

Web VistA Remote Access Management (WebVRAM)

User Guide



December 2019

Department of Veterans Affairs

Office of Information and Technology (OIT)

Revision History

Date	Revision	Description	Author
12/6/2019	1.9	Technical Writer review and edit.	K. Robbins, 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.	E. Clark, WebVRAM PMO Team
12/3/2019	1.7	Updated to address comments from Health Product Support.	K. Robbins, 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 Team
10/29/2019	1.5	Technical Writer review and edit.	K. Robbins, 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.	E. Clark, WebVRAM PMO Team
10/24/2019	1.3	Changed date on cover page to current month.	E. Clark, WebVRAM PMO Team
9/16/2019	1.2	Added clarification for FBCS users.	E. Clark, WebVRAM PMO Team
8/27/2019	1.1	Technical Writer review and edit.	K. Robbins, VA OIT EPMO
8/23/2019	1.0	Baseline.	WebVRAM PMO Team

Table of Contents

1. Introduction	1
1.1. Purpose.....	1
1.2. Document Orientation.....	1
1.2.1. Organization of the Manual	1
1.2.2. Assumptions	2
1.2.3. Coordination.....	2
1.2.4. Disclaimers	2
1.2.4.1. Software Disclaimer	2
1.2.4.2. Documentation Disclaimer	2
1.2.5. Documentation Conventions	3
1.2.6. References and Resources.....	3
1.3. Enterprise Service Desk and Organizational Contacts.....	3
2. System Summary	4
2.1. System Configuration.....	4
2.2. Data Flows	5
2.3. User Access Levels	7
2.4. Continuity of Operation	7
3. Getting Started	8
3.1. Logging in to WebVRAM	9
3.2. Update eSignature Code and Details	10
4. Using the Software – VistA Sites Page	13
4.1. Remote Session: Launch Mode	13
4.1.1. Launch Mode: Reflection	15
4.1.1.1. Launching Different Multiple Remote VistA Sessions	16
4.1.1.2. Launching Simultaneous Multiple VistA Sessions at a Single Site	17
4.1.1.2.1. CPAC Users: Configure Tile View for Multiple VistA Sessions at the Same Site.....	20
4.1.2. Launch Mode: CPRS	23
4.1.2.1. Launching Multiple CPRS Sessions	25
4.1.3. Launch Mode: Synchronize.....	26
4.2. Changing Verify Code.....	27
4.3. Exit System.....	28
5. Troubleshooting.....	29
5.1. Special Instructions for Error Correction.....	29
5.1.1. Unauthorized Access Error	29
5.1.2. Reflection Fails to Launch.....	29
5.1.3. Other Errors	29
6. Acronyms and Abbreviations	30

List of Figures

Figure 1: WebVRAM High-level System Interfaces	5
Figure 2: WebVRAM High-level Application Design	5
Figure 3: WebVRAM Data Flow and User Navigation	7
Figure 4: WebVRAM Terms and Conditions for Usage Screen.....	9
Figure 5: WebVRAM Login Screen	9
Figure 6: WebVRAM Home Screen	10
Figure 7: Tools Dropdown – Update eSignature Code.....	10
Figure 8: Update eSignature Code Screen	11
Figure 9: Update eSignature Details	11
Figure 10: Launch Mode Dropdown	14
Figure 11: Launch Reflection Button	15
Figure 12: VistA Login	15
Figure 13: Launch Multiple Reflection Sessions to Different Remote VistA Systems....	16
Figure 14: Reflection Workspace Settings Access.....	17
Figure 15: Reflection – Configure User Interface Link.....	18
Figure 16: Reflection – Change User Interface Mode	19
Figure 17: Reflection – Cascading View of Multiple Same-site Sessions.....	20
Figure 18: Reflection – Arrange Windows Icon and Dropdown	21
Figure 19: Reflection – Arrange Windows Tile Vertical Selection.....	21
Figure 20: Reflection – Tile Vertical View	22
Figure 21: Launch CPRS Button	23
Figure 22: CPRS Version Screen.....	23
Figure 23: PIV Select a Certificate Screen	24
Figure 24: CPRS Login Screen	24
Figure 25: Launch Synchronize Button	26
Figure 26: WebVRAM Login – Change Verify Code	27
Figure 27: WebVRAM Logout	28

List of Tables

Table 1: Documentation Symbols and Descriptions	3
Table 2: Enterprise Service Desk Support Information.....	3
Table 3: Acronyms and Abbreviations.....	30

1. Introduction

In April 2011, the Executive Director of Office of Information 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 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.

1.1. 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.

1.2. Document Orientation

The document orientation is shown below in Sections 1.2.1 through 1.2.6.

1.2.1. 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.

1.2.2. 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. They 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 Administrator.

1.2.3. 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 3 below.

WebVRAM software and documentation disclaimers include disclaimers “as written” in all VA user documentation and are shown below in Sections 1.2.4.1 and 1.2.4.2.

1.2.4. Disclaimers

1.2.4.1. 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 and/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.

1.2.4.2. 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.

1.2.5. 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**.

1.2.6. References and Resources

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

1.3. 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): 1-855-673-4357
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.

2. System Summary

WebVRAM is a web-based, cloud-hosted application utilizing VA Enterprise Architecture and Design principles which facilitates user access to multiple remote VistA systems and related applications such as Computerized Patient Record System (CPRS) and the Fee Basis Claim System (FBCS), 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 Internet Explorer version 11.0.



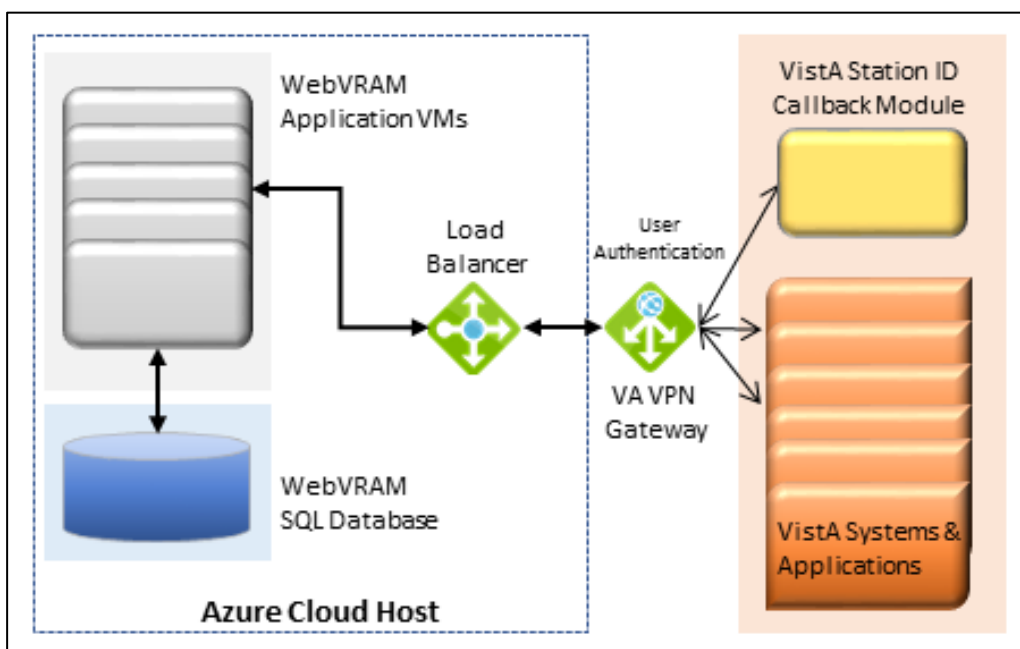
CAUTION: The ability to access remote VistA systems provided by WebVRAM relies on the use of the Micro Focus® Reflection® Workspace (Reflection) application provided with the standard VA image on all VA laptops/workstations. The Reflection software is only approved for use by VA with the Internet Explorer web browser. Other web browsers will not support automated access to remote VistA systems provided by the WebVRAM application.

2.1. 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 1. 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.

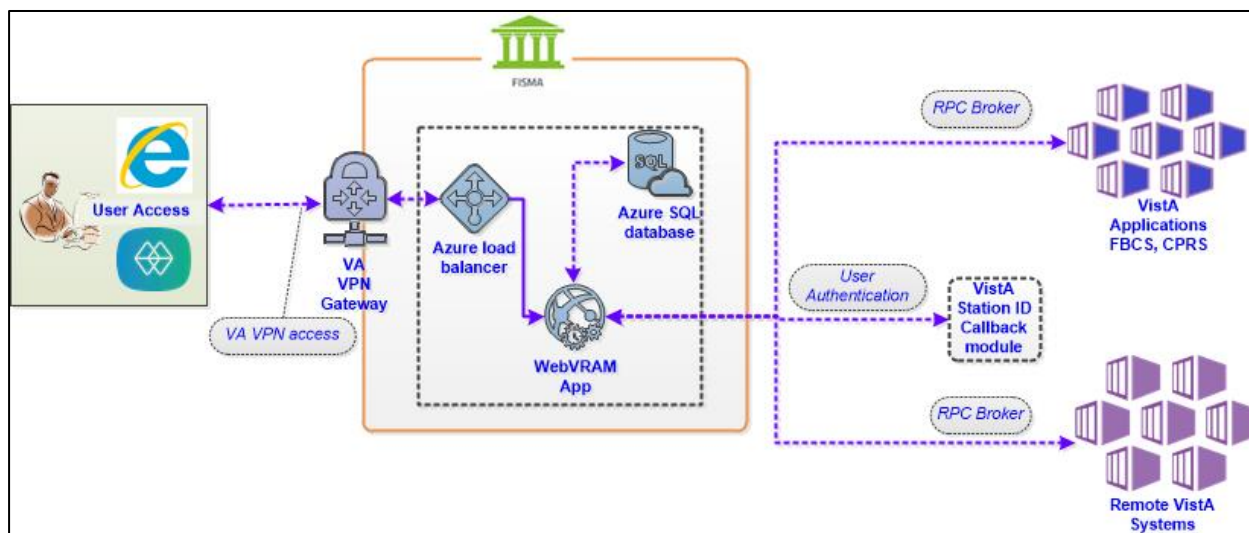
Figure 1: WebVRAM High-level System Interfaces



2.2. Data Flows

Figure 2 provides a high-level architectural view of the WebVRAM solution. A discussion follows this diagram regarding data flows from a user perspective.

Figure 2: 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:

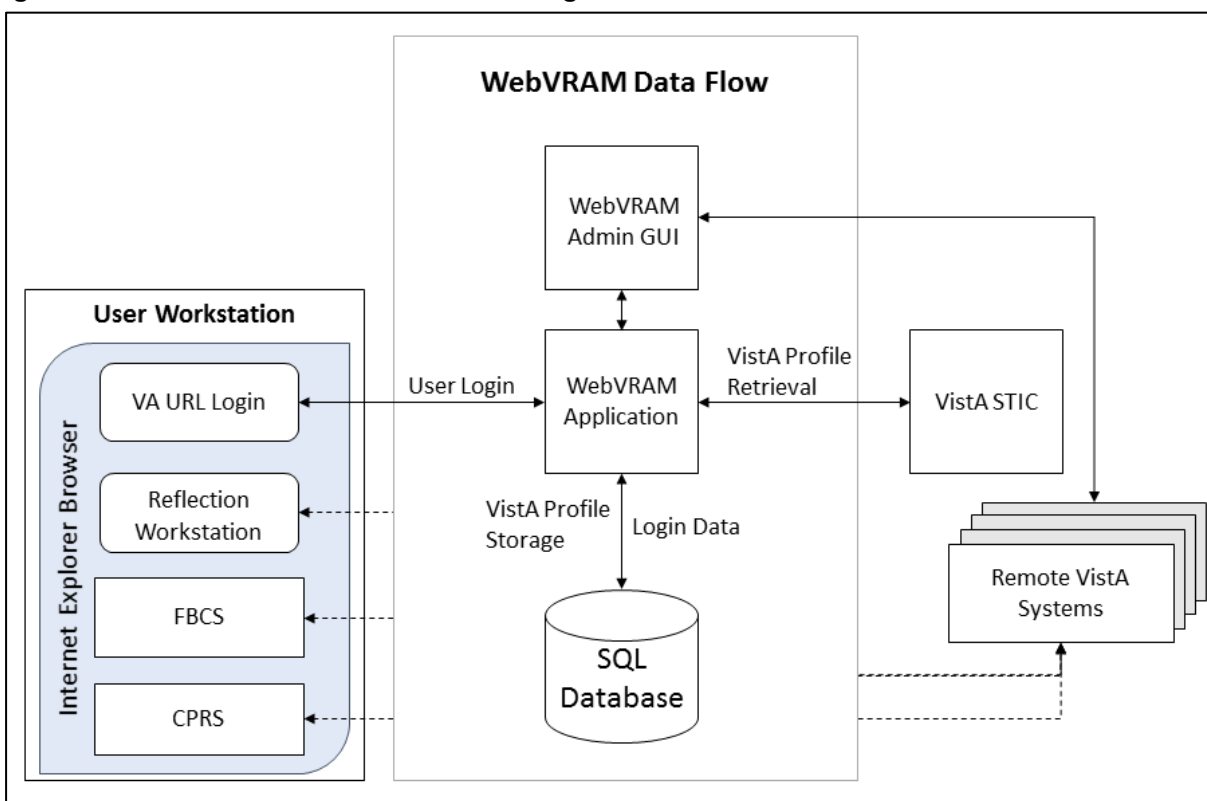
- VistA authorized menus and keys
- Electronic signature,
- User title
- Service/section
- Name
- Degree
- National Provider Identifier (NPI)
- NPI Status

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) he/she 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 by their line management to access the Fee Basis Claim System (FBCS), the FBCS security keys in their local VistA profile will be used by WebVRAM to allow FBCS access. 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 3 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 3: WebVRAM Data Flow and User Navigation



2.3. 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.

2.4. 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 similar to what the user experienced in the primary production environment.

3. Getting Started

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

1. A WebVRAM user must have an active VA Network profile, and an active “home” or local VistA user profile. Please coordinate with your business line manager to complete the VA onboarding processes required to obtain VA network access and to establish a local VistA user profile.
2. The user obtains permission from their business line management to use the WebVRAM application to access remote VistA systems and perform job-related work at those locations.
3. Once permission is obtained, the user works with their business line management and follows the business-defined process to:
 - a. Contact their local IT Support Staff or log an Enterprise Service Desk ticket to have this item added to their local VistA User Profile:
 - i. WEBG WEBVRAM GUI Secondary Menu Option
 - b. Contact the WebVRAM Business Administrator assigned to their business unit to request their user profile be added to the WebVRAM database, which will allow login to the application.
4. All users need to complete this step, unless they have already done so. To prepare for future 2-Factor Authentication (2FA)/ Personal Identification Verification (PIV) login to WebVRAM, the user must perform a one-time link of their home VistA user profile to their PIV login capabilities through the Identify and Access Management (IAM) Link My Account process.

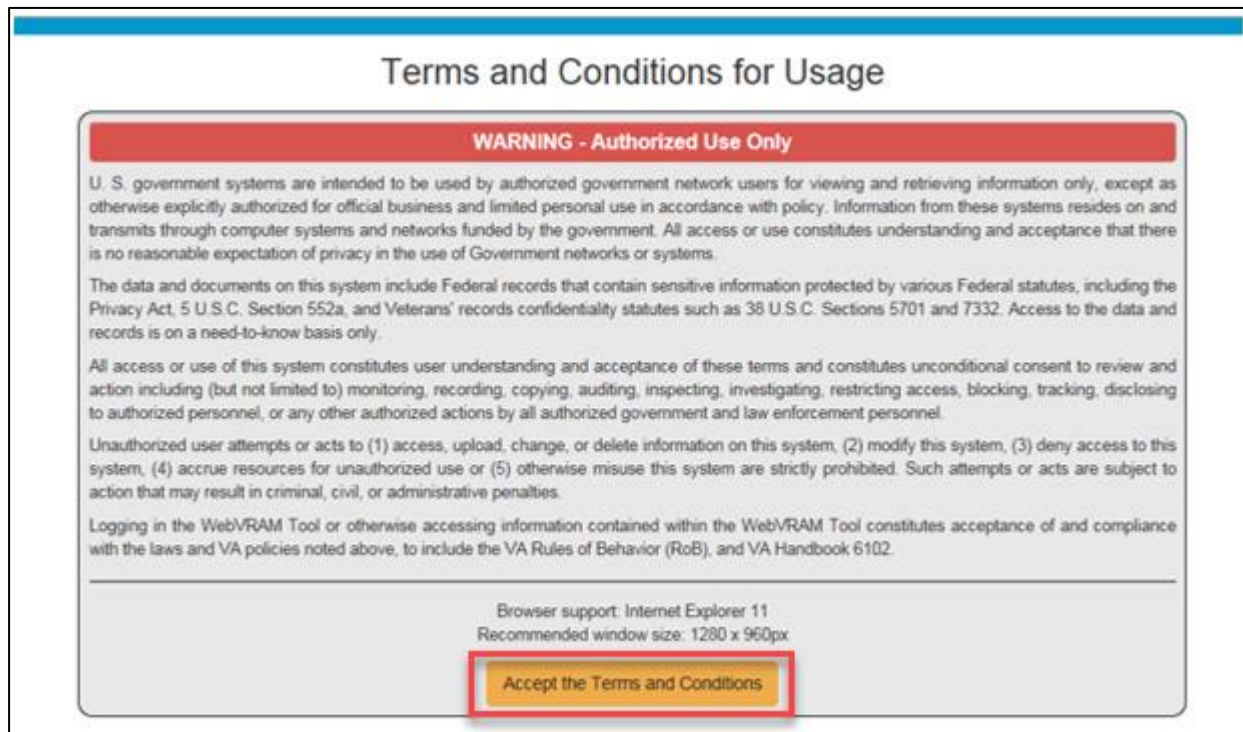
To perform the link, follow the instructions in the YourIT/Service Now (SNOW) Knowledge Article entitled, “[How do I bind or link my PIV card to my VistA/CPRS account?](#)”

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

3.1. Logging in to WebVRAM

1. From your Internet Explorer browser, navigate to the WebVRAM home page at this link: <https://WebVRAM.va.gov/>
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 4: WebVRAM Terms and Conditions for Usage Screen



Terms and Conditions for Usage

WARNING - Authorized Use Only

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

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

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

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

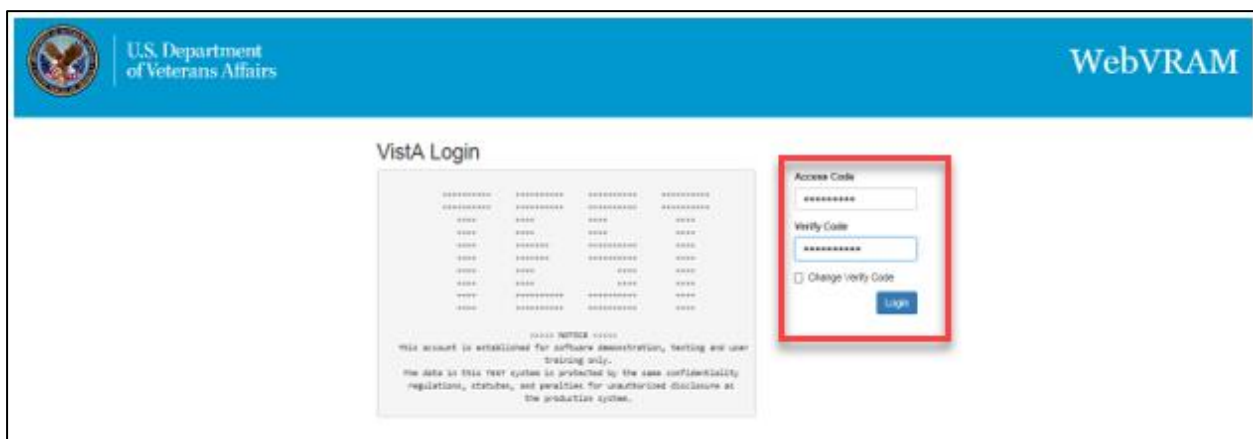
Logging in the WebVRAM Tool or otherwise accessing information contained within the WebVRAM Tool constitutes acceptance of and compliance with the laws and VA policies noted above, to include the VA Rules of Behavior (RoB), and VA Handbook 6102.

Browser support: Internet Explorer 11
Recommended window size: 1280 x 960px

Accept the Terms and Conditions

3. The next web page displayed is the WebVRAM Login page. Enter your local Vista Access and Verify Codes and click **Login** to access the application features.

Figure 5: WebVRAM Login Screen



U.S. Department of Veterans Affairs **WebVRAM**

Vista Login

Access Code

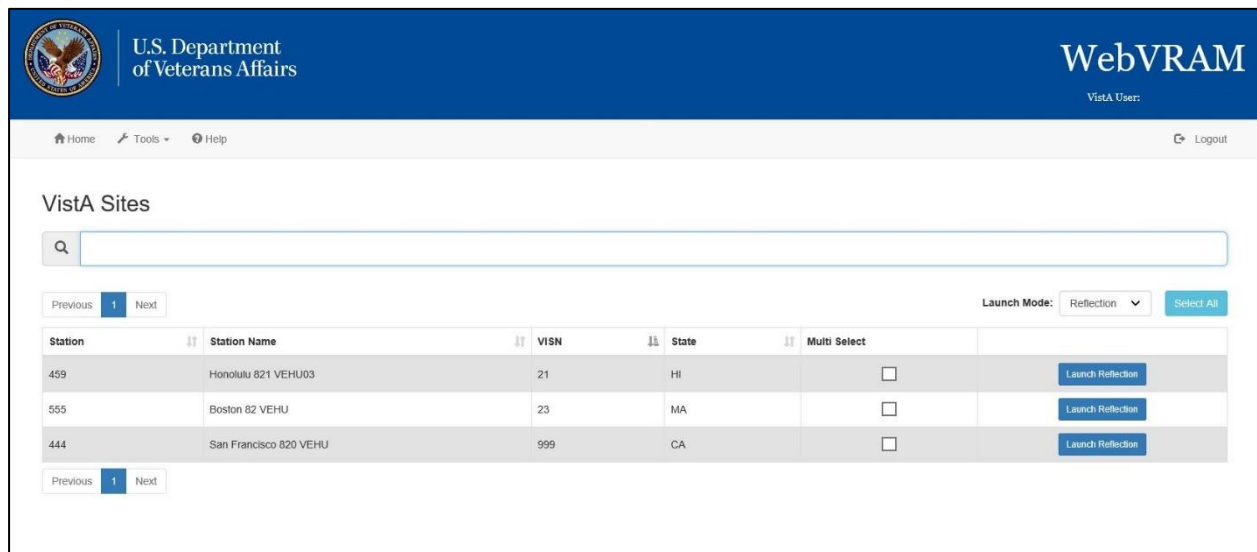
Verify Code

☐ Change Verify Code

Login

4. The WebVRAM application's home page is displayed. In some instances, during login, a window will open with a request to update your Electronic Signature (eSignature) code. See Section 3.2 Update eSignature Code for instructions for updating this code and associated data.

Figure 6: WebVRAM Home Screen



3.2. Update eSignature Code and Details

The Update eSignature Code window may appear during the first login to WebVRAM. The user may also choose at any time to 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**.

Figure 7: Tools Dropdown – Update eSignature Code



Figure 8: Update eSignature Code Screen

The screenshot shows the 'Update eSignature Code' dialog box overlaid on the VistA Sites application interface. The dialog box has a title bar with the text 'Update eSignature Code' and a close button (X). Below the title bar, there is an 'Instructions' section stating: 'eSignature code must be 6 to 20 characters in length with no control or lowercase characters.' Below the instructions, there are two input fields: 'New eSignature Code' and 'Confirm eSignature Code'. The 'New eSignature Code' field contains the placeholder text 'new eSignature code'. The 'Confirm eSignature Code' field contains the placeholder text 'confirm eSignature code'. At the bottom right of the dialog box, there are two buttons: 'Update' (with a floppy disk icon) and 'Cancel' (with an X icon).

To update the eSignature Code:

1. 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 and/or numbers can be used.
2. Enter the same new eSignature code in the **Confirm eSignature Code** field, then click **Update**.

Figure 9: Update eSignature Details

The screenshot shows the 'Update eSignature Details' dialog box. The dialog box has a title bar with the text 'Update eSignature Details' and a close button (X). Below the title bar, there are several input fields: 'eSignature Name' (with a blacked-out placeholder), 'eSignature Title' (with the text 'IT SPECIALIST'), 'eSignature Initials' (with a blacked-out placeholder), 'Office Phone Number' (with a blacked-out placeholder), 'Voice Pager Number' (with the placeholder text 'Voice Pager Number'), and 'Digital Pager Number' (with the placeholder text 'Digital Pager Number'). At the bottom right of the dialog box, there are two buttons: 'Save changes' (with a floppy disk icon) and 'Cancel' (with an X icon).

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**. Enter the following data elements in the appropriate fields:

- 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. Using the Software – VistA Sites Page

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

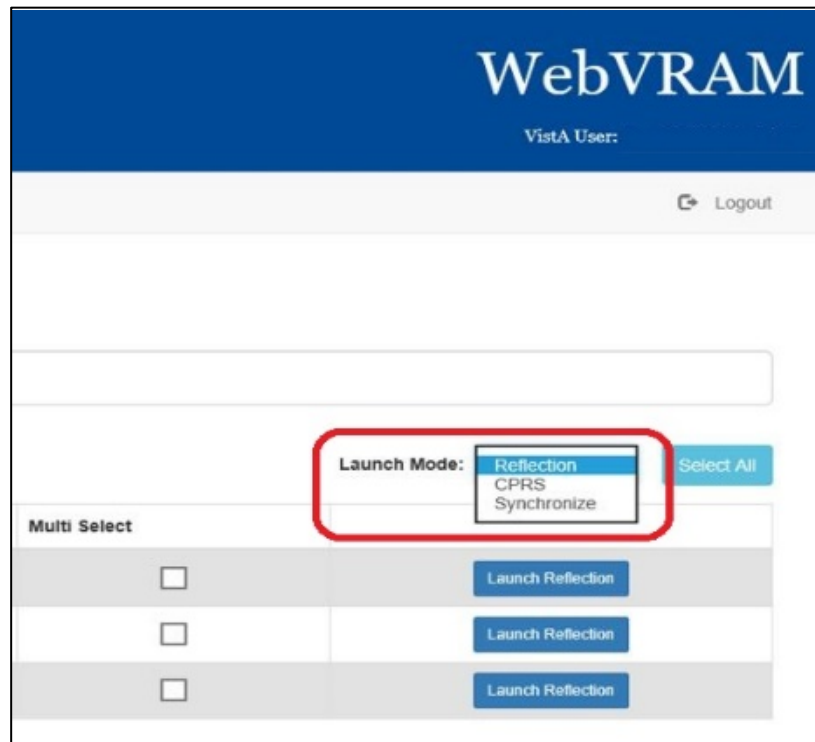
4.1. Remote Session: Launch Mode

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

Available drop-down options are:

- Reflection – This option is used to launch a remote VistA session with Reflection to connect to a remote VistA system already assigned to the user’s profile.
- CPRS – This option is used to launch a remote VistA CPRS session at the selected remote location.
- Synchronize – Similar to launching Reflection, *if the user does not need to perform work at the remote location*, this option is used to connect to and setup or update an active VistA login account at a remote VistA site. If there are changes to the user’s local VistA profile, the Synchronize option will push those changes to the selected remote location(s). If the user’s line management determines that he/she needs access to a new VistA site, the new location can be added to the user’s WebVRAM profile by the business-appointed WebVRAM Administrator.

Figure 10: Launch Mode Dropdown



4.1.1. 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. Click on **Launch Reflection**. WebVRAM will launch Reflection and log the user into the remote VistA site that was selected.



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

Figure 11: Launch Reflection Button

Station	Station Name	VISN	State	Multi Select	
459	Honolulu 821 VEHU03	21	HI	<input type="checkbox"/>	Launch Reflection
555	Boston 82 VEHU	23	MA	<input type="checkbox"/>	Launch Reflection
444	San Francisco 820 VEHU	999	CA	<input type="checkbox"/>	Launch Reflection

Previous 1 Next

4. Once the **Launch Reflection** button is clicked, 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, similar to what the user has access to in their local VistA system, as shown in the screen shot below.

Figure 12: VistA Login

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

Restore date:   MAR 25,2019

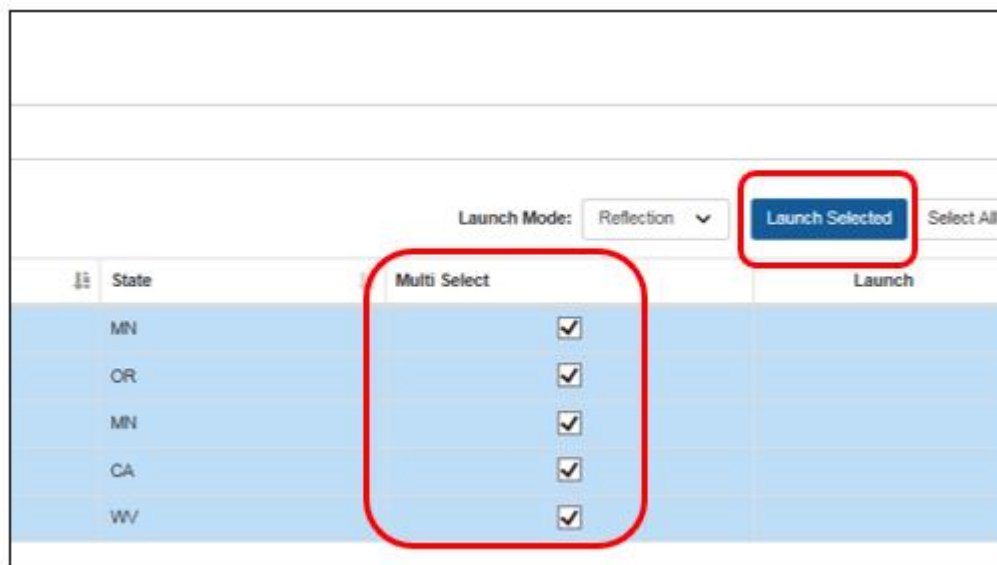
Volume set: TOU:TBAISCSVR  UCI: TBA  Device: FTA741: (10.232.129.61/)

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

4.1.1.1. Launching Different Multiple Remote VistA Sessions

Multiple VistA sessions at different remote VistA locations can be launched together by checking the box for each VistA to be launched simultaneously in the **Multi Select** column on the user's home page. When one or more boxes to launch Reflection are checked, the **Launch Mode** selection option changes to **Launch Selected**. Clicking the **Launch Selected** button, with one or more boxes checked in the **Multi Select** column, then launches different multiple VistA sessions at the same time. Figure 13 shows the boxes checked for each site the user intends to launch, and the **Launch Selected** mode for performing this action.

Figure 13: 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.

4.1.1.2. Launching Simultaneous Multiple VistA Sessions at a Single Site

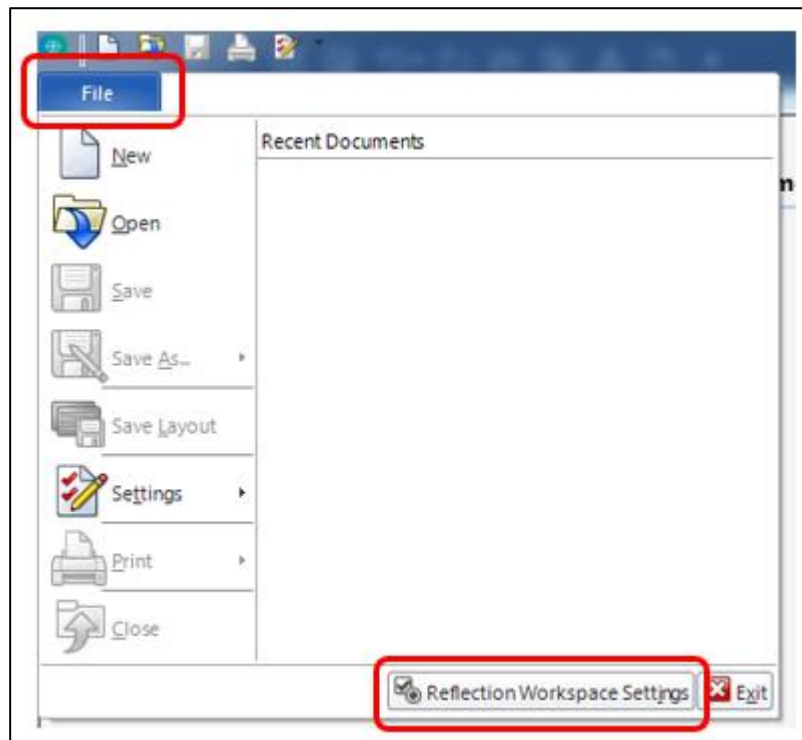
Launching simultaneous multiple Reflection connection sessions at the same site is done by launching the first session from the WebVRAM home page as discussed in Section 4.1.1 Launch Mode: Reflection, then repeating the launch steps to launch additional simultaneous connection sessions to the same VistA 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.

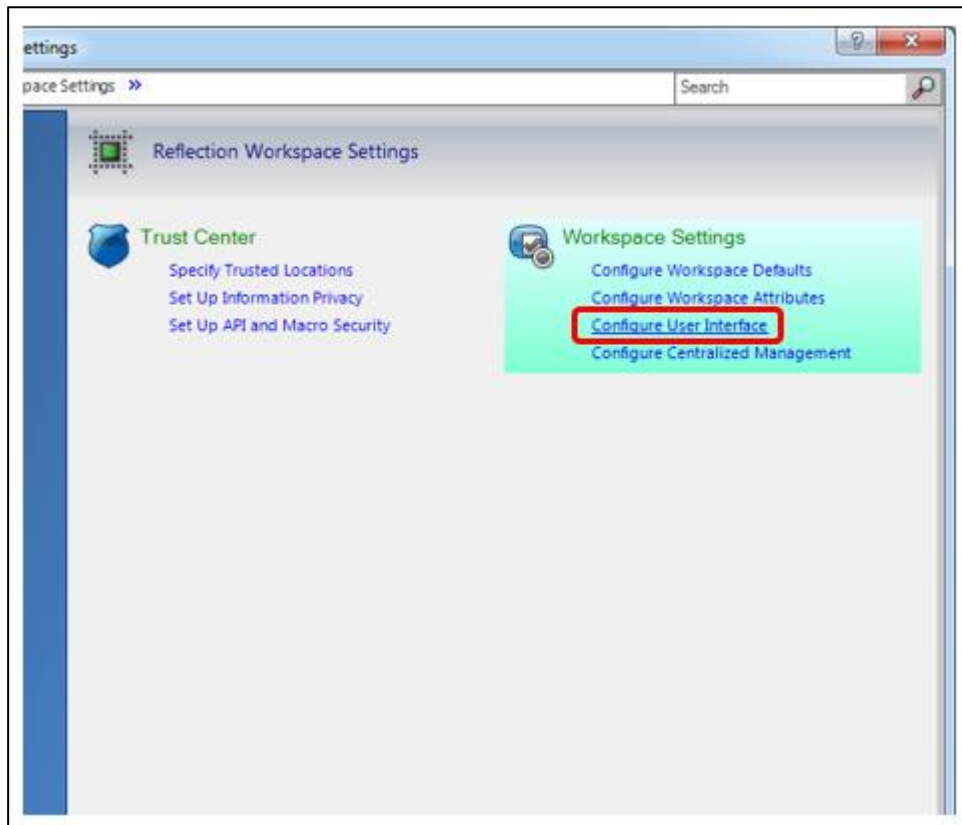
1. Open *Reflection Workspace* on your workstation. In the upper left corner, click the **File** tab.
2. In the pop-up window that opens, click on **Reflection Workspace Settings** in the lower right corner, as shown below.

Figure 14: Reflection Workspace Settings Access



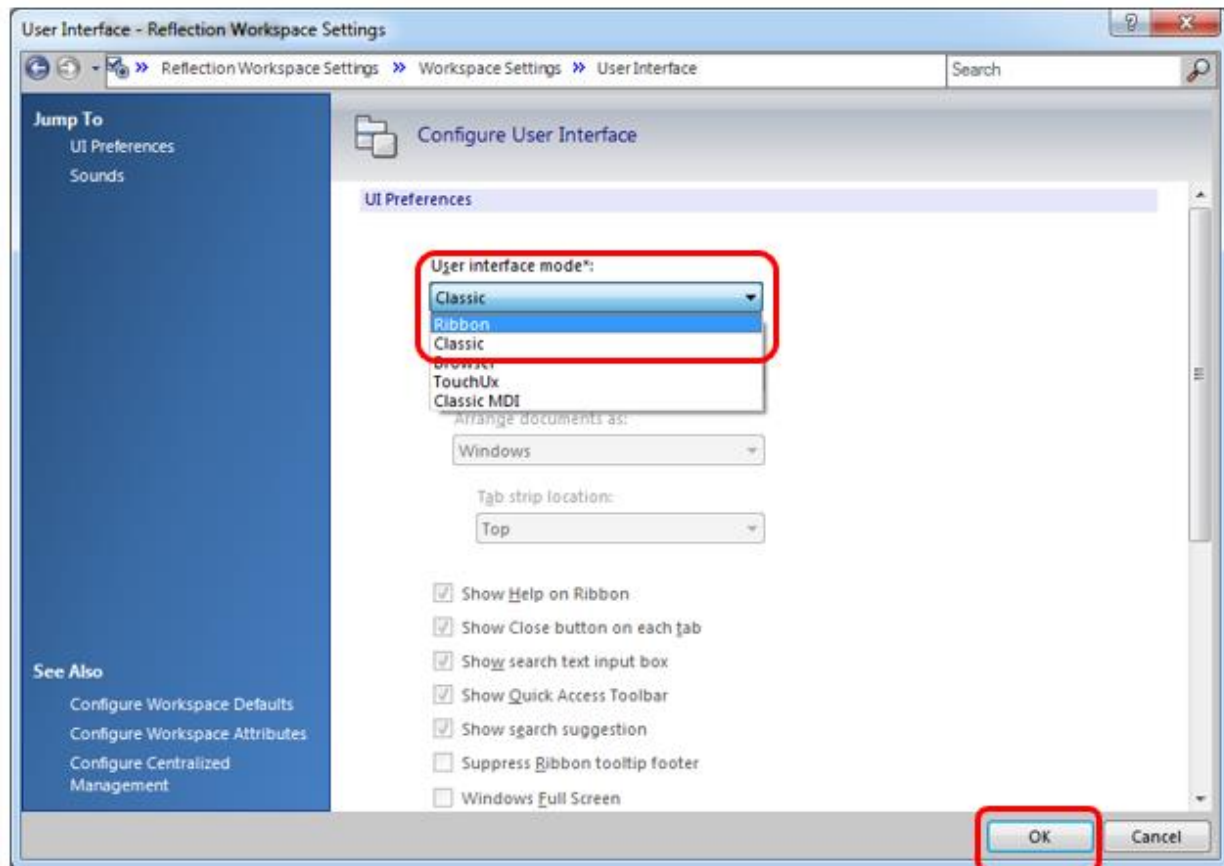
3. In the pop-up window that opens, under **Workspace Settings**, click on **Configure User Interface**, as shown below.

Figure 15: 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 16: Reflection – Change User Interface Mode



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

4.1.1.2.1. CPAC Users: Configure Tile View for Multiple VistA Sessions at the Same Site

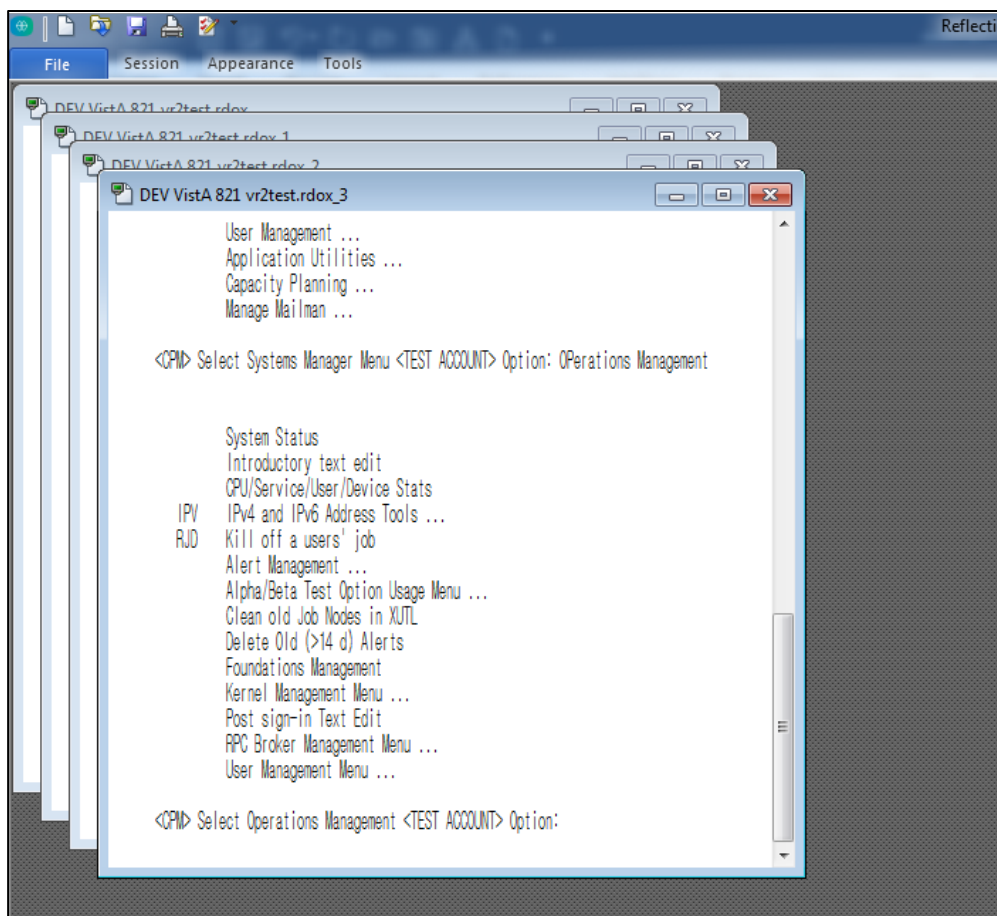
For CPAC users who need to view more than one simultaneous VistA session at the same site, arranging these sessions in a tile view must be done manually within Reflection during initial use of WebVRAM. The following steps will create a tile view for the remote VistA site connections the first time these 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 17: 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 18: Reflection – Arrange Windows Icon and Dropdown

