Card Login for Step-Up Authentication		
+	AcS: Update Security Questions in Credential Service Provider (CSP) Identity Proofing (IP)		
+	AcS: Forgot User ID in Credential Service Provider (CSP) Identity Proofing (IP)		

4. Select job aid

APPENDIX G: Set up Adobe Flash Player

How to Bypass the Silhouette Overlay to Gain Access to the Adobe Flash Player Settings Panel

With the implementation of the mandatory silhouette usage during Step 5 of the VHIC Card Request process, there is a potential issue that may occur where the Adobe Flash Player Settings panel becomes inaccessible to the user wherein they cannot access the 'Allow' button preventing access to full camera functionality.

Step 1

The following steps demonstrate a work around that will allow the user to bypass this situation should the need arise.

If the following screen is presented to the user, they will need to follow these steps to bypass the silhouette and gain access to the Adobe Flash Player Settings panel:



Step 2

The user will need to click on the 'Capture' button located below the card image. This will remove the silhouette and allow access to the settings panel.

IMPORTANT: Rather than simply clicking on the 'Allow' button, the user will want to RIGHT CLICK on the 'Allow' button and then select Settings... from the available menu.



Step 3

Once on the Privacy tab of the Flash Player settings, the user should select 'Allow' and also select the 'Remember' box so that this check will not appear the next time the photo capture page is accessed.



Step 4

The user should then be presented with a simple white screen/square where the Veteran's image should appear. At this point, the user should click the 'Reset' button at the bottom of the card image, which will then bring the silhouette back up and allow the camera to kick in making the Veteran visible. The image can now be captured and the user can continue with the Card Request process.

Step 1 Enter Search Terms	Step 2 Select Veteran	Step 3 Verify Identity Attributes	Step 4 Proof Veteran	Step 5 Capture Veteran Image	Step 6 Save Card Request
----------------------------------------	------------------------------------	------------------------------------------------	-----------------------------------	-------------------------------------------	---------------------------------------

Face must be straight forward

Reset Accept

APPENDIX H: Guidelines for Scanning Barcode

Turn on the barcode reader and aim it at the center of the barcode ensuring the entire length of the barcode is within the lighted area. Wait for the reader to pick up the data. Many readers will also emit an audible beep. If necessary, vary the distance and angle between the reader and the barcode until the entire length of the barcode is illuminated. As shown in the images above, the red dot represents the center focal point of the scan and the lines represent the area being read. In the two incorrect examples of a failed scan, the center point is not within the area of the barcode, nor is the scanner reading all of the lines in the barcode and therefore cannot be read.

Examples of a Successful Scan:



Examples of a Failed Scan:

