

**Web Veteran's Health Information Systems and  
Technology Architecture Remote Access  
Management (WebVRAM)  
User Guide**



**March 2024**

**Department of Veterans Affairs**

**Office of Information and Technology**

## Revision History

Date	Document Revision	Description	Author
3/2/2024	10.0	Updated for Release 10.0. Angular and Bootstrap updates.	WebVRAM Project Team, VA OIT EPMO
12/14/2023	9.0	Updated for Release 9.0. Updated Section <a href="#">6.1.4. Other Errors</a> to reflect updated YourIT ticket interface.	WebVRAM Project Team, VA OIT EPMO
8/23/2023	8.1	Reviewed for patch WEBG*3*17 – No changes were required. This patch does not make any changes to GUI or user-facing components.	WebVRAM Project Team, VA OIT EPMO
8/23/2023	8.0	Release 8.0: Updated Month/date in cover page and footers	WebVRAM Project Team, VA OIT EPMO
3/16/2023	7.0	Updated Date on Cover page and Footers	WebVRAM Project Team, VA OIT EPMO
2/7/2023	7.0	Added <a href="#">Section 2.4</a> : System Maintenance	WebVRAM Project Team, VA OIT EPMO
12/20/2022	6.2	Release 6.2 changes: <ul style="list-style-type: none"> <li>• Updated date info on cover page</li> <li>• Updated date on footers area</li> <li>• Updated Screenshot for: <ul style="list-style-type: none"> <li>• Figure 8 - WebVRAM Home Screen</li> <li>• Figure 13 - Launch Reflection Button</li> <li>• Figure 23 – Launch CPRS button</li> <li>• Figure 28 – Launch CPRS Button</li> <li>• Figure 33 – Launch New VA EHR Button</li> <li>• Figure 35 – Launch Synchronize Button</li> <li>• Figure 36 – Launch Synchronize Successful</li> <li>• Figure 38 – My Profile Page</li> <li>• Figure 39 – My Business Unit and Admins Page</li> </ul> </li> </ul>	WebVRAM Project Team, VA OIT EPMO

10/05/2022	6.0	<p>Updates for WebVRAM Release 6.0:</p> <ul style="list-style-type: none"> <li>• Updated screenshot for Figure 7: WebVRAM Home Screen</li> <li>• Added Section <a href="#">5.3 User Profile</a></li> <li>• <a href="#">Added new images in section 5.3 User Profile</a></li> </ul>	WebVRAM Project Team, VA OIT EPMO
9/6/2022	5.0.2	<p>Updates for WebVRAM Release 5.0.2:</p> <p>Updated Screenshots for following:</p> <ul style="list-style-type: none"> <li>• Section 4, Figure 6, 6a: WebVRAM Login Screen</li> <li>• Section 5.1.17; added screenshot Figure 34a: Launch Synchronize Successful</li> </ul>	WebVRAM Project Team, VA OIT EPMO
7/20/2022	5.0	Updated instructions and screenshots in Section 5 and 5.1.2	WebVRAM Project Team, VA OIT EPMO
7/8/2022	5.0	Removed all references to Internet Explorer browser as it is no longer supported.	WebVRAM Project Team, VA OIT EPMO
6/24/2022	5.0	<p>Updated for WebVRAM Release 5.0,</p> <p>Added Section to Document IAM/PIV feature:</p> <p>4.2. IAM / PIV Login - Link PIV to your Home VistA site</p> <p>4.3.IAM / PIV Login – Login to WebVRAM with PIV Card</p> <p>Updated Section 5.1.2 to reflect new Launch CPRS workflow related to IAM/PIV feature, removed figure 25.</p>	WebVRAM Project Team, VA OIT EPMO

2/23/2022	4.1	Added Quick Start Section <a href="#">1</a> (Quick Start Guide).	WebVRAM Team, VA Office of Information and Technology (OIT) Development, Security, and Operations (DevSecOps) Software Product Management (SPM)
12/9/2021	4.0	<p>Updated for WebVRAM Release 4.0, (associated with informational VistA patch WEBG*3*5):</p> <ul style="list-style-type: none"> <li>• Updated Section <a href="#">2.5</a> (References and Resources) to replace "Rational" with "Jira."</li> <li>• Updated verbiage in Sections <a href="#">3.1</a> (System Summary), <a href="#">0</a> (Logging in to WebVRAM), and <a href="#">5.3</a> (Changing Verify Code) to add Microsoft Edge as a supported internet browser.</li> <li>• Replaced <a href="#">Figure 5</a> (WebVRAM High-level System Interfaces).</li> <li>• Replaced <a href="#">Figure 6</a> (WebVRAM High-level Application Design) and updated Alt Text.</li> <li>• Replaced <a href="#">Figure 7</a> (WebVRAM Data Flow and User Navigation) and updated Alt Text.</li> <li>• Replaced <a href="#">Figure 8</a> (WebVRAM Terms and Conditions for Usage Screen).</li> <li>• Replaced <a href="#">Figure 9</a> (WebVRAM PIV Login Screen).</li> <li>• Added details to introduction of Section <a href="#">5</a> (Using the Software).</li> <li>• Corrected step 3 of Section <a href="#">5.1.8</a> (Access CPRS at Remote Sites Using CPRS Desktop Launcher); <i>a user MUST synchronize to a remote site using WebVRAM at least every <b>29</b> days to keep their VistA profile active at that site.</i></li> <li>• Replaced <a href="#">Figure 48</a> (WebVRAM Login – Change Verify Code).</li> </ul>	WebVRAM Team, VA Office of Information and Technology (OIT) Development, Security, and Operations (DevSecOps) Software Product Management (SPM)

		<ul style="list-style-type: none"> <li>Added directions on how to submit a ticket to Enterprise Service Desk to Section <a href="#">6.1.4</a> (Other Errors).</li> <li>Removed references to Fee Basis Claims System (FBCS) from Sections <a href="#">3.1</a> (System Summary), <a href="#">3.3</a> (Data Flows), and Appendix <a href="#">A</a> (Appendix A – Acronyms and Abbreviations).</li> <li>Added “WEBG” to Appendix <a href="#">A</a> (Appendix A – Acronyms and Abbreviations).</li> </ul>	
4/8/2021	3.0	<p>Updated for WebVRAM Release 3.0 (associated with VistA patch WEBG*3*1):</p> <ul style="list-style-type: none"> <li>Added Section <a href="#">5.1.8</a> (Access CPRS at Remote Sites Using CPRS Desktop Launcher).</li> <li>Added note regarding use of Joint Legacy viewer to Section <a href="#">5.1.9</a> (New VA EHR Integration with WebVRAM).</li> <li>Edited note in Section <a href="#">5.1.10</a> (Launch ).</li> <li>Added Section <a href="#">6.1.3</a> (Duplicate VistA Accounts at Remote Site).</li> <li>Retitled Section 6 to Appendix <a href="#">A</a> (Appendix A – Acronyms and Abbreviations).</li> </ul>	WebVRAM Project Team, VA OIT EPMO
10/22/2020	2.1	<p>Updated for WebVRAM Release 2.0 (New VA EHR Integration):</p> <ul style="list-style-type: none"> <li>Added information about DIVISION field to Section <a href="#">4</a> (Getting Started), step 3.</li> <li>Updated link to TRM in Section <a href="#">5.1.7</a> (Launching Multiple CPRS Sessions).</li> <li>Added Section <a href="#">5.1.9</a> (New VA EHR Integration with WebVRAM) and subsection <a href="#">5.1.10</a> (Launch ).</li> </ul>	WebVRAM Project Team, VA OIT EPMO

4/21/2020	2.0	<p>Updated for WebVRAM Release 1.2 (associated with information-only patch WEBG*1.0*1):</p> <ul style="list-style-type: none"> <li>• Added NOTE regarding PIV linkage to Section <a href="#">4</a> (Getting Started), step 4.</li> <li>• Added NOTE regarding accessing Home VistA to Section <a href="#">0</a> (Logging in to WebVRAM), step 3.</li> <li>• Updated <a href="#">Figure 9</a> (WebVRAM PIV Login Screen).</li> <li>• Entirely rewrote Section <a href="#">0</a> (Logging in to WebVRAM), step 5.</li> <li>• Updated <a href="#">Figure 12</a> (Tools Drop-down – Update eSignature Code).</li> <li>• Clarified verbiage in Section <a href="#">4.1</a> (Update eSignature Code and Details), steps 1 and 3.</li> <li>• Added Section <a href="#">5.1.1</a> (Launch Mode: Reflection), step 3.</li> <li>• Clarified verbiage in Section <a href="#">5.1.5</a> (Launch Mode: CPRS), steps 3, 4, and 5.</li> <li>• Added Section <a href="#">5.1.6</a> (Launch Mode: CPRS with Custom Reflection Profiles).</li> <li>• Added <a href="#">Figure 52</a> (Unauthorized Access Error Message).</li> <li>• Various minor formatting and verbiage changes.</li> </ul>	WebVRAM Project Team, VA OIT EPMO
12/6/2019	1.9	Technical Writer review and edit.	Technical Writer, VA OIT EPMO
12/5/2019	1.8	Added Section <a href="#">4.1.1.2.1</a> CPAC Users: Configure Tile View for Multiple VistA Sessions at the Same Site.	WebVRAM PMO Team
12/3/2019	1.7	Updated to address comments from Health Product Support.	Technical Writer, VA OIT EPMO
11/26/2019	1.6	<p>Updated Section <a href="#">1.2.2</a> Assumptions and <a href="#">Section 3</a> Getting Started.</p> <p>Added Section <a href="#">3.2</a> Update eSignature Code and Details.</p> <p>Technical Writer review and edit.</p>	WebVRAM Project Team, VA OIT EPMO
10/29/2019	1.5	Technical Writer review and edit.	Technical Writer, VA OIT EPMO
10/25/2019	1.4	Added content to launch multiple VistA and CPRS sessions, plus changing Reflection settings to support multiple sessions to the same VistA site.	WebVRAM PMO Team

10/24/2019	1.3	Changed date on cover page to current month.	WebVRAM PMO Team
9/16/2019	1.2	Added clarification for FBCS users.	WebVRAM PMO Team
8/27/2019	1.1	Technical Writer review and edit.	Technical Writer, VA OIT EPMO
8/23/2019	1.0	Baseline.	WebVRAM PMO Team

## Table of Contents

<b>1.</b>	<b>Quick Start Guide .....</b>	<b>2</b>
<b>2.</b>	<b>Introduction.....</b>	<b>6</b>
<b>2.1</b>	<b>Purpose .....</b>	<b>6</b>
<b>2.2</b>	<b>Document Orientation .....</b>	<b>7</b>
2.2.1	Organization of the Manual.....	7
2.2.2	Assumptions.....	7
2.2.3	Coordination .....	7
<b>2.3</b>	<b>Disclaimers .....</b>	<b>7</b>
2.3.1	Software Disclaimer.....	7
2.3.2	Documentation Disclaimer .....	8
<b>2.4</b>	<b>Documentation Conventions .....</b>	<b>8</b>
<b>2.5</b>	<b>References and Resources.....</b>	<b>8</b>
<b>2.6</b>	<b>Enterprise Service Desk and Organizational Contacts .....</b>	<b>9</b>
<b>3.</b>	<b>System Maintenance .....</b>	<b>9</b>
<b>3.1</b>	<b>System Summary .....</b>	<b>9</b>
<b>3.2</b>	<b>System Configuration.....</b>	<b>9</b>
<b>3.3</b>	<b>Data Flows.....</b>	<b>10</b>
<b>3.4</b>	<b>User Access Levels .....</b>	<b>12</b>
<b>3.5</b>	<b>Continuity of Operation .....</b>	<b>13</b>
<b>4.</b>	<b>Getting Started .....</b>	<b>13</b>
<b>4.1</b>	<b>Update eSignature Code and Details .....</b>	<b>16</b>
<b>4.2</b>	<b>IAM / PIV Login - Link PIV to your Home VistA site .....</b>	<b>18</b>
<b>4.3</b>	<b>IAM / PIV Login – Login to WebVRAM with PIV Card .....</b>	<b>20</b>
<b>5.</b>	<b>Using the Software.....</b>	<b>22</b>
<b>5.1</b>	<b>Remote Session: Launch Mode .....</b>	<b>23</b>
5.1.1	Launch Mode: Reflection.....	24
5.1.2	Launching Different Multiple Remote VistA Sessions .....	25
5.1.3	Launching Simultaneous Multiple VistA Sessions at a Single Site .....	26
5.1.4	CPAC Users: Configure Tile View for Multiple VistA Sessions at the Same Site .....	29
5.1.5	Launch Mode: CPRS .....	32
5.1.6	Launch Mode: CPRS with Custom Reflection Profiles .....	34
5.1.7	Launching Multiple CPRS Sessions .....	37



5.1.8	Access CPRS at Remote Sites Using CPRS Desktop Launcher .....	38
5.1.9	New VA EHR Integration with WebVRAM.....	39
5.1.10	Launch New VA EHR Button .....	41
<b>5.2</b>	<b>Launch Mode: Synchronize .....</b>	<b>42</b>
<b>5.3</b>	<b>Changing Verify Code .....</b>	<b>43</b>
<b>5.4</b>	<b>User Profile .....</b>	<b>44</b>
<b>5.5</b>	<b>Exit System.....</b>	<b>45</b>
<b>6.</b>	<b>Troubleshooting .....</b>	<b>46</b>
<b>6.1</b>	<b>Special Instructions for Error Correction .....</b>	<b>46</b>
6.1.1	Unauthorized Access Error .....	46
6.1.2	Reflection Fails to Launch.....	46
6.1.3	Duplicate VistA Accounts at Remote Site .....	47
6.1.4	Other Errors.....	47
<b>A.</b>	<b>Appendix A – Acronyms and Abbreviations .....</b>	<b>52</b>

## List of Figures

Figure 1: Micro Focus Reflection File Open Setting Change, 1 of 4.....	3
Figure 2: Micro Focus Reflection File Open Setting Change, 2 of 4.....	4
Figure 3: Micro Focus Reflection File Open Setting Change, 3 of 4.....	4
Figure 4: Micro Focus Reflection File Open Setting Change, 4 of 4.....	5
Figure 5: WebVRAM High-level System Interfaces.....	10
Figure 6: WebVRAM High-level Application Design.....	10
Figure 7: WebVRAM Data Flow and User Navigation.....	12
Figure 8: WebVRAM Terms and Conditions for Usage Screen .....	13
Figure 9: WebVRAM PIV Login Screen .....	14
Figure 10: WebVRAM A/V Code Login Screen .....	14
Figure 11: WebVRAM Home Screen .....	15
Figure 12: Tools Drop-down – Update eSignature Code.....	16
Figure 13: Update eSignature Code Screen .....	16
Figure 14: Update eSignature Details.....	17
Figure 15: Terms and Conditions .....	18
Figure 16: Sign In With VA PIV Card .....	19
Figure 17: PIV Card Not Linked Error .....	19
Figure 18: VA Single Sign-On page.....	20
Figure 19: WebVRAM Terms and Conditions page .....	20
Figure 20: WebVRAM PIV Card Sign-in page.....	21

Figure 21: ActivClient Login .....	21
Figure 22: WebVRAM Application Home Page .....	21
Figure 23: Launch Mode Drop-down .....	24
Figure 24: Launch Reflection Button .....	25
Figure 25: VistA Login .....	25
Figure 26: Launch Multiple Reflection Sessions to Different Remote VistA Systems .....	26
Figure 27: Reflection Workspace Settings Access .....	27
Figure 28: Reflection – Configure User Interface Link.....	28
Figure 29: Reflection – Change User Interface Mode .....	29
Figure 30: Reflection – Cascading View of Multiple Same-site Sessions.....	30
Figure 31: Reflection – Arrange Windows Icon and Drop-down .....	31
Figure 32: Reflection – Arrange Windows Tile Vertical Selection.....	31
Figure 33: Reflection – Tile Vertical View.....	32
Figure 34: Launch CPRS Button.....	32
Figure 35: CPRS Version Screen .....	33
Figure 36: Windows Security: VistA Login - Certificate Selection screen .....	33
Figure 37: Tools Menu, Reflection Profiles Option .....	34
Figure 38: Reflection Profiles Screen.....	35
Figure 39: Launch CPRS Button.....	36
Figure 40: CPRS Version Screen .....	36
Figure 41: PIV Select a Certificate Screen.....	37
Figure 42: CPRS Login Screen .....	37
Figure 43: WebVRAM New VA EHR Connections User Workflow.....	40
Figure 44: Launch New VA EHR Button.....	41
Figure 45: New VA EHR PIV Login Screen .....	42
Figure 46: Launch Synchronize Button.....	43
Figure 47: Launch Synchronize Successful .....	43
Figure 48: WebVRAM Login – Change Verify Code.....	44
Figure 49: My Profile page.....	45
Figure 50: My Business Unit and Admins page .....	45
Figure 51: WebVRAM Logout .....	46
Figure 52: Unauthorized Access Error Message .....	46
Figure 53: Duplicate VistA Account Error .....	47
Figure 54: yourIT Desktop Icon .....	48
Figure 55: yourIT Desktop Icon .....	48
Figure 56: Report an Issue button.....	48
Figure 57: Report a New Issue .....	49
Figure 58: Report a New Issue continued .....	49
Figure 59: User Information .....	49
Figure 60: Report an Issue fields .....	50

Figure 61: Report an Issue fields cont'd ..... 50

Figure 62: Further Details and Submit Issue ..... 51

**List of Tables**

Table 1: Documentation Symbols and Descriptions..... 8

Table 2: Enterprise Service Desk Support Information ..... 9

Table 3: Acronyms and Abbreviations..... 52

# 1. Quick Start Guide

To access the WebVRAM application, the user follows these initial process steps:

1. A user must obtain permission from their Business Line Director to use the WebVRAM application to access remote VistA systems and perform job-related work at those locations.
2. A WebVRAM user must have an active VA Network Profile (known as an Active Directory profile as seen in the Global Access List (GAL) in Outlook) and be able to login to the VA network directly via the Cisco VPN or Citrix.
3. A user must have a current Home VistA user account in a VA Medical Center (VAMC) VistA System. If you do not, submit an ESD request to get a *Production* VistA account established in the VAMC VistA System nearest to your place of residence.
4. A user must have the **WEBG WEBVRAM GUI Secondary Menu Option** added to your Home VistA account. This is done by submitting an ePAS request to your local IT Support Staff or Automated Data Processing Application Coordinator (ADPAC) requesting that this menu option be added to your Home VistA account.
5. A user must have a current and correct **DIVISION** value in their Home VistA account. Submit an ESD request assigned to your local IT Support staff check your Home VistA account to verify that the **DIVISION field** is not blank or incorrectly assigned.



**IMPORTANT: If the DIVISION field is blank or incorrect, the user may not be able to connect to all authorized remote VistA sites through WebVRAM.**

6. When steps 1 – 5 are completed, a user must contact the WebVRAM Business Unit Administrator, assigned to the user's business unit, to request their user profile be added to the WebVRAM database, which will allow login to the application.
7. All users need to complete this step one time only. To prepare for 2-Factor Authentication (2FA)/Personal Identification Verification (PIV) login to WebVRAM, the user must perform a one-time link of their Home VistA user account to their PIV login capabilities through the Identify and Access Management (IAM) Link My Account process.

