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

September 2025

Department of Veterans Affairs

Office of Information and Technology

Revision History

Date	Document Revision	Description	Author
9/25/2025	18.0	Updates for Release 18.0	WebVRAM Project Team
8/27/2025	17.0	Updates for Release 17.0 – Updated screenshots of older versions of WebVRAM	WebVRAM Project Team
5/29/2025	16.0	Updates for Release 16.0 – Updated Section 1.1 with note about disallowing EHR home site selection. Updated Section 5.1.7 Launching Multiple CPRS Sessions. Removed obsolete Caution statement.	WebVRAM Project Team
5/29/2025	15.1.0	Updates for Release 15.1.0 - Updated Section 5.2 – Launch Mode Synchronize. Updated Section 5.3.2 Expiring or Expired Verify Codes.	WebVRAM Project Team
4/24/2025	15.0	Updates for Release 15.0 - Updated Section 4.4.1 – Access Control Policy. Updated Section 5.1.1 – Launch Mode Reflection. Updated section 5.3.2 - Expiring or Expired Verify Codes. Added Section 6.1.4 Network Connectivity	WebVRAM Project Team
3/14/2025	14.0	Updates for Release 14.0 – Updated section 4.4.2 – Remote Sites Synchronization Updated Section 5.3 - Changing Verify Code and added sections 5.3.1- Changing Active Verify Code and 5.3.2 - Expiring or Expired Verify Codes	WebVRAM Project Team
1/8/2025	13.0.1	Updates for Release 13.0.1	WebVRAM Project Team
12/14/2024	13.0	Updates for Release 13.0	WebVRAM Project Team
11/13/2024	12.0.2	Updates for Release 12.0.2	WebVRAM Project Team
10/4/2024	12.0.1	Updates for Release 12.0.1	WebVRAM Project Team
9/23/2024	12.0	Updates for Release 12.0	WebVRAM Project Team
8/03/2024	11.0.5	Updated for Release 11.0.5. Added section 5.1.12 PSO/ WebVRAM PSDRPH Security Key	WebVRAM Project Team, VA OIT EPMO

7/24/2024	11.0.4	Updated for Release 11.0.4.	WebVRAM Project Team, VA OIT EPMO
7/4/2024	11.0.3	Updated for Release 11.0.3. Added section 5.1.9 Prescription Drug-Monitoring Program (PDMP)	WebVRAM Project Team, VA OIT EPMO
6/4/2024	11.0.2	Updated for Release 11.0.2.	WebVRAM Project Team, VA OIT EPMO
5/11/2024	11.0.1	Updated for Release 11.0.1	WebVRAM Project Team, VA OIT EPMO
5/11/2024	11.0	Updated for Release 11.0. Added new account request process to section 1. Quick Start Guide. Added section 4.4 Account Maintenance and Timeouts.	WebVRAM Project Team, VA OIT EPMO
4/12/2024	10.0.3	Updated for Release 10.0.3	WebVRAM Project Team, VA OIT EPMO
4/8/2024	10.0.2	Updated for Release 10.0.2	WebVRAM Project Team, VA OIT EPMO
3/12/2024	10.0.1	Updated for Release 10.0.1	WebVRAM Project Team, VA OIT EPMO
3/2/2024	10.0	Updated for Release 10.0.	WebVRAM Project Team, VA OIT EPMO
12/14/2023	9.0	Updated for Release 9.0. Updated Section 6.1.4. Other Errors 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 Section 2.4: System Maintenance	WebVRAM Project Team, VA OIT EPMO
12/20/2022	6.2	Release 6.2 changes: • Updated date info on cover page • Updated date on footers area • Updated Screenshot for: • Figure 8 - WebVRAM Home Screen • Figure 13 - Launch Reflection Button • Figure 23 – Launch CPRS button • Figure 28 – Launch CPRS Button • Figure 33 – Launch New VA EHR Button • Figure 35 – Launch Synchronize Button • Figure 36 – Launch Synchronize Successful • Figure 38 – My Profile Page • Figure 39 – My Business Unit and Admins Page	WebVRAM Project Team, VA OIT EPMO
10/05/2022	6.0	Updates for WebVRAM Release 6.0: • Updated screenshot for Figure 7: WebVRAM Home Screen • Added Section 5.3 User Profile	WebVRAM Project Team, VA OIT EPMO
9/6/2022	5.0.2	Updates for WebVRAM Release 5.0.2: Updated Screenshots for following: • Section 4, Figure 6, 6a: WebVRAM Login Screen • Section 5.1.17; added screenshot Figure 34a: Launch Synchronize Successful	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	Updated for WebVRAM Release 5.0, Added Section to Document IAM/PIV feature: 4.2. IAM / PIV Login - Link PIV to your Home VistA site 4.3.IAM / PIV Login – Login to WebVRAM with PIV Card Updated Section 5.1.2 to reflect new Launch CPRS workflow related to IAM/PIV feature, removed figure 25.	WebVRAM Project Team, VA OIT EPMO
2/23/2022	4.1	Added Quick Start Section 1 (Quick Start Guide).	WebVRAM Project Team, VA OIT EPMO
12/9/2021	4.0	Updated for WebVRAM Release 4.0, (associated with informational VistA patch WEBG*3*5): • Updated Section 3.5 (References and Resources) to replace "Rational" with "Jira." • Updated verbiage in Sections 4.1 (System Summary), 0 (Logging in to WebVRAM), and 6.3 (Changing Verify Code) to add Microsoft Edge as a supported internet browser. • Replaced Figure 8 (WebVRAM High-level System Interfaces). • Replaced Figure 9 (WebVRAM High-level Application Design) and updated Alt Text. • Replaced Figure 10 (WebVRAM Data Flow and User Navigation) and updated Alt Text. • Replaced Figure 11 (WebVRAM Terms and Conditions for Usage Screen). • Replaced Figure 12 (WebVRAM PIV Login Screen). • Added details to introduction of Section 5.4 (Account Maintenance and Timeouts • Access Control Policy – 90 Day Inactivity	WebVRAM Project Team, VA OIT EPMO

		• Access Control Policy and Procedures AC-2(3) requires accounts that have been inactive 90 days or more to be disabled. If a user does not log in within this time, their WebVRAM account will be disabled automatically. Warning emails will be automatically sent to users who approach account termination due to inactivity, with reminders sent after 80, 85, and 89 days of inactivity. If a user account is disabled, the user will need to contact their Business Unit Administrator to re-establish access to WebVRAM. Remote Sites 29 Day Synchronization Users must synchronize to each of their remote sites within 29 days of previous login. Accounts that have not synchronized to a given site will have their remote VistA Profile disabled at that site. This may be done by selecting 'Synchronize' on the Sites page, or by connecting to the site by CPRS or Reflections through WebVRAM. Please see section 5.1.8 for more details. • Using the Software). • Corrected step 3 of Section 5.1.8 (Access CPRS at Remote Sites Using CPRS Desktop Launcher); *a user MUST synchronize to a remote site using WebVRAM at least every **29** days to keep their VistA profile active at that site.* • Replaced Figure 51 (WebVRAM Login – Change Verify Code). • Added directions on how to submit a ticket to Enterprise Service Desk to Section 6.1.4 (Other Errors). • Removed references to Fee Basis Claims System (FBCS) from Sections 3.1 (System Summary), 3.3 (Data Flows), and Appendix 0 (Appendix A – Acronyms and Abbreviations). • Added "WEBG" to Appendix 0 (Appendix A – Acronyms and Abbreviations).	

4/8/2021	3.0	Updated for WebVRAM Release 3.0 (associated with VistA patch WEBG*3*1): • Added Section 5.1.8 (Access CPRS at Remote Sites Using CPRS Desktop Launcher). • Added note regarding use of Joint Legacy viewer to Section 5.1.9 (Prescription Drug-Monitoring Program (PDMP) • The Pharmacist and/or Provider can use the PDMP Query in CPRS at the remote VistA site, for all sites that have this capability integrated. • New VA EHR Integration with WebVRAM). • Edited note in Section 5.1.11 (Launch). • Added Section 6.1.3 (Duplicate VistA Accounts at Remote Site). • Retitled Section 6 to Appendix 0 (Appendix A – Acronyms and Abbreviations).	WebVRAM Project Team, VA OIT EPMO
10/22/2020	2.1	Updated for WebVRAM Release 2.0 (New VA EHR Integration): • Added information about DIVISION field to Section 4 (Getting Started), step 3. • Updated link to TRM in Section 5.1.7 (Launching Multiple CPRS Sessions). • Added Section 5.1.9 (Prescription Drug-Monitoring Program (PDMP) • The Pharmacist and/or Provider can use the PDMP Query in CPRS at the remote VistA site, for all sites that have this capability integrated. • New VA EHR Integration with WebVRAM) and subsection 5.1.11 (Launch).	WebVRAM Project Team, VA OIT EPMO

4/21/2020	2.0	Updated for WebVRAM Release 1.2 (associated with information-only patch WEBG*1.0*1): • Added NOTE regarding PIV linkage to Section 4 (Getting Started), step 4. • Added NOTE regarding accessing Home VistA to Section 0 (Logging in to WebVRAM), step 3. • Updated Figure 12 (WebVRAM PIV Login Screen). • Entirely rewrote Section 0 (Logging in to WebVRAM), step 5. • Updated Figure 15 (Tools Drop-down – Update eSignature Code). • Clarified verbiage in Section 4.1 (Update eSignature Code and Details), steps 1 and 3. • Added Section 5.1.1 (Launch Mode: Reflection), step 3. • Clarified verbiage in Section 5.1.5 (Launch Mode: CPRS), steps 3, 4, and 5. • Added Section 5.1.6 (Launch Mode: CPRS with Custom Reflection Profiles). • Added Figure 55 (Unauthorized Access Error Message). • Various minor formatting and verbiage changes.	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 4.1.1.2.1 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	Updated Section 1.2.2 Assumptions and Section 3 Getting Started. Added Section 3.2 Update eSignature Code and Details. Technical Writer review and edit.	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

1. Quick Start Guide 15
   1.1 How to Request Access to WebVRAM Screen 15
   1.2 WebVRAM Invitation 16
   1.3 Request Access Directly to BU Director 17
2. Introduction 21
   2.1 Purpose 21
   2.2 Document Orientation 22
      2.2.1 Organization of the Manual 22
      2.2.2 Assumptions 22
      2.2.3 Coordination 22
   2.3 Disclaimers 22
      2.3.1 Software Disclaimer 22
      2.3.2 Documentation Disclaimer 23
   2.4 Documentation Conventions 23
   2.5 References and Resources 23
   2.6 Enterprise Service Desk and Organizational Contacts 24
3. System Maintenance 24
   3.1 System Summary 24
   3.2 System Configuration 24
   3.3 Data Flows 25
   3.4 User Access Levels 27
   3.5 Continuity of Operation 28
4. Getting Started 28
   4.1 Update eSignature Code and Details 32
   4.2 IAM / PIV Login - Link PIV to your Home VistA site 35
   4.3 IAM / PIV Login – Login to WebVRAM with PIV Card 36
   4.4 Account Maintenance and Timeouts 39
      4.4.1 Access Control Policy – 90 Day Inactivity 39
      4.4.2 Synchronization 39
      4.4.3 Remote Site Refresh Process 39
      4.4.4 Remote Site Refresh Log Screen 41
5. Using the Software 43
   5.1 Remote Session: Launch Mode 43
      5.1.1 Launch Mode: Reflection 44
      5.1.2 Launching Different Multiple Remote VistA Sessions 46

5.1.3 Launching Simultaneous Multiple VistA Sessions at a Single Site 47
5.1.4 CPAC Users: Configure Tile View for Multiple VistA Sessions at the Same Site 50
5.1.5 Launch Mode: CPRS 53
5.1.6 Launch Mode: CPRS with Custom Reflection Profiles 55
5.1.7 Launching Multiple CPRS Sessions 59
5.1.8 Access CPRS at Remote Sites Using CPRS Desktop Launcher 59
5.1.9 Prescription Drug-Monitoring Program (PDMP) 60
5.1.10 New VA EHR Integration with WebVRAM 60
5.1.11 Launch New VA EHR Button 61
5.1.12 PSO/WebVRAM PSDRPH Security Key 62
5.2 Launch Mode: Synchronize 62
5.3 Changing Verify Code 64
5.3.1 Changing Active Verify Code 64
5.3.2 Expiring or Expired Verify Codes 66
5.4 User Profile 67
5.5 Exit System 69
6. Troubleshooting 69
6.1 Special Instructions for Error Correction 69
6.1.1 Unauthorized Access Error 69
6.1.2 Reflection Fails to Launch 70
6.1.3 Duplicate VistA Accounts at Remote Site 71
6.1.4 Network Connectivity 71
6.1.5 Other Errors 72

List of Figures

Figure 1: How to Request Access to WebVRAM Screen 15
Figure 2: WebVRAM Business Units List 16
Figure 3: Confirmation 16
Figure 4: Micro Focus Reflection File Open Setting Change, 1 of 4 18
Figure 5: Micro Focus Reflection File Open Setting Change, 2 of 4 19

Figure 6: Micro Focus Reflection File Open Setting Change, 3 of 4....19
Figure 7: Micro Focus Reflection File Open Setting Change, 4 of 4....20
Figure 8: WebVRAM High-level System Interfaces....25
Figure 9: WebVRAM High-level Application Design....26
Figure 10: WebVRAM Data Flow and User Navigation....27
Figure 11: WebVRAM Terms and Conditions for Usage Screen....28
Figure 12: WebVRAM PIV Login Screen....29
Figure 13: Other Sign-In Options window – AV code....29
Figure 14: WebVRAM A/V Code Login Screen....30
Figure 15: Other Sign-In Options window - Network ID....30
Figure 16: User ID and Password login boxes....31
Figure 17: WebVRAM Home Screen....32
Figure 18: Tools Drop-down – Update eSignature Code....32
Figure 19: Update eSignature Code Screen....33
Figure 20: Update eSignature Details....34
Figure 21: Terms and Conditions....35
Figure 22: Sign In With VA PIV Card....35
Figure 23: PIV Card Not Linked Error....36
Figure 24: VA Single Sign-On page....36
Figure 25: WebVRAM Terms and Conditions page....37
Figure 26: WebVRAM PIV Card Sign-in page....37
Figure 27: ActivClient Login....38
Figure 28: WebVRAM Application Home Page....38
Figure 29: Remote Site Refresh In process....40
Figure 30: Remote Site Refresh Success Banner....40
Figure 31: Remote Site Refresh error banner....40
Figure 32: Accessing Remote Site Refresh Log from View Logs button....41
Figure 33: Remote Site Refresh Log page....42
Figure 34: Detailed Site Refresh Log....42
Figure 35: Accessing Remote Site Refresh Log from Tools menu....42
Figure 36: Launch Mode Drop-down....44
Figure 37: Launch Reflection Button....45
Figure 38: VistA Login....46
Figure 39: Launch Multiple Reflection Sessions to Different Remote VistA Systems....46
Figure 40: Reflection Workspace Settings Access....48
Figure 41: Reflection – Configure User Interface Link....49
Figure 42: Reflection – Change User Interface Mode....50
Figure 43: Reflection – Cascading View of Multiple Same-site Sessions....51
Figure 44: Reflection – Arrange Windows Icon and Drop-down....52
Figure 45: Reflection – Arrange Windows Tile Vertical Selection....52

Figure 46: Reflection – Tile Vertical View 53
Figure 47: Launch CPRS Button 53
Figure 48: CPRS Version Screen 54
Figure 49: Windows Security: VistA Login - Certificate Selection screen 55
Figure 50: Tools Menu, Reflection Profiles Option 55
Figure 51: Reflection Profiles Screen 56
Figure 52: Launch CPRS Button 57
Figure 53: CPRS Version Screen 58
Figure 54: PIV Select a Certificate Screen 58
Figure 55: CPRS Login Screen 59
Figure 56: WebVRAM New VA EHR Connections User Workflow 61
Figure 57: Launch New VA EHR Button 61
Figure 58: New VA EHR PIV Login Screen 62
Figure 59: Launch Synchronize Button 63
Figure 60: Launch Synchronize Successful 63
Figure 61: Multi Select 64
Figure 62: Select All 64
Figure 63: Other Sign-In Options 65
Figure 64: WebVRAM Login – Change Verify Code 65
Figure 65: Update Access and Verify Code 66
Figure 66: Verify Code Expiring Soon Window 66
Figure 67: Change Verify Code - Expired Code PIV login 67
Figure 68: My Profile page 68
Figure 69: My Business Unit and Admins page 68
Figure 70: WebVRAM Logout 69
Figure 71: Unauthorized Access Error Message 70
Figure 72: Duplicate VistA Account Error 71
Figure 73: yourIT Desktop Icon 72
Figure 74: yourIT Desktop Icon 72
Figure 75: Report an Issue button 73
Figure 76: Report a New Issue 73
Figure 77: Report a New Issue continued 73
Figure 78: User Information 74
Figure 79: Report an Issue fields 74
Figure 80: Report an Issue fields cont'd 75
Figure 81: Further Details and Submit Issue 75

List of Tables

Table 1: Documentation Symbols and Descriptions 23
Table 2: Enterprise Service Desk Support Information 24
Table 3: Acronyms and Abbreviations 76

1. Quick Start Guide

1.1 How to Request Access to WebVRAM Screen

When a user who does not have access to WebVRAM attempts to open the website, a message appears with instructions on how to gain access.

Figure 1: How to Request Access to WebVRAM Screen

Users should click the *Business Units* link to see a list of all existing active WebVRAM Business Units and their directors. Click on the appropriate business unit's Request Access button to send a request for access to the director and CC'd to the Business Unit's Administrators (BUA). If your organization does not appear on the list, the document linked on the screen will open the *Process to Add a New Business Unit to WebVRAM* Portable Digital Format (pdf) document.

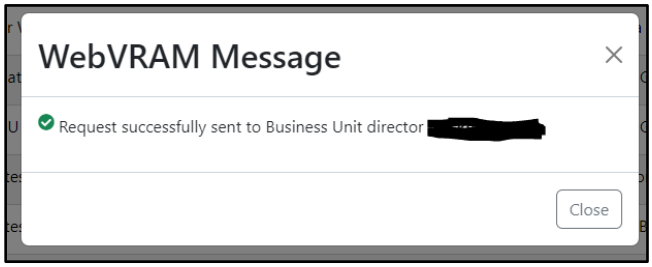
IMPORTANT: Any new user must have an enabled Active Directory profile and active home VistA account and must be able to access it with Access and Verify codes to use this process.

IMPORTANT: Users will not be able to select a Home VistA site that has been converted to the VA EHR site. Users will need to select a different site that is not a VA EHR site.

Figure 2: WebVRAM Business Units List

A confirmation window appears notifying the user that the request has been sent. Once the request is approved, the Business Unit Administrator will create and update the user's WebVRAM Profile and provision their approved remote VistA Sites. The user will then be able to log into WebVRAM.

Figure 3: Confirmation



1.2 WebVRAM Invitation

Alternately, a user may receive an invitation email from their BUA asking them to join WebVRAM. In this case, the BUA will already have approval from the Business Unit Director. The email will contain a Request Access link. This link will be valid for 24 hours and will be uniquely keyed to the invited user. Do not forward this link to anyone else, it will only work for the user it was sent to and only for 24 hours. Fill out the linked form with the requested information and submit your request.

IMPORTANT: Any new user must have an enabled Active Directory profile and active home VistA account and must be able to access it with Access and Verify codes to use the invitation process.

1.3 Request Access Directly to BU Director

To directly request access to WebVRAM, follow these 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 Enterprise Service Desk (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 completed the required TMS training course WebVRAM for Users Training (VA 4553089) and submitted the certificate to their Business Unit Administrator (BUA).
5. A user must have the **WEBG WEBVRAM GUI** *Secondary Menu Option* added to their 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.
6. 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 to 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.
7. When steps 1 – 6 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.
8. 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 link the PIV card, follow the instructions in the Service Now (SNOW)/yourIT 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.