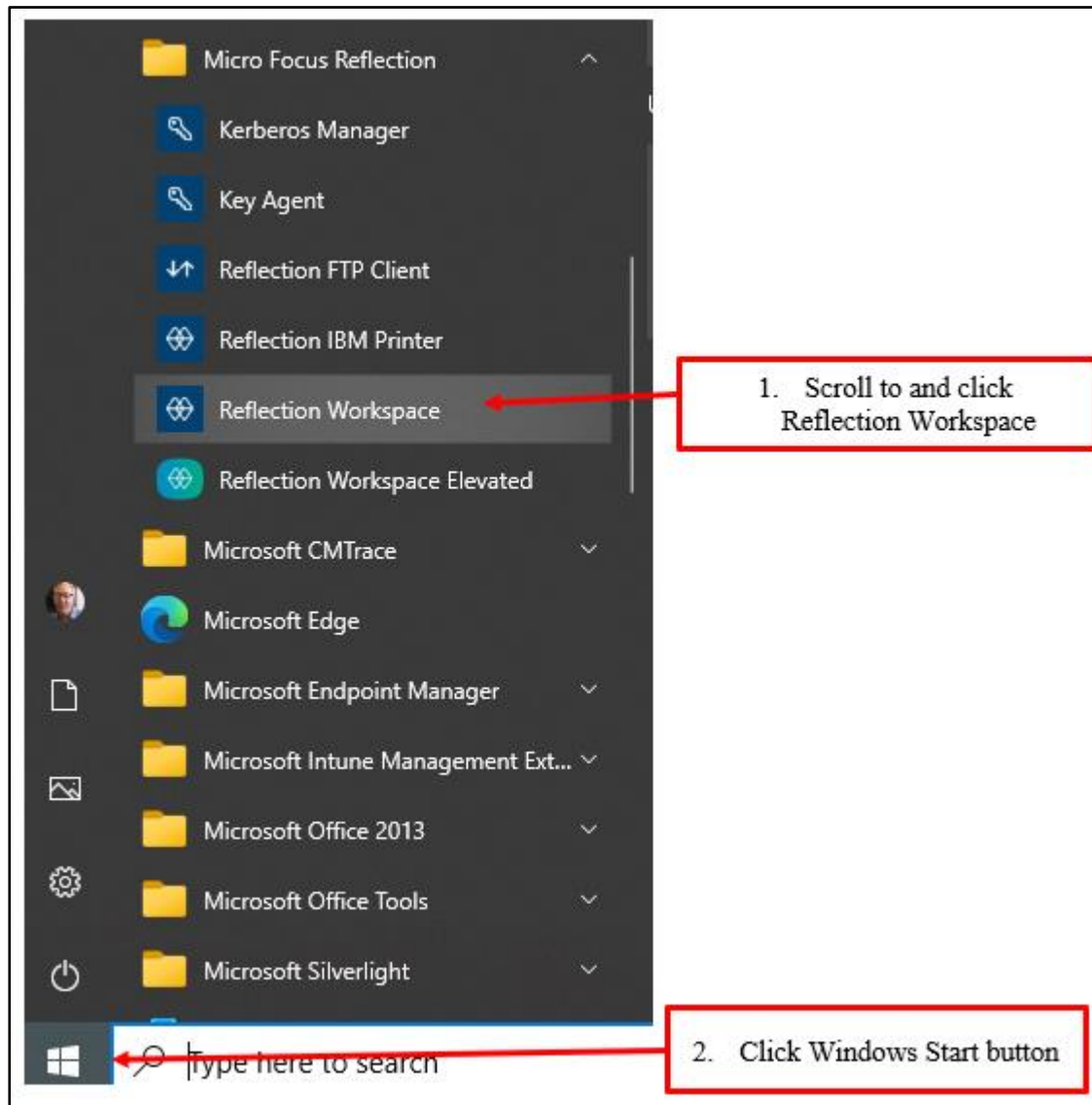
To perform the link, follow the instructions in the yourIT/Service Now (SNOW) Knowledge Article entitled, "How do I bind or link my PIV card to my VistA/CPRS

account?"

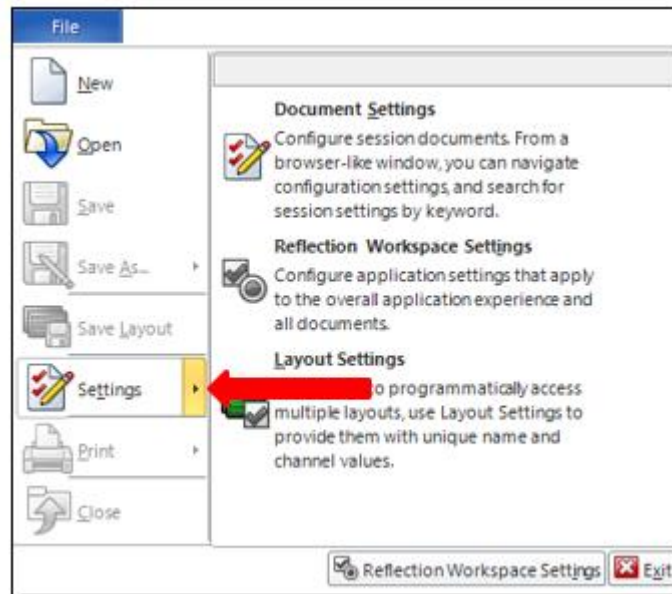
Alternatively, the user may call the ESD to request help to perform the Link My Account process.

8. The user must open **Reflection Workspace** on their workstation, access the **Settings** for that application, select **Specify Trusted Locations** then uncheck the *Open files only from trusted locations* box, followed by clicking **OK** as shown here.

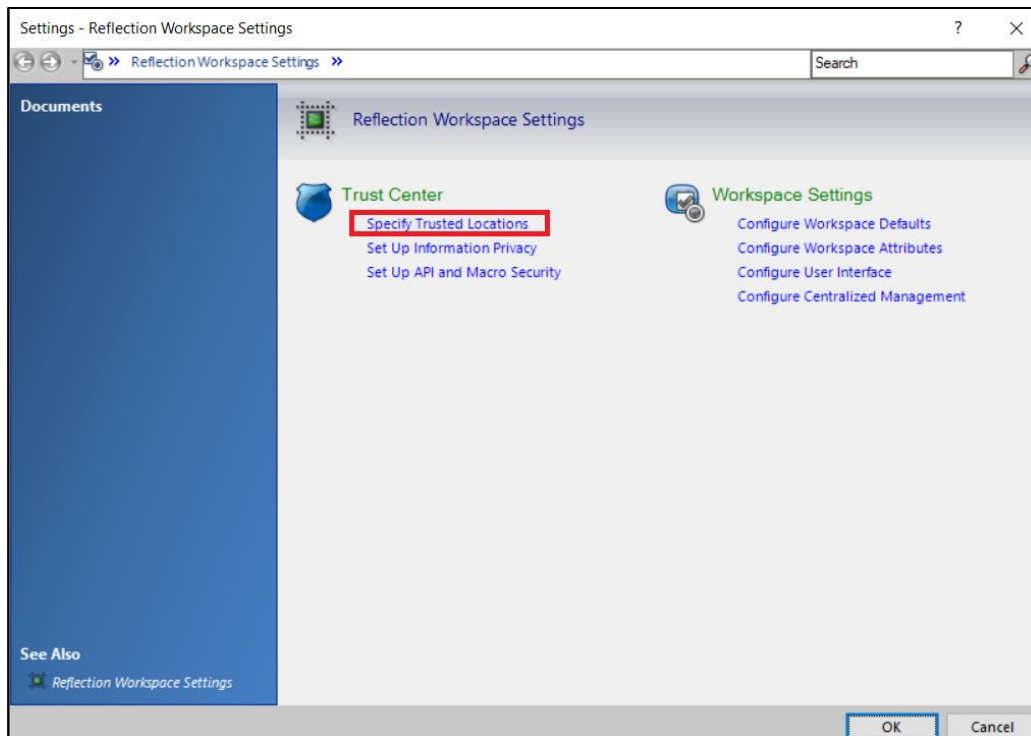
**Figure 1: Micro Focus Reflection File Open Setting Change, 1 of 4**



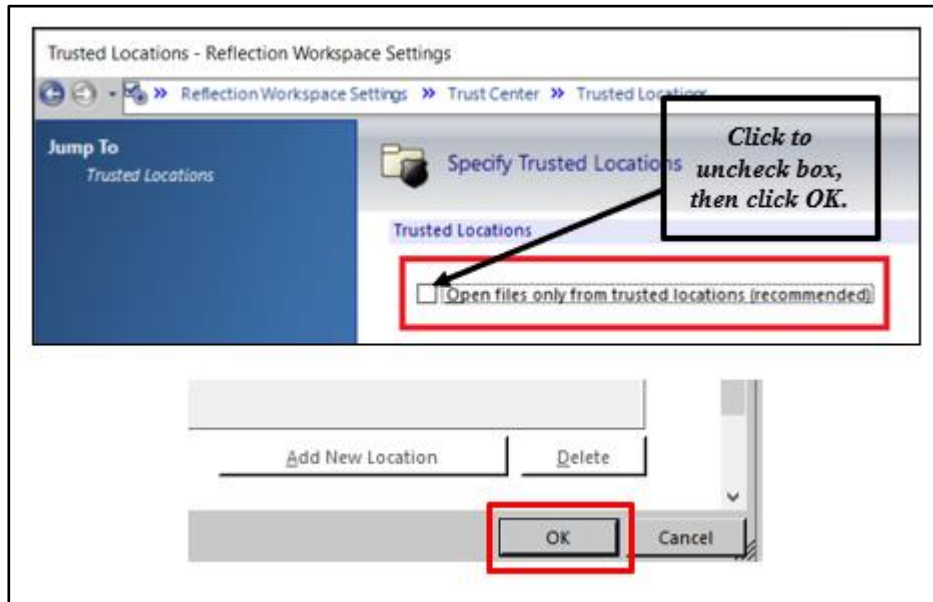
**Figure 2: Micro Focus Reflection File Open Setting Change, 2 of 4**



**Figure 3: Micro Focus Reflection File Open Setting Change, 3 of 4**



**Figure 4: Micro Focus Reflection File Open Setting Change, 4 of 4**



9. After all the above steps are completed, the user can login to WebVRAM, select a remote site to perform work at, then launch a connection session to that site and WebVRAM will log them into all remote sites they are authorized to access using their Home Vista Access and Verify Codes. Details regarding WebVRAM login and launching connection sessions to remote sites are provided in the next sections.



**IMPORTANT: If due to network latency the Reflection session takes longer than normal to connect to the remote site and log you into Vista at that site, the user may receive an “Invalid Access or Verify Code” error and will need to manually enter their Home Vista Access and Verify codes at the next prompt.**

10. If you change work locations and your Windows Active Directory (GAL) ID changes while at the same time your Home Vista location and profile change, you must contact your Business Unit Administrator and work with them to make the appropriate changes in your WebVRAM profile. Failure to do so will prevent you from accessing the WebVRAM application.
11. If you move to another job, leave VA for other work, or retire from VA, you must contact your Business Unit Administrator so they can disable your WebVRAM user profile.

## 2. Introduction

In April 2011, the Executive Director of Office of Information and Technology (OIT) Field Operations challenged the Director, Region Field Program Office (FPO), with finding a technology solution to solve access control complexities for the Consolidated Patient Account Center (CPAC). As a result, a Single Sign On (SSO) project was chartered to develop a local application, utilizing existing capabilities of the VistA CLAIMS System and Remote Procedure Call (RPC) Broker that would potentially be migrated to the VA enterprise to allow remote access (read and write), using a single set of credentials, for organizations requiring access to information resources provided by Veterans Health Information Systems and Technology Architecture (VistA).

The VistA Remote Access Management (VRAM) application was developed to address these access control complexities. VRAM was deployed to CPAC users to allow remote terminal emulation and certain Graphical User Interface (GUI) application connectivity to perform consolidated Medical Care Cost Fund/Recovery and other activities as part of the CPAC mission.

To promote process improvement, implementation of the Web VistA Remote Access Management (WebVRAM) application provides a web-based application to move the VRAM functionality to a cloud computing environment in keeping with the VA Enterprise Cloud initiatives and policy direction. The WebVRAM application will continue to offer a solution which allows synchronization of account credentials by replacing the prior model of user authorization through the VistA CLAIMS system and leveraging the VistA Station ID Callback module (STIC) at user login while maintaining an internal user table that can be electronically populated with user profiles, VistA menus, and keys.

With the cloud-hosted application, users of WebVRAM will continue to enjoy consistency in access to disparate VistA systems while system administrators and systems security personnel experience a reduction in account management activities and standardization of access according to nationally approved access standards. The web-based offering enhances the efficiency achieved by both OIT and Veterans Health Administration (VHA) business partners in obtaining access to disparate VistA systems and enterprise-wide data required to perform VA national-level program business functions. Veteran patient care can be improved as it will take less time for the care provider to access disparate Veteran records across the VA enterprise.

### 2.1 Purpose

The purpose of the WebVRAM User Guide is to familiarize users with the key features and navigational elements of the application. Additionally, this guide provides technical information to system administrators, IT support staff, and other authorized users. It will be updated as needed in subsequent releases.



## **2.2 Document Orientation**

The document orientation is shown below in Sections 2.2.1 through 2.5.

### **2.2.1 Organization of the Manual**

The major sections of the User Guide are shown in the Table of Contents above.

The target audience for this guide includes authorized users, system administrators, and IT support staff.

### **2.2.2 Assumptions**

This guide was written with the following assumptions:

- WebVRAM users are authorized by business line management to access the application.
- Users are authorized to access and use VistA applications to perform their jobs.
- The user has a basic knowledge of WebVRAM access and options.
- Users of the WebVRAM application have current VA Network access and an active local or Home VistA user profile. The user must also arrange to have the WEBG WEBVRAM GUI Secondary menu option added to their VistA profile. That menu option is required for the user to be able to login to the WebVRAM application.
- The primary menu option at the user's Home Vista system is a standard VistA menu name (not a custom menu name).
- Required local Security Keys are identified and incorporated into User Account Profiles by an authorized WebVRAM Business Unit Administrator.

### **2.2.3 Coordination**

Users must obtain approval from their line manager to access and use the WebVRAM application in the performance of their job. The process for obtaining approval is outlined in Section 4 below.

WebVRAM software and documentation disclaimers include disclaimers "as written" in all VA user documentation and are shown below in Sections 2.3.1 and 2.3.2.

## **2.3 Disclaimers**

### **2.3.1 Software Disclaimer**

This software was developed at the Department of Veterans Affairs (VA) by employees of the Federal Government in the course of their official duties. Pursuant to Title 17 Section 105 of the United States Code, this software is not subject to copyright

protection and is in the public domain. VA assumes no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic. We would appreciate acknowledgement if the software is used. This software can be redistributed or modified freely if any derivative works bear some notice that they are derived from it, and any modified versions bear some notice that they have been modified.

### 2.3.2 Documentation Disclaimer



The appearance of external hyperlink references in this manual does not constitute endorsement by the Department of Veterans Affairs (VA) of this website or the information, products, or services contained therein. The VA does not exercise any editorial control over the information you may find at these locations. Such links are provided and are consistent with the stated purpose of the VA.

## 2.4 Documentation Conventions

This manual uses several methods to highlight different aspects of the material.

Various symbols are used throughout the documentation to alert the reader to special information. The table below gives a description of each of these symbols.

**Table 1: Documentation Symbols and Descriptions**

Symbol	Description
	<b>NOTE:</b> Used to inform the reader of general information including references to additional reading material.
	<b>CAUTION:</b> Used to caution the reader to take special notice of critical information.

“Snapshots” of computer online displays (i.e., character-based screen captures/dialogs) and computer source code are shown in a non-proportional font and enclosed within a box. Also included are Graphical User Interface (GUI) Microsoft Windows images (i.e., dialogs or forms).

User's responses to online prompts (e.g., manual entry, taps, clicks, etc.) will be shown in **boldface type**.

## 2.5 References and Resources

- WebVRAM System Design Document
- WebVRAM Requirement Elaboration Document
- WebVRAM User Stories and Backlog – Jira Repository

## 2.6 Enterprise Service Desk and Organizational Contacts

Enterprise Service Desk (ESD) support information is provided in the table below.

**Table 2: Enterprise Service Desk Support Information**

Name	Role	Org	Contact Info
OIT Enterprise Service Desk	Tier 1 Support	OIT	Enterprise Service Desk (ESD)
OIT Enterprise Service Desk	Tier 2 Support	OIT	Tier 1 ESD will escalate tickets to Tier 2 Support as required for issue resolution.
OIT Enterprise Service Desk	Tier 3 Application Support	OIT	Tier 2 Support will escalate tickets to Tier 3 Support as required for issue resolution.

## 3. System Maintenance

WebVRAM defines the personnel and roles to whom the system maintenance procedures and notifications are disseminated are to be the Information System Owner (ISO), Information System Security Officer (ISSO), applicable WebVRAM system support staff, OCCHD (Office of Connected Care Help Desk) helpdesk, Enterprise Service Desk (ESD), and system users.

### 3.1 System Summary

WebVRAM is a web-based, cloud-hosted application utilizing VA Enterprise Architecture and Design principles to facilitate user access to multiple remote VistA systems and related applications such as Computerized Patient Record System (CPRS), without requiring the user to establish login authentication and credentials at each VistA where Veteran data is to be viewed. The need for multiple VistA sessions, with separate user profile login to each VistA instance, is eliminated.

Application features are provided through a Graphical User Interface (GUI). The VA-approved web browser for accessing WebVRAM is Microsoft Edge version 91.0.864.67 or greater.

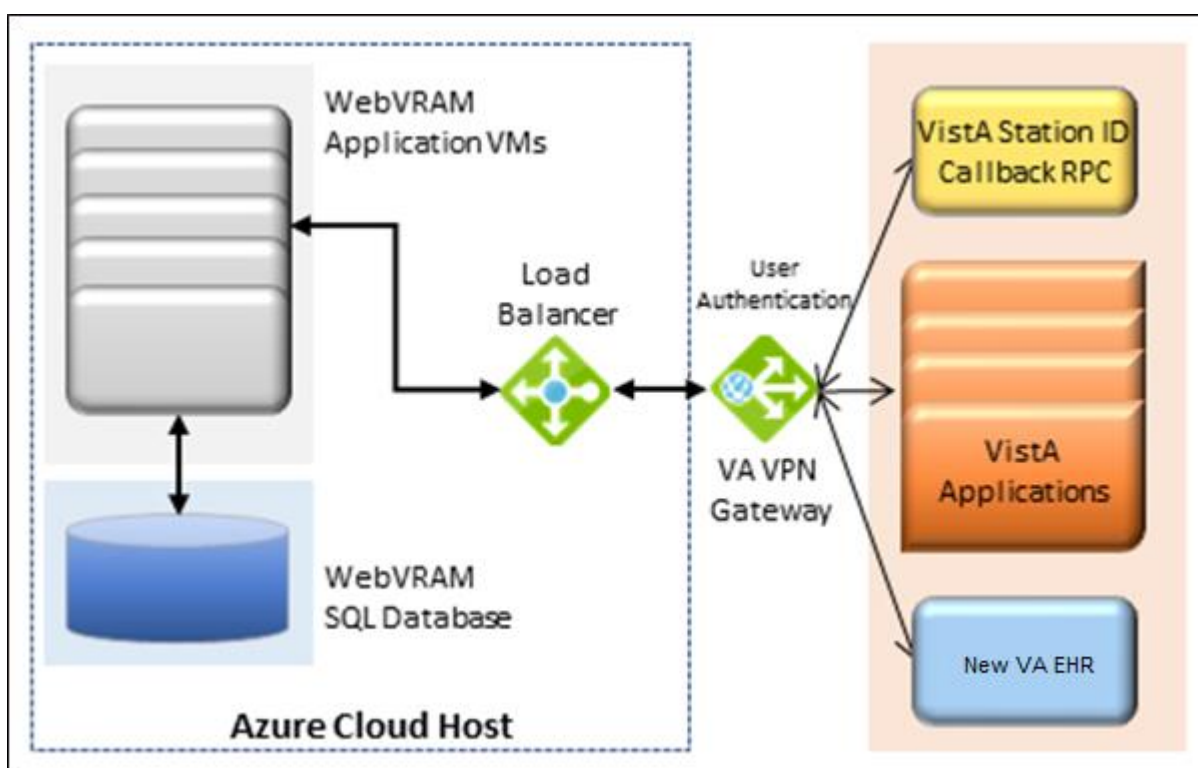
### 3.2 System Configuration

The WebVRAM solution is dependent on the user's local VistA system and the Station ID Callback module (STIC) for user authentication. A user must have a user profile archived and active in their local VistA system to be granted access to the WebVRAM application.

Detailed design and architecture are available for technical review in the WebVRAM System Design Document (SDD). Relationships between systems are shown in Figure 5. This diagram shows the WebVRAM servers hosting the application, known as Virtual

Machines (VMs), residing in the Azure Cloud (host) connected to an Azure Structured Query Language (SQL) database. The VMs and SQL database are accessible from the VA Network through a Load Balancer connected to the VA Virtual Private Network (VPN) Gateway. While the Azure Cloud is located within and part of the VA Network of systems, it is shown below separately from the VistA applications and the VistA STIC for data flow purposes. The figure further shows that user authentication (verifying the user is an authorized VA and WebVRAM user) is performed as the STIC is called by the WebVRAM application to validate the user's credentials on their local VistA system. The STIC also allows them to connect through the WebVRAM application to assigned remote VistA systems.

**Figure 5: WebVRAM High-level System Interfaces**



### 3.3 Data Flows

Figure 6 provides a high-level architectural view of the WebVRAM solution. A discussion follows this diagram regarding data flows from a user perspective.

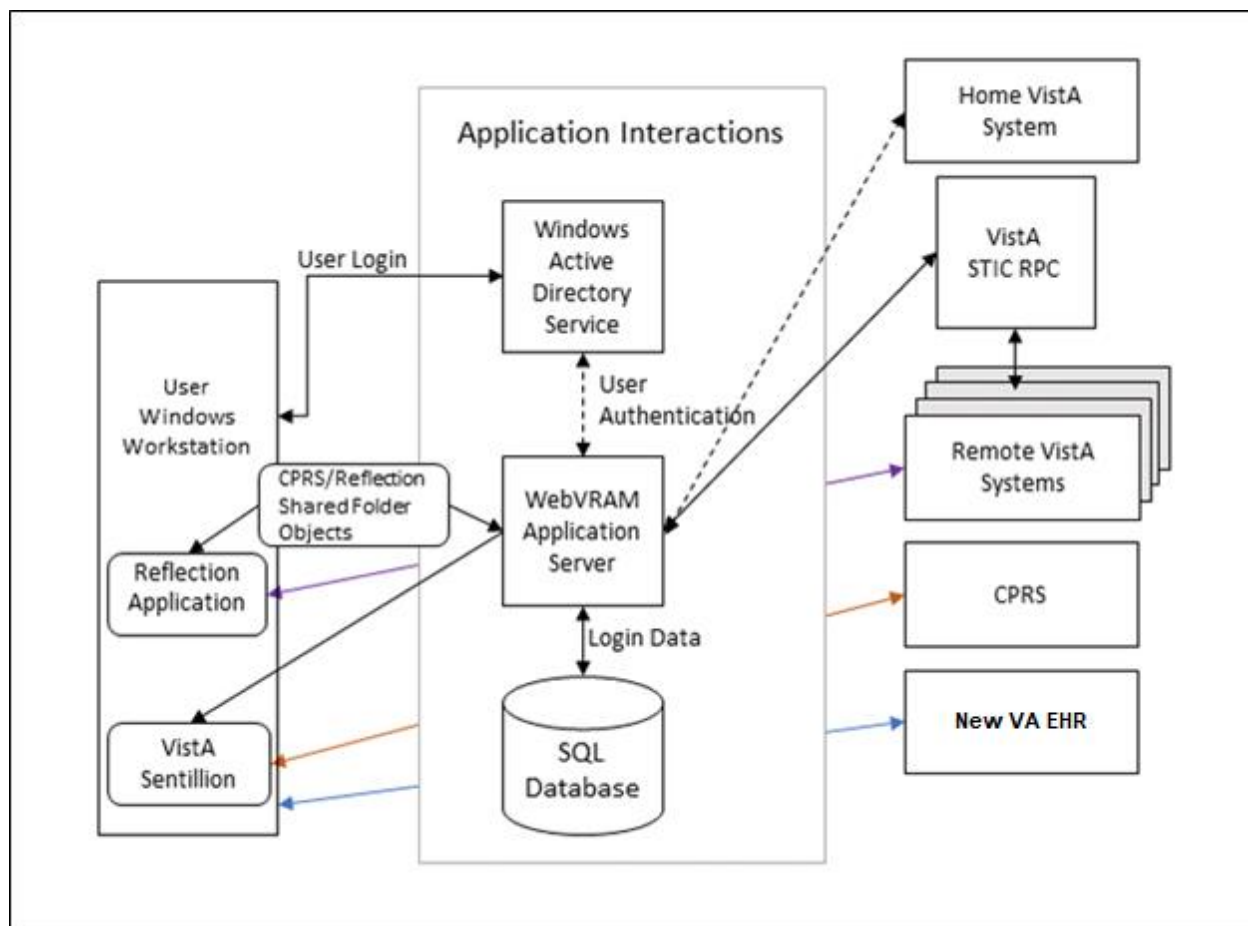
**Figure 6: WebVRAM High-level Application Design**



The application launches a Micro Focus Reflection session (terminal emulation software) from the user's workstation, passes the single-use token to the target remote Vista system(s), and the Reflection emulator gives the user a Vista login screen without having to enter Access and Verify codes a second time. Multiple simultaneous Vista sessions to various remote locations can be initiated with WebVRAM. If the user is also authorized to access the Computerized Patient Record System (CPRS), they will be able to launch CPRS from the WebVRAM GUI site selection page.

Figure 7 provides an overview of the data flow during a user login and remote Vista connection session, and it provides more detail of the software and objects involved in the data flow.

**Figure 7: WebVRAM Data Flow and User Navigation**



### 3.4 User Access Levels

The WebVRAM application does not differentiate users by role. The application provides a mechanism to access multiple Vista systems where the user may or may not have existing credentials. All WebVRAM users have the same privileges regarding access to the software. The only restrictions that apply to the use of the application are based on

the VistA applications, menus, and security keys the user is authorized to use in the performance of their job. The same VistA applications the user is authorized to access on their local workstation will be available for use at each remote VistA system after WebVRAM provides access to the system.

### 3.5 Continuity of Operation

The WebVRAM application will be available for VA enterprise use 99.5% of the time, 24 hours a day, 365 days/year. In the event of a disaster affecting the VA Azure Cloud hosting environment where the application and associated database reside, a replication of the production environment, the application, and WebVRAM operations will be made to a failover site in a separate geographical location. Access to the WebVRAM application will be provided within a few hours of that replication to the failover site. Performance of the application within the failover environment will be like what the user experienced in the primary production environment.

## 4. Getting Started

Logging in to WebVRAM

1. From Microsoft Edge browser, navigate to the WebVRAM home page.
2. The Terms and Conditions web page will be the first page displayed. Read through the conditions and click **Accept the Terms and Conditions** as shown below.

**Figure 8: WebVRAM Terms and Conditions for Usage Screen**

Terms and Conditions for Usage

**WARNING - Authorized Use Only**

U. S. government systems are intended to be used by authorized government network users for viewing and retrieving information only, except as otherwise explicitly authorized for official business and limited personal use in accordance with policy. Information from these systems resides on and transmits through computer systems and networks funded by the government. All access or use constitutes understanding and acceptance that there is no reasonable expectation of privacy in the use of Government networks or systems.

The data and documents on this system include Federal records that contain sensitive information protected by various Federal statutes, including the Privacy Act, 5 U.S.C. Section 552a, and Veterans' records confidentiality statutes such as 38 U.S.C. Sections 5701 and 7332. Access to the data and records is on a need-to-know basis only.

All access or use of this system constitutes user understanding and acceptance of these terms and constitutes unconditional consent to review and action including (but not limited to) monitoring, recording, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized government and law enforcement personnel.

Unauthorized user attempts or acts to (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, (4) accrue resources for unauthorized use or (5) otherwise misuse this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties.

Logging in the WebVRAM Tool or otherwise accessing information contained within the WebVRAM Tool constitutes acceptance of and compliance with the laws and VA policies noted above, to include the VA Rules of Behavior (RoB), and VA Handbook 6102.

Browser support: Microsoft Edge 93 or greater  
Recommended window size: 1280 x 960px

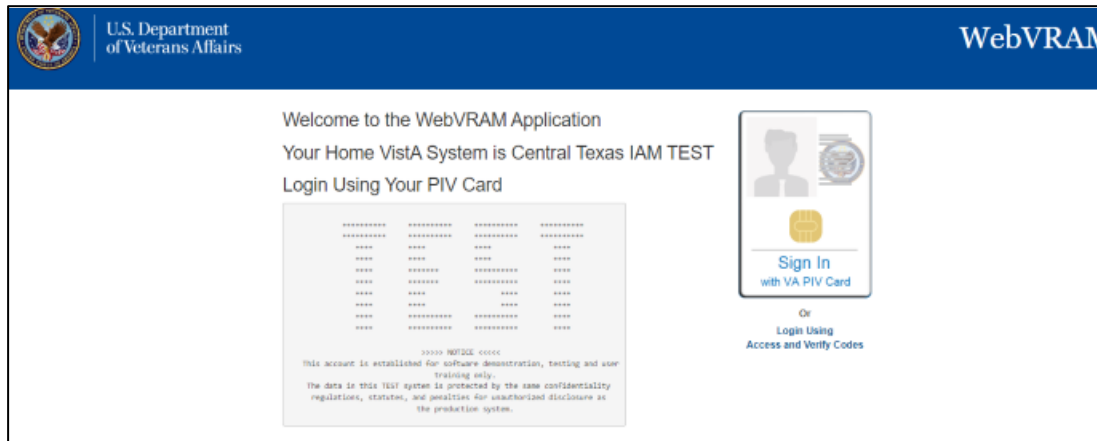
Accept the Terms and Conditions

3. The next web page displayed is the WebVRAM Login page.



**NOTE:** The user's Home VistA System is displayed above the login screen. There is no need to use WebVRAM to access the user's Home VistA system because the user can already login directly to access VistA applications at their Home VistA site.

**Figure 9: WebVRAM PIV Login Screen**

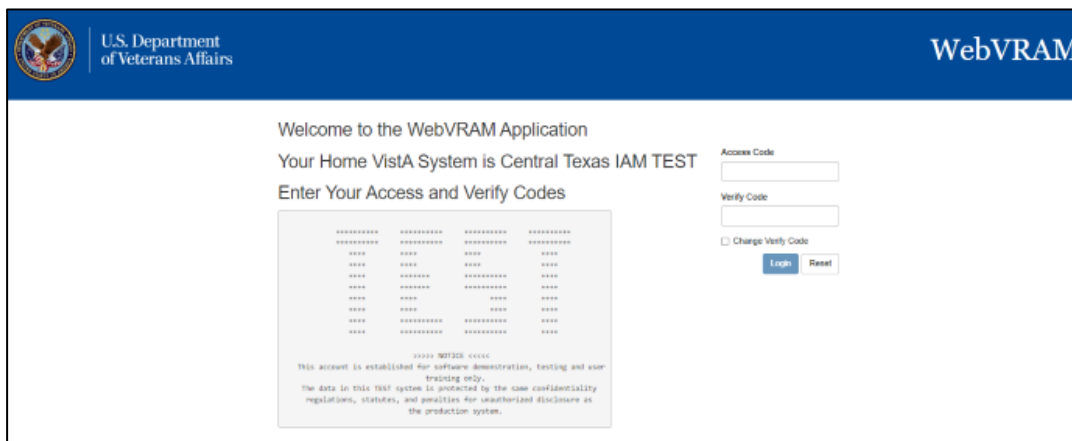


The screenshot shows the WebVRAM PIV Login screen. At the top, there is a blue header with the U.S. Department of Veterans Affairs logo on the left and the WebVRAM logo on the right. Below the header, the text reads: "Welcome to the WebVRAM Application", "Your Home VistA System is Central Texas IAM TEST", and "Login Using Your PIV Card". In the center, there is a large rectangular area with a grid of asterisks representing a PIV card. To the right of this area is an image of a PIV card with the text "Sign In with VA PIV Card". Below the PIV card image, there is a link that says "Or Login Using Access and Verify Codes". At the bottom of the PIV card area, there is a small text box that reads: "\*\*\*\*\* NOTICE \*\*\*\*\* This account is established for software demonstration, testing and user training only. The data in this VistA system is protected by the same confidentiality regulations, statutes, and penalties for unauthorized disclosure as the production system."

4. To log in with PIV Card, click on the **"Sign In with a VA PIV Card"** image. The user will then be prompted to enter their PIV PIN to authenticate.

5. To log in with Access and Verify Codes, click on the [Login Using Access and Verify Codes](#) link. The user will then be prompted to enter their local VistA Access and Verify Codes and click **Login** to access the application.

**Figure 10: WebVRAM A/V Code Login Screen**



The screenshot shows the WebVRAM A/V Code Login screen. At the top, there is a blue header with the U.S. Department of Veterans Affairs logo on the left and the WebVRAM logo on the right. Below the header, the text reads: "Welcome to the WebVRAM Application", "Your Home VistA System is Central Texas IAM TEST", and "Enter Your Access and Verify Codes". In the center, there is a large rectangular area with a grid of asterisks representing a PIV card. To the right of this area, there are two input fields: "Access Code" and "Verify Code". Below these fields is a checkbox labeled "Change Verify Code". At the bottom of the input fields, there are two buttons: "Login" and "Reset". At the bottom of the PIV card area, there is a small text box that reads: "\*\*\*\*\* NOTICE \*\*\*\*\* This account is established for software demonstration, testing and user training only. The data in this VistA system is protected by the same confidentiality regulations, statutes, and penalties for unauthorized disclosure as the production system."



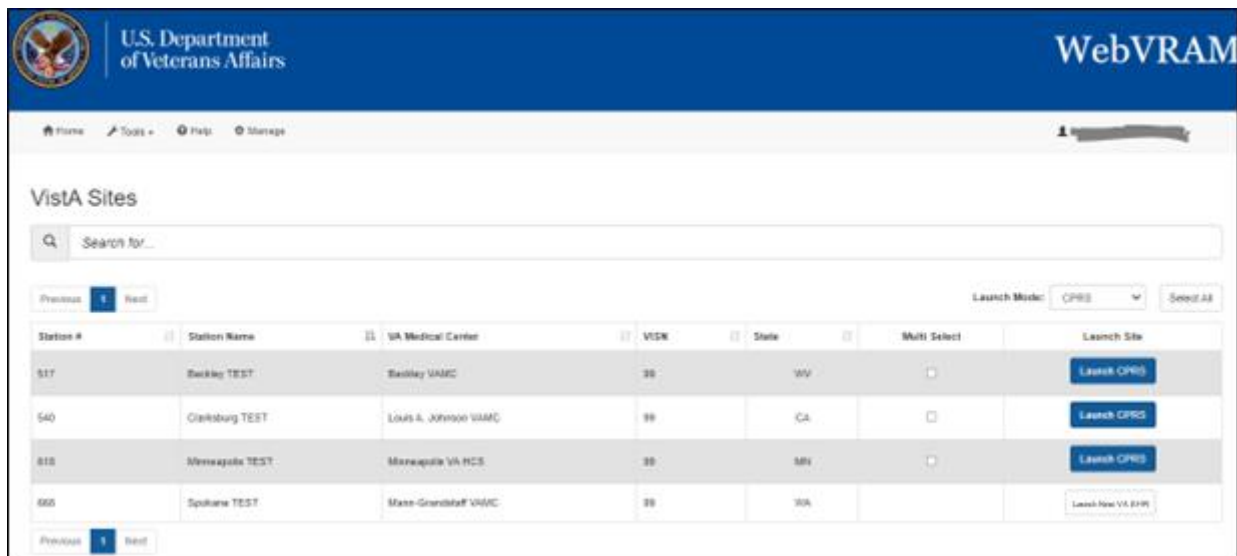
- The WebVRAM application's home page is displayed. Sometimes during login, based on your Home VistA user profile, a window may open with a request to update your Electronic Signature (eSignature) code. See Section 4.1 Update eSignature Code for instructions for updating this code and associated data.

**i NOTE:** The user's Home VistA system will NOT be displayed in the list of VistA sites the user can access because the user can already login directly to access VistA applications at their Home VistA site. The user does NOT need WebVRAM to access their Home VistA system.



**CAUTION:** If a user already has access to a remote VistA site, with active credentials and customized menus and keys at that remote site, AND their custom profile setup at the remote site is DIFFERENT from the profile at their Home VistA system, DO NOT use WebVRAM to access that specific remote site. Instead, continue logging directly into that remote site to perform work. When WebVRAM is used to access a remote site, some of the user's Home VistA profile data, combined with their WebVRAM profile data, overwrites the remote site profile, and may change the custom options of that remote profile. WebVRAM is intended to provide VistA access to remote sites where the user does NOT have active VistA credentials with an already established custom user profile.

**Figure 11: WebVRAM Home Screen**



## 4.1 Update eSignature Code and Details

The Update eSignature Code window will appear during the first login to WebVRAM. The user should enter the eSignature Code and profile information that exists in their Home VistA profile. The user may also choose at any time to change or update their eSignature Code in their Home VistA system and pass the new code to remote VistA systems by clicking **Tools**, then **Update eSignature Code**, and if needed, **Update eSignature Details** to update Title, etc.

Figure 12: Tools Drop-down – Update eSignature Code

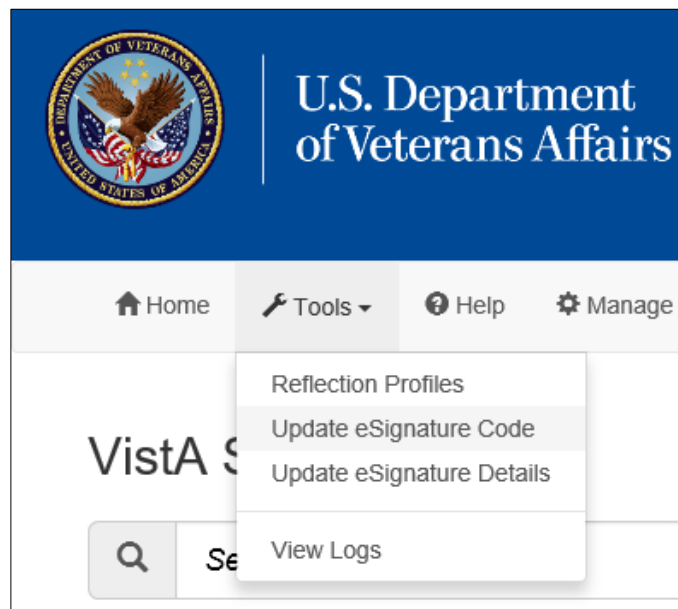


Figure 13: Update eSignature Code Screen

The screenshot shows the "Update eSignature Code" window overlaid on the WebVRAM interface. The window has a title bar with the text "Update eSignature Code" and a close button (X). Below the title bar, there are instructions: "Instructions: eSignature code must be 6 to 20 characters in length with no control or lowercase characters." Below the instructions, there are two input fields: "New eSignature Code" with a placeholder "new eSignature code" and "Confirm eSignature Code" with a placeholder "confirm eSignature code". At the bottom right of the window, there are two buttons: "Update" (with a refresh icon) and "Cancel" (with an X icon).

To update the eSignature Code:

1. If you wish to change your Home VistA eSignature code, enter a new eSignature code in the **New eSignature Code** field. According to VA policy and VistA parameters, the signature code must be 6 to 20 characters in length with no control or lowercase characters. Letters or numbers can be used. If you do NOT wish to change your Home VistA eSignature code, click **Cancel** to exit this option.
2. Enter the same new eSignature code in the **Confirm eSignature Code** field, then click **Update**.

**Figure 14: Update eSignature Details**

3. A second window should appear to allow the user to **Update eSignature Details**. This page can also be accessed from the WebVRAM main page at any time by clicking **Tools**, then **Update eSignature Details**. If you wish to change eSignature profile data, enter the following data elements in the appropriate fields. If you do NOT want to change your eSignature profile data, click **Cancel** to exit this option.
  - a. **eSignature Name** (user's name as it appears in VistA)
  - b. **eSignature Title** (user's title as stored in their VistA profile)
  - c. **eSignature Initials** (user's initials as stored in their VistA profile)
  - d. **Office Phone Number** (user's office phone number, or cellular phone)
  - e. **Voice Pager Number** (optional; enter data if the user wants that information updated or added to their VistA eSignature information)

- f. **Digital Pager Number** (optional; enter data if the user wants that information updated or added to their VistA eSignature information)
4. After adding data to each field, click **Save Changes** to update the VistA local eSignature information. This same information will be passed to and used at each remote site where the user performs work, when the remote site is accessed through WebVRAM.

## 4.2 IAM / PIV Login - Link PIV to your Home VistA site

WebVRAM R5 introduces new feature that allows users to login using their PIV Cards instead of the Login with Access and Verify Codes. This section will describe the process of linking the user's PIV Cards to their WebVRAM Home VistA site.

### To Link your PIV Card:

1. Navigate to WebVRAM URL: [WebVRAM Home Page](#)
2. The Terms and Conditions for Usage is displayed; Click on the **"Accept the Terms and Conditions"** button

Figure 15: Terms and Conditions

U.S. Department of Veterans Affairs

WebVRAM

### Terms and Conditions for Usage

**WARNING - Authorized Use Only**

U. S. government systems are intended to be used by authorized government network users for viewing and retrieving information only, except as otherwise explicitly authorized for official business and limited personal use in accordance with policy. Information from these systems resides on and transmits through computer systems and networks funded by the government. All access or use constitutes understanding and acceptance that there is no reasonable expectation of privacy in the use of Government networks or systems.

The data and documents on this system include Federal records that contain sensitive information protected by various Federal statutes, including the Privacy Act, 5 U.S.C. Section 552a, and Veterans' records confidentiality statutes such as 38 U.S.C. Sections 5701 and 7332. Access to the data and records is on a need-to-know basis only.

All access or use of this system constitutes user understanding and acceptance of these terms and constitutes unconditional consent to review and action including (but not limited to) monitoring, recording, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized government and law enforcement personnel.

Unauthorized user attempts or acts to (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, (4) accrue resources for unauthorized use or (5) otherwise misuse this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties.

Logging in the WebVRAM Tool or otherwise accessing information contained within the WebVRAM Tool constitutes acceptance of and compliance with the laws and VA policies noted above, to include the VA Rules of Behavior (RoB) and VA Handbook 6102.

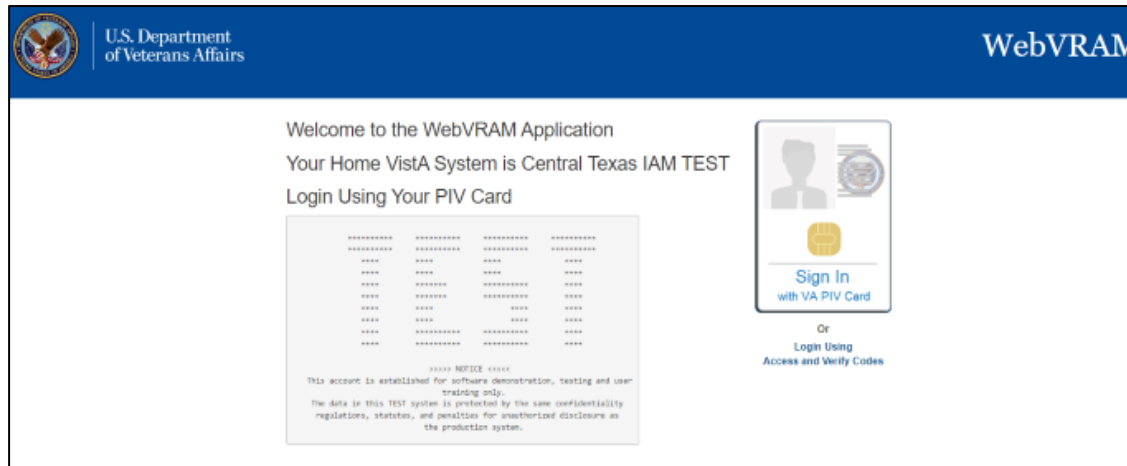
Browser support: Internet Explorer 11 or Microsoft Edge 93  
Recommended window size: 1280 x 960px

[Accept the Terms and Conditions](#)

v5.0.0-20220601

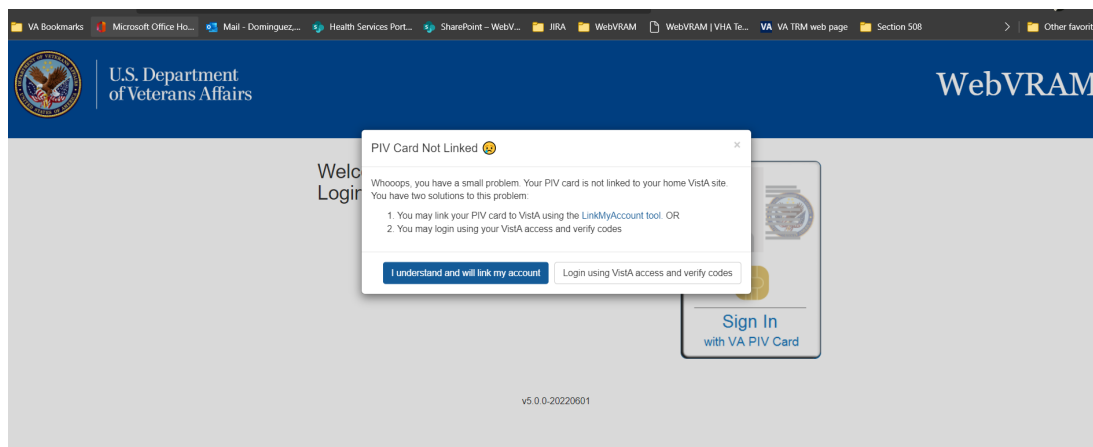
3. Click on the **"Sign In with a VA PIV Card"** button

**Figure 16: Sign In With VA PIV Card**



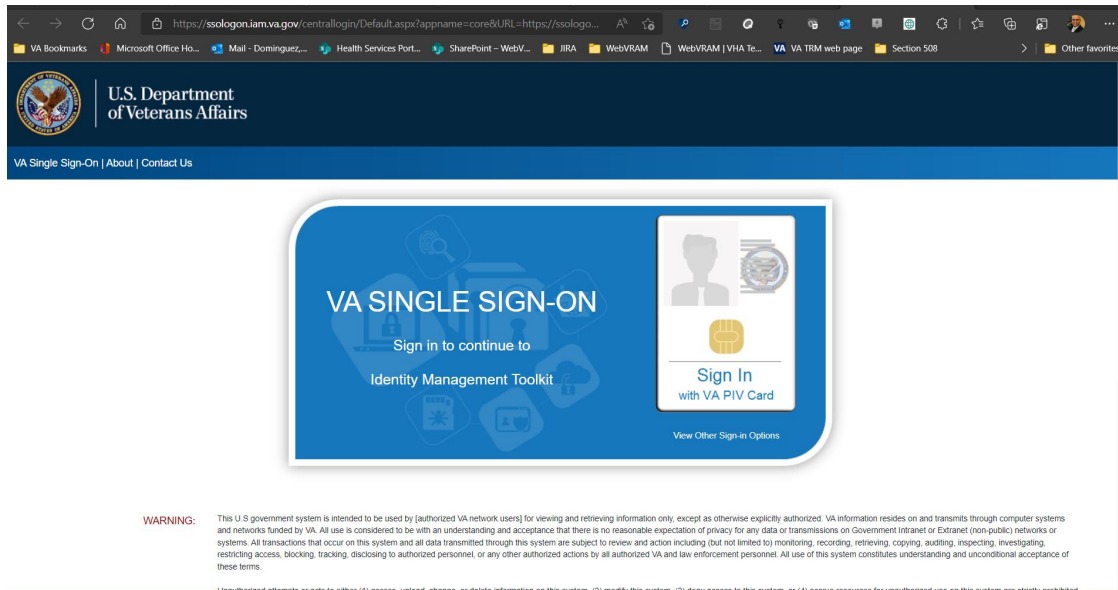
4. The **"PIV Card not Linked"** pop-up screened is displayed
5. Click on the **"I understand and will link my account"** button

**Figure 17: PIV Card Not Linked Error**



6. The **"VA Single Sign-On to IAM Toolkit"** is displayed
7. Click on the **"Sign In with a VA PIV Card"** button

Figure 18: VA Single Sign-On page

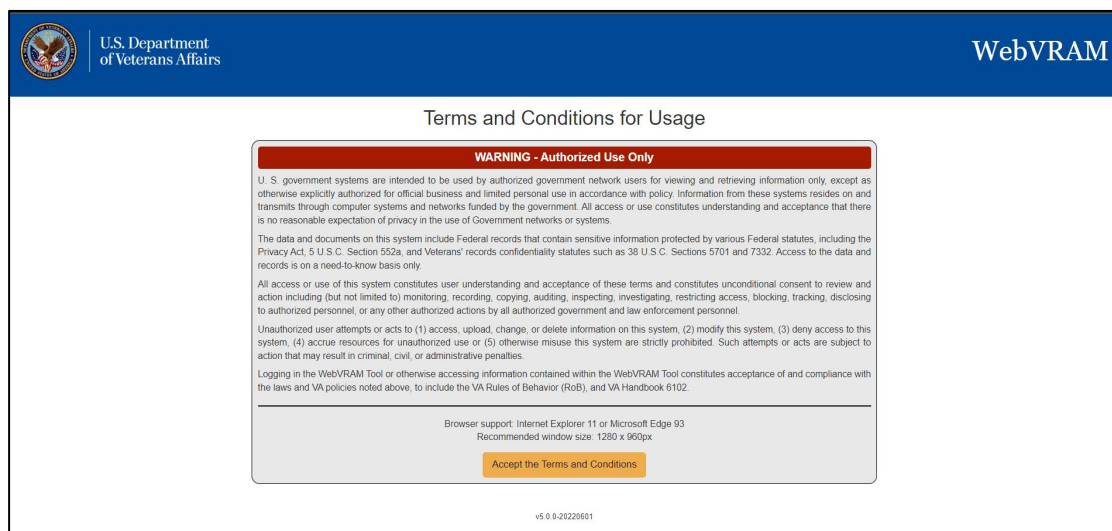


## 4.3 IAM / PIV Login – Login to WebVRAM with PIV Card

To login to WebVRAM utilizing your PIV Card:

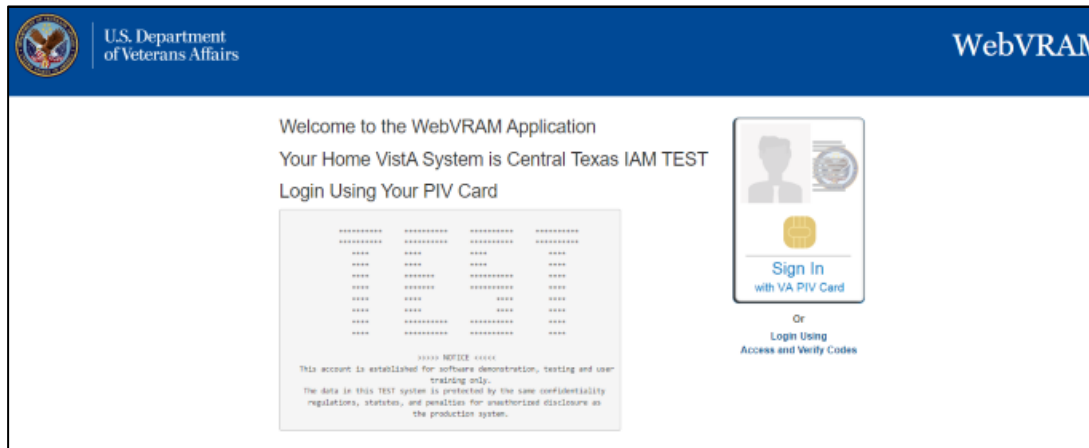
1. Navigate to WebVRAM URL: [WebVRAM Home Page](#)
2. The Terms and Conditions for Usage is displayed; Click on the **“Accept the Terms and Conditions”** button

Figure 19: WebVRAM Terms and Conditions page



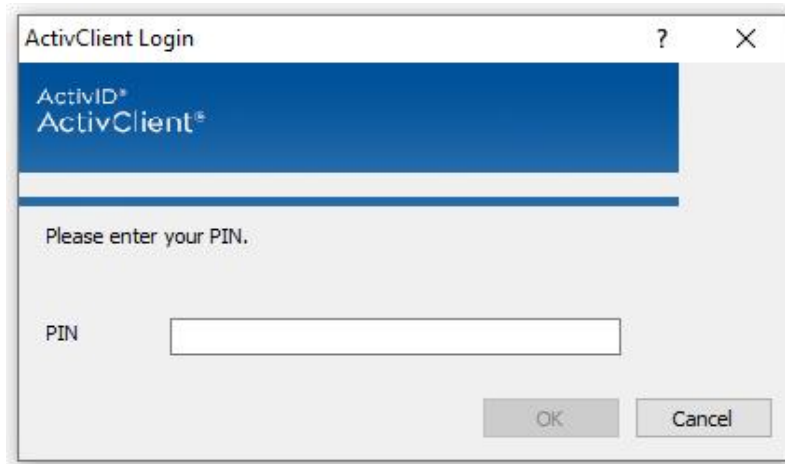
3. Click on the **“Sign In with a VA PIV Card”** button

**Figure 20: WebVRAM PIV Card Sign-in page**



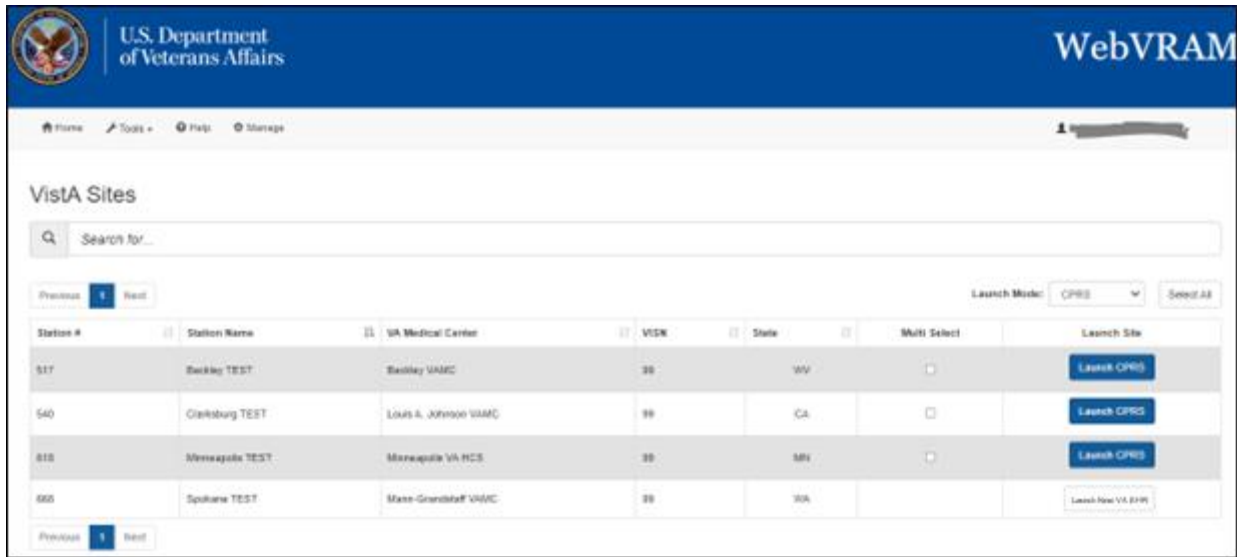
4. The ActivClient screen comes up, prompting the user to enter their PIN.
5. Enter PIN and click **OK**

**Figure 21: ActivClient Login**



6. The WebVRAM application's home page is displayed.

**Figure 22: WebVRAM Application Home Page**



- Sometimes during login, based on your Home VistA user profile, a window may open with a request to update your Electronic Signature (eSignature) code. See Section 4.1 Update eSignature Code for instructions for updating this code and associated data.

## 5. Using the Software

This section describes the system menu first encountered by the user, as well as the navigation paths to functions noted on the screen.

**How WebVRAM Works:** The software allows authorized users to access remote VA Medical Center or Health Care System sites, outside of their Home/local VA site, they are authorized to access by their Business Unit Director, by passing their Home VistA profile menus, keys, person class, user class, and other profile data to the remote site where they can login to the remote site using their Home VistA Access and Verify codes. This process makes it possible for WebVRAM users to access remote sites with **one** set of login credentials instead of maintaining separate profiles with separate credentials for several remote sites.

**What WebVRAM does NOT do:** The software can NOT be used to login to the user's Home VistA system or launch a local CPRS session. This is by design, because a user has no need for WebVRAM to retrieve their Home VistA profile and pass it back to their Home VistA system with their Access and Verify codes. Users can already login directly to their Home VistA system, and there is no need for WebVRAM to do that for them.

The software should also NOT be used if a user already has an active profile at a remote site that has been established using **custom** menus and keys for specific work the user performs at that remote location. If this is the case, contact your WebVRAM Business



Unit Administrator and instruct them to **leave that remote site off your WebVRAM VistA Sites list** so you do not accidentally use WebVRAM to connect to that site. If that site is in your list and you connect to it using WebVRAM, your Home VistA profile will overwrite the custom profile at that remote site, and the features you did have access to in VistA or CPRS will likely stop working.



**NOTE:** WebVRAM will timeout if left idle for more than 15 minutes. Under certain circumstances involving patient safety, some users may be permitted longer timeouts if requested by the Business Unit Director with sufficient rationale. With rare exceptions, users who are members of multiple Business Units are not permitted to have extended timeouts.

## 5.1 Remote Session: Launch Mode

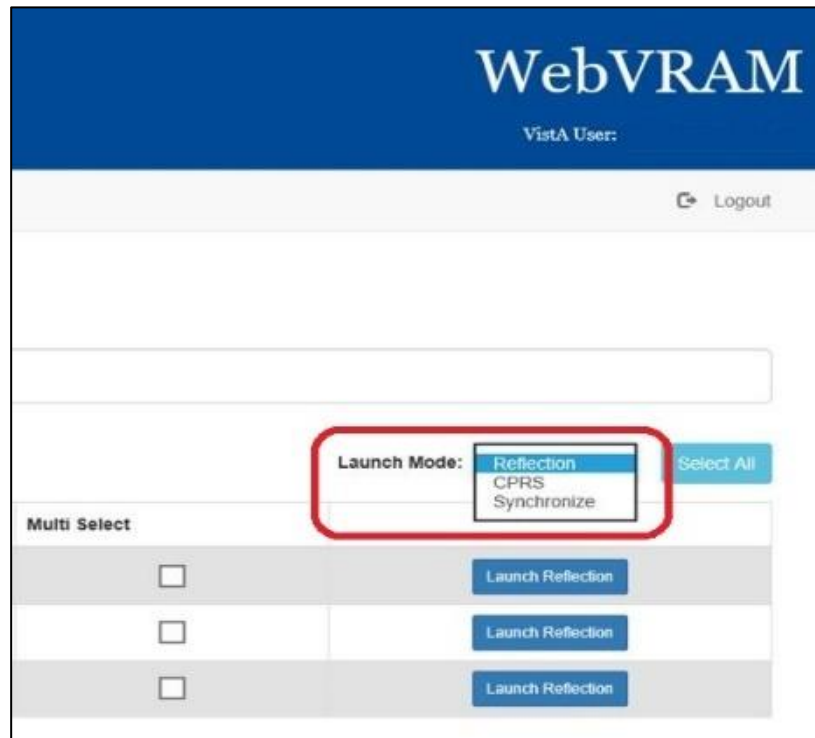
1. Login to WebVRAM.
2. From the WebVRAM home page, select the Station Name of the remote VistA site to which the user wants to connect. The Launch Mode provides a drop-down menu from which the user can select the Launch Mode to use. The drop-down selection defaults to "Reflection."

Available drop-down options are:

- Reflection – This option is used to launch a remote VistA session with Reflection to connect to a remote VistA system already assigned to the user's profile.
- CPRS – This option is used to launch a remote VistA CPRS session at the selected remote location.
- Synchronize – Similar to launching Reflection, *if the user does not need to perform work at the remote location or wishes to start a CPRS session using the CPRS Launcher desktop application (not part of the WebVRAM application) or a Goldstar directory link*, this option is used to connect to and setup or update an active VistA login account at a remote VistA site. Those who use CPRS Launcher or a Goldstar Directory to access CPRS at a remote site after they have synchronized with WebVRAM, will need to synchronize every 29 days to each of their remote sites using WebVRAM so their remote VistA accounts remain active at those sites. Otherwise, their remote VistA accounts will terminate automatically after 30 days from the last time they synchronized using WebVRAM, and they will not be able to launch CPRS at that site using CPRS Launcher or a Goldstar Directory. This is a required security feature for the WebVRAM application. The VET-HOME business unit has an extended synchronization window due to unique patient safety requirements. If the user launches CPRS from WebVRAM at any remote site, their remote VistA profile at that site will not expire because WebVRAM updates the

termination date in that remote profile with a new 30-day period every time the user launches CPRS from WebVRAM. If there are changes to the user's Home VistA account and those changes are also made to their WebVRAM profile, the Synchronize option will push those changes to the selected remote location(s). If the user's line management determines a need for access to a new VistA site, the new location can be added to the user's WebVRAM profile by the business designated WebVRAM Business Unit Administrator.

**Figure 23: Launch Mode Drop-down**



### 5.1.1 Launch Mode: Reflection

1. Login to WebVRAM.
2. From the WebVRAM home page, select the Station Name of the remote VistA site to which the user wants to connect.
3. If the VistA site the user needs to connect to is not shown in the first 20 sites listed on the home page, the user can use the search window to quickly locate the VistA site. The user can search by Station Name, Station ID, VISN, and State.
4. Click on **Launch Reflection**. WebVRAM will launch Reflection and log the user into the remote VistA site that was selected.



**NOTE:** Reflection is the built-in workstation software that allows the user to connect to and work in the selected remote VistA system.

**Figure 24: Launch Reflection Button**

The screenshot shows the 'VistA Sites' interface. At the top is a search bar. Below it are 'Previous', '1', and 'Next' buttons. To the right is a 'Launch Mode' dropdown set to 'Reflection' and a 'Select All' button. The main table has columns: Station #, Station Name, VA Medical Center, VISN, State, Multi Select, and Launch Site. The first row (Station # 517) has the 'Launch Reflection' button highlighted with a red box. The other rows also have 'Launch Reflection' buttons, with the third row (Station # 665) also showing a 'Launch New VA EHR' button.

Station #	Station Name	VA Medical Center	VISN	State	Multi Select	Launch Site
517	Beckley TEST	Beckley VAMC	99	WV	<input type="checkbox"/>	Launch Reflection
540	Clarksburg TEST	Louis A. Johnson VAMC	99	CA	<input type="checkbox"/>	Launch Reflection
665	Spokane TEST	Mann-Grandstaff VAMC	99	WA	<input type="checkbox"/>	Launch Reflection Launch New VA EHR
615	Minneapolis TEST	Minneapolis VA HCS	99	MN	<input type="checkbox"/>	Launch Reflection

- Once the **Launch Reflection** button is selected, the application will launch the user's desktop Reflection software and make the connection to the remote VistA system where the user will be logged in for VistA access. The VistA "roll and scroll" features will be available to the user, like what the user has access to in their local VistA system, as shown in the screen shot below.

**Figure 25: VistA Login**

```

The data in this TEST system is protected by the same confidentiality
regulations, statutes, and penalties for unauthorized disclosure as
the production system.

Restore date:    MAR 25,2019

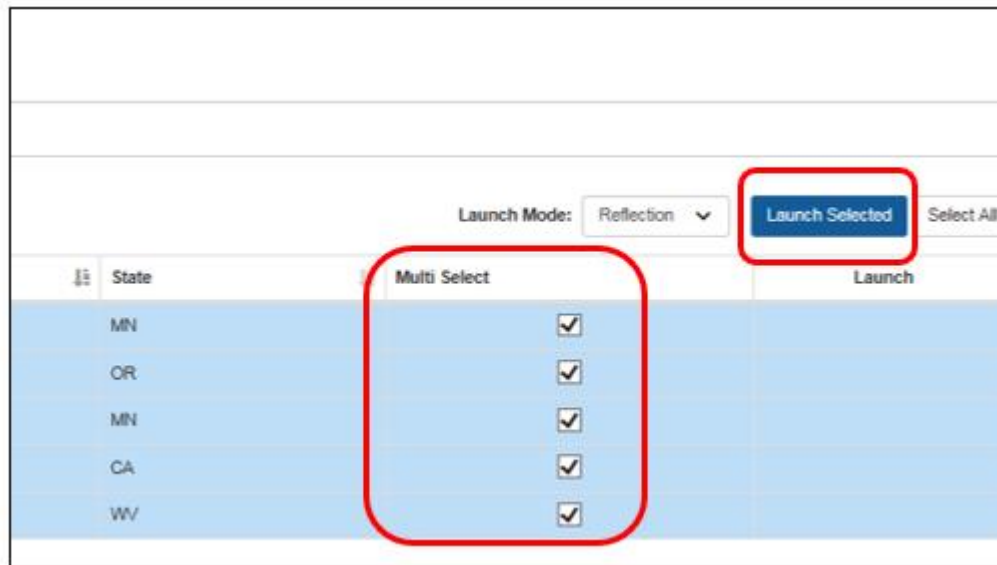
Volume set: TOU: EXAMPLE      UCI:   XXX   Device:  EXAMPL: (### . ### . ### . ###)

ACCESS CODE:  *****
VERIFY CODE:  *****
  
```

### 5.1.2 Launching Different Multiple Remote VistA Sessions

Multiple VistA sessions at different remote VistA locations can be launched together by checking the box for each VistA to be launched simultaneously in the **Multi Select** column on the user's home page. When one or more boxes to launch Reflection are checked, the **Launch Mode** selection option changes to **Launch Selected**. Clicking the **Launch Selected** button, with one or more boxes checked in the **Multi Select** column, then launches different multiple VistA sessions at the same time. Figure 26 shows the boxes checked for each site the user intends to launch, and the **Launch Selected** mode for performing this action.

**Figure 26: Launch Multiple Reflection Sessions to Different Remote VistA Systems**



**CAUTION:** If a connection to a particular site fails when multiple Reflection sessions are launched, it can be due to several factors outside of the control of the WebVRAM application, such as network latency issues, down time at the remote site, user profile configuration issues at the remote site, local VistA user profile configuration issues, etc. If connection to a site fails during a multiple launch sequence, the entire launch sequence, from that site forward, is terminated by WebVRAM so the user can see and capture the error that occurred when the connection failed. For example, if five sites were selected and launched, and the third site fails to connect during launch, sites four and five will not be launched to allow the user to immediately see the connection error displayed. That error message can then be shared with the Enterprise Service Desk when the user logs a ticket to request help in resolving the issue. Sites four and five can then be launched after capturing the error independently, or together by checking the **Multi Select** box adjacent to each of those sites and clicking the **Launch Selected** button.

### 5.1.3 Launching Simultaneous Multiple VistA Sessions at a Single Site

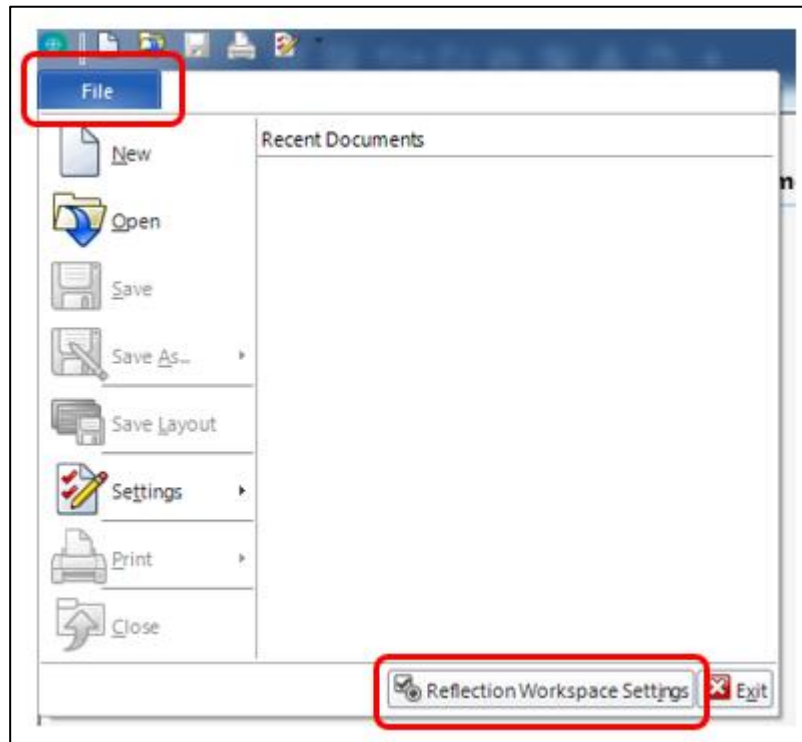
Launching simultaneous multiple Reflection connection sessions at the same site is done by launching the first session from the WebVRAM home page as discussed in Section 5.1.1 Launch Mode: Reflection, then repeating the launch steps to launch additional simultaneous connection sessions to the same VistA system at the same time.



**CAUTION:** For this to work, Micro Focus Reflection must have a configuration setting in place to allow simultaneous multiple sessions to be opened. Follow the steps below to ensure this configuration setting is in place.

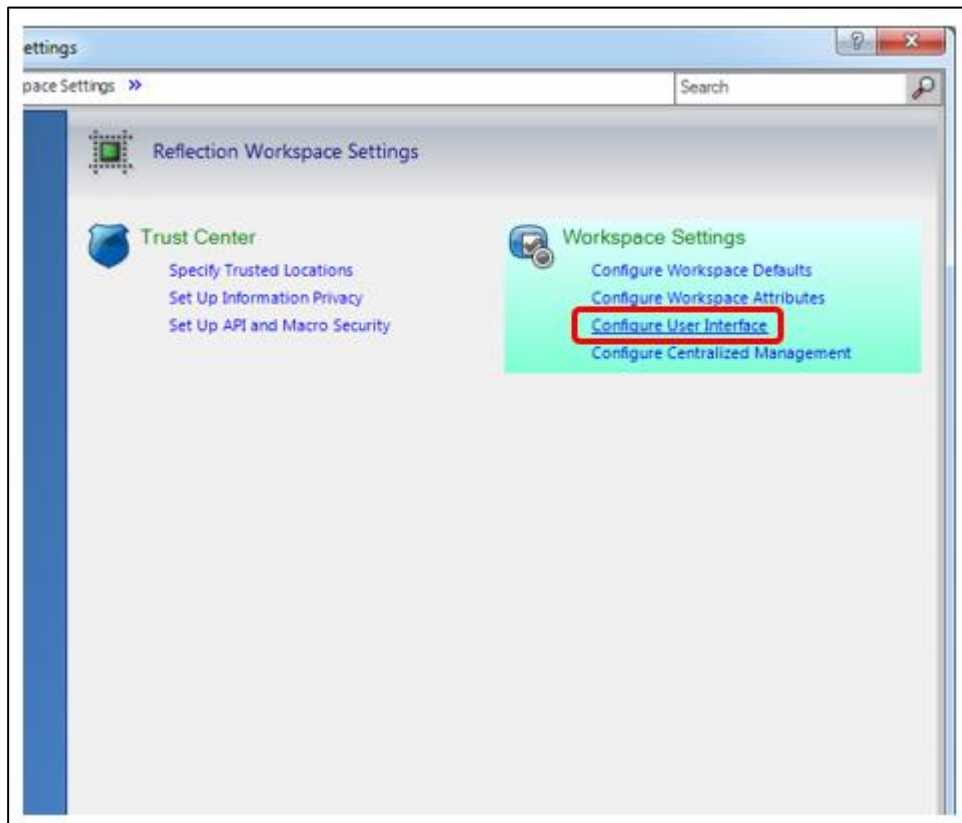
1. Open *Reflection Workspace* on your workstation. In the upper left corner, click the **File** tab.
2. In the pop-up window that opens, click on **Reflection Workspace Settings** in the lower right corner, as shown below.

**Figure 27: Reflection Workspace Settings Access**



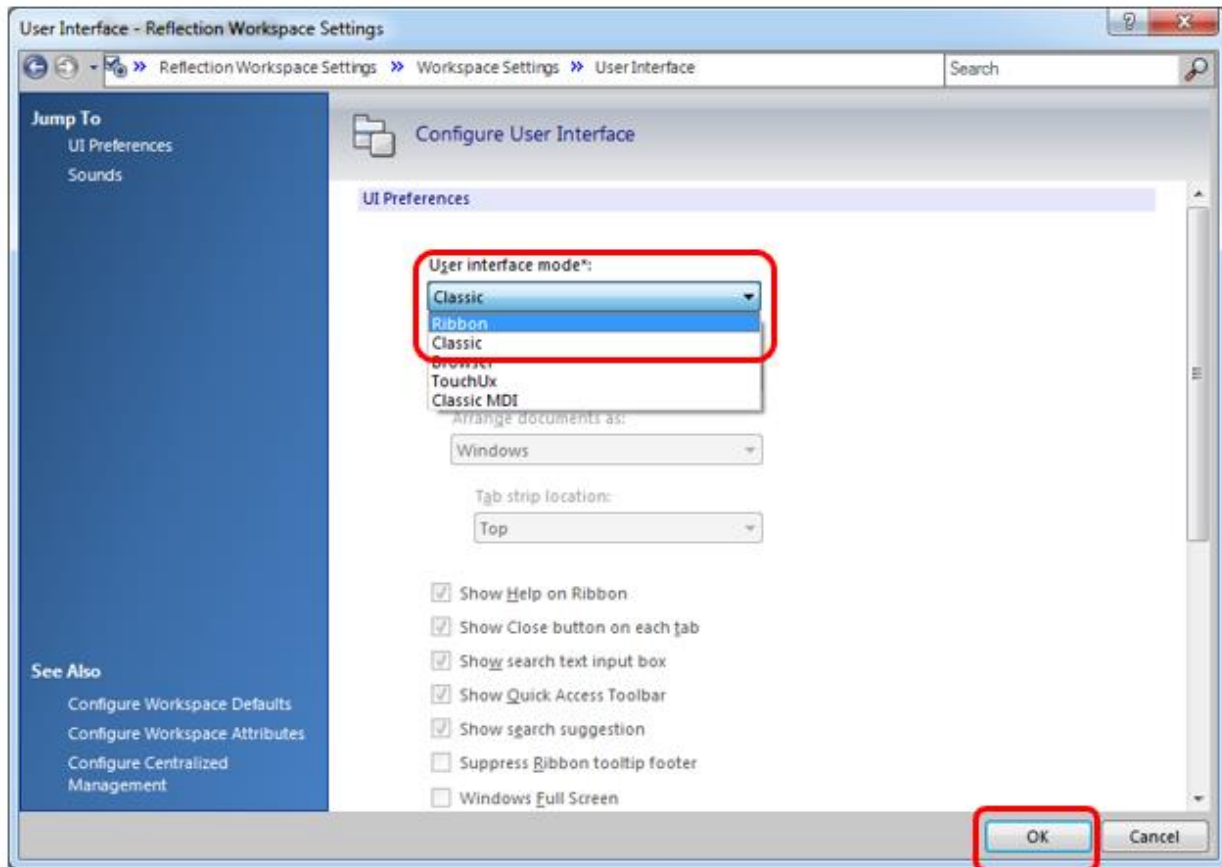
3. In the pop-up window that opens, under **Workspace Settings**, click on **Configure User Interface**, as shown below.

**Figure 28: Reflection – Configure User Interface Link**



4. In the next pop-up window, use the drop-down option in the **User Interface Mode\*** box to select the **Ribbon** setting. Click **OK** in the bottom right corner to save changes, as shown below.

**Figure 29: Reflection – Change User Interface Mode**



5. With this setting change, the user can now open simultaneous multiple sessions to one VistA remote site.

#### **5.1.4 CPAC Users: Configure Tile View for Multiple VistA Sessions at the Same Site**

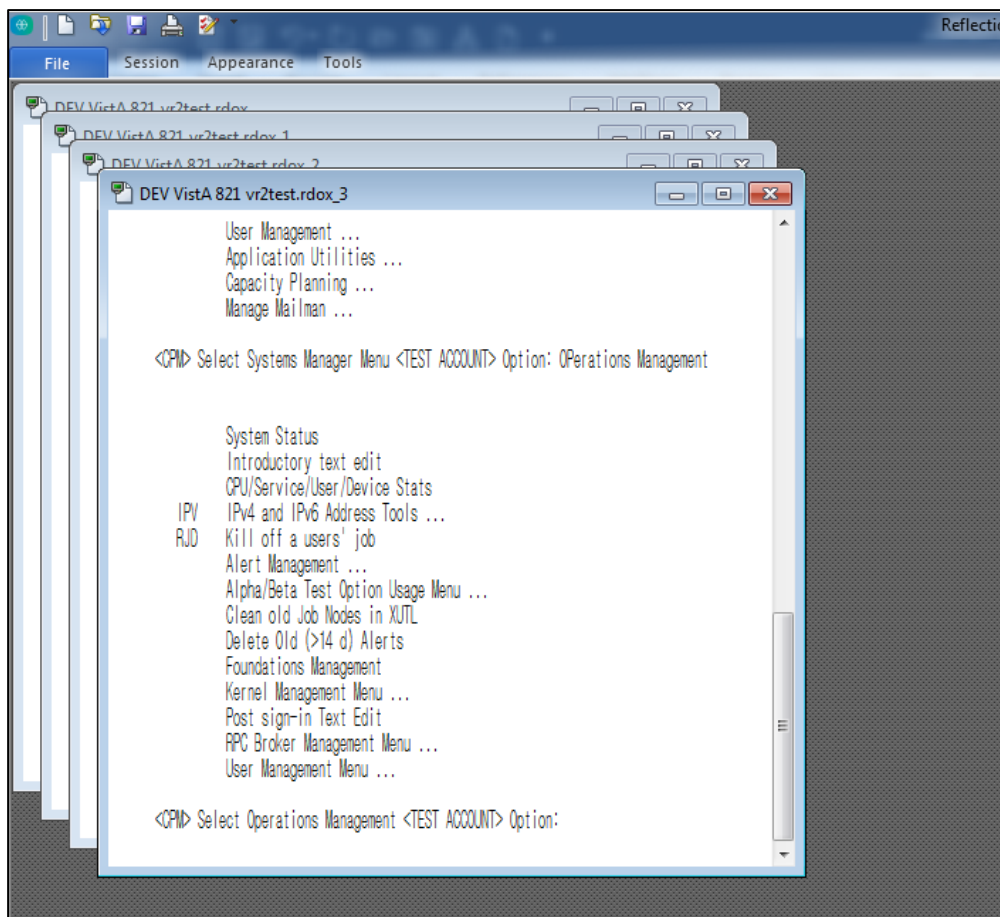
For CPAC users who need to view more than one simultaneous VistA session at the same site, arranging these sessions in a tile view must be done manually within Reflection during initial use of WebVRAM. The following steps will create a tile view for the remote VistA site connections the first time these connections are established. After configuring the view during the first connection to the remote site through WebVRAM, the tile view of up to four sessions will be presented automatically each time you use WebVRAM to establish multiple session connections to this same site.

To set up the tile view at additional remote sites, repeat these configurations steps during the first multi-session connection to each remote site established through WebVRAM.

These steps will set up the tile view configuration in Reflection for viewing multiple sessions at the same VistA site:

1. Launch the first session to connect to the remote site through WebVRAM. After Reflection opens and logs the user in, proceed to Step 2.
2. Launch a second, third, and, if needed, fourth session to the same site through WebVRAM. Reflection will now show all four sessions in a cascading view as shown below.

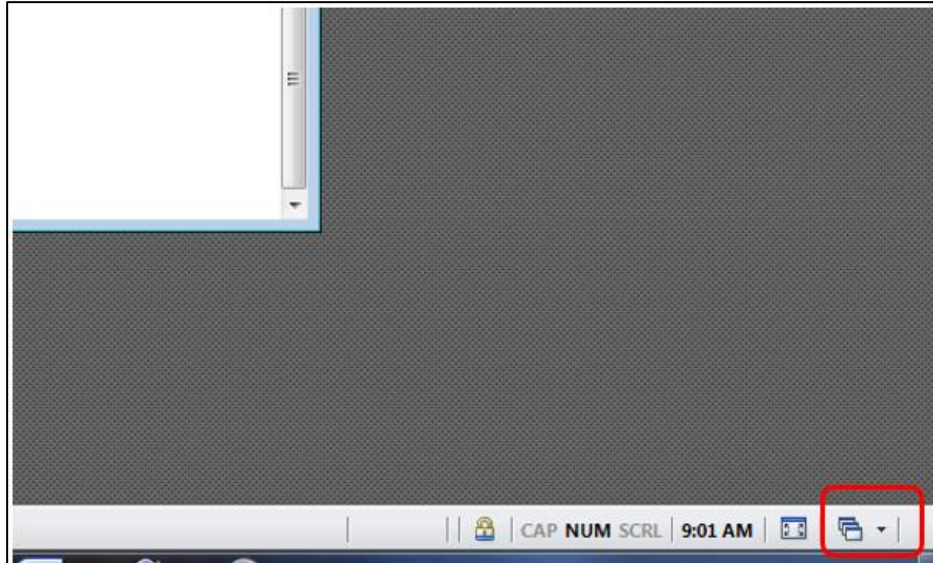
**Figure 30: Reflection – Cascading View of Multiple Same-site Sessions**



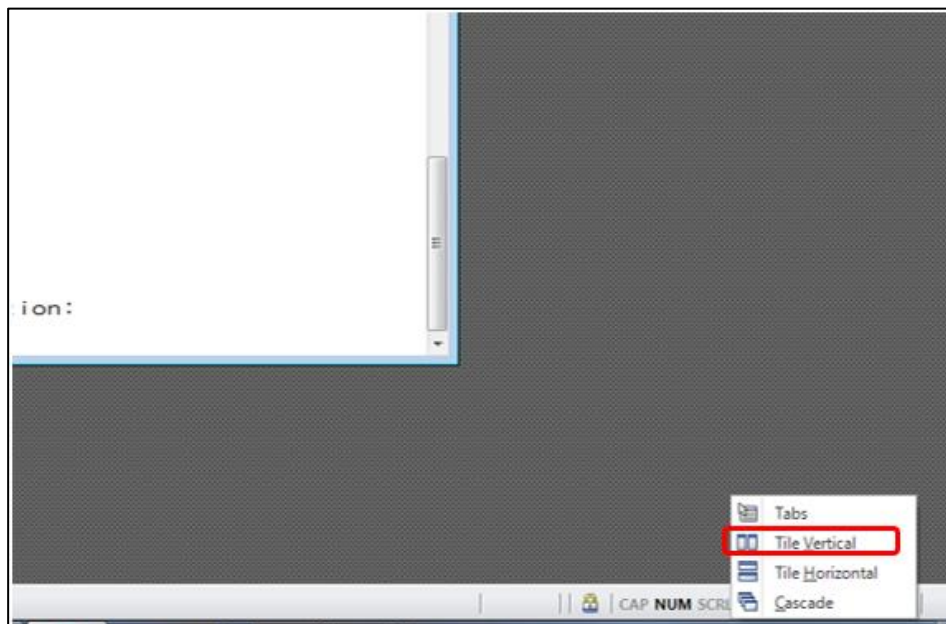


3. In the lower right-hand corner of the Reflection window, click on the **Arrange Windows icon**, and select **Tile Vertical** from the drop-down menu, as shown below.

**Figure 31: Reflection – Arrange Windows Icon and Drop-down**

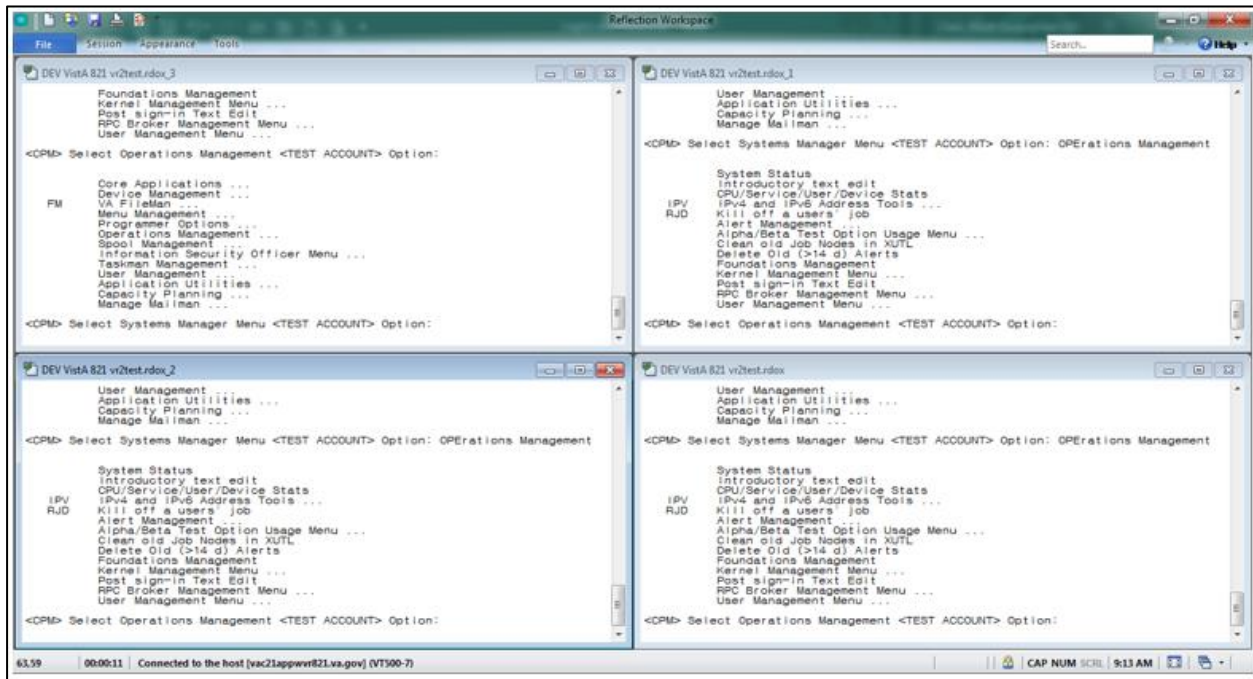


**Figure 32: Reflection – Arrange Windows Tile Vertical Selection**



4. With these selections, Reflection will present a tile view of all four sessions. Each session is shrunk in size to be fully visible within one quadrant of the screen.  
For a larger view of these sessions, click the **Full Screen icon** in the lower right-hand corner of the screen to the left of the Arrange Windows icon.

Figure 33: Reflection – Tile Vertical View



### 5.1.5 Launch Mode: CPRS

1. Login to WebVRAM.
2. From the WebVRAM home page, click on the Launch Mode drop-down and select **CPRS**.
3. Locate the Station Name of the remote VistA site to which to connect. Click on **Launch CPRS**. WebVRAM will launch CPRS and log the user into the remote VistA site that was selected.

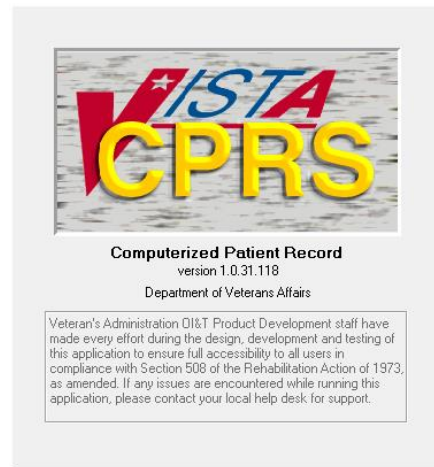
Figure 34: Launch CPRS Button

The screenshot shows the WebVRAM home page. The header includes the U.S. Department of Veterans Affairs logo and the WebVRAM title. The main content area is titled 'VistA Sites' and contains a search bar and a table of VistA sites. The 'Launch Mode' dropdown is set to 'CPRS'. The 'Launch CPRS' button for the first site, Beckley TEST, is highlighted with a red box.

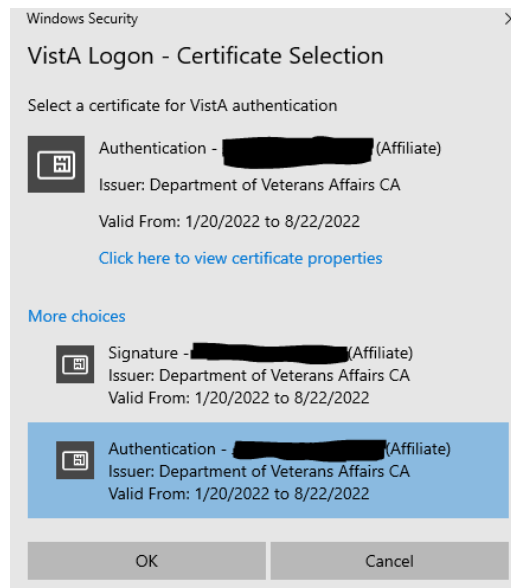
Station #	Station Name	VA Medical Center	VISN	State	Multi Select	Launch Site
517	Beckley TEST	Beckley VAMC	99	WV	<input type="checkbox"/>	<a href="#">Launch CPRS</a>
540	Clarksburg TEST	Louis A. Johnson VAMC	99	CA	<input type="checkbox"/>	<a href="#">Launch CPRS</a>
618	Minneapolis TEST	Minneapolis VA HCS	99	MN	<input type="checkbox"/>	<a href="#">Launch CPRS</a>
668	Spokane TEST	Mann-Grandstaff VAMC	99	WA	<input type="checkbox"/>	<a href="#">Launch Center</a>

4. WebVRAM R5.0 is now integrated with the IAM PIV 2FA login process. The **CPRS Version Screen** appears, along with the **Windows Security: VistA Login - Certificate Selection** screen as shown below.

**Figure 35: CPRS Version Screen**



**Figure 36: Windows Security: VistA Login - Certificate Selection screen**



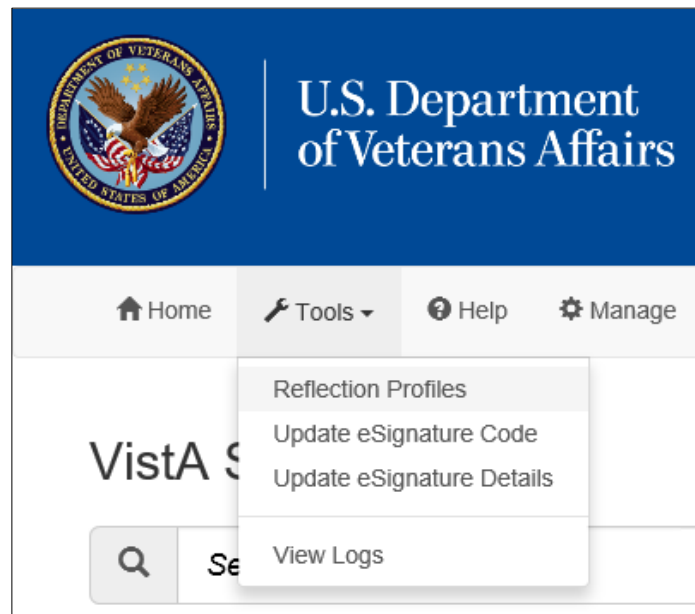
5. Select the Authentication Certificate and click **OK**. The CPRS VistA Login screen appears.
6. NOTE: If the user logged in to WebVRAM with Access and Verify Codes, the user needs to click on **Cancel** in the Windows Security screen. The user will then be prompted to enter the Access and Verify Code (of your Home VistA site) and click **OK**.
7. WebVRAM application will launch the user's desktop CPRS software and make the connection to the remote system where the user will be logged in for CPRS

access. Upon successful connection, the CPRS patient selection screen will appear.

### 5.1.6 Launch Mode: CPRS with Custom Reflection Profiles

1. Login to WebVRAM.
2. From the WebVRAM main page, click on **Tools** and select **Reflection Profiles** from the drop-down menu. The Reflection Profiles screen is displayed.

**Figure 37: Tools Menu, Reflection Profiles Option**



3. The Reflection Profiles screen will display a list of custom Reflection ".rdox" profiles. The default profile is: "SessionTemplate.rdox." There are additional profiles based on business processes.

**Figure 38: Reflection Profiles Screen**

Reflection Profiles

Previous 1 Next


Profile Name	File Name	Current Profile
AM Accounts Management CPAC	AM-Accounts-Management-CPAC.rdox	<input type="radio"/>
AM Accounts Management Follow Up Master	AM-Accounts-Management-Follow-Up-Master.rdox	<input type="radio"/>
AM Accounts Management Follow Up Refunds	AM-Accounts-Management-Follow-Up-Refunds.rdox	<input type="radio"/>
AM Accounts Management Payer Analysis	AM-Accounts-Management-Payer-Analysis.rdox	<input type="radio"/>
AM Accounts Management Refund Team	AM-Accounts-Management-Refund-Team.rdox	<input type="radio"/>
Billing HINES	Billing-HINES.rdox	<input type="radio"/>
OPECC Outpatient Pharmacy Electronic Claims Coordinators	OPECC-Outpatient-Pharmacy-Electronic-Claims-Coordinators.rdox	<input type="radio"/>
Session Template	SessionTemplate.rdox	<input checked="" type="radio"/>
UR Utilization Review	UR-Utilization-Review.rdox	<input type="radio"/>
VS Veterans Services CPAC	VS-Veterans-Services-CPAC.rdox	<input type="radio"/>
VS Veterans Services Master	VS-Veterans-Services-Master.rdox	<input type="radio"/>

Previous 1 Next

Update User Cancel

4. Select from the following Reflection VT Session files, then click the **Update User** button:
  - AM-Accounts-Management-CPAC.rdox
  - AM-Accounts-Management-Follow-Up-Master.rdox
  - AM-Accounts-Management-Follow-Up-Refunds.rdox
  - AM-Accounts-Management-Payer-Analysis.rdox
  - AM-Accounts-Management-Refund-Team.rdox
  - Billing-HINES.rdox
  - OPECC-Outpatient-Pharmacy-Electronic-Claims-Coordinators.rdox
  - SessionTemplate.rdox
  - UR-Utilization-Review.rdox
  - VS-Veterans-Services-CPAC.rdox
  - VS-Veterans-Services-Master.rdox
5. From the WebVRAM home page, click on the Launch Mode drop-down and select **CPRS**.
6. Locate the Station Name of the remote VistA site to which to connect. Click on **Launch CPRS**. WebVRAM will launch CPRS and log the user into the remote VistA site that was selected.

Figure 39: Launch CPRS Button



U.S. Department  
of Veterans Affairs

WebVRAM

Home

Tools

Help

Manage

Launch Mode: CPRS

Select All

Vista Sites

Search for...

Previous

1

Next

Station #	Station Name	VA Medical Center	VISN	State	Multi Select	Launch Site
517	Beckley TEST	Beckley VAMC	99	WV	<input type="checkbox"/>	<div>Launch CPRS</div>
540	Clarksburg TEST	Louis A. Johnson VAMC	99	CA	<input type="checkbox"/>	<div>Launch CPRS</div>
618	Minneapolis TEST	Minneapolis VA HCS	99	MN	<input type="checkbox"/>	<div>Launch CPRS</div>
668	Spokane TEST	Mann-Grandstaff VAMC	99	WA		<div>Launch Cerner</div>


Previous

1

Next

7. The CPRS version screen appears, along with the PIV Select a Certificate screen. Click **Cancel** on the PIV Select a Certificate screen, as shown below.

Figure 40: CPRS Version Screen



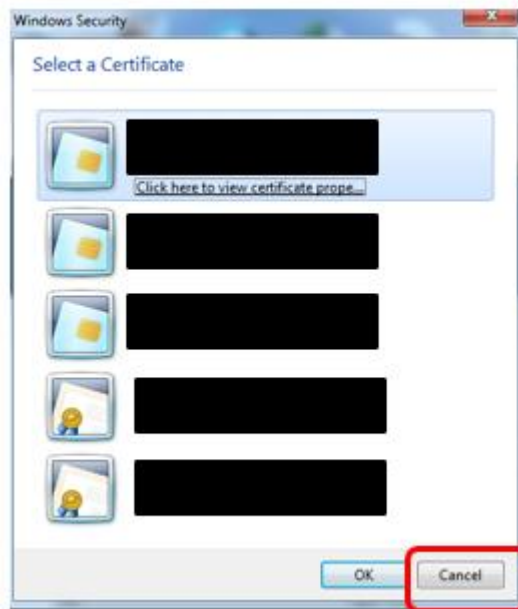
Computerized Patient Record

version 1.0.31.118

Department of Veterans Affairs

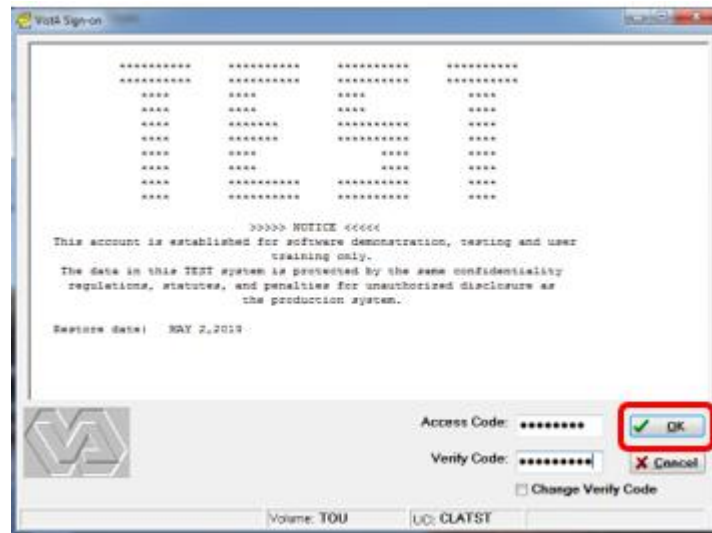
Veteran's Administration OI&T Product Development staff have made every effort during the design, development and testing of this application to ensure full accessibility to all users in compliance with Section 508 of the Rehabilitation Act of 1973, as amended. If any issues are encountered while running this application, please contact your local help desk for support.

**Figure 41: PIV Select a Certificate Screen**



8. The CPRS VistA Login screen appears. Enter your Access and Verify codes to the remote CPRS VistA site. Upon successful entry of those codes, the CPRS patient selection screen will appear.

**Figure 42: CPRS Login Screen**



9. The user is now able to use the selected Reflection Profile to perform business functions.

### **5.1.7 Launching Multiple CPRS Sessions**

Multiple CPRS sessions may be launched from the WebVRAM home page. Similar to launching different multiple Reflection sessions as discussed in Section 5.1.2, multiple



CPRS sessions to different VistA sites can be performed by changing the **Launch Mode** as outlined in Section 5.1.5 above, then clicking the checkboxes in the **Multi Select** column. Clicking the **Launch Selected** button will then launch simultaneous multiple CPRS sessions.



**CAUTION: Until WebVRAM is integrated with IAM services for 2FA PIV login, Access and Verify Codes must be entered into each CPRS Login session that opens to gain access to CPRS through that session.** With multiple sessions of CPRS launched at the same time, the login screens for each session may be hidden behind other open application windows on the desktop. Other application windows may need to be minimized to see all CPRS login sessions.

Also, the user may not be able to add Access and Verify codes to each login screen before one or more of them time out and must be relaunched. It is recommended that the user create a VistA “shortcut” Access/Verify (A/V) pair that can be copied and pasted into the Access Code field in each CPRS login window. This is done by combining the Access and Verify codes into a single A/V code “string” with the Access code separated from the Verify code in that string using a semi-colon. For example, if the user’s local VistA Access Code is **USER123** and the Verify Code is **LOGIN321**, then the combined A/V code string would be **USER123;LOGIN321**. This string can be pasted into the Access Code field of CPRS (or VistA, or any VistA integrated application, including WebVRAM) without the need to enter the Access and Verify codes separately in each field. Once it is pasted into the Access Code field, press **<Enter>** or click **OK** to login.

**Do not save the A/V code “string” on your local computer.** Follow VA procedures for protecting passwords. If password storage is needed, refer to the [VA Technical Reference Model \(TRM\)](#) to find approved password management software.

### 5.1.8 Access CPRS at Remote Sites Using CPRS Desktop Launcher

The WebVRAM application was not designed to be used at the same time as the CPRS Desktop Launcher to access CPRS patient data at remote sites. The CPRS Desktop Launcher is a separate application from WebVRAM, and it provides access to CPRS at remote sites using different pathways and connection features.

One of the security features of WebVRAM is setting a 30-day expiration date on each remote VistA profile created or updated when a user first connects to (synchronizes) a remote site through the WebVRAM application. By design and in keeping with VA security guidelines, if the remote VistA profile established by a user when first synchronizing to a remote site is not accessed through WebVRAM for 30 days after the initial connection is made, the remote VistA profile will terminate on day 31.



It has become common practice to connect to a remote site through WebVRAM to establish a remote VistA profile and instead of using WebVRAM to launch CPRS at that remote site after that, to use the CPRS Desktop Launcher to access patient records at that remote site. Then, after the WebVRAM synchronization first establishes the remote VistA profile, WebVRAM is no longer used to access CPRS at that remote site. If this practice is followed, the user must be aware of the following:

1. The VistA profile established at the remote site when the user connects through WebVRAM the first time will be terminated on day 31 after that “synchronization” event.
2. On day 31 after that synchronization, if the user does not synchronize to the remote site using WebVRAM on that day and tries to use only the CPRS Desktop Launcher to access patient records at that remote site, their CPRS login will be denied, and they will not be able to open CPRS at that site. This is because their VistA profile at that site will have been terminated at the end of the day before, and CPRS will not allow user access to the patient record at that site with a terminated VistA profile.
3. If a user wishes to use only the CPRS Desktop Launcher and not WebVRAM to access patient records at the remote site, they **MUST** synchronize to that remote site using WebVRAM at least every 29 days to keep their VistA profile active at that site. Performing a synchronization to the remote site to update the user’s VistA profile, and resetting a new 30-day expiration cycle, only takes a few seconds in WebVRAM and can be accomplished by selecting the **Synchronize** option from the Launch Mode drop-down, and then clicking the **Launch Synchronize** button associated with the remote site. It is NOT necessary to launch CPRS at the remote site and then login to CPRS to reset the VistA profile 30-day expiration date. This **must** be done at least **every 29 days** for each remote site the user accesses to continue using the CPRS Desktop Launcher to work with patient records at those sites.



**NOTE:** The VET-HOME Business Unit has an extended synchronization timeout of 90 days due to patient safety requirements of the providers in that business unit. The same restrictions apply with a 90-day window rather than a 30-day window for that business unit. An alert will be sent to VET-HOME providers who have not synchronized one or more sites within 85 to 90 days.

### 5.1.9 New VA EHR Integration with WebVRAM

As VistA sites convert from VistA CPRS to the New VA Electronic Health Record (EHR), WebVRAM will provide a mechanism for users to connect to the New VA EHR at those

sites, while continuing to give users the ability to connect to remote VistA systems they are authorized to access.



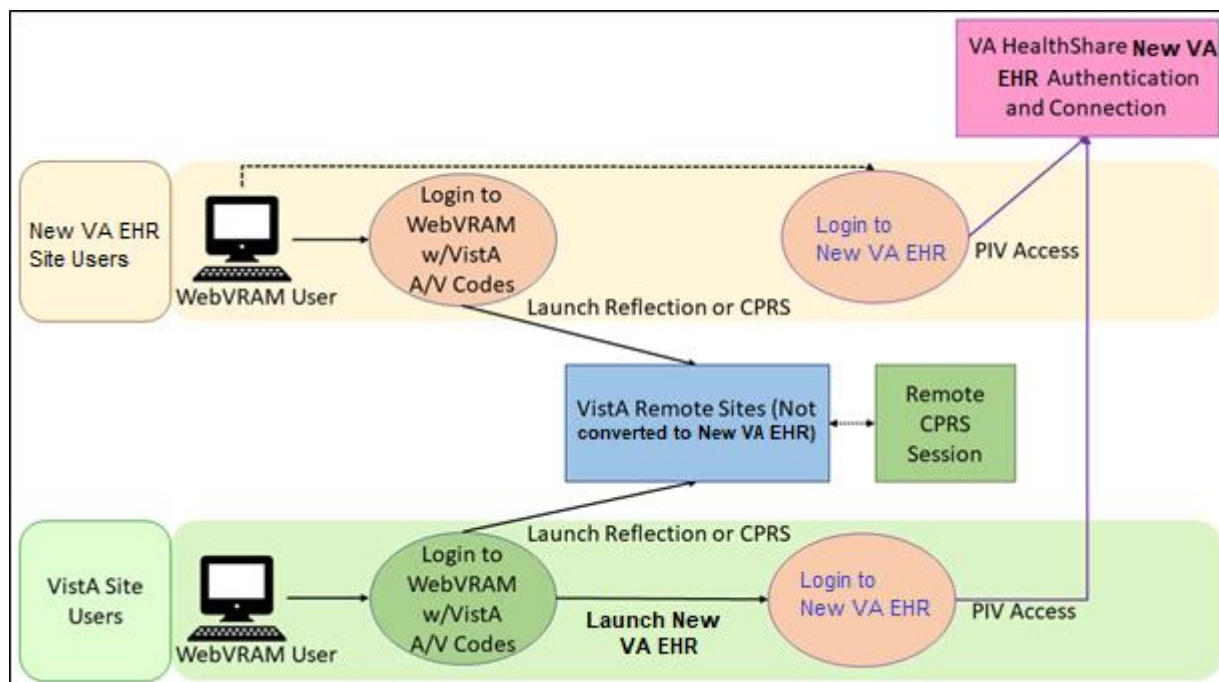
**NOTE:** Since the initial New VA EHR rollout will not replace all VistA functions, in addition to accessing the New VA EHR, the user can still access certain VistA functions at remote New VA EHR sites. Providers must use Joint Legacy Viewer (JLV) at a New VA EHR-converted site to view historical VistA patient data.

The user workflow is as follows:

1. Users whose Home VistA site has converted to New VA EHR will:
  - a. Access New VA EHR to conduct work at local site by directly navigating to the New VA EHR PIV login web page, not by going through WebVRAM.
  - b. Access remote New VA EHR sites from the Launch New VA EHR button on the WebVRAM site listing page.
  - c. Continue to access remote VistA sites through WebVRAM as usual.
2. Users whose Home VistA site is still using the VistA EHR (CPRS) will:
  - a. Continue to access local VistA directly, not through WebVRAM.
  - b. Access remote New VA EHR sites from the Launch New VA EHR button on the WebVRAM site listing page.
  - c. Continue to access remote VistA sites through WebVRAM as usual.

Figure 43 shows the user flow to access New VA EHR and remote VistA sites as VA locations are converted from the VistA EHR to the New VA EHR.

**Figure 43: WebVRAM New VA EHR Connections User Workflow**

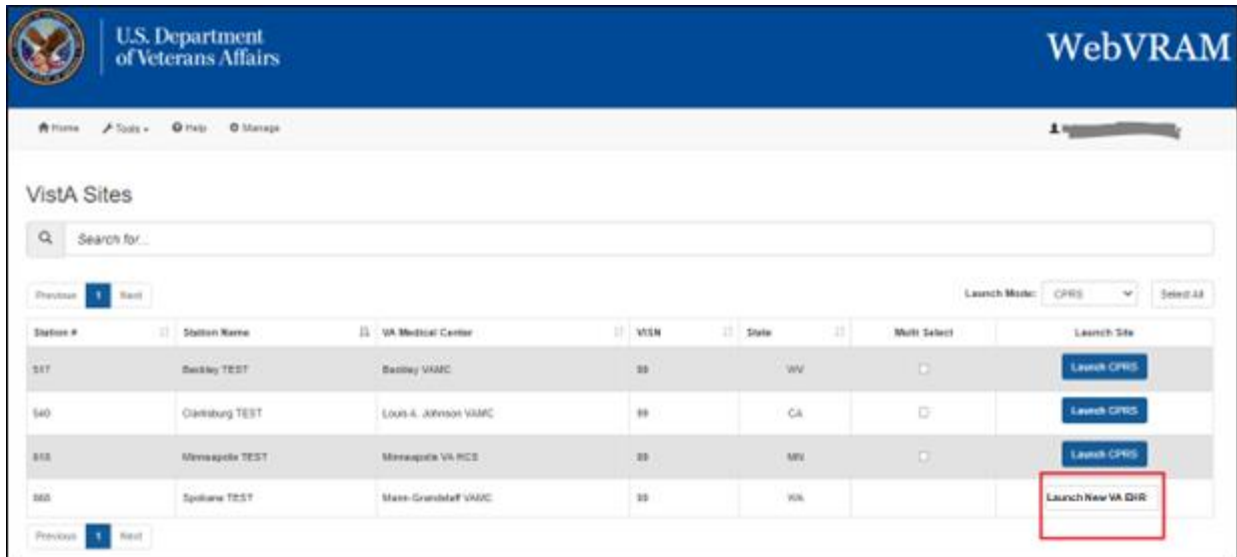


### 5.1.10 Launch New VA EHR Button

1. From the WebVRAM home page, select a remote site to which to connect. If that site has been converted to the New VA EHR, a **Launch New VA EHR** button will be displayed.

**i NOTE:** If a site has converted to the New VA EHR, the **Launch New VA EHR** button is displayed alongside the existing **Launch Reflection** button since the initial New VA EHR rollout will not replace all VistA functions. Sites that have not yet converted to New VA EHR do not have the **Launch New VA EHR** button available.

Figure 44: Launch New VA EHR Button



2. Selecting the **Launch New VA EHR** button will open a web browser session for the user to complete direct PIV login to the New VA EHR application at that site.

**Figure 45: New VA EHR PIV Login Screen**

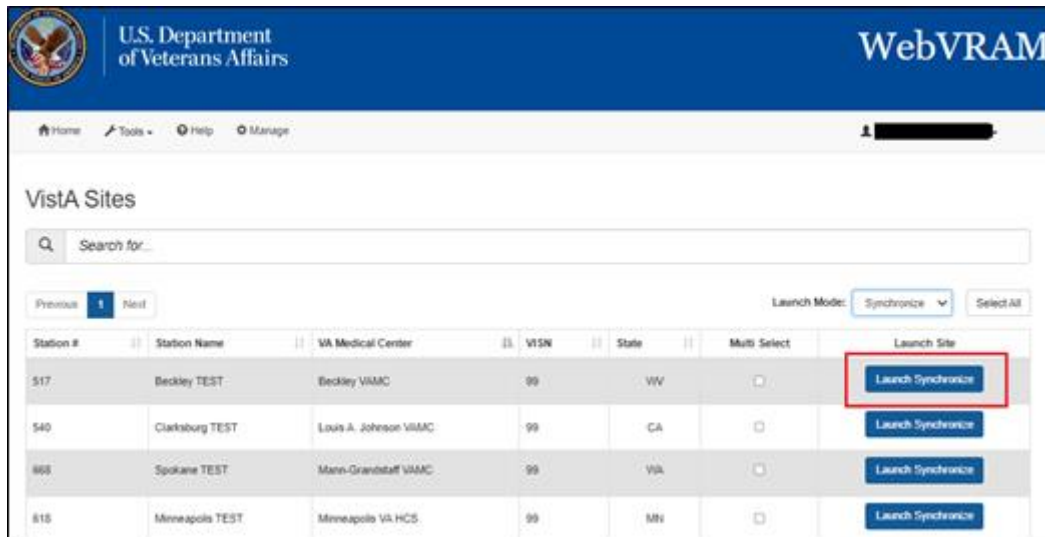


## 5.2 Launch Mode: Synchronize

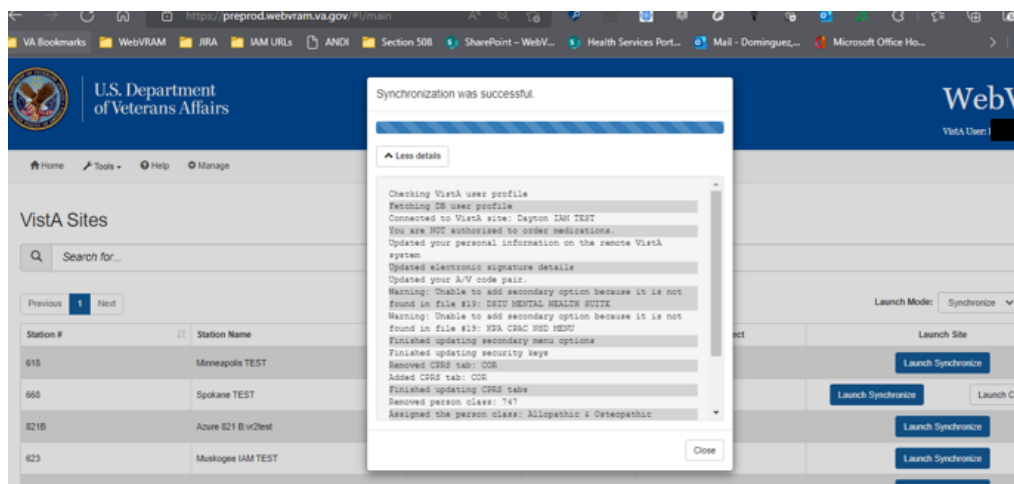
1. Login to WebVRAM.
2. From the WebVRAM home page, select the Launch Mode drop-down and select **Synchronize**. Then select the Station Name of the remote VistA site to which to connect.
3. Select the **Launch Synchronize** button.

4. WebVRAM will launch Synchronize to connect to the selected VistA site.
5. Synchronize updates and syncs up your personal information on the remote VistA system.

**Figure 46: Launch Synchronize Button**



**Figure 47: Launch Synchronize Successful**



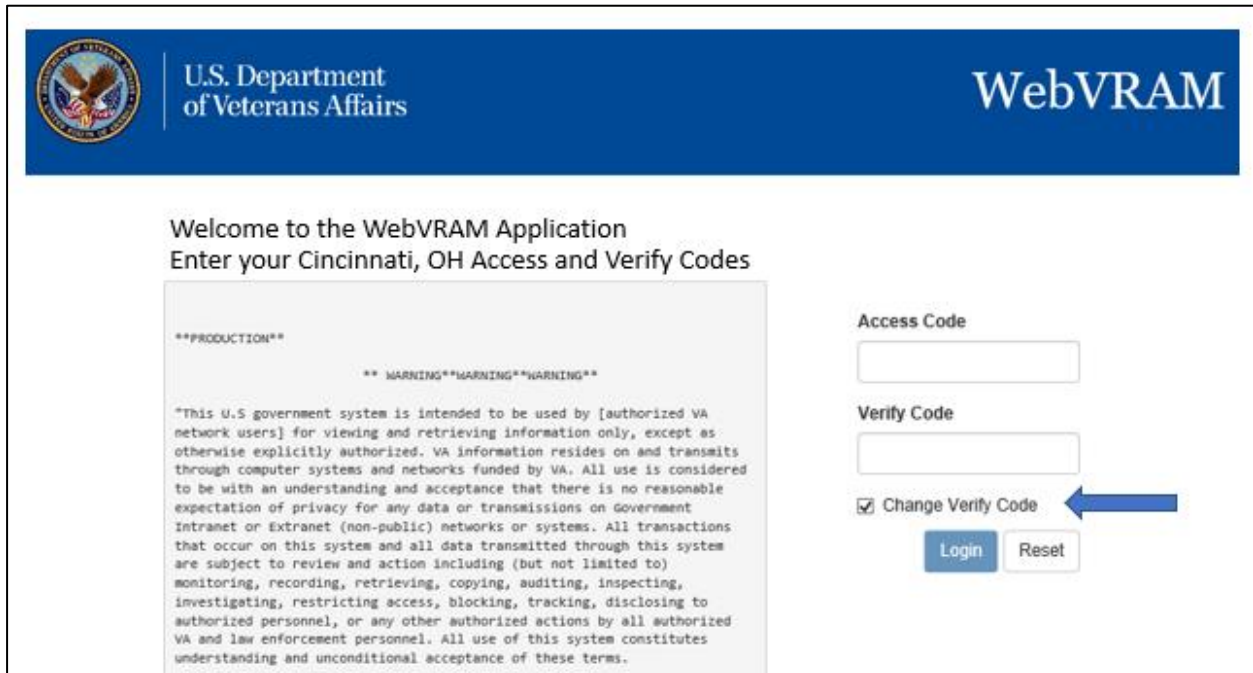
## 5.3 Changing Verify Code

This option allows the user to change their VistA Verify Code, as needed, using the WebVRAM application.

1. From Microsoft Edge browser, navigate to the [WebVRAM Home Page](#).
2. The Terms and Conditions web page is displayed. Click **Accept the Terms and Conditions**.

3. The Login page is displayed.
4. Enter your local VistA Access and Verify Codes and click the **Change Verify Code** checkbox.
5. Click **Login**.

**Figure 48: WebVRAM Login – Change Verify Code**



The screenshot shows the WebVRAM login interface. At the top, there is a blue header with the U.S. Department of Veterans Affairs logo on the left and the text 'U.S. Department of Veterans Affairs' and 'WebVRAM' on the right. Below the header, the main content area has a white background. On the left, there is a gray box containing a disclaimer:   
\*\*PRODUCTION\*\*  
\*\* WARNING\*\*WARNING\*\*WARNING\*\*  
"This U.S government system is intended to be used by [authorized VA network users] for viewing and retrieving information only, except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms."  
On the right, there are two input fields: 'Access Code' and 'Verify Code'. Below these fields is a checkbox labeled 'Change Verify Code' which is checked. A blue arrow points to this checkbox. Below the checkbox are two buttons: 'Login' and 'Reset'.

6. The user's VistA login screen is displayed, and the user follows the VistA prompts to create a new VistA Verify code.
7. Note that once the change has been made, your new Verify code will be required for all future logins to your local VistA system and the WebVRAM application.