9. 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 4: Micro Focus Reflection File Open Setting Change, 1 of 4

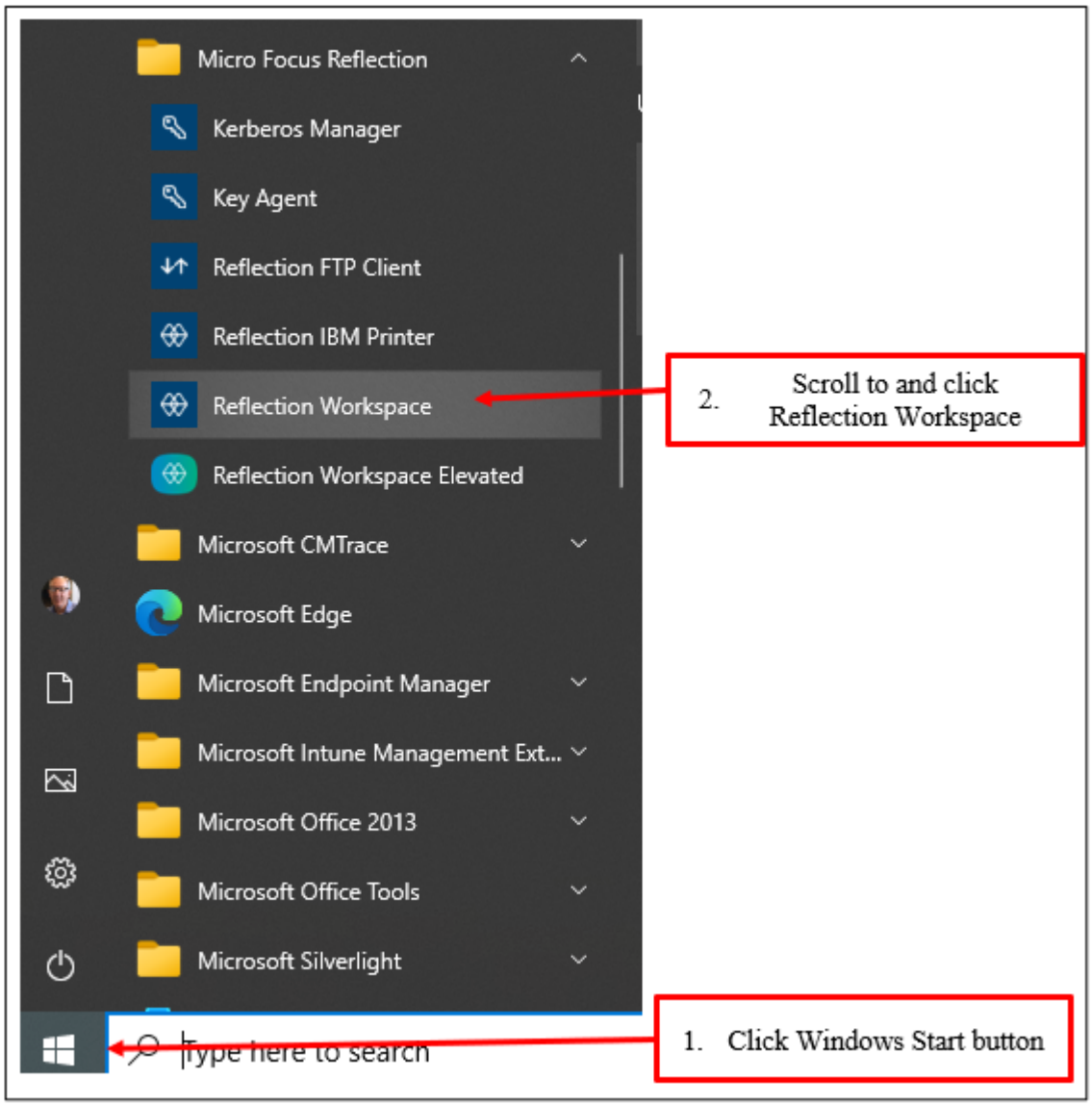


Figure 5: Micro Focus Reflection File Open Setting Change, 2 of 4

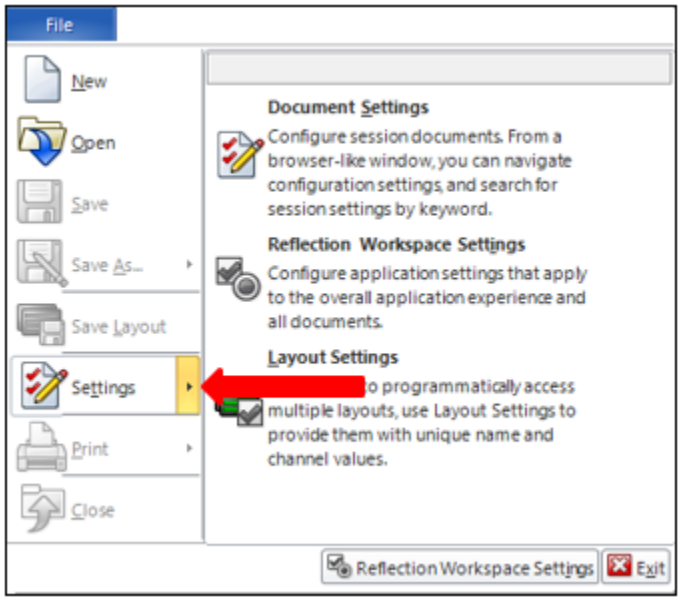


Figure 6: Micro Focus Reflection File Open Setting Change, 3 of 4

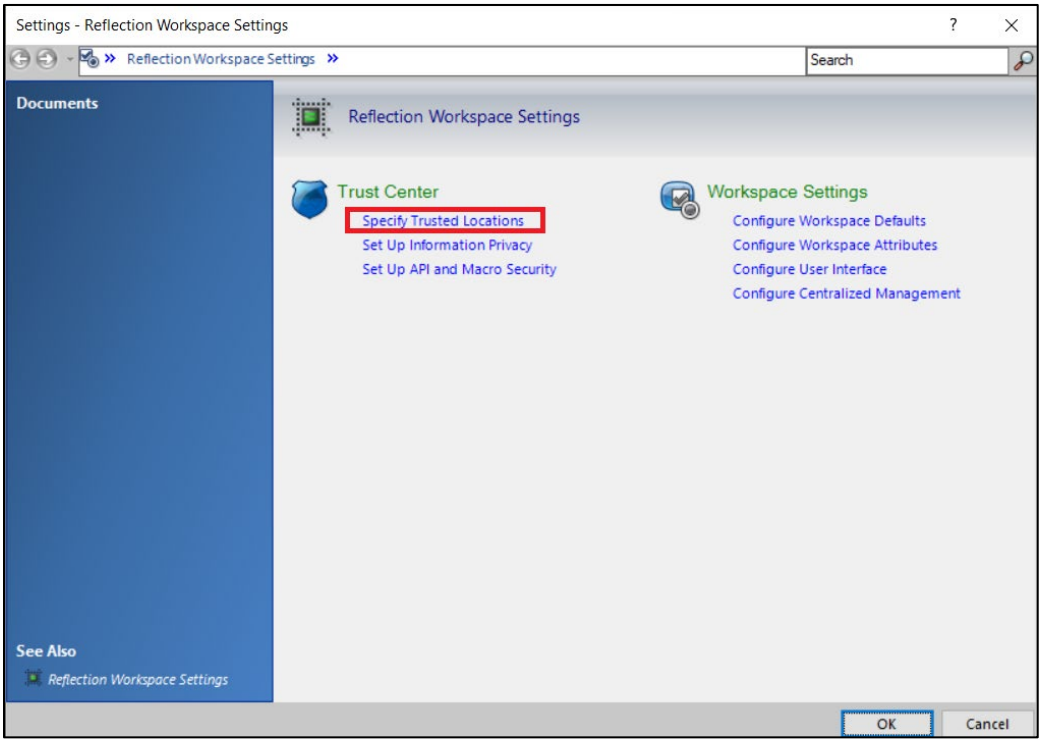
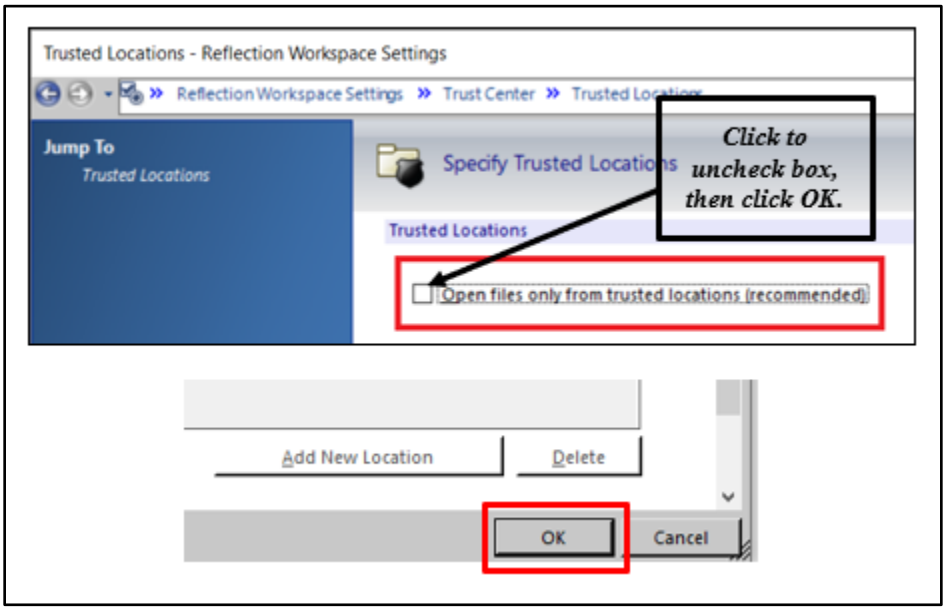


Figure 7: Micro Focus Reflection File Open Setting Change, 4 of 4



10. 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.

11. 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.

12. 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 2.6.

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
	**NOTE:** Used to inform the reader of general information including references to additional reading material.
	**CAUTION:** 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.

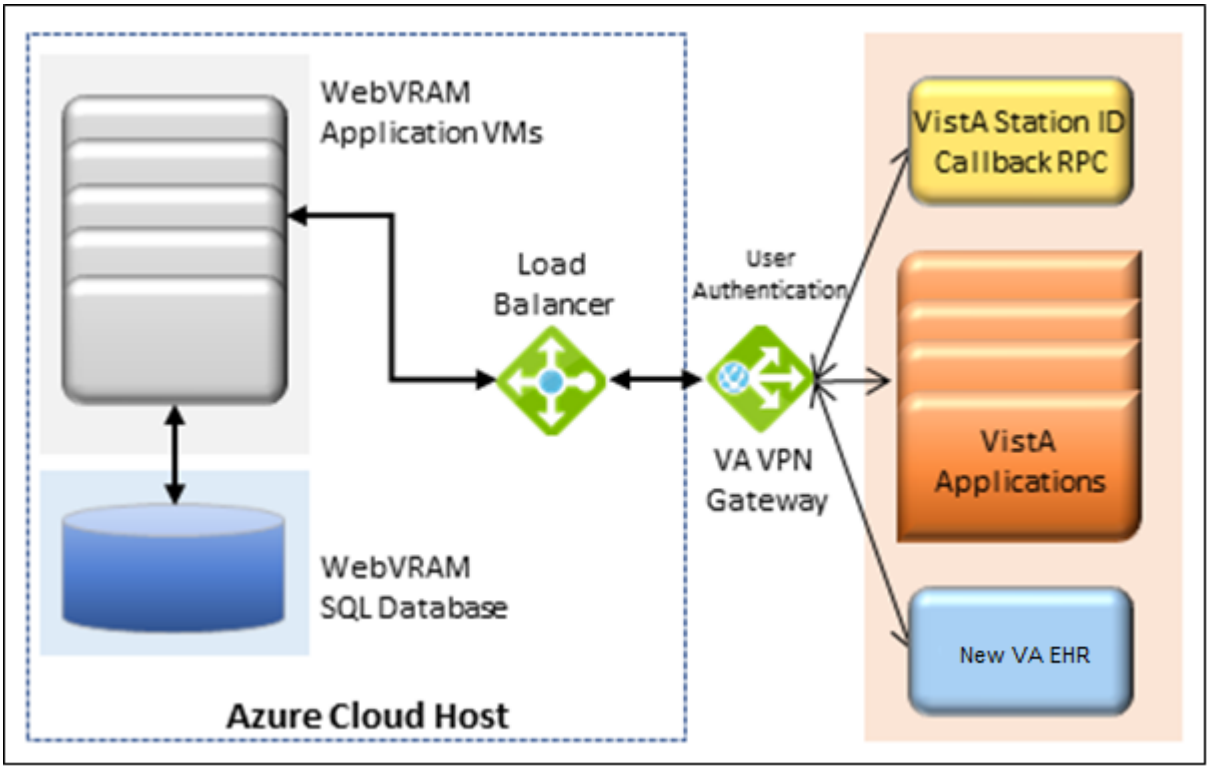
3.2 System Configuration

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 8. 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.

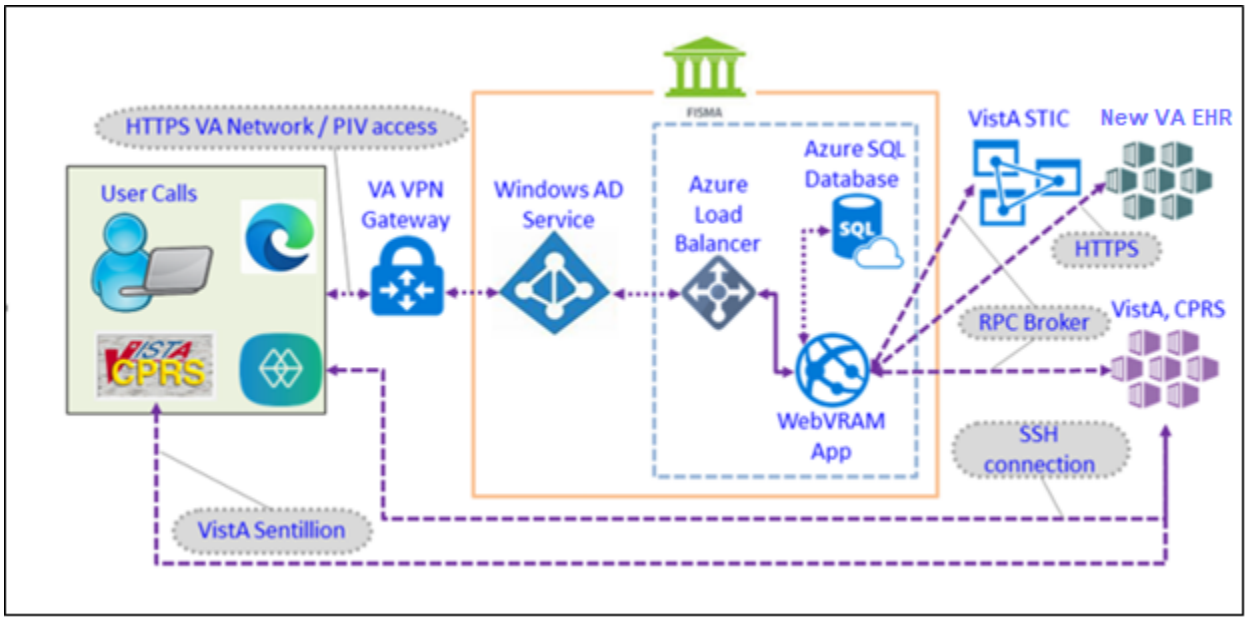
Figure 8: WebVRAM High-level System Interfaces



3.3 Data Flows

Figure 9 provides a high-level architectural view of the WebVRAM solution. A discussion follows this diagram regarding data flows from a user perspective.

Figure 9: WebVRAM High-level Application Design



Using their local VistA Access and Verify codes, the user logs in to the WebVRAM application through the VA intranet portal Uniform Resource Locator (URL) or web address. The application calls the STIC to check the user's local VistA system and validates user credentials. If a user's local VistA profile is active, the user profile is retrieved from the local VistA system and sent to the WebVRAM application for storage in the WebVRAM User Table.

The user profile includes:

- VistA authorized menus and keys
- Electronic signature
- User title
- Service/section
- Name
- Degree
- National Provider Identifier (NPI)
- NPI Status

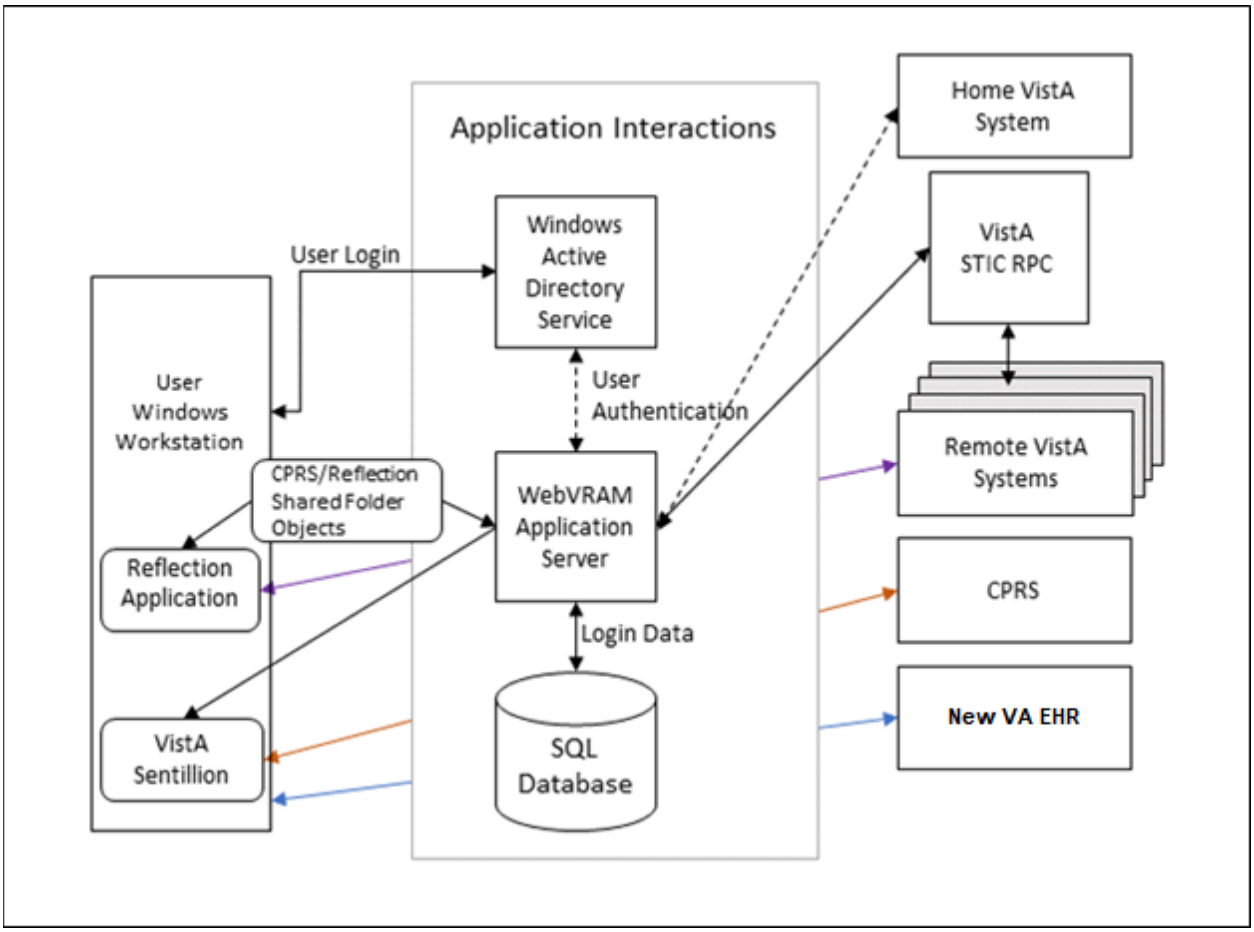
After the user is verified as an authorized user, the user is logged into the WebVRAM GUI and allowed to select or identify the remote VistA system(s) and is approved by their business line management to access. During user login, the application captures and stores the user login transaction, including date/time of login and user identifiers in

an SQL database for auditing purposes. No Personally Identifiable Information (PII) is included in the login stored transaction.

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 10 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 10: 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

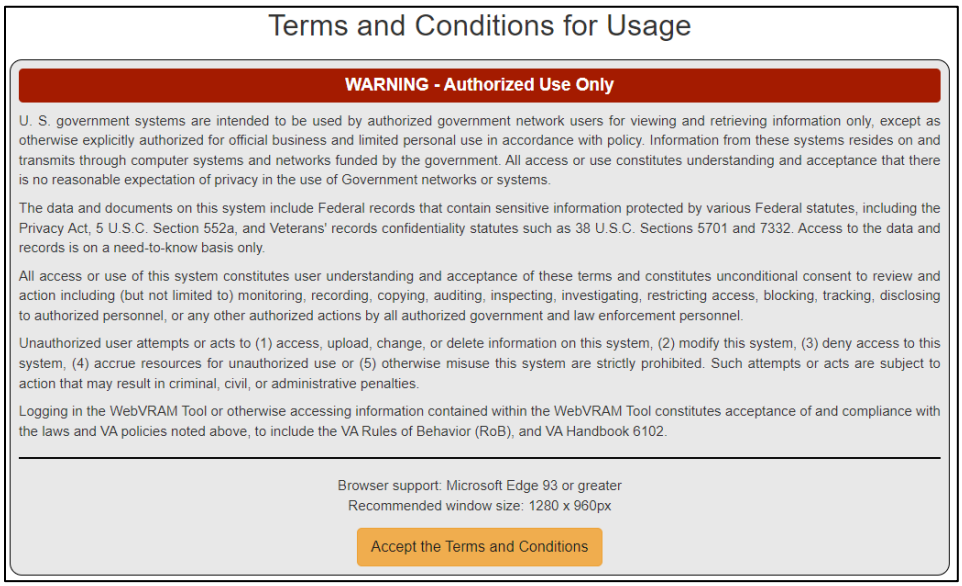
The WebVRAM application will be available for VA enterprise use 99.5% of the time, 24 hours a day, 365 days/year. In the event of a disaster affecting the VA Azure Cloud hosting environment where the application and associated database reside, a replication of the production environment, the application, 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.

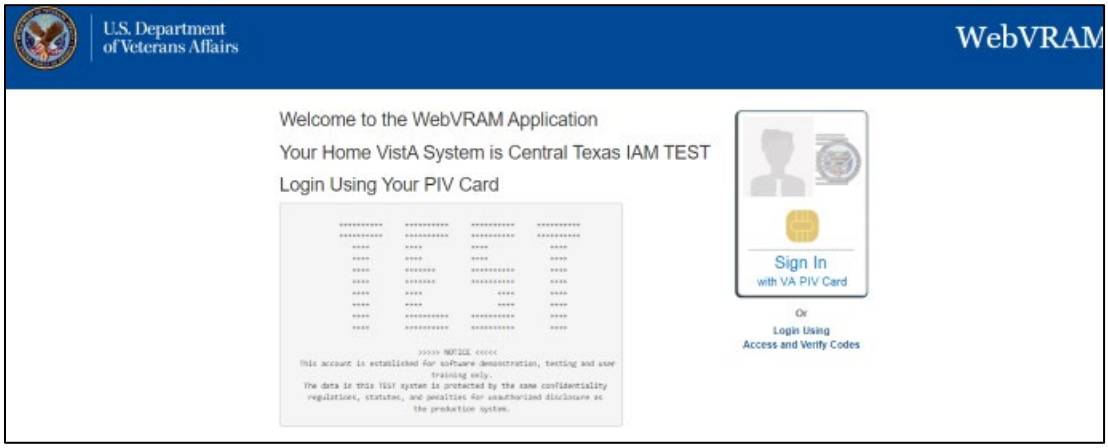
Figure 11: WebVRAM Terms and Conditions for Usage Screen



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

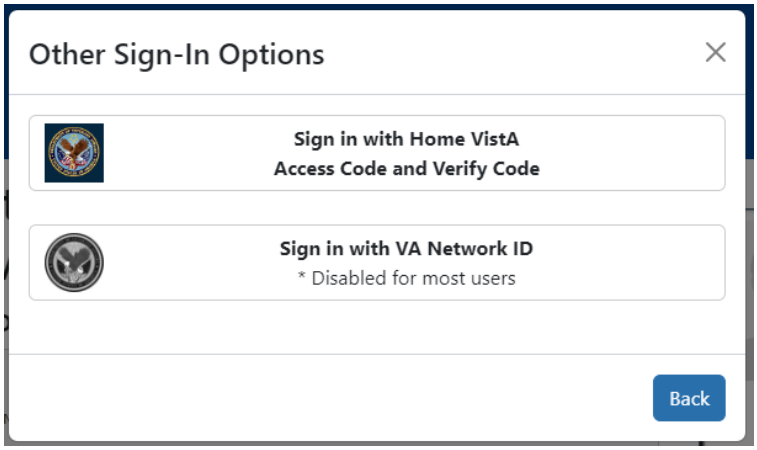
NOTE: The user's Home VistA System is displayed above the login screen. There is no need to use WebVRAM to access the user's Home VistA system because the user can already login directly to their Home VistA site to access VistA applications.

Figure 12: WebVRAM PIV Login Screen



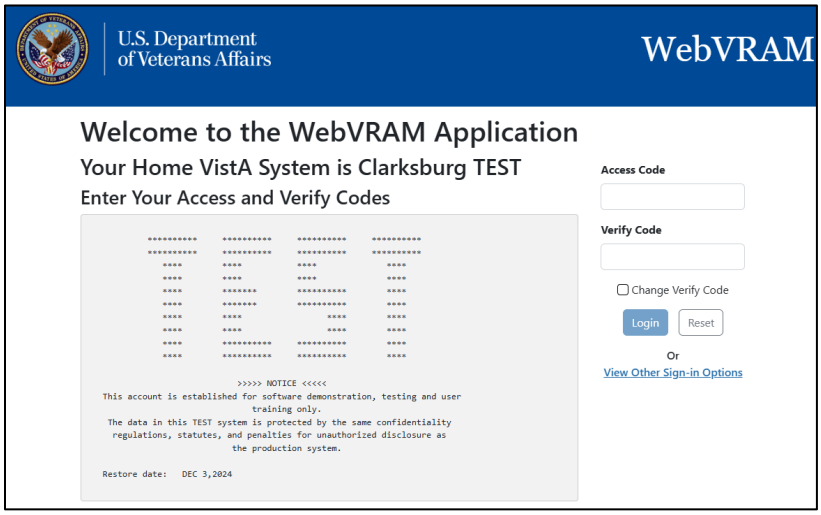
4. To log in with PIV Card, click on the "**Sign In with VA PIV Card**" image. The user will then be prompted to enter their PIV PIN to authenticate.
5. To log in with Access and Verify Codes, click on the Login Using Access and Verify Codes link. The Other Sign-In Options window will appear, prompting the user to select Sign in with Home VistA Access Code and Verify Code. Select this option to continue.

Figure 13: Other Sign-In Options window – AV code



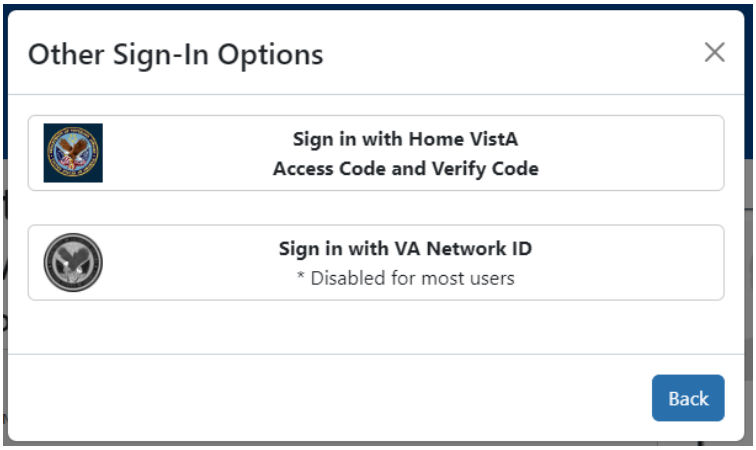
6. The user will then be prompted to enter their local VistA Access and Verify Codes and click **Login** to access the application.

Figure 14: WebVRAM A/V Code Login Screen



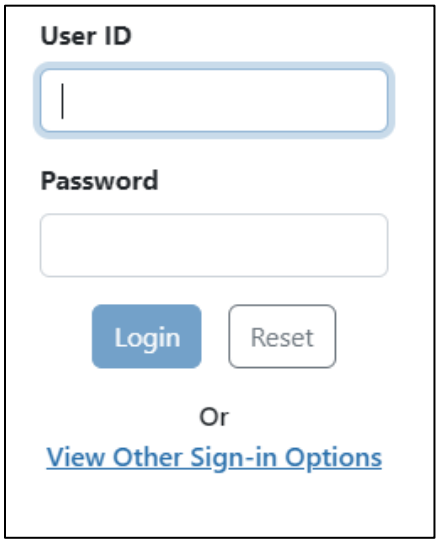
7. To log in with VA Network User ID and Password, select Sign in with VA Network ID. This option will be disabled for most users and is used when a user has an active PIV exemption.

Figure 15: Other Sign-In Options window - Network ID



The User ID and Password options appear on the sign-in screen. Enter your Network ID and Password and click Login.

Figure 16: User ID and Password login boxes

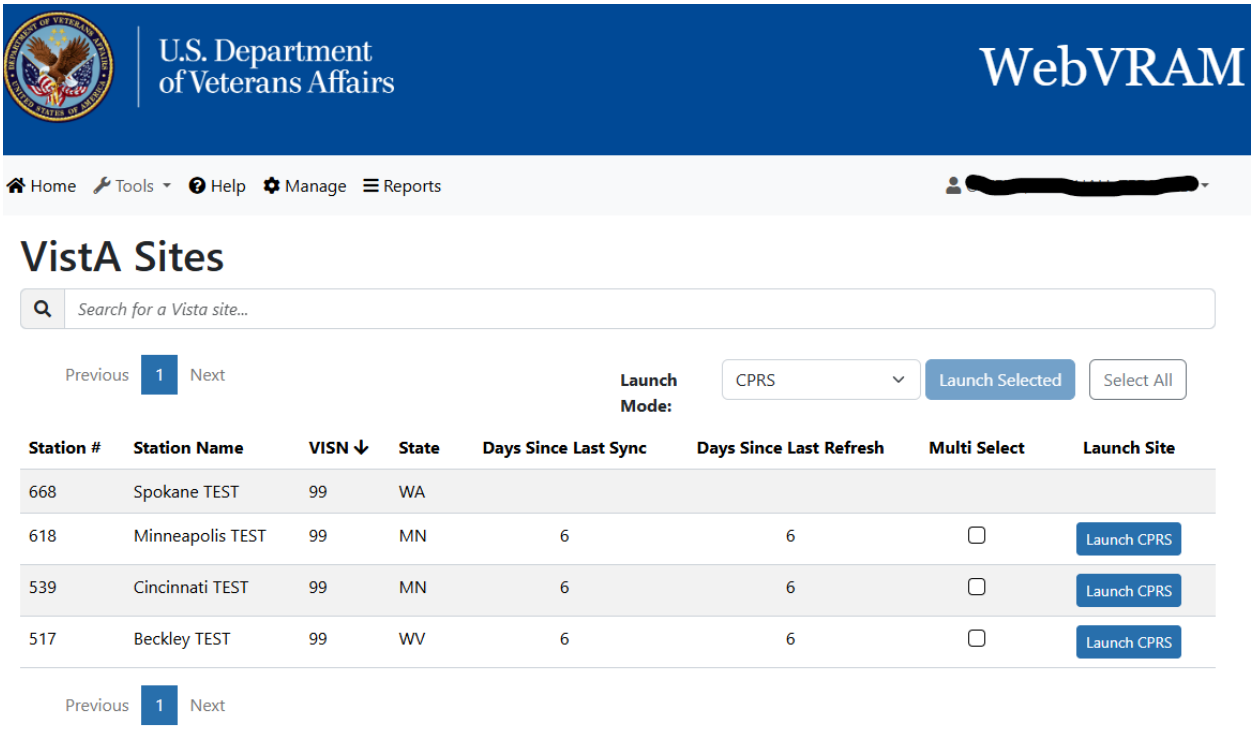


8. The WebVRAM application's home page is displayed. Sometimes during login, based on your Home VistA user profile, a window may open with a request to update your Electronic Signature (eSignature) code. See Section 4.1 Update eSignature Code for instructions for updating this code and associated data.

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 their Home VistA system to access VistA applications. 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 17: 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 18: Tools Drop-down – Update eSignature Code

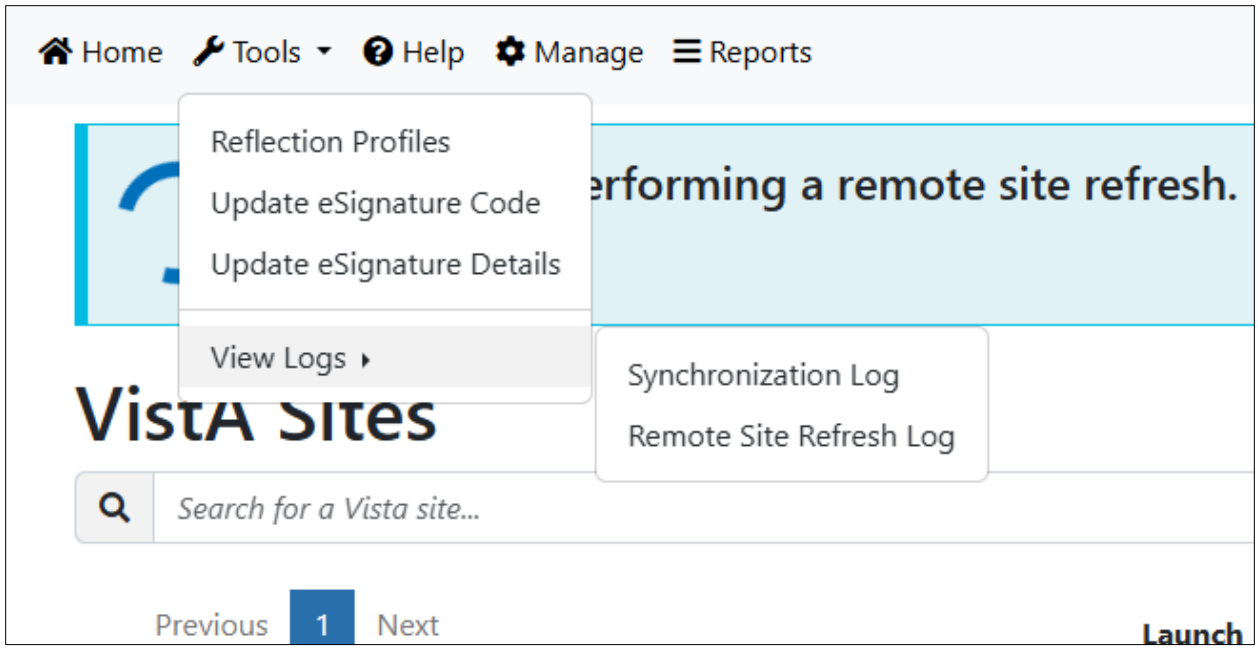
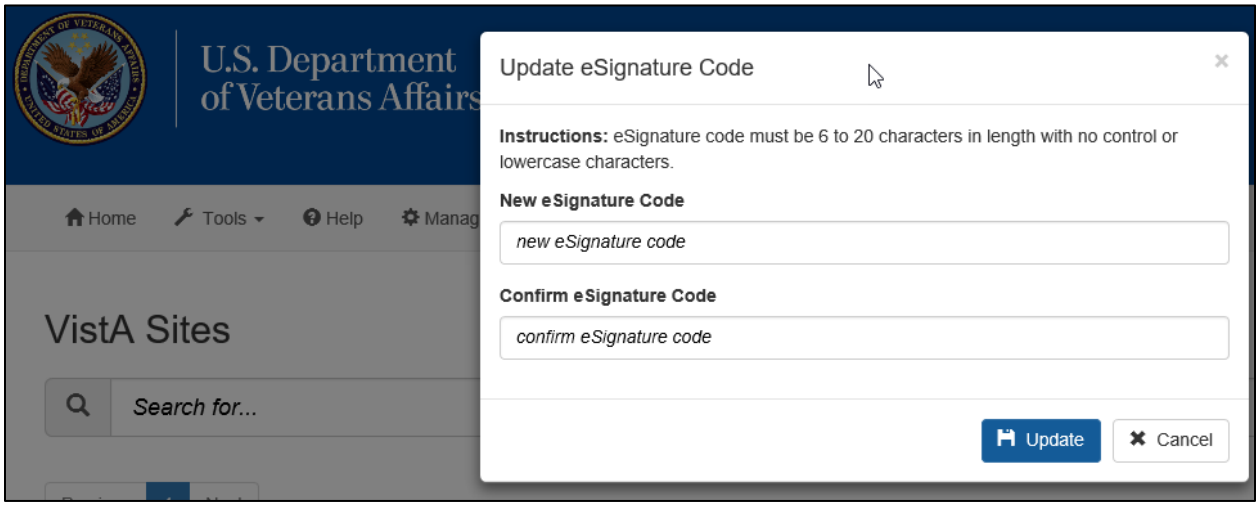


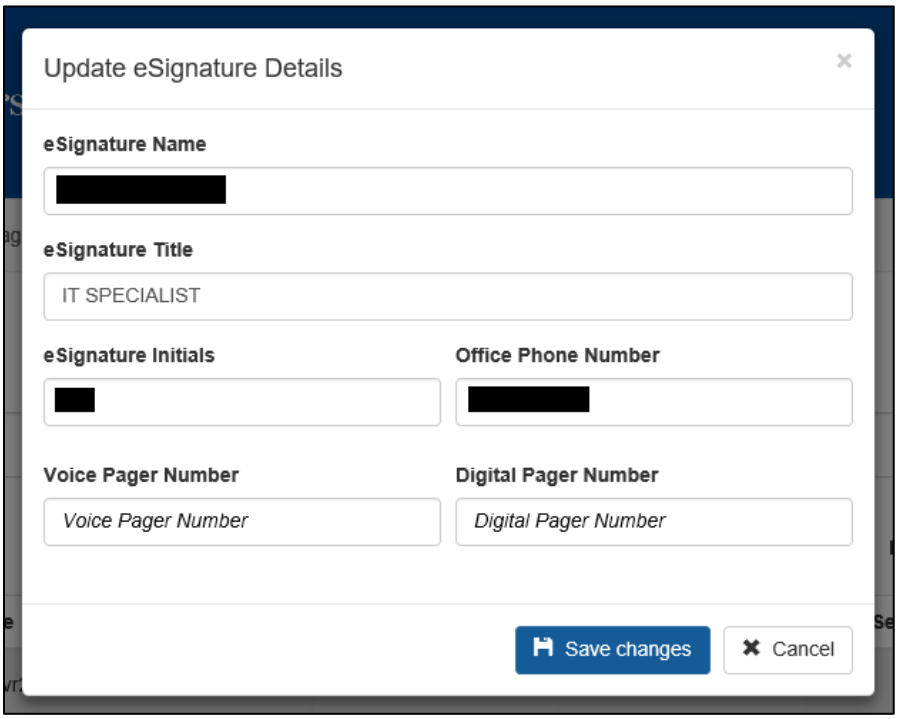
Figure 19: Update eSignature Code Screen



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 20: 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.

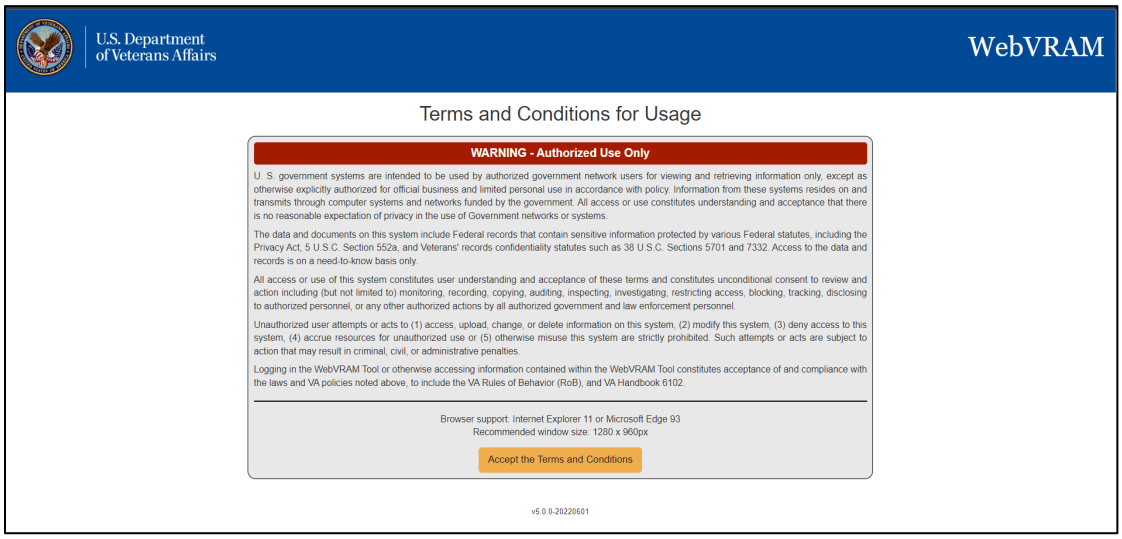
4.2 IAM / PIV Login - Link PIV to your Home VistA site

WebVRAM 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:

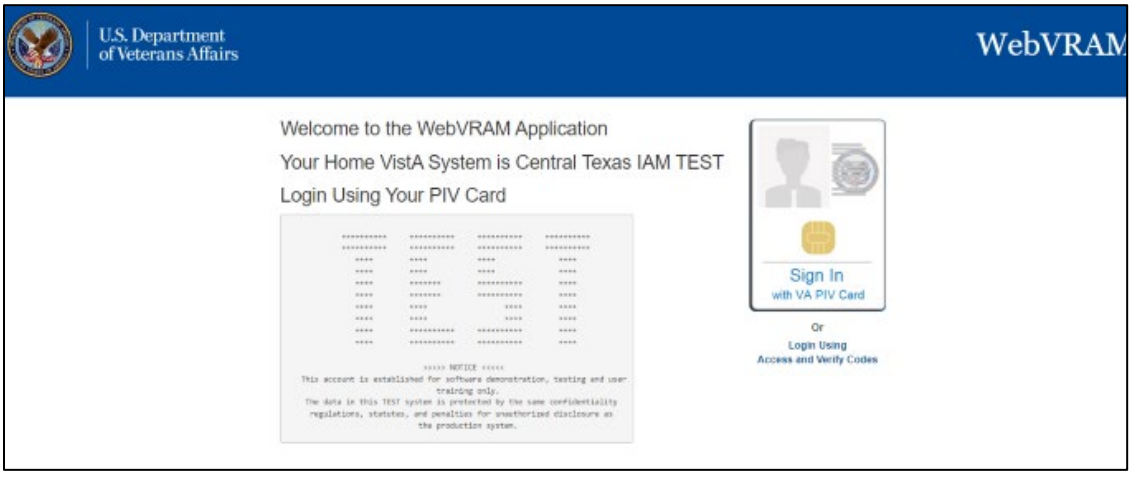
1. Navigate to WebVRAM Home Page
2. The Terms and Conditions for Usage is displayed; Click on the "**Accept the Terms and Conditions**" button

Figure 21: Terms and Conditions



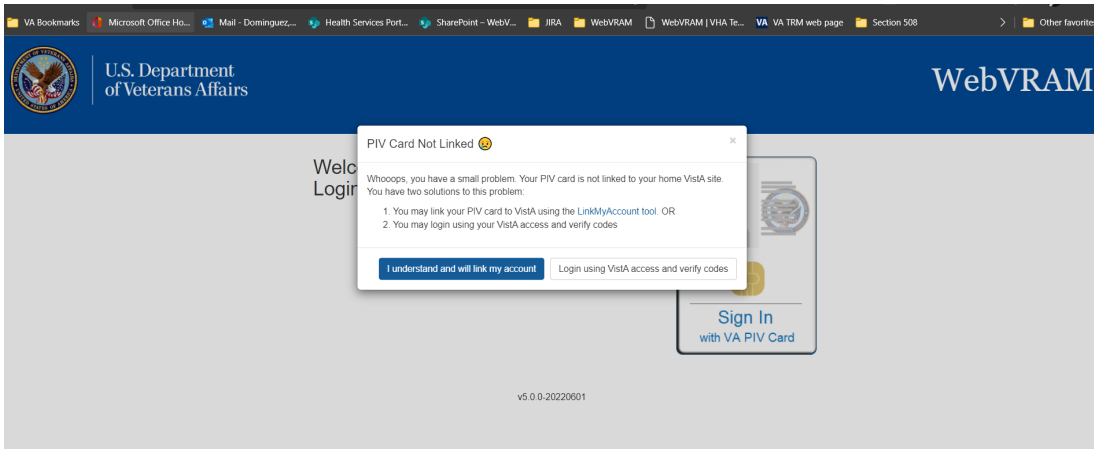
3. Click on the "**Sign In with a VA PIV Card**" button

Figure 22: Sign In With VA PIV Card



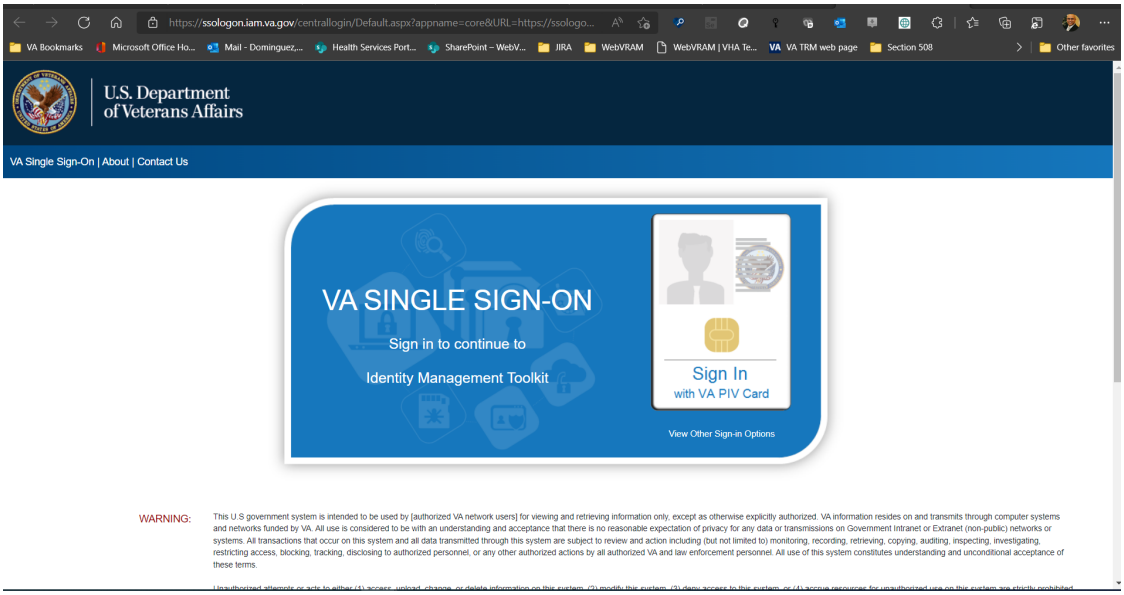
4. The "**PIV Card not Linked**" pop-up screened is displayed
5. Click on the "**I understand and will link my account**" button

Figure 23: 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 24: VA Single Sign-On page



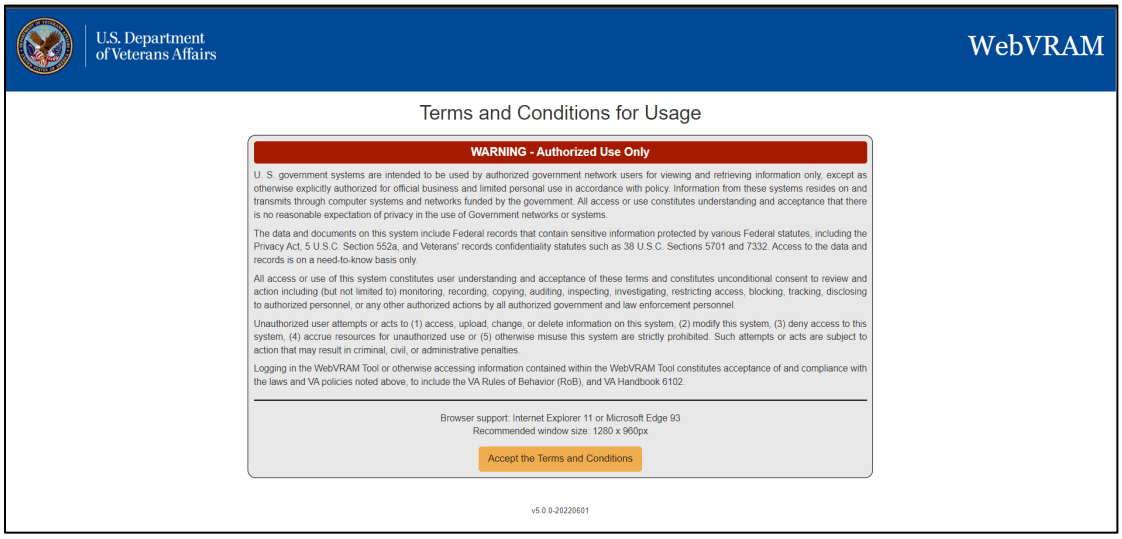
4.3 IAM / PIV Login – Login to WebVRAM with PIV Card

To login to WebVRAM utilizing your PIV Card:

1. Navigate to WebVRAM Home Page

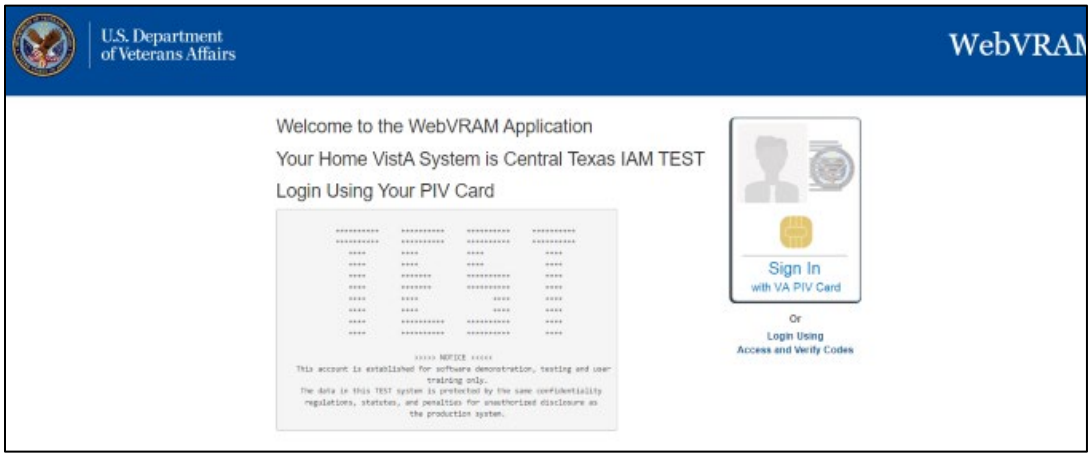
2. The Terms and Conditions for Usage is displayed; Click on the "**Accept the Terms and Conditions**" button

Figure 25: WebVRAM Terms and Conditions page



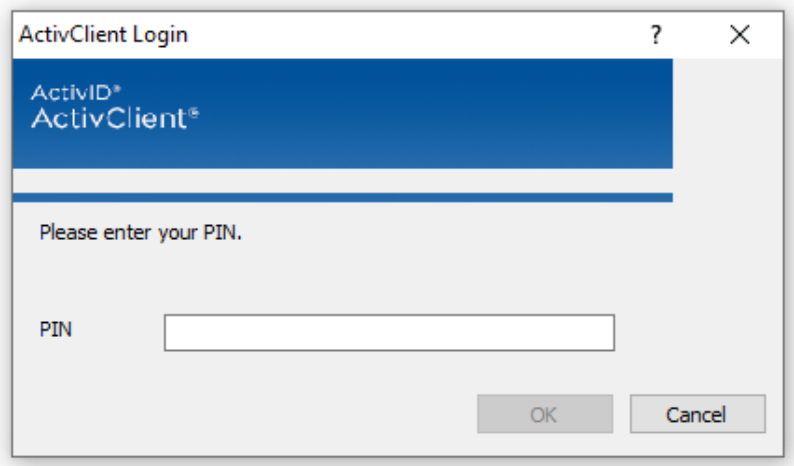
3. Click on the "**Sign In with a VA PIV Card**" button

Figure 26: WebVRAM PIV Card Sign-in page



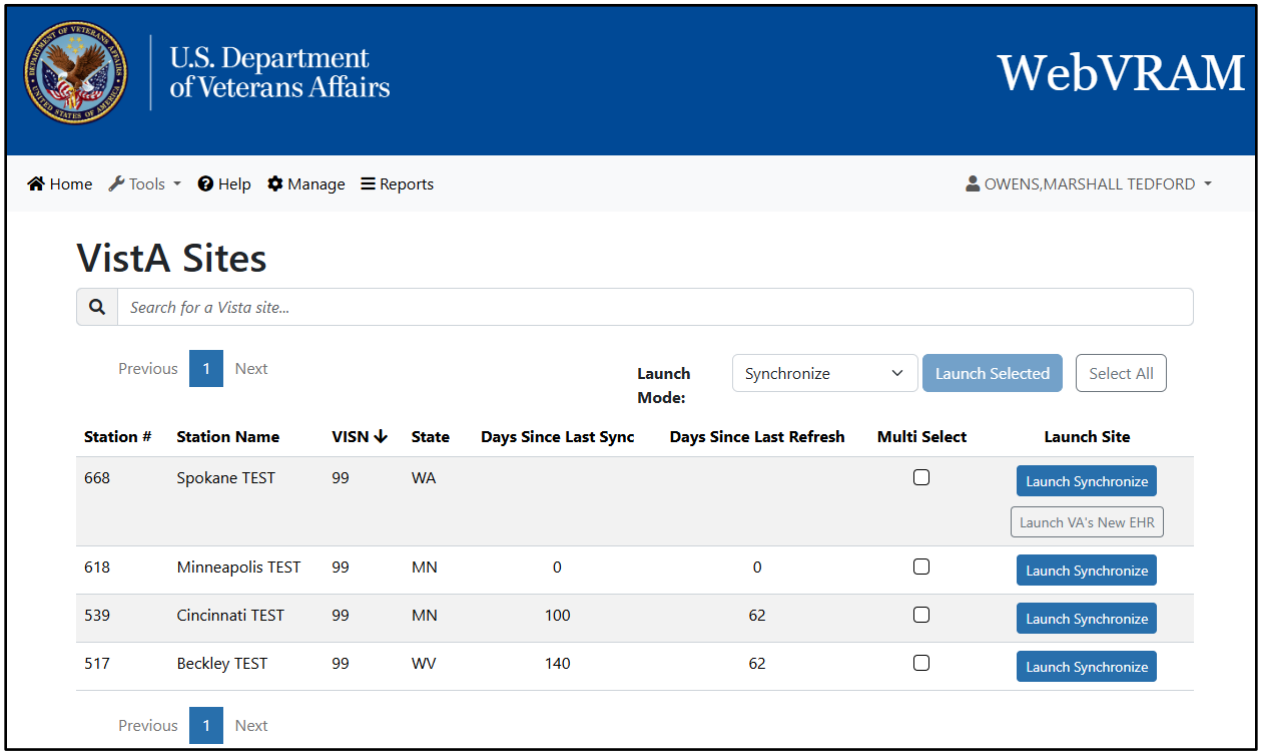
4. The ActivClient screen comes up, prompting the user to enter their PIN.
5. Enter PIN and click **OK**

Figure 27: ActivClient Login



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

Figure 28: WebVRAM Application Home Page



7. 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.

4.4 Account Maintenance and Timeouts

4.4.1 Access Control Policy – 90 Day Inactivity

Access Control Policy and Procedures AC-2(3) requires accounts that have been inactive 90 days or more to be disabled. If a user does not log in within this time frame, their WebVRAM account will be disabled automatically. Warning emails will be automatically sent to users who approach account termination due to inactivity, with reminders sent after 80, 85, and 89 days of inactivity. A re-enabled user has seven days to log in to prevent their account from being disabled for inactivity again.

If a user account is disabled, the user will need to contact their Business Unit Administrator to re-establish access to WebVRAM.

4.4.2 Synchronization

If a change is made to a user's WebVRAM user profile, it is advisable for the user to perform a synchronization to all sites as soon as it is convenient so that WebVRAM can push the change to the user's VistA profile at all remote VistA sites. If a synchronization to all sites is not performed by the user, the change will be pushed to the remote VistA site the next time the user connects to the site through WebVRAM using the Reflection, CPRS, or Synchronize launch mode. In all three of these instances, WebVRAM performs a synchronization to the remote VistA site.

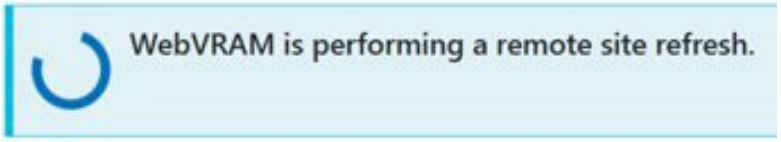
The 'Days Since Last Sync' field on the WebVRAM site listing page shows how many days have passed since the user last connected to the remote VistA site through WebVRAM using the Reflection, CPRS, or Synchronize launch mode.

4.4.3 Remote Site Refresh Process

Upon logging in to WebVRAM, a Remote Site Refresh process runs in the background, connects to each of the user's remote VistA sites and sets the Last Login date to the current date. The user can utilize WebVRAM as they normally do while the background process is running. WebVRAM executes this process daily, the first time the user logs in, to keep the user's remote VistA sites active for the next 90 days.

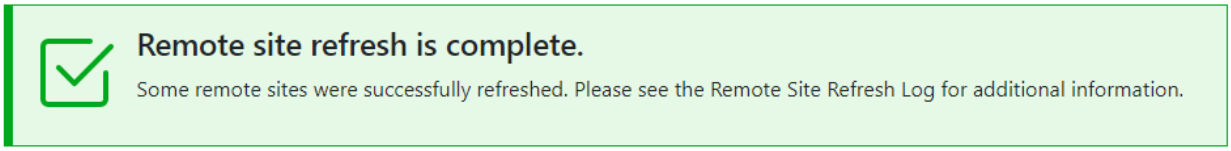
A banner will appear showing that the Remote Site refresh is running.

Figure 29: Remote Site Refresh In process



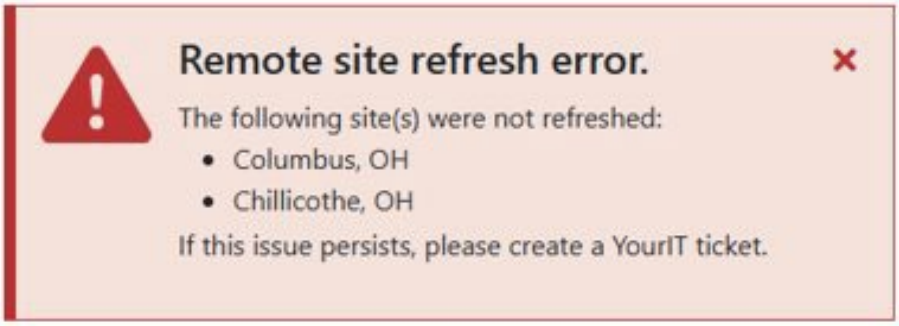
Once it is completed, the banner will display the results of the refresh. If the refresh is successful, a green banner with a checkmark and a message indicating the process was successful will be displayed.

Figure 30: Remote Site Refresh Success Banner



If the refresh was not successful at one or more sites, a red banner with an exclamation mark and a message indicating the process was not successful along with which sites were not successful will be displayed.

Figure 31: Remote Site Refresh error banner



NOTE: This is not truly an error and does not need be reported to the WebVRAM team unless it persists for more than 24 hours. This refresh error only means that the site was not refreshed. Since the Remote Site Refresh only checks every 24 hours, it takes at least that long for a change to be reflected in the message banners.

The Remote Site Refresh process does not pass any user profile information to the remote VistA sites. To pass user profile information, the user must connect to the remote VistA site through WebVRAM using the Reflection, CPRS, or Synchronize launch mode. Please see section 4.4.2 Synchronization for more details.

Prior to completion of the current day's Remote Site Refresh, the 'Days Since Last Refresh' field on the user's site list shows how many days have passed since the site had a successful refresh. Upon completion of the current day's Remote Site Refresh, the field changes to 0 for all sites that were successfully refreshed.

If the user has never connected to the remote VistA site through WebVRAM using the Reflection, CPRS, or Synchronize launch mode, the site will not be refreshed by the Remote Site Refresh process. This is normal and there is no need for concern. However, if an error occurs during the Remote Site Refresh, WebVRAM will display an error banner. In this case, the user should create a Service Now (SNOW)/yourIT ticket if the issue persists for more than 24 hours.

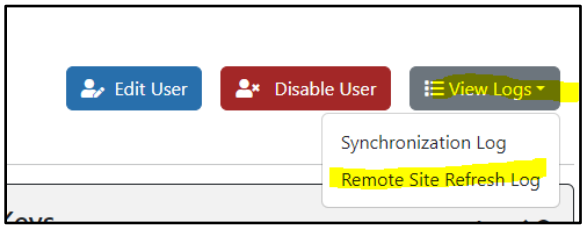
CAUTION: If the number in the 'Days Since Last Sync' field is higher than the 'Days Since Last Refresh' field, this indicates a site connection issue has occurred. If this happens, please create a Service Now (SNOW)/yourIT ticket or phone the ESD to resolve the issue.

NOTE: Any new site added to the user's WebVRAM profile after the current day's Remote Site Refresh has completed will be refreshed the next time the Remote Site Refresh process is performed, provided the user has connected to the remote site through WebVRAM using the Reflection, CPRS, or Synchronize launch mode.

4.4.4 Remote Site Refresh Log Screen

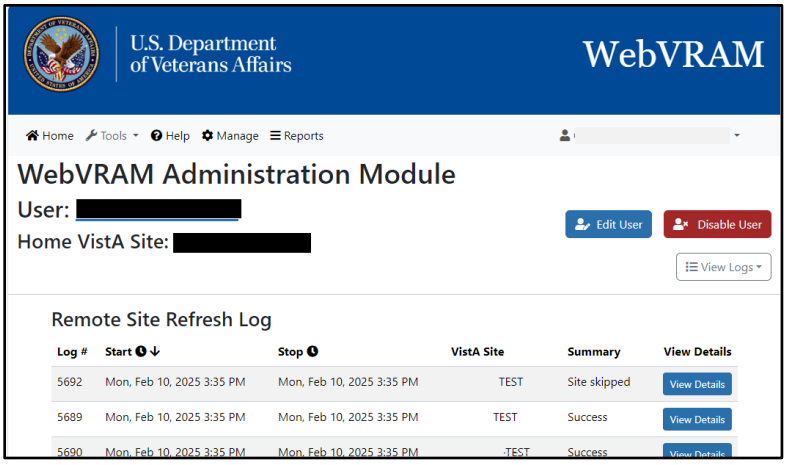
A new log screen can be found in the user's profile. The Remote Site Refresh log can be accessed from the User Profile Screen. Select View Logs > Remote Site Refresh Log.

Figure 32: Accessing Remote Site Refresh Log from View Logs button



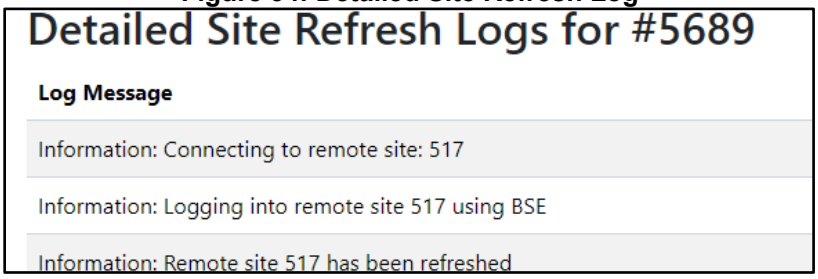
The Remote Site Refresh Log screen displays log number, start, and stop dates for the Remote Site Refresh, sites, and a summary of results, with a View Details button to show more information. A warning entry is generally not a problem, merely a notice, but an error should be reported with a SNOW/yourIT ticket or a call to the ESD.

Figure 33: Remote Site Refresh Log page



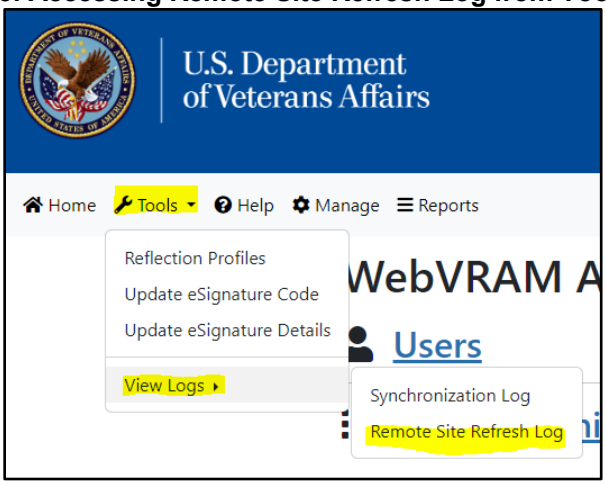
Clicking the View Details button shows the detailed Log Messages for the site.

Figure 34: Detailed Site Refresh Log



The Remote Site Refresh Log screen can also be accessed from the top-level navigation Tools > View Logs > Remote Site Refresh Log.

Figure 35: Accessing Remote Site Refresh Log from Tools menu



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. 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 multiple 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. 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 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 justification. With rare exceptions, users who are members of multiple Business Units are not permitted to have extended timeouts.

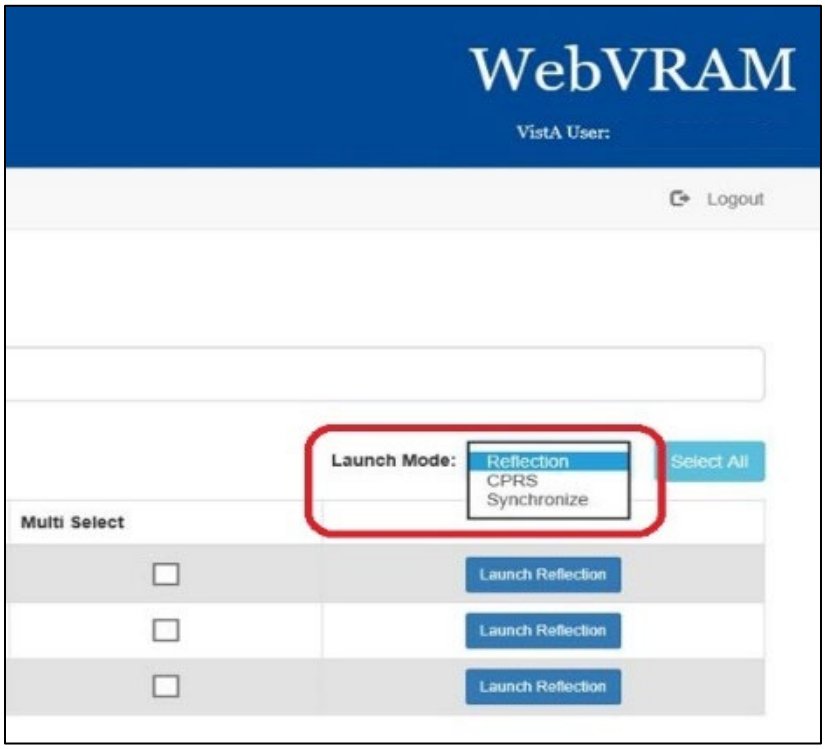
5.1 Remote Session: Launch Mode

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 VistA session with Reflection at the selected remote location.
- CPRS – This option is used to launch a remote VistA CPRS session at the selected remote location.
- Synchronize – This option is used to connect to and setup or update an active VistA profile at a remote VistA site. 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 WebVRAM Business Unit Administrator. After the new VistA site is added, the user should synchronize to the site so that WebVRAM can create a VistA user profile at that site.

Figure 36: Launch Mode Drop-down



5.1.1 Launch Mode: Reflection

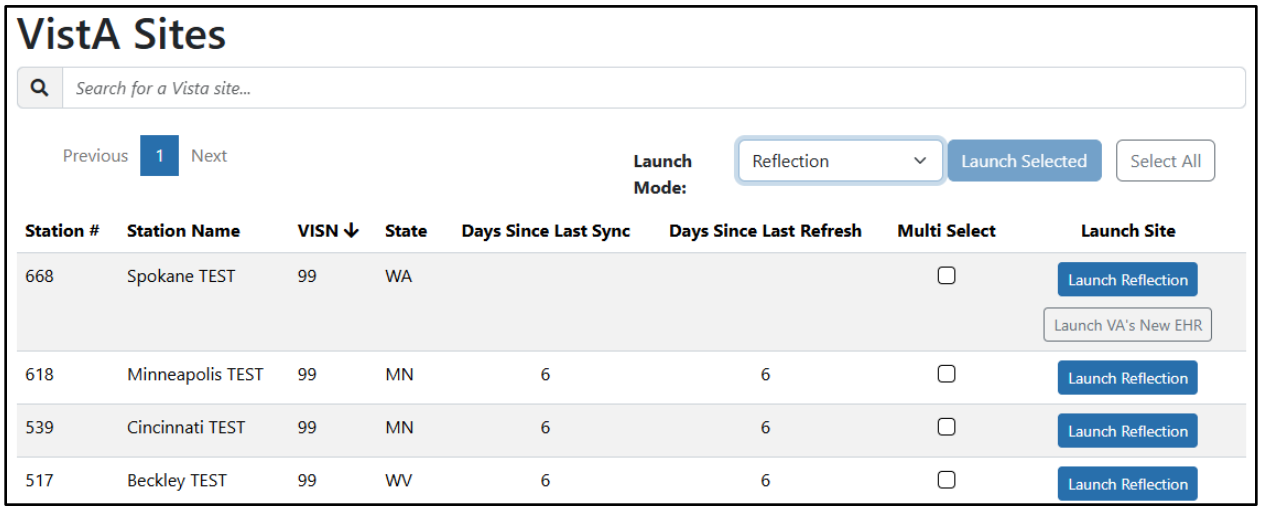
1. Login to WebVRAM.
2. From the WebVRAM home page, select the Station Name of the remote VistA site to which the user wants to connect.

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.

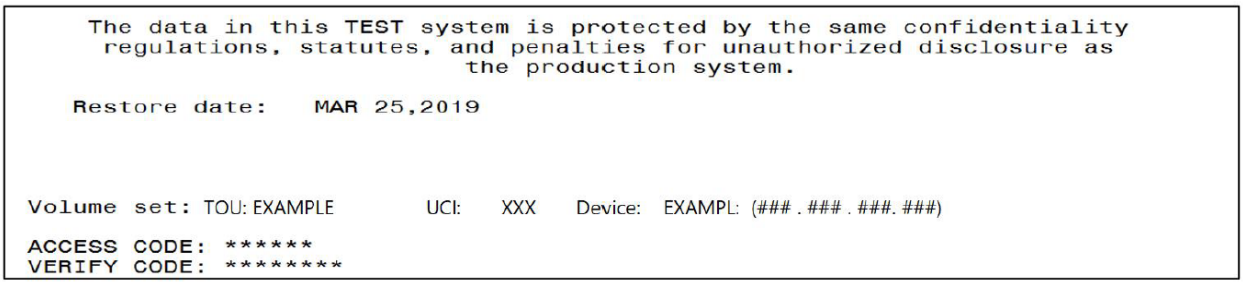
   NOTE: If your Reflection session times out, if you have logged in to WebVRAM with your PIV card, you will be able to re-establish your connection using your PIV credential rather than needing to use Access and Verify codes to re-establish the Reflection session.

Figure 37: Launch Reflection Button



5. 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.

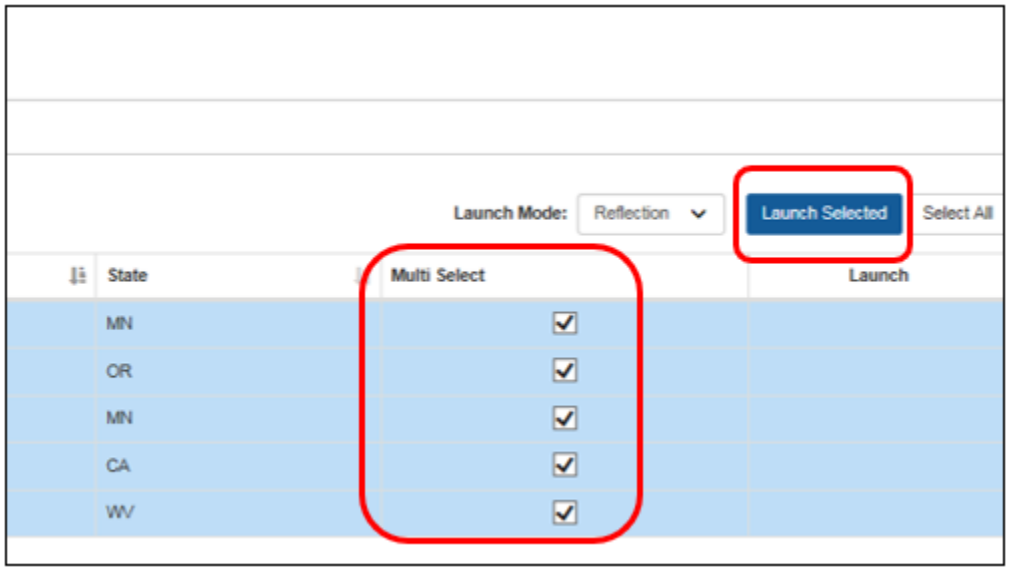
Figure 38: VistA Login



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. The figure below shows the boxes checked for each site the user intends to launch, and the **Launch Selected** mode for performing this action.

Figure 39: 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.

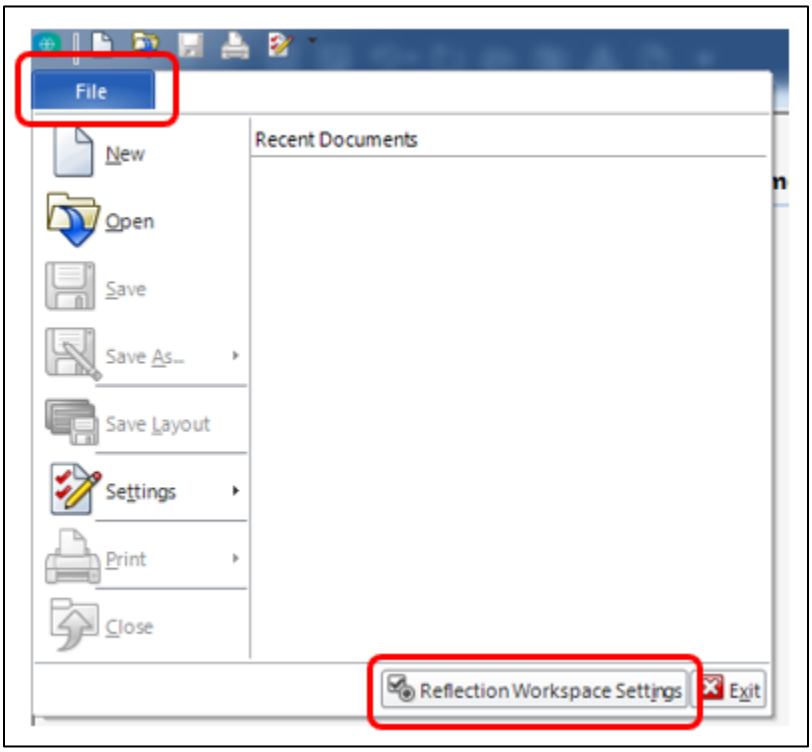
5.1.3 Launching Simultaneous Multiple VistA Sessions at a Single Site

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.

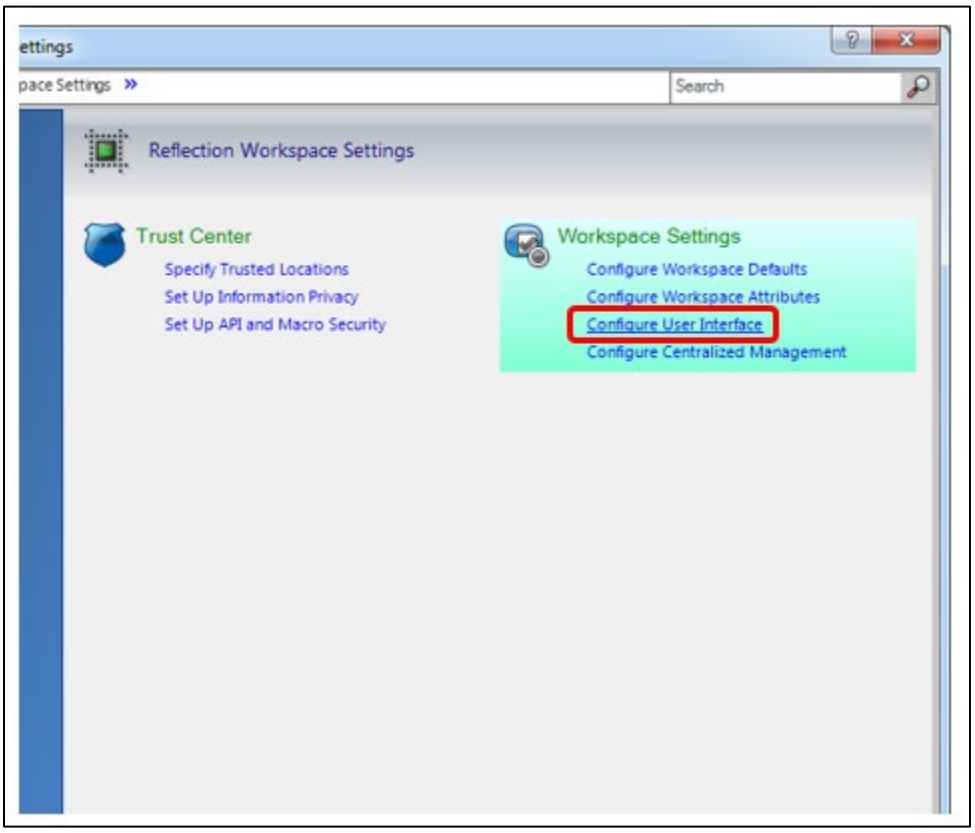
1. Open *Reflection Workspace* on your workstation. In the upper left corner, click the **File** tab.
2. In the pop-up window that opens, click on **Reflection Workspace Settings** in the lower right corner, as shown below.

Figure 40: Reflection Workspace Settings Access



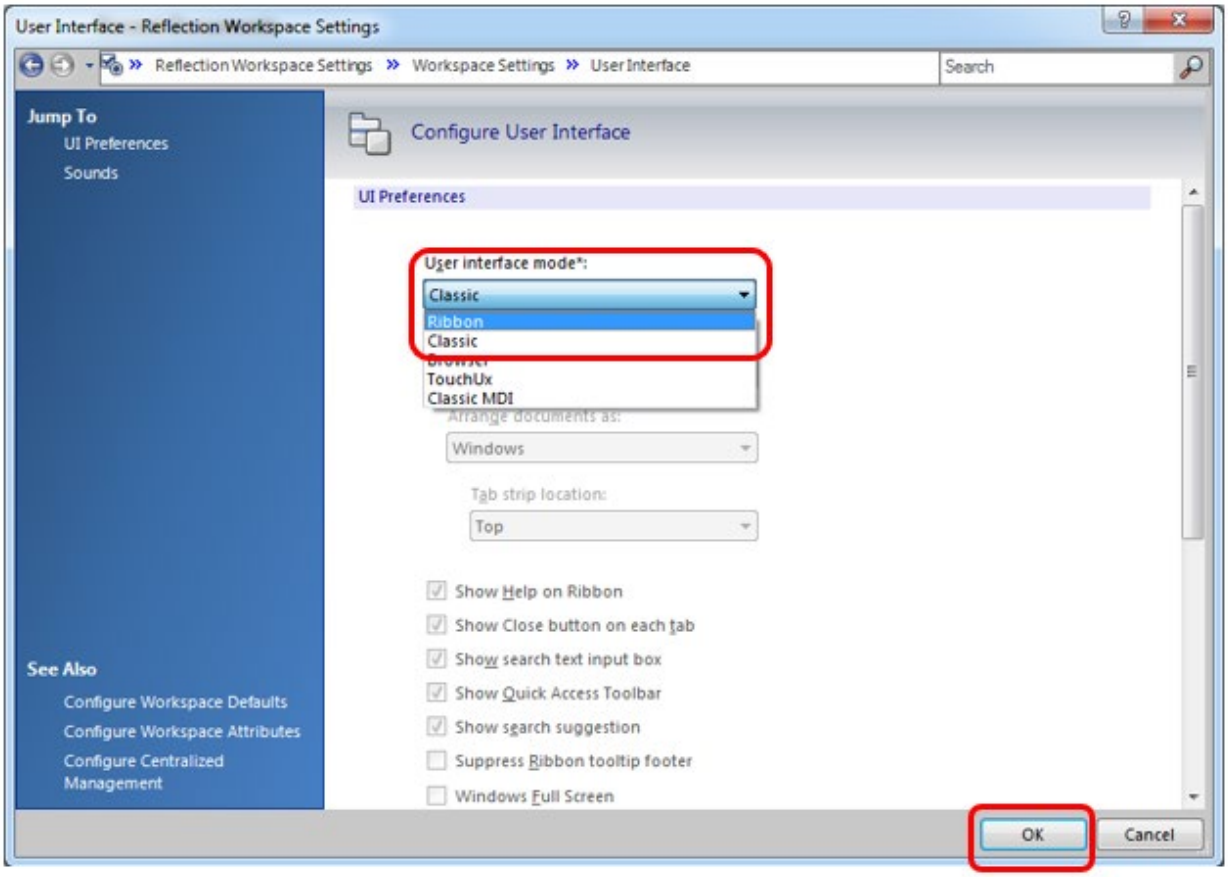
3. In the pop-up window that opens, under **Workspace Settings**, click on **Configure User Interface**, as shown below.

Figure 41: 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 42: 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

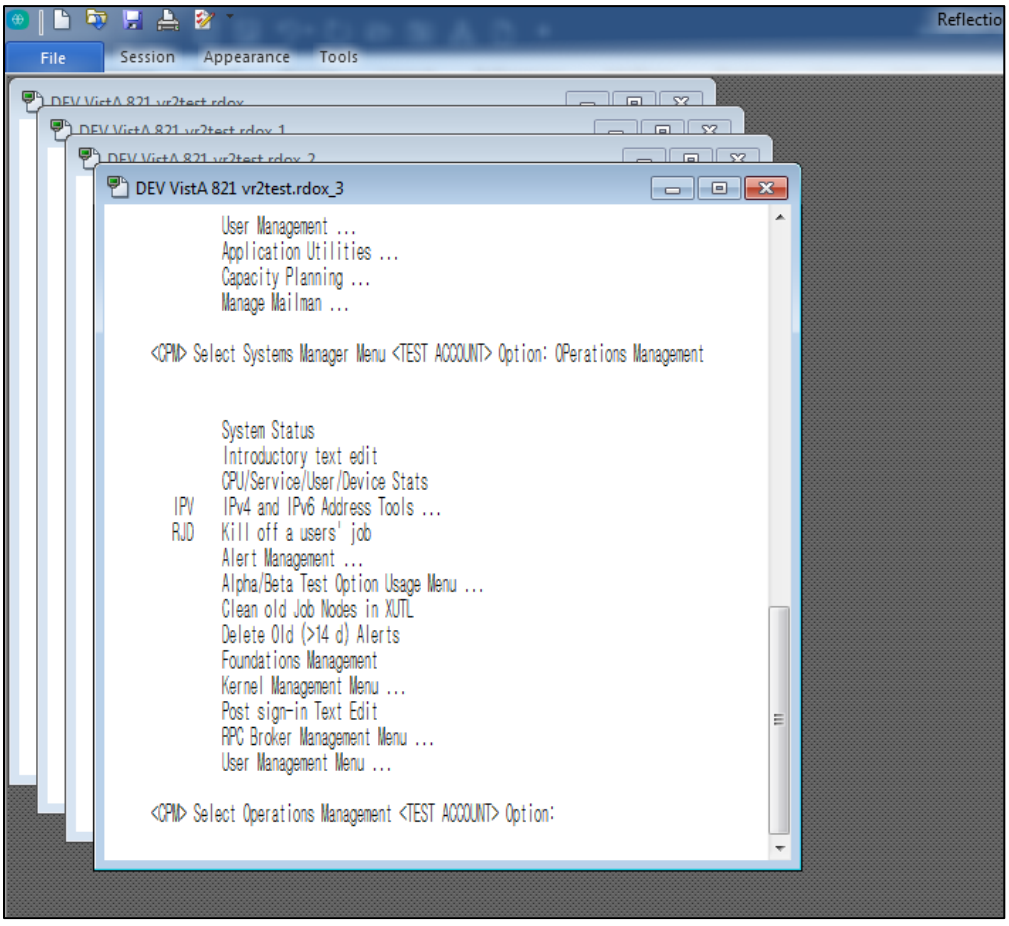
For CPAC users who need to view more than one simultaneous VistA session at the same site, arranging these sessions in a tile view must be done manually within Reflection during initial use of WebVRAM. The following steps will create a tile view for the remote VistA site connections the first time these 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 43: 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 44: Reflection – Arrange Windows Icon and Drop-down

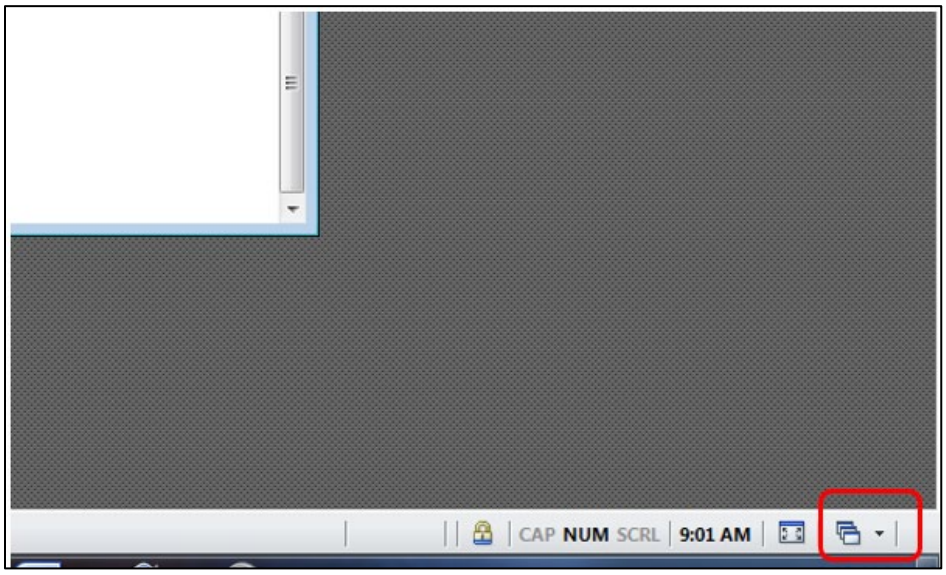
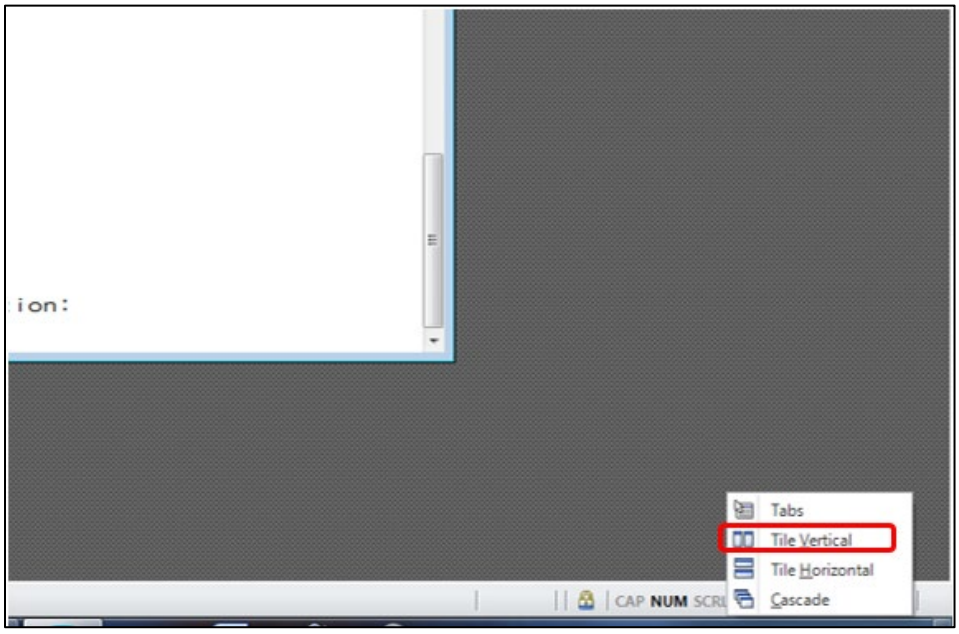


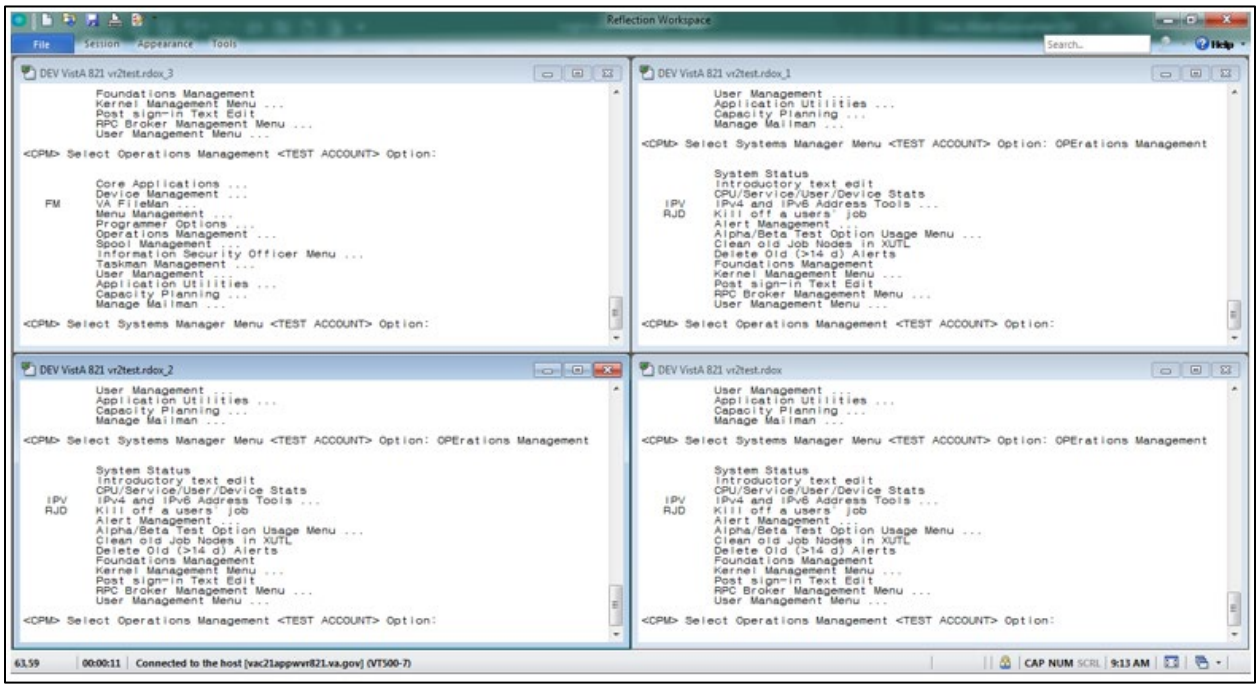
Figure 45: Reflection – Arrange Windows Tile Vertical Selection



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.

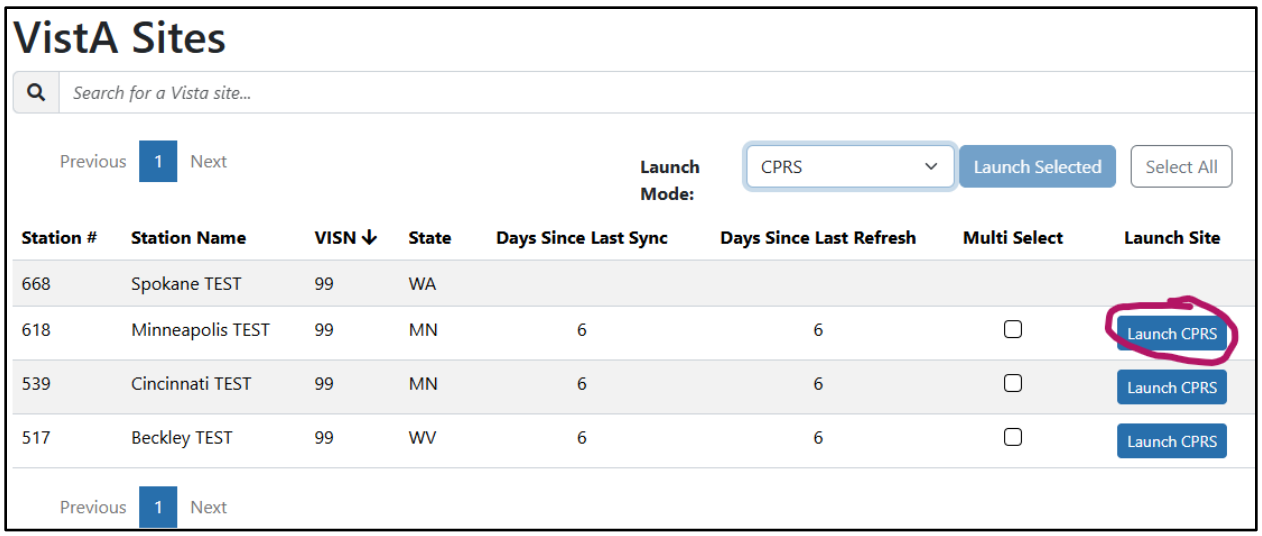
Figure 46: Reflection – Tile Vertical View



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 47: Launch CPRS Button



4. WebVRAM is 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 48: CPRS Version Screen

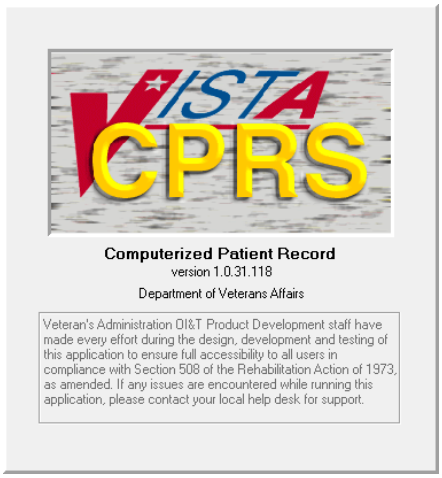
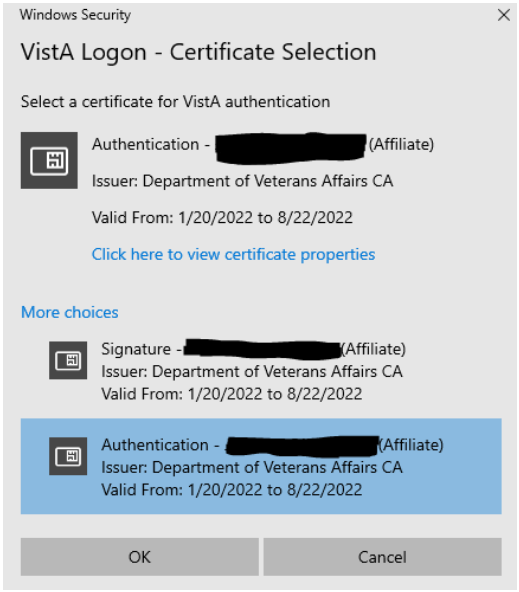


Figure 49: Windows Security: VistA Login - Certificate Selection screen

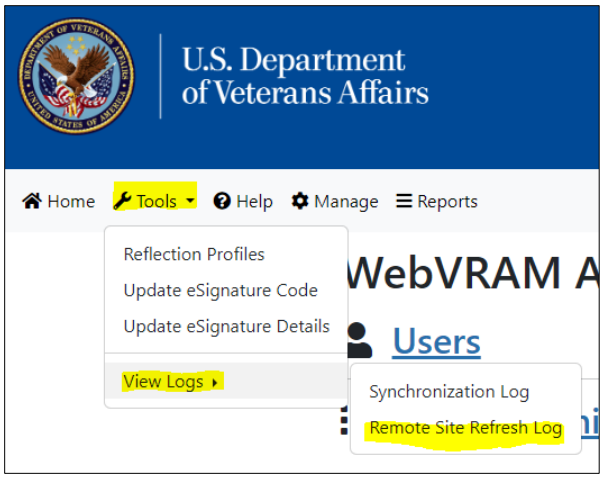


5. Select the Authentication Certificate and click **OK**. The CPRS VistA Login screen appears.
6. NOTE: If the user logged in to WebVRAM with Access and Verify Codes, the user needs to click on **Cancel** in the Windows Security screen. The user will then be prompted to enter the Access and Verify Code (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

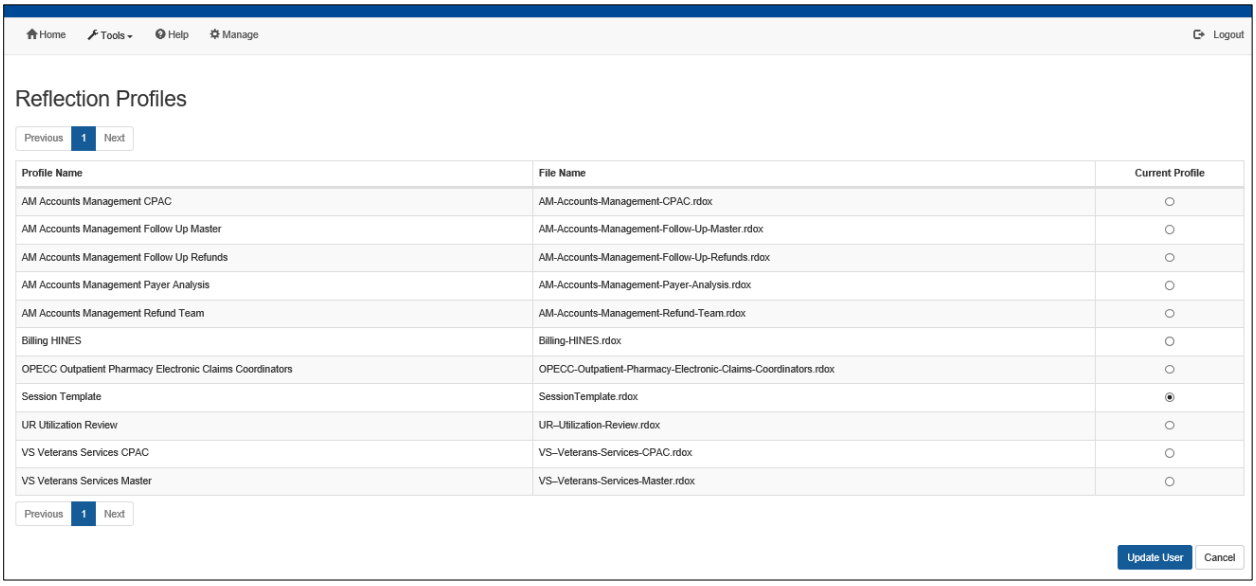
1. Login to WebVRAM.
2. From the WebVRAM main page, click on **Tools** and select **Reflection Profiles** from the drop-down menu. The Reflection Profiles screen is displayed.

Figure 50: 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 51: Reflection Profiles Screen

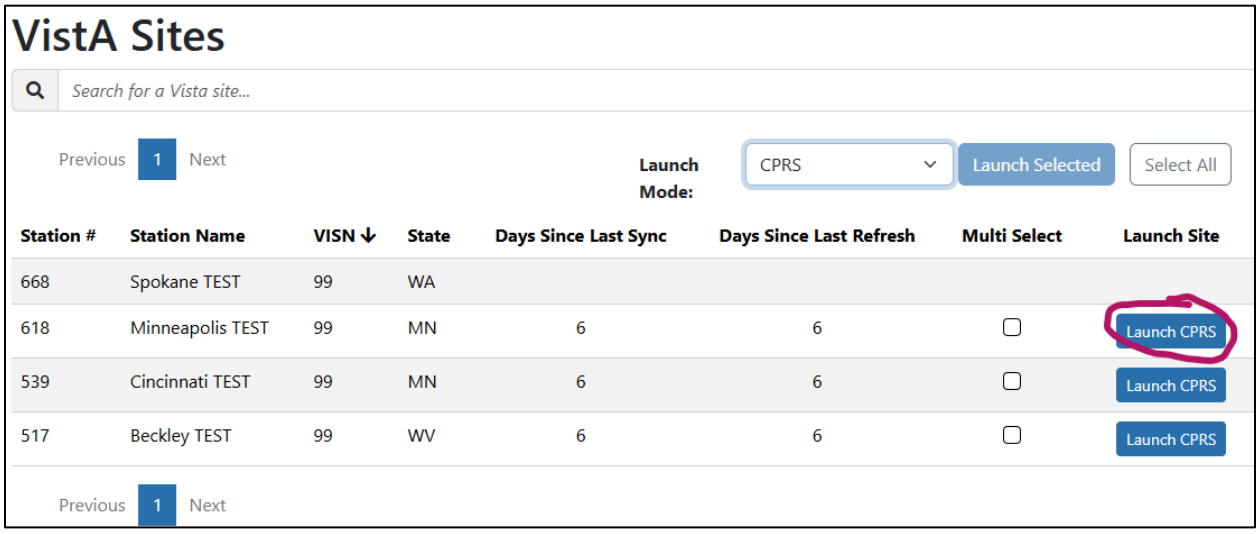


4. Select from the following Reflection VT Session files, then click the **Update User** button:
   - AM-Accounts-Management-CPAC.rdox
   - AM-Accounts-Management-Follow-Up-Master.rdox
   - AM-Accounts-Management-Follow-Up-Refunds.rdox
   - AM-Accounts-Management-Payer-Analysis.rdox
   - AM-Accounts-Management-Refund-Team.rdox
   - 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 52: Launch CPRS Button



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 53: CPRS Version Screen

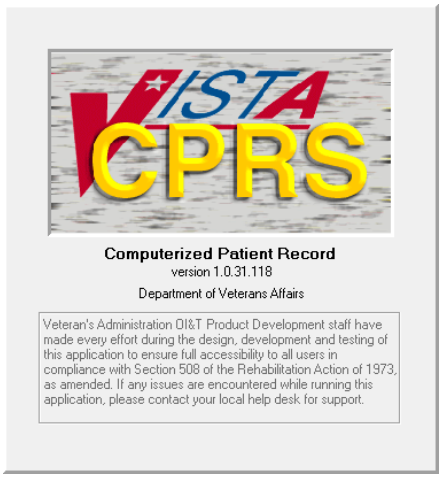
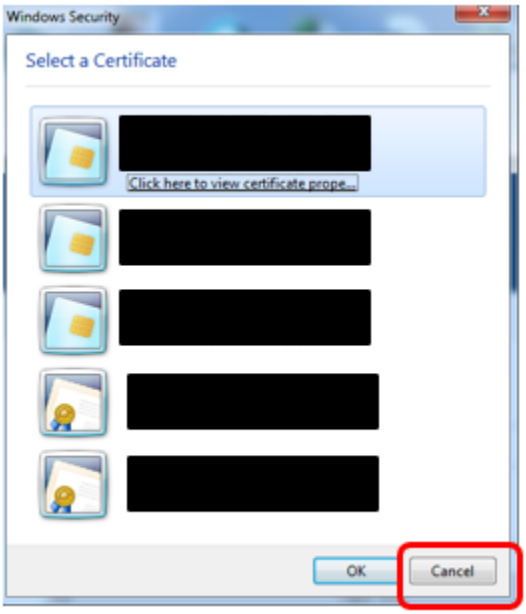
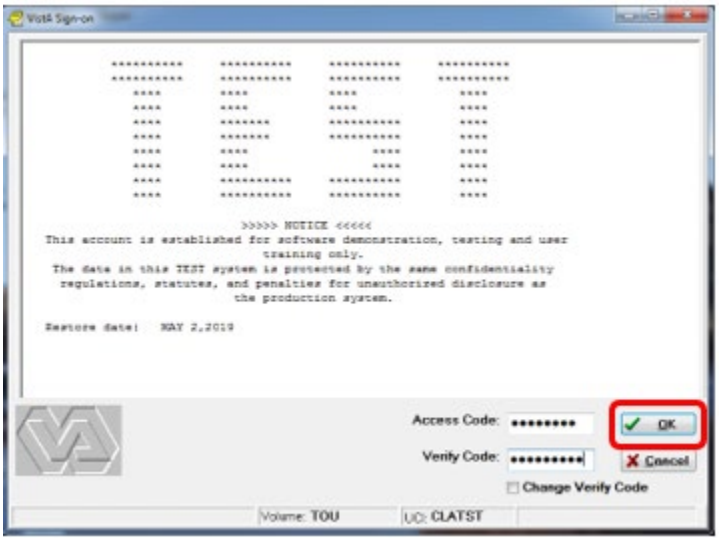


Figure 54: PIV Select a Certificate Screen



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 55: 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 launched 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: Do not save the A/V codes" 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.

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 for 90 days after the initial connection is made, the remote VistA profile will terminate on day 91. This is a security policy enforced by the VistA systems. To prevent this, the user **MUST** login to WebVRAM at least once every 89 days. WebVRAM's Remote Site Refresh

process will refresh all the user's remote VistA sites to keep them active. After the Remote Site Refresh process completes, the user can log off WebVRAM and continue to use CPRS Desktop Launcher to access CPRS patient data at remote VistA sites for another 89 days.

5.1.9 Prescription Drug-Monitoring Program (PDMP)

The Pharmacist and/or Provider can use the PDMP Query in CPRS at the remote VistA site, for all sites that have this capability integrated.

5.1.10 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.

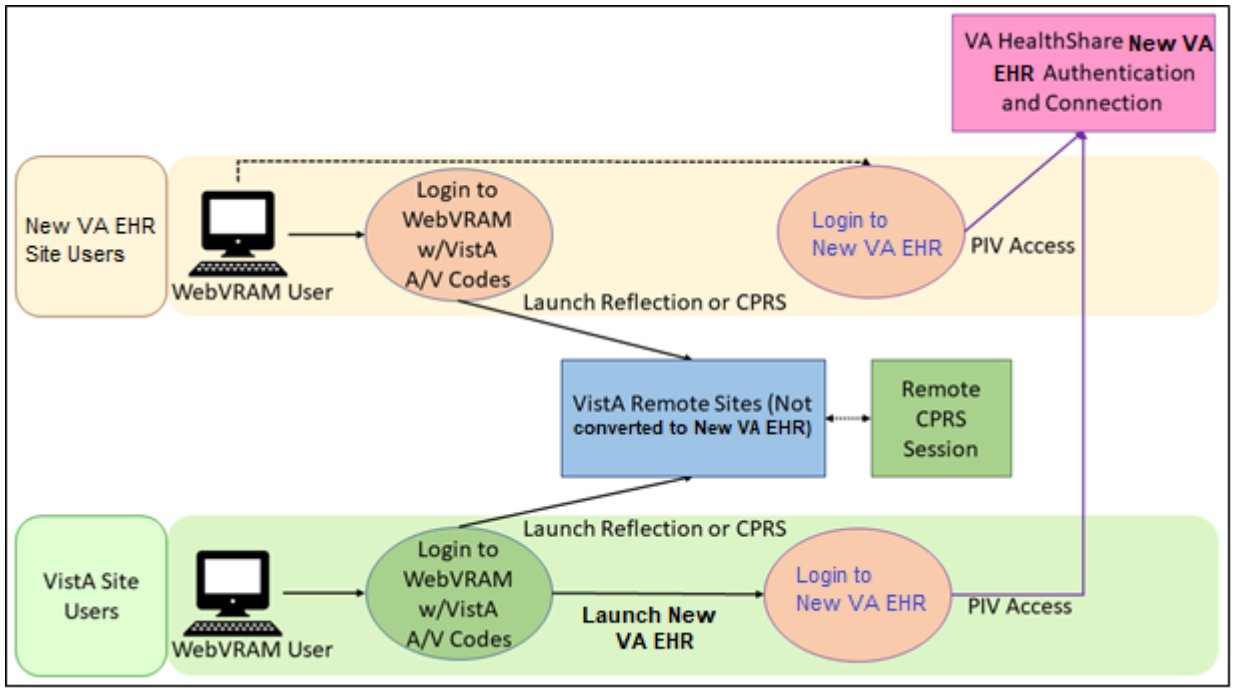
NOTE: Since the initial New VA EHR rollout will not replace all VistA functions, in addition to accessing the New VA EHR, the user can still access certain VistA functions at remote New VA EHR sites. Providers must use Joint Legacy Viewer (JLV) at a New VA EHR-converted site to view historical VistA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

The below figure 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 56: WebVRAM New VA EHR Connections User Workflow

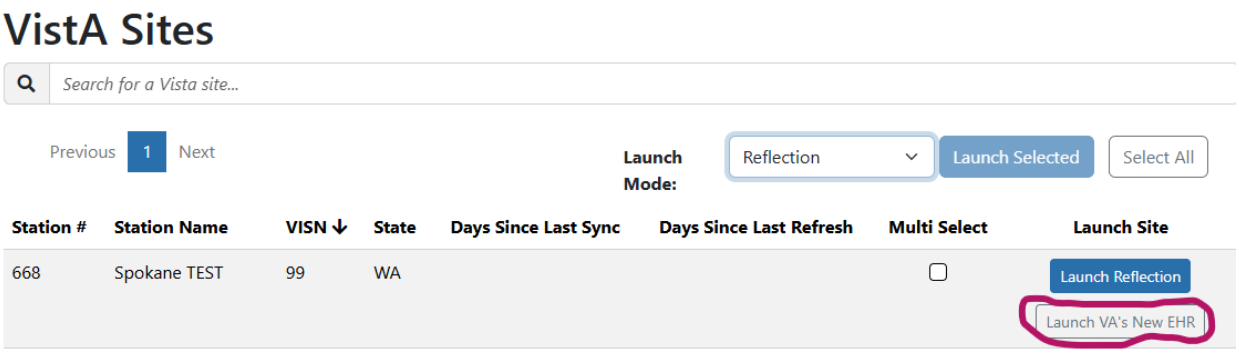


5.1.11 Launch New VA EHR Button

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.

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. New VA EHR sites are not selectable as a user's WebVRAM Home VistA.

Figure 57: 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 58: New VA EHR PIV Login Screen

5.1.12 PSO/WebVRAM PSDRPH Security Key

The RPC "PSO EPCS PSDRPH FILER" will be used to allocate/de-allocate and audit the assignment/dismission of the PSDRPH key.

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 profile information on the remote VistA system.

Figure 59: Launch Synchronize Button

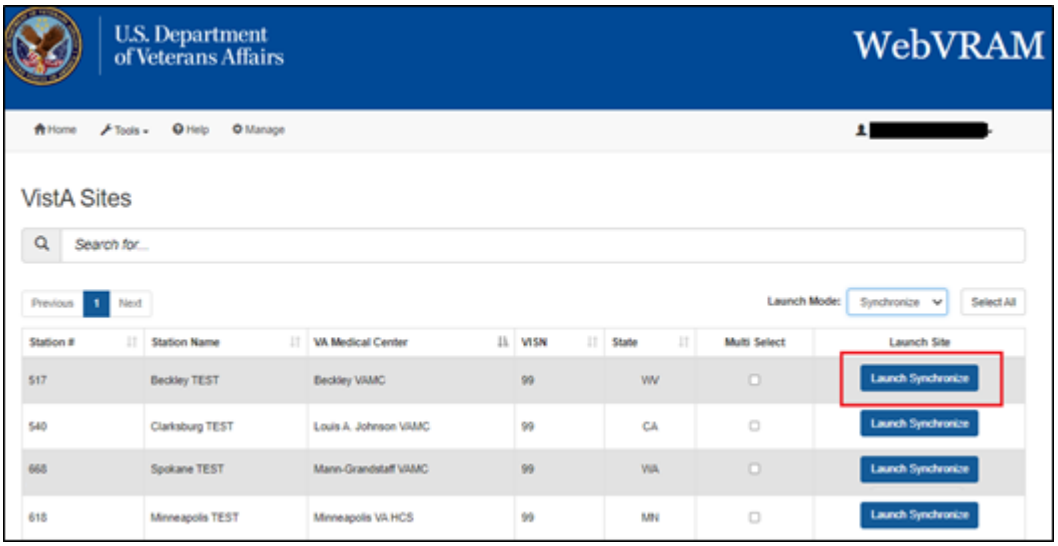
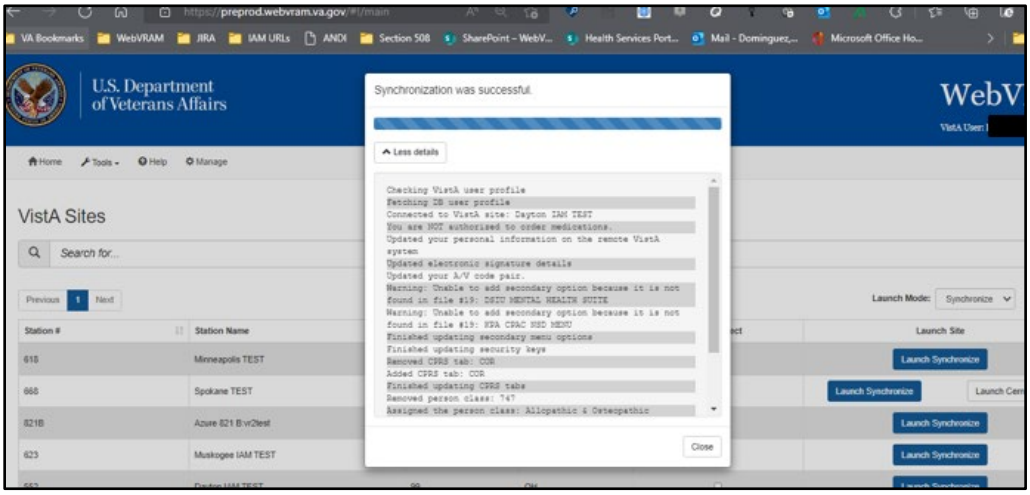
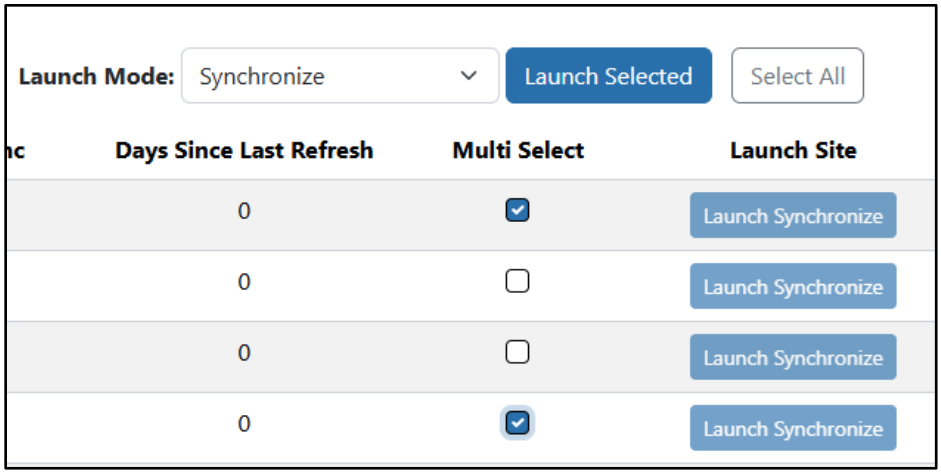


Figure 60: Launch Synchronize Successful



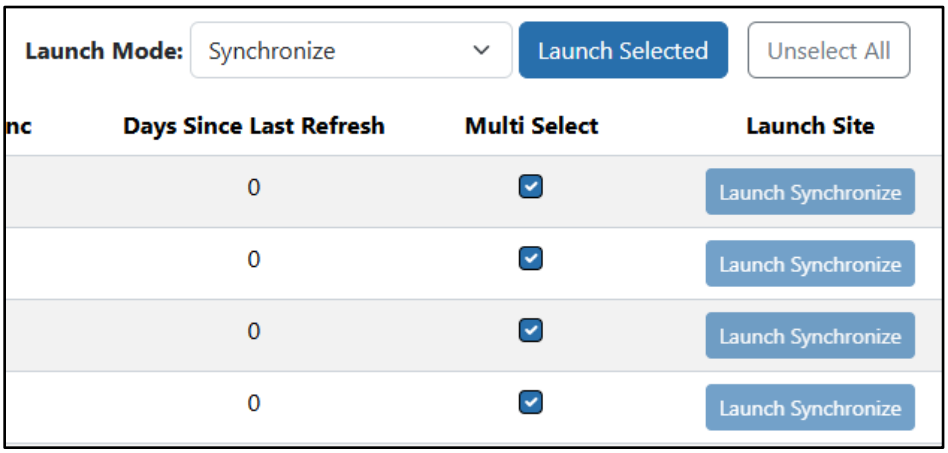
You can synchronize to multiple sites by selecting the Multi Select checkboxes for sites you wish to synchronize and clicking the 'Launch Selected' button.

Figure 61: Multi Select



You can synchronize to all sites by selecting 'Select all' and clicking the 'Launch Selected' button.

Figure 62: Select All



NOTE: 'Select All' only selects all sites on the current visible page. To sync to sites on subsequent pages, you must use 'Select All' and 'Launch Selected' on each page.

5.3 Changing Verify Code

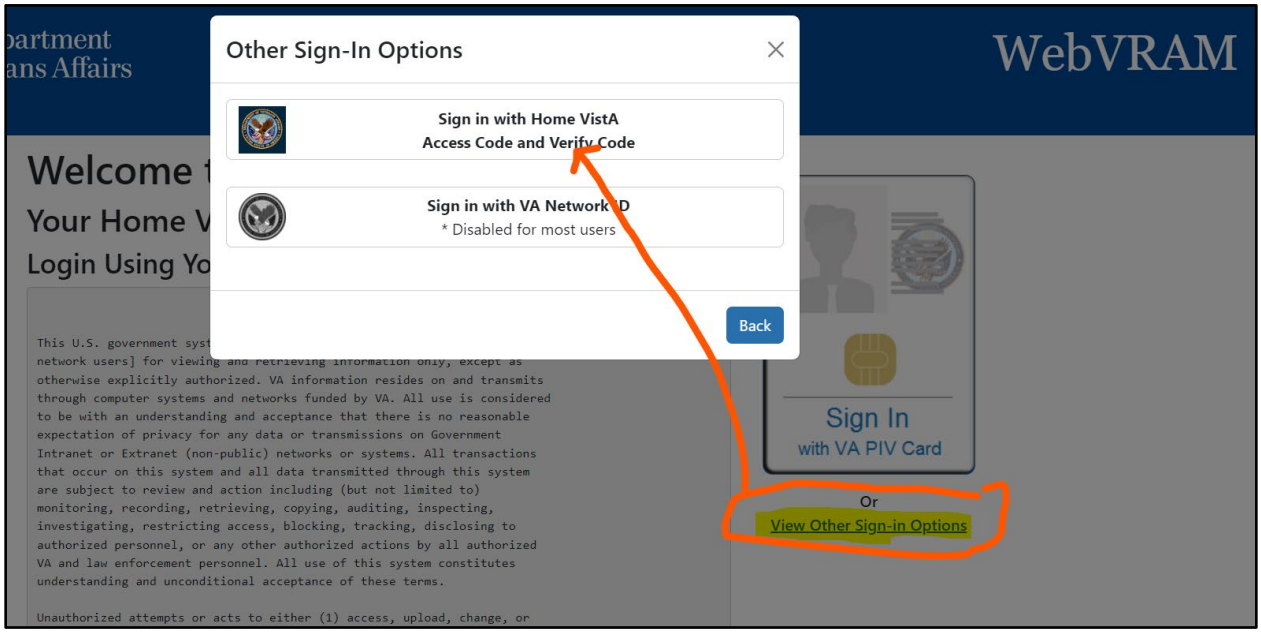
5.3.1 Changing Active Verify Code

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.

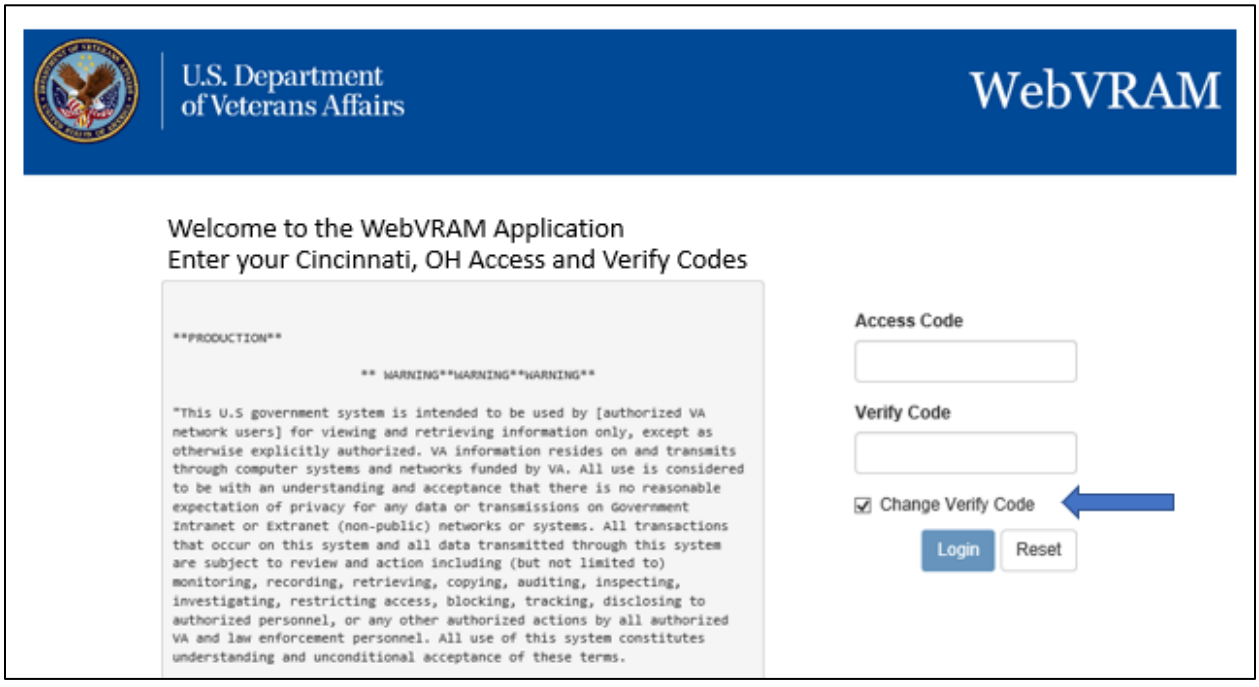
2. The Terms and Conditions web page is displayed. Click **Accept the Terms and Conditions**.
3. The Login page is displayed. Select View Other Sign-in Options and select the 'Sign in with Home VistA Access Code and Verify Code' button.

Figure 63: Other Sign-In Options



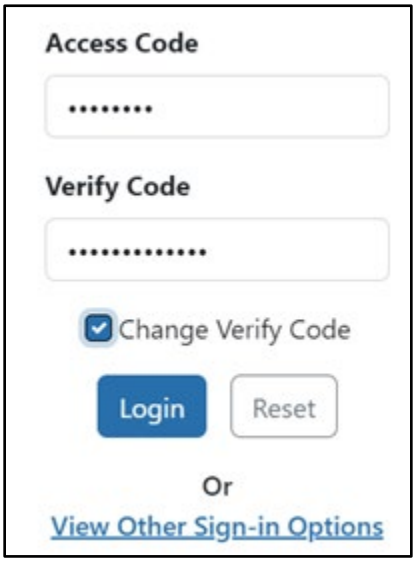
4. Click the 'Change Verify Code' checkbox

Figure 64: WebVRAM Login – Change Verify Code



5. Select 'Login'
6. Enter your local VistA Access and Verify Codes and click the **Change Verify Code** checkbox.
7. Click **Login**

Figure 65: Update Access and Verify Code

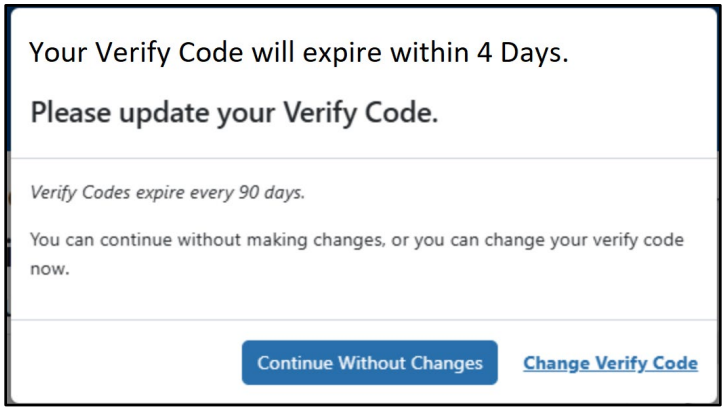


8. Note that once the change has been made, the new Verify code will apply to all future A/V code logins to your local VistA system and the WebVRAM application.

5.3.2 Expiring or Expired Verify Codes

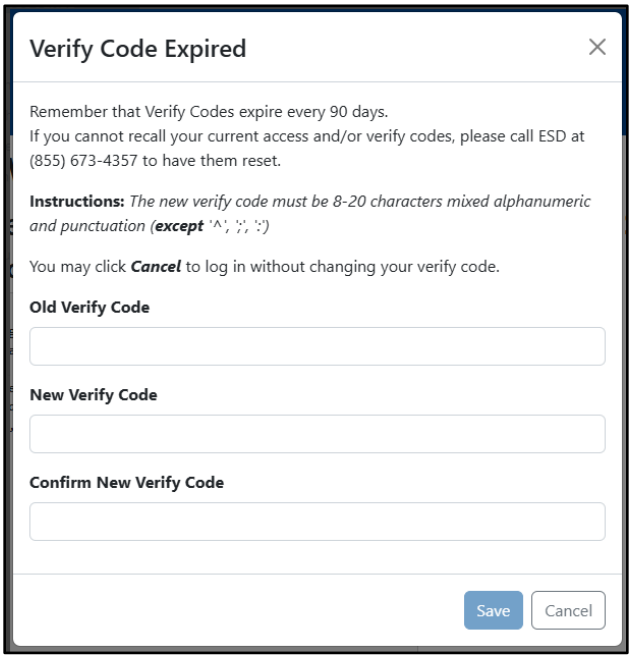
If the user's Verify Code (at their local VistA) will expire within 5 days, or if the Verify Code (at their local VistA) is already expired, WebVRAM will provide a popup asking the user to change their Verify Code. If the user has logged in with their PIV card, you will be prompted for the Old Verify Code.