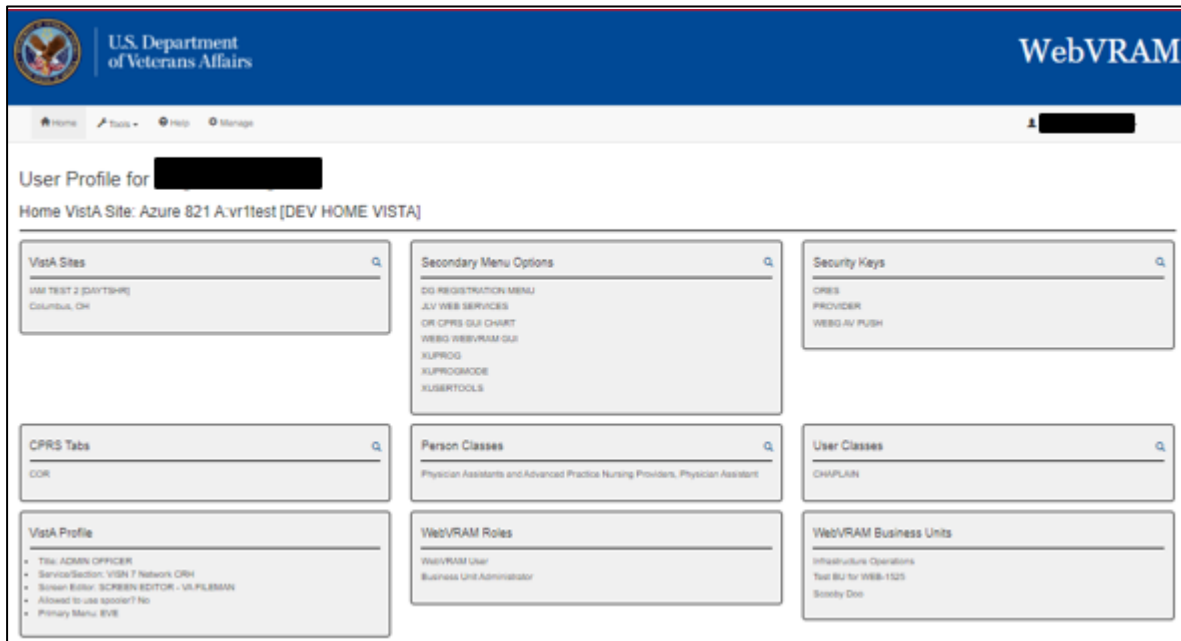
## 5.4 User Profile

To view the User Profile information, click on the Username located on the upper right-hand side of the application's page. The drop-down menu will display the following selections:

- My Profile
- My Business Units and Admins

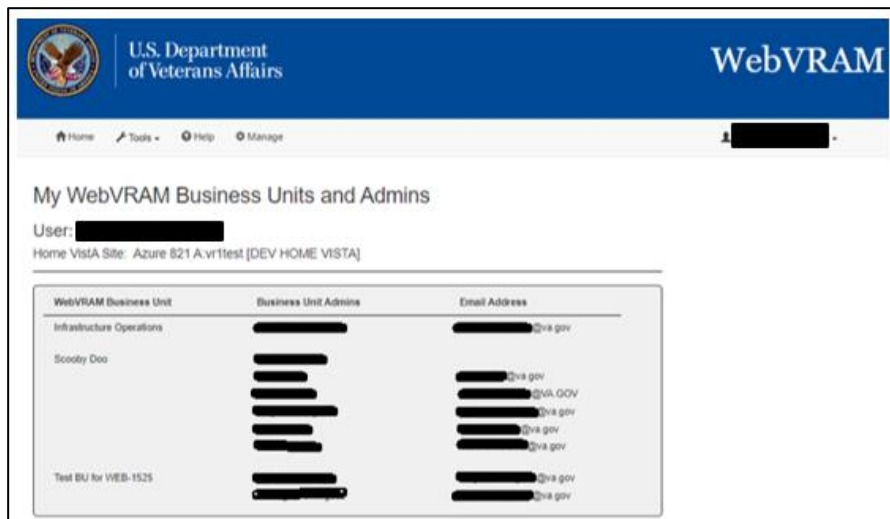
To view the user's profile, click on the Username and select **My Profile** from the drop-down menu; the browser will display the User's Profile page.

Figure 49: My Profile page



From the drop-down menu, click on the Username and select on **My Business Unit and Admins** from the drop-down menu; the browser will display the list of Business Units and BU Administrators for the user.

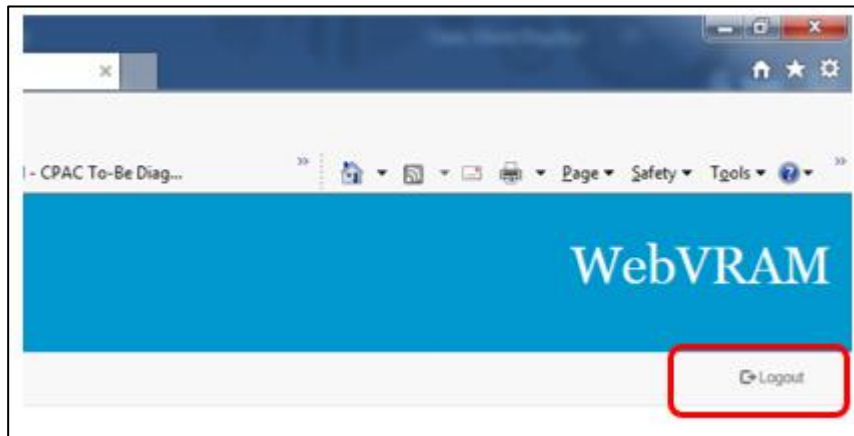
Figure 50: My Business Unit and Admins page



## 5.5 Exit System

When you are finished with the work you need to perform, click **Logout** in the upper right corner of the screen.

**Figure 51: WebVRAM Logout**



## 6. Troubleshooting

For troubleshooting, please contact the Enterprise Service Desk (ESD) at 1-855-673-4357.

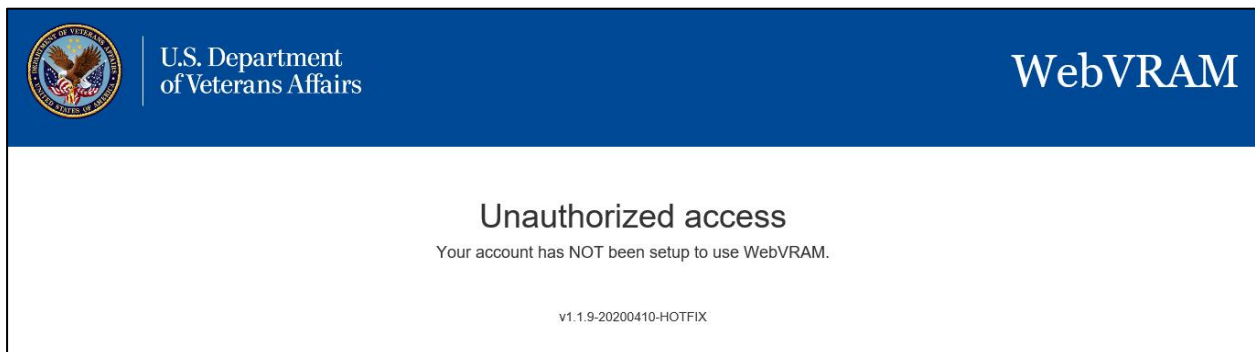
### 6.1 Special Instructions for Error Correction

#### 6.1.1 Unauthorized Access Error

If the user experiences an “Unauthorized Access” error when attempting to login to the WebVRAM application, their user profile has not yet been added to the WebVRAM User Table.

To resolve, the user should contact their business line manager and request that their user profile be added to the WebVRAM User Table by the business designated WebVRAM Business Unit Administrator.

**Figure 52: Unauthorized Access Error Message**



#### 6.1.2 Reflection Fails to Launch

If the user’s Reflection Desktop software fails to launch on their laptop or desktop, the user should create a ticket through Service Now (SNOW)/yourIT or phone the ESD to resolve the issue.



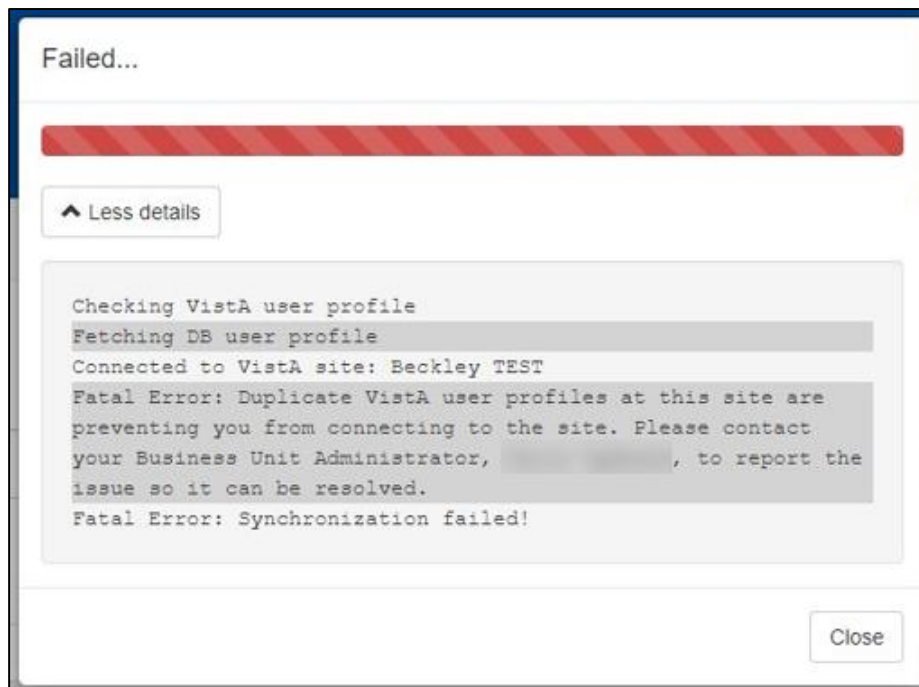
### 6.1.3 Duplicate VistA Accounts at Remote Site

WebVRAM will check for duplicate VistA profiles at remote sites that may interfere with a user's attempt to synchronize, add, or update VistA profile data at the remote site.

WebVRAM will display an error message (in a pop-up window) when a user attempts to connect to a remote site where potential duplicate VistA accounts are detected.

Contact your Business Unit Administrator for assistance in resolving duplicate VistA account errors. Do NOT open an ESD ticket; your Business Unit Administrator will open an ESD ticket if needed.

**Figure 53: Duplicate VistA Account Error**



### 6.1.4 Other Errors

For all other errors encountered during use of the WebVRAM application, create a ticket through Service Now (SNOW)/yourIT or phone the ESD.

**i NOTE:** Any errors encountered with CPRS or VistA once a remote connection is established by the WebVRAM application will need to be resolved by submitting a SNOW/yourIT ticket or phoning the ESD.

How to submit an ESD ticket using SNOW/yourIT for a WebVRAM issue:

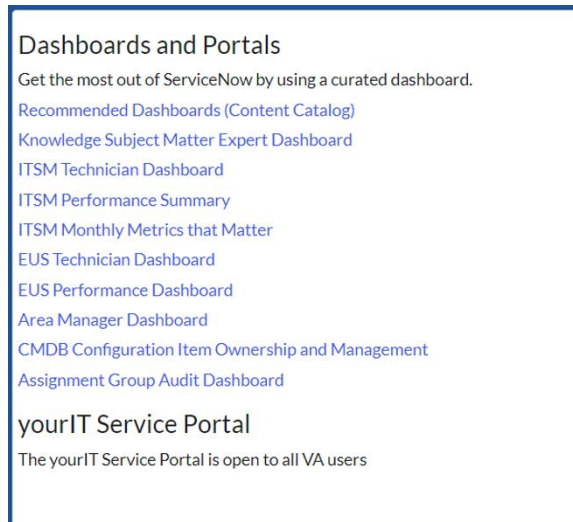
1. Double-click the yourIT icon on your desktop to open yourIT or go to the YourIT site in your browser.

**Figure 54: yourIT Desktop Icon**



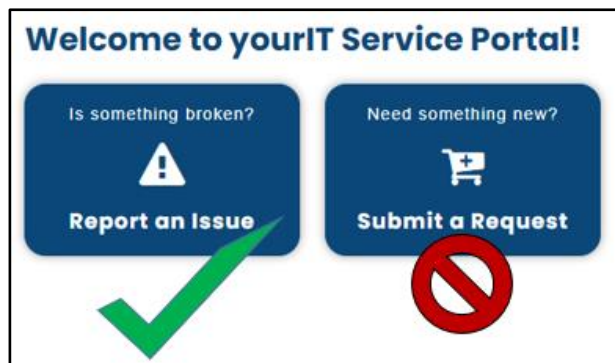
2. From the main ITIL User Dashboard page, select the link under yourIT Service Portal

**Figure 55: yourIT Desktop Icon**



3. Select the 'Report an Issue' button. Do not select 'Submit a Request'

**Figure 56: Report an Issue button**



4. Review the current issues list. If your issue is included, click the 'thumbs up' icon and close your browser. The issue is already being worked on. If your issue is not included, then click the 'Report a New Issue' button.

**Figure 57: Report a New Issue**

Are you experiencing any of the issues below?

New York, NY - HPI - Telecom - Available - Limited Functionality - New York Regional Benefit Office (New York, NY)  
Started 12/19/2023 1:43 PM EST | #INC30407953  
👍 I'm experiencing this too - report an issue for me

If you are not experiencing any of the issues listed, please continue to report a new issue. [Report a New Issue →](#)

5. Click the NO option when asked if your issue is related to Veteran's Benefit Management Systems (VBMS). WebVRAM is not associated to this application.

**Figure 58: Report a New Issue continued**

## Report an Issue

Is your issue related to Veterans Benefits Management System (VBMS) application? ⓘ

6. Fill in the Affected End User (\*Who are you submitting this issue for?), preferred contact method, phone number, and email address.

**Figure 59: User Information**

## Report an Issue

Request assistance with an issue you are having. An incident record will be created and managed through to successful resolution. You will also be notified of progress.

If your issue requires **IMMEDIATE** attention or if you need a password reset, please contact the Enterprise Service Desk. You may also access Self-Service for a 1 Day PIV Exemption at [AccessVA](#).

### User Information (Step 1 of 3)

\* Indicates a required field

\*Who are you submitting this issue for?

ⓘ [ ] ✕ ▾

\*Preferred Contact Method ⓘ

If "Other" is selected, please enter contact detail in Tell Us More field on next page. ✕

Email [ ] ▾

\*Best Follow-up Phone Number

(555 )555-5555

\*Email

example.user@va.gov

[Next Page: Issue Details](#)

7. Fill in the requested fields. Request that the ESD route the ticket to **SPM.Health.PCS.Sub\_4.WebVRAM**. For Category, select 'Software' and for Subcategory, select 'Web'. Enter the WebVRAM URL for the URL issue field.

**Figure 60: Report an Issue fields**

**Report an Issue**

Request assistance with an issue you are having. An incident record will be created and managed through to successful resolution. You will also be notified of progress.

If your issue requires **IMMEDIATE** attention or if you need a password reset, please contact the **Enterprise Service Desk** at (855) 673-4357. You may also access **Self-Service** for a 1 Day PIV Exemption at [AccessVA](#).

**Issue Details (Step 2 of 3)**

\* Indicates a required field

To comply with Personally Identifiable Information (PII) regulations, responses for this field should not disclose any information pertaining to personal identification such as social security number (SSN), passport number, driver's license, patient identification number, financial or credit numbers, etc.

\* Brief Description of Issue

Sample Issue

Articles that may help resolve your issue ▼

\* Is this issue happening at a VA Location? (If Telework, select No)

☐ Yes ☐ No

\* Tell us more about your issue including the best way to contact you

Sample Issue. Please route to SPM.Health.PCS.Sub\_4.WebVRAM

\* Category ⓘ

Please choose the category that most closely identifies your incident (Facility, Hardware, Security, Service, or Software). ✕

Software

\* Subcategory ⓘ

Please choose the subcategory that further explains your incident. ✕

Web

8. At the bottom of this page, add any relevant attachments and select 'Next Page: Further Details'

**Figure 61: Report an Issue fields cont'd**

If your issue requires **IMMEDIATE** attention or if you need a password reset, please contact the **Enterprise Service Desk**. You may also access **Self-Service** for a 1 Day PIV Exemption at [AccessVA](#).

\* Select the Name, EE Number and/or Hostname of your affected system

The device I am looking for is not on the list

Attachments (Optional)

Add file or drop files here

or

Add attachments

Previous Page: User Information

Next Page: Further Details

9. Select severity and 'no' for the active initiative field, and click Submit Issue.

**Figure 62: Further Details and Submit Issue**

## Report an Issue

Request assistance with an issue you are having. An incident record will be created and managed through to successful resolution. You will also be notified of progress.

**If your issue requires IMMEDIATE attention or if you need a password reset, please contact the Enterprise Service Desk. You may also access Self-Service for a 1 Day PIV Exemption at [AccessVA](#).**

### Further Details (Step 3 of 3)

\* Indicates a required field

\* Impact of Issue?

A Work Around is Available

Select if this issue relates to an active initiative (Optional)

-- None --

☐ Affects Informatics Patient Safety (Health IT, Vista/CPRS)

[Previous Page: Issue Details](#) [Submit Issue](#)

## A. Appendix A – Acronyms and Abbreviations

Acronyms and definitions are provided throughout the document with first use and are also collected in the table below.

**Table 3: Acronyms and Abbreviations**

<b>Term</b>	<b>Definition</b>
2FA	2-Factor Authentication
AD	Active Directory
ADPAC	Automated Data Processing Application Coordinator
BUA	Business Unit Administrator
CAC	Common Access Card
COR	Contracting Officer Representative or Clinical Orders Repository
CPAC	Consolidated Patient Account Center
CPRS	Computerized Patient Record System
EHR	Electronic Health Record
ePAS	Electronic Permission Access System
ESD	Enterprise Service Desk
ESO	Enterprise Security Operations
FISMA	Federal Information Security Management Act
FPO	Field Program Office
GAL	Global Address List
GUI	Graphical User Interface
HCS	Health Care System (large multi-site medical center)
IAM	Identify and Access Management
ICU	Intensive Care Unit
IEN	Internal Entry Number
ISSO	Information System Security Officer
IT	Information Technology
MHA	Mental Health Assistant (application launched from within CPRS)
NARS	National Automated Response System
NPI	National Provider Identifier
OCC	Office of Community Care
OCCHD	Office of Community Care Help Desk
OIT	Office of Information and Technology
PHI	Protected Health Information
PII	Personally Identifiable Information

Term	Definition
PIN	Personal Identification Number
PIV	Personal Identification Verification
PIV	Personal Identification and Validation
RPC	Remote Procedure Call
RPT	Not an acronym. This is Report tab in VistA
SDD	System Design Document
SNOW	Service Now, also called yourIT
SOP	Standard Operating Procedure
SQL	Structured Query Language
SSN	Social Security Number
SSO	Single Sign On
STIC	Station ID Callback Module
TELE	Short for Telemedicine
URL	Uniform Resource Locator
VAMC	VA Medical Center
VDL	VA Document Library
VHA	Veterans' Health Administration
VistA	Veterans' Health Information Systems and Technology Architecture
VM	Virtual Machine
VPN	Virtual Private Network
VRAM	VistA Remote Access Management
WAM	WebVRAM Administration Module
WEBG	<i>Not an acronym.</i> WEBG is the VistA namespace for the WebVRAM application, used to integrate the web software with VistA applications.
WebVRAM	Web VistA Remote Access Management
WUT	WebVRAM User Table