Figure 66: Verify Code Expiring Soon Window



Enter your Old Verify Code (if requested) and New Verify code in both the New and Confirm Verify Code boxes and click Save.

Figure 67: Change Verify Code - Expired Code PIV login



If the user logged in using Access and Verify codes, then the Old Verify Code will already be captured by WebVRAM, and it will not be required when creating a new Verify Code.

Enter your New Verify Code in both text boxes and click Save. Alternately, you can select Cancel and proceed to login without updating your Verify code.

CAUTION: If the VA experiences a PIV system outage or other interruption to PIV functionality, and your Verify code is expired, you will need to open an ESD Ticket to update the code to log in to WebVRAM. ESD is likely to have limited availability during such an event. It is recommended to keep your Verify code up to date.

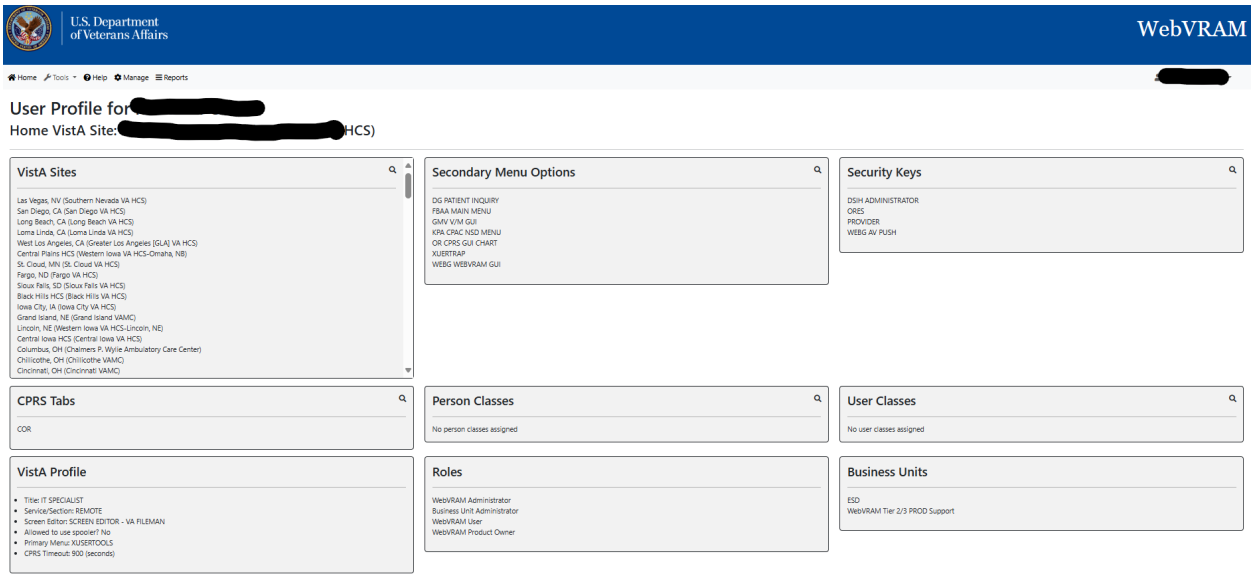
5.4 User Profile

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

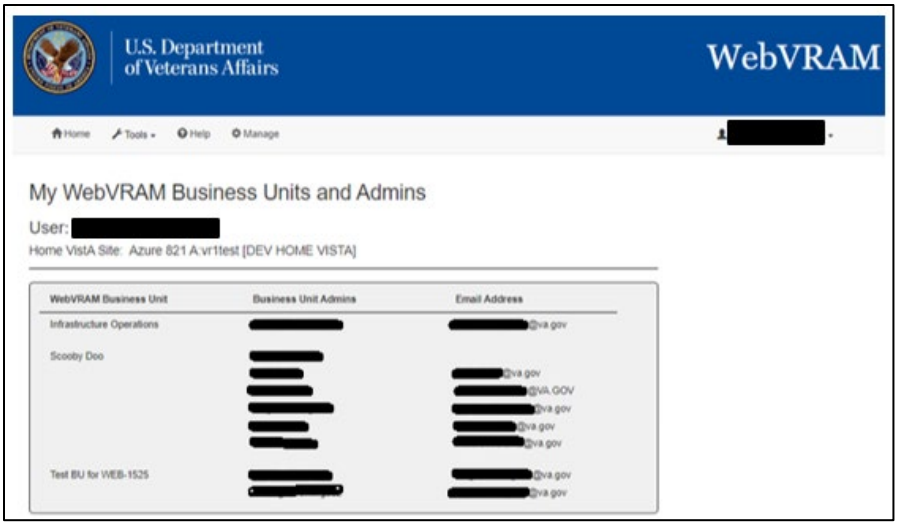
To view the user's profile, click on the Username and select **My Profile** from the drop-down menu; the browser will display the User's Profile page.

Figure 68: 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.

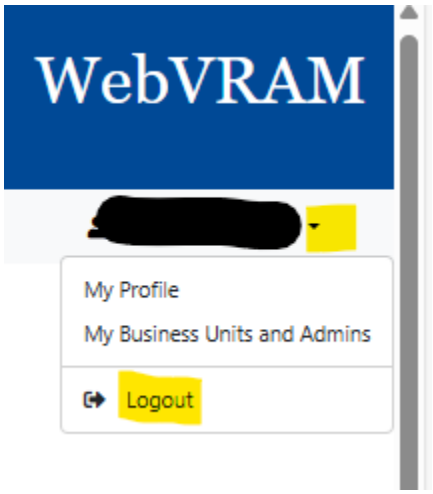
Figure 69: My Business Unit and Admins page



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 70: WebVRAM Logout



6. Troubleshooting

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

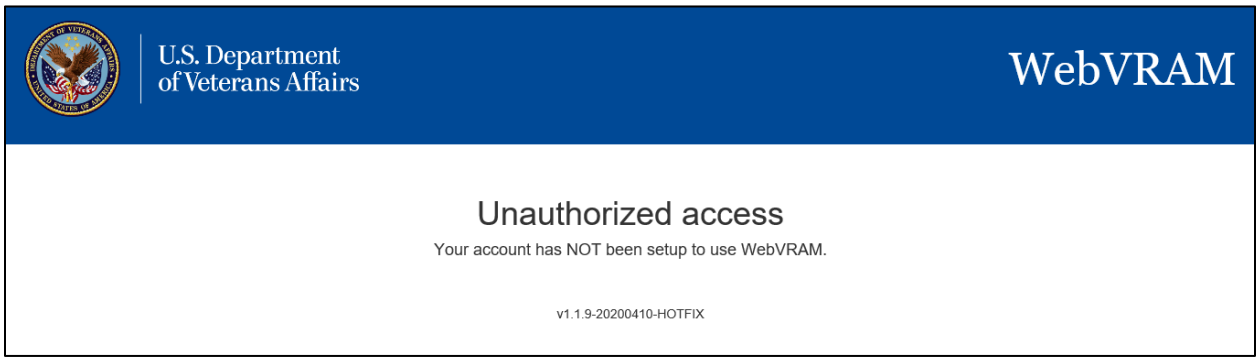
6.1 Special Instructions for Error Correction

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 71: 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.

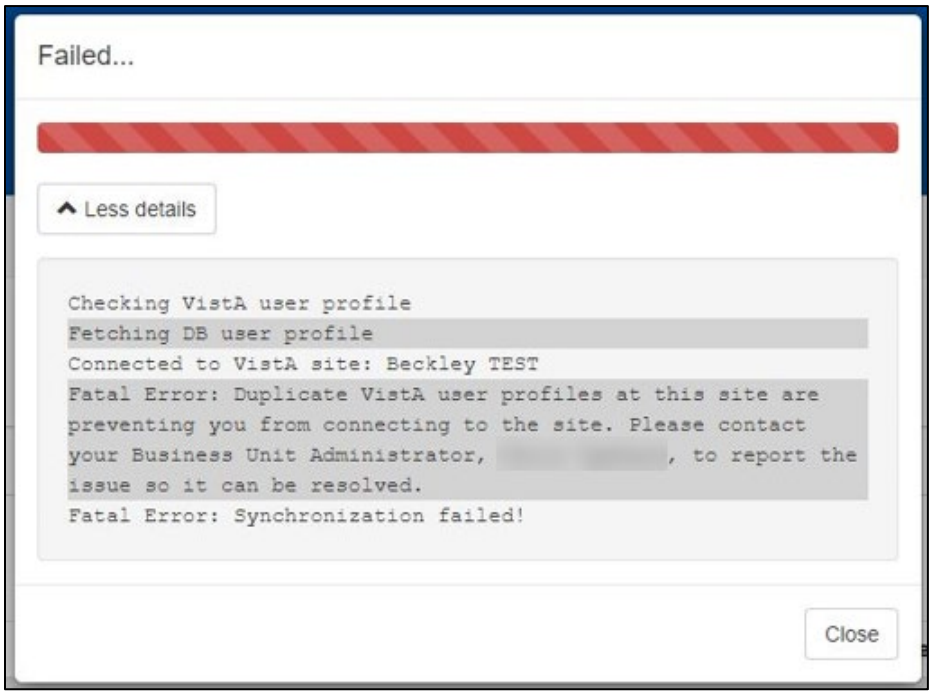
6.1.3 Duplicate VistA Accounts at Remote Site

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 72: Duplicate VistA Account Error



6.1.4 Network Connectivity

If there is a network issue preventing access to the user's home VistA, then the PIV card login image and A/V code input form will be disabled. A warning message will appear advising you to submit a YourIT ticket.

Check the YourIT main page for any announcements of network outages and follow any instructions provided on that page. If there is a local outage, contact your Local IT team or the ESD and open a ticket.

6.1.5 Other Errors

For all other errors encountered during use of the WebVRAM application, create a ticket through Service Now (SNOW)/yourIT or call the ESD. The ESD can only update Access and Verify codes via telephone.

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 calling the ESD.

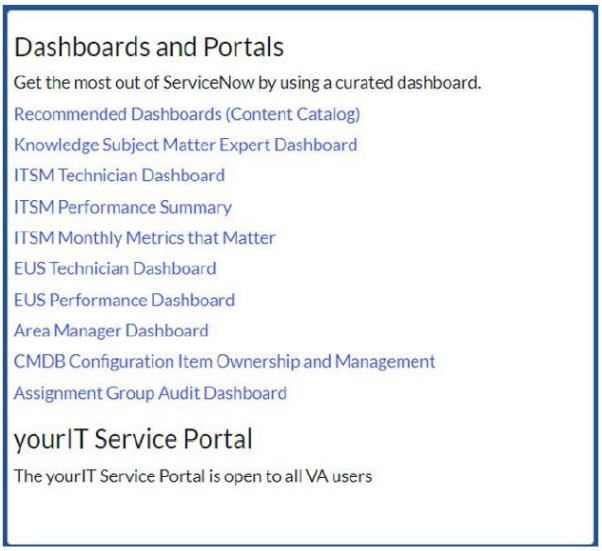
How to submit an ESD ticket using SNOW/yourIT for a WebVRAM issue:

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

Figure 73: yourIT Desktop Icon

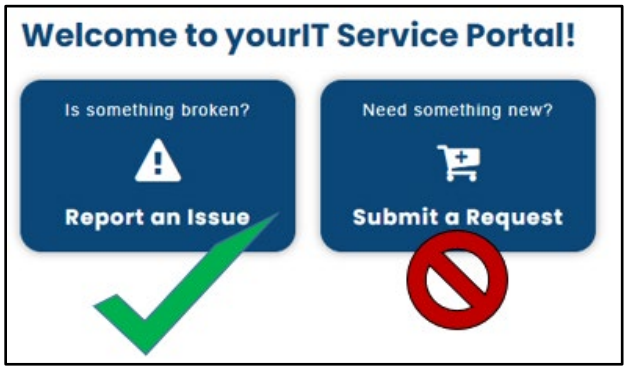
2. From the main ITIL User Dashboard page, select the link under yourIT Service Portal

Figure 74: yourIT Desktop Icon



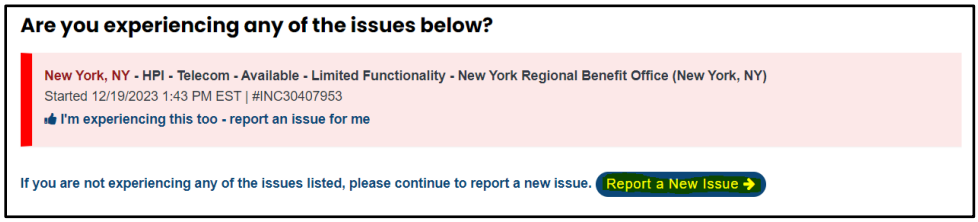
3. Select the 'Report an Issue' button. Do not select 'Submit a Request'

Figure 75: Report an Issue button



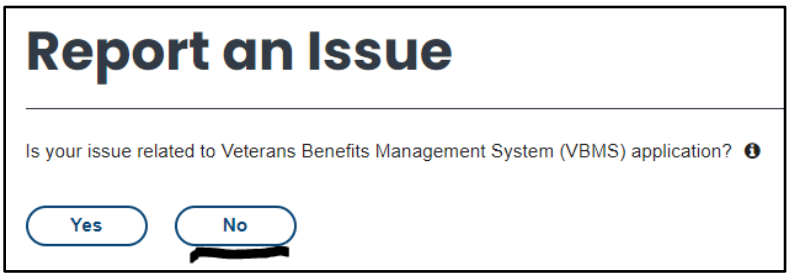
4. Review the current issues list. If your issue is included, click the 'thumbs up' icon and close your browser. The issue is already being worked on. If your issue is not included, then click the 'Report a New Issue' button.

Figure 76: Report a New Issue



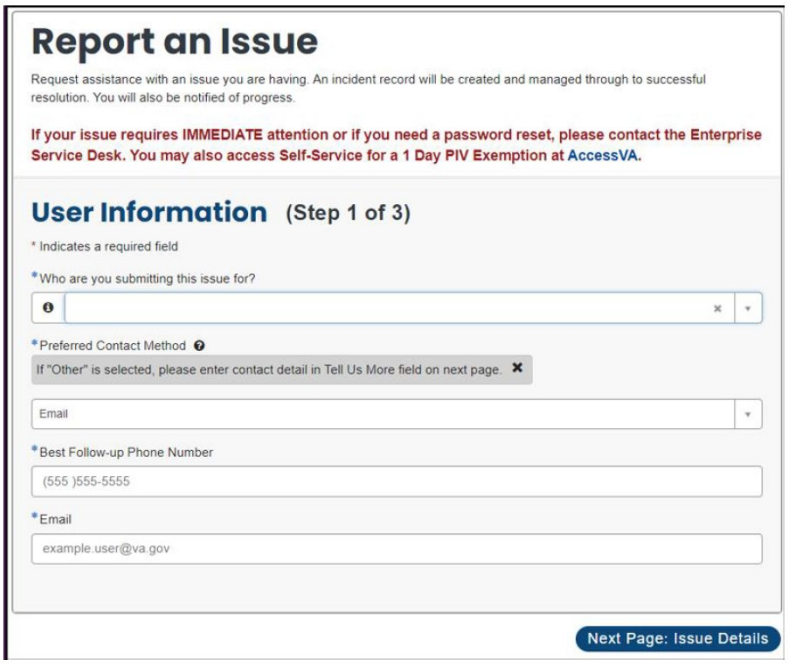
5. Click the NO option when asked if your issue is related to Veteran's Benefit Management Systems (VBMS). WebVRAM is not associated with this application.

Figure 77: Report a New Issue continued



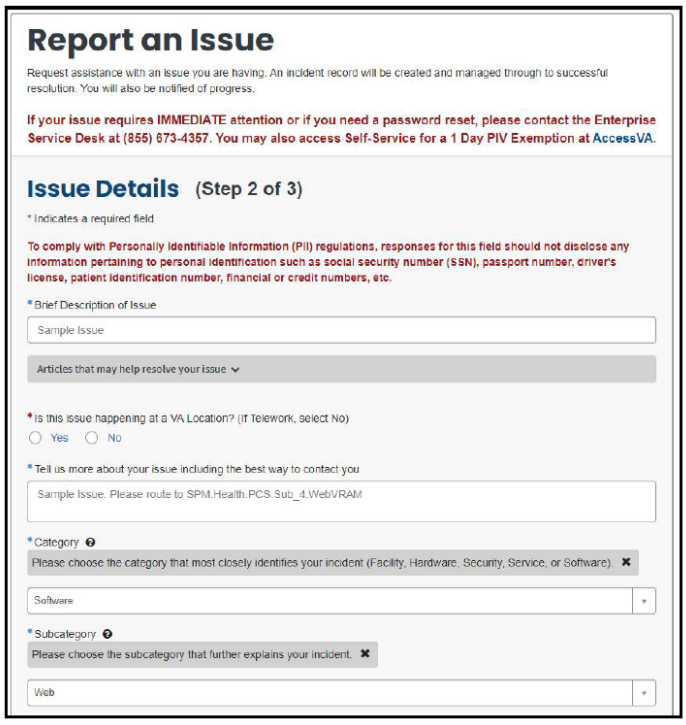
6. Fill in the Affected End User (*Who are you submitting this issue for?), preferred contact method, phone number, and email address.

Figure 78: User Information



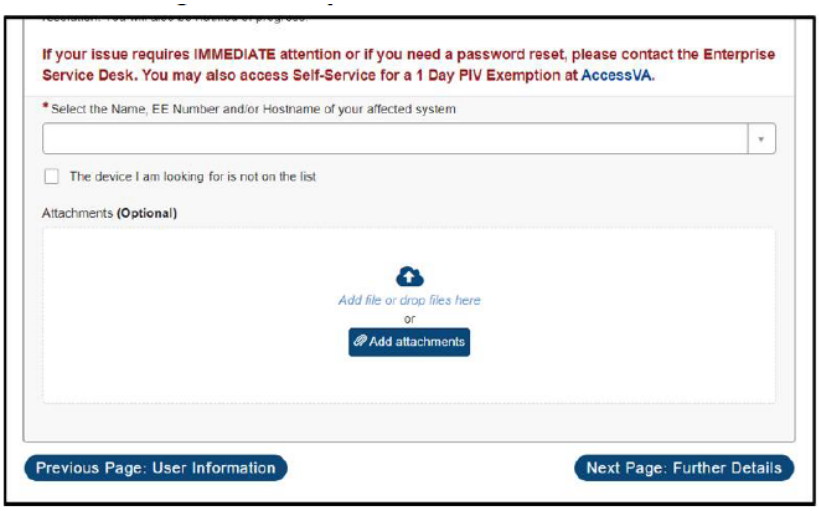
7. Fill in the requested fields. Request that the ESD route the ticket to **SPM.Health.PCS.Sub_4.WebVRAM.** For Category, select 'Software' and for Subcategory, select 'Web'. Enter the WebVRAM URL for the URL issue field.

Figure 79: Report an Issue fields



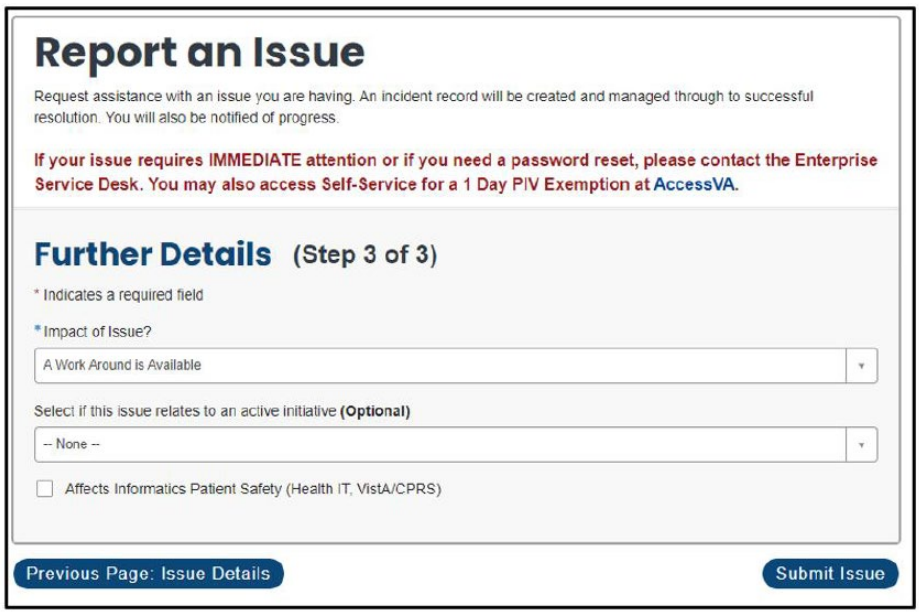
8. At the bottom of this page, add any relevant attachments and select ‘Next Page: Further Details’

Figure 80: Report an Issue fields cont'd



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

Figure 81: Further Details and Submit Issue



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

Term	Definition
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
PDF	Portable Document Format
PHI	Protected Health Information

Term	Definition
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identification Verification
PIV	Personal Identification and Validation
PDMP	Prescription Drug-Monitoring Program
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	*Not an acronym.* 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