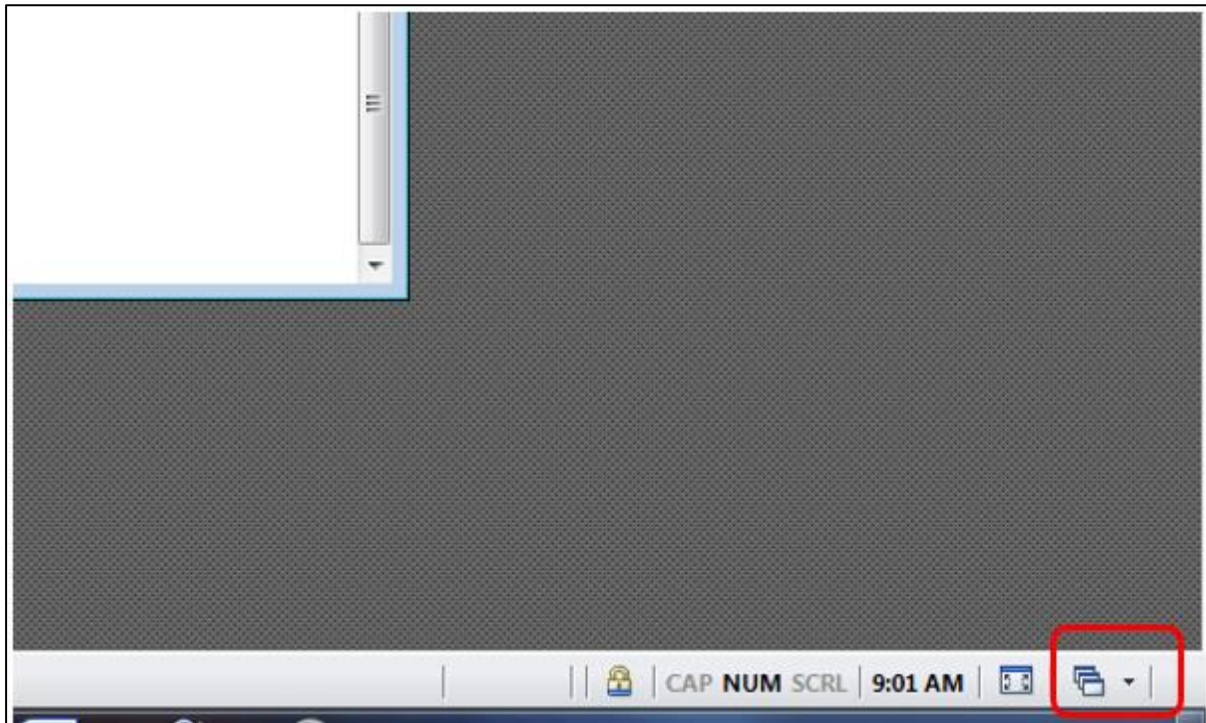
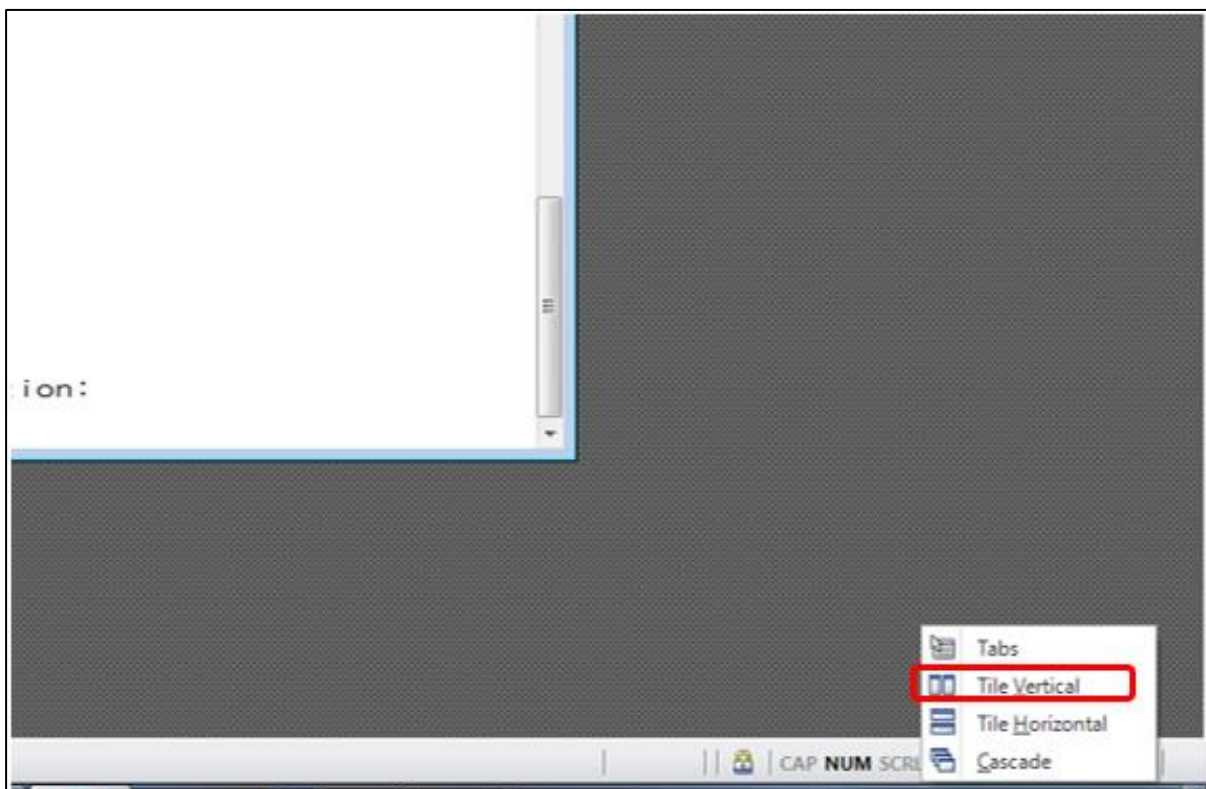


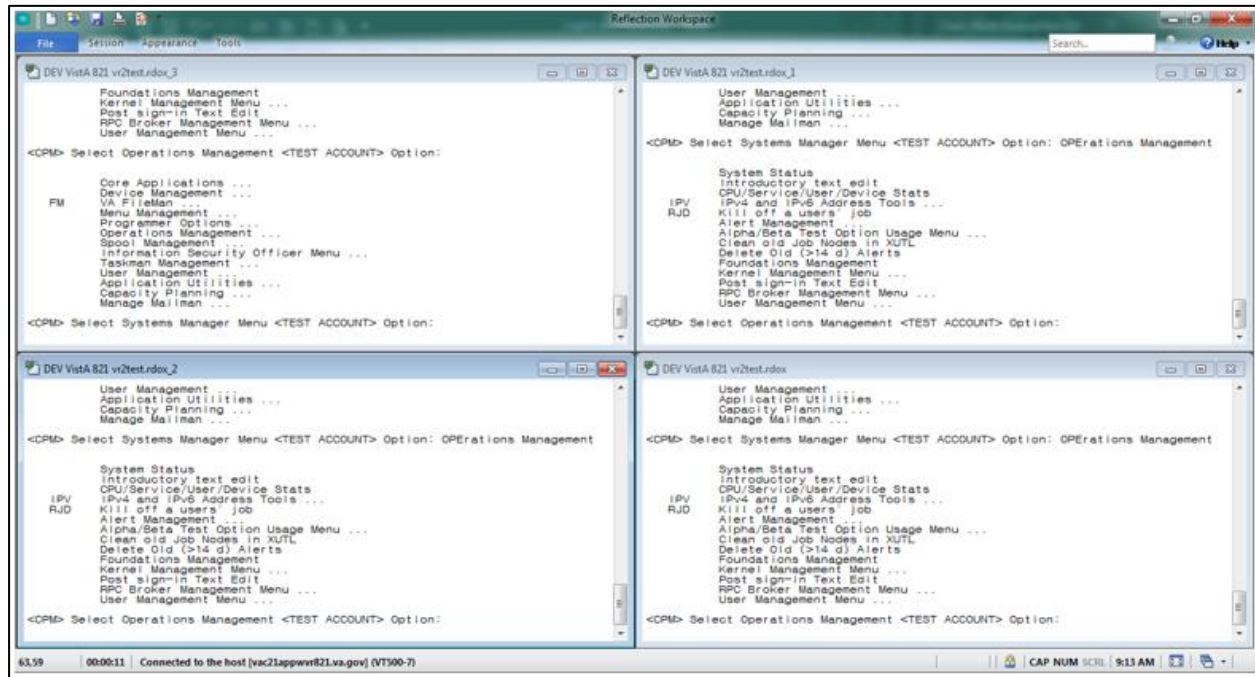
Figure 19: Reflection – Arrange Windows Tile Vertical Selection



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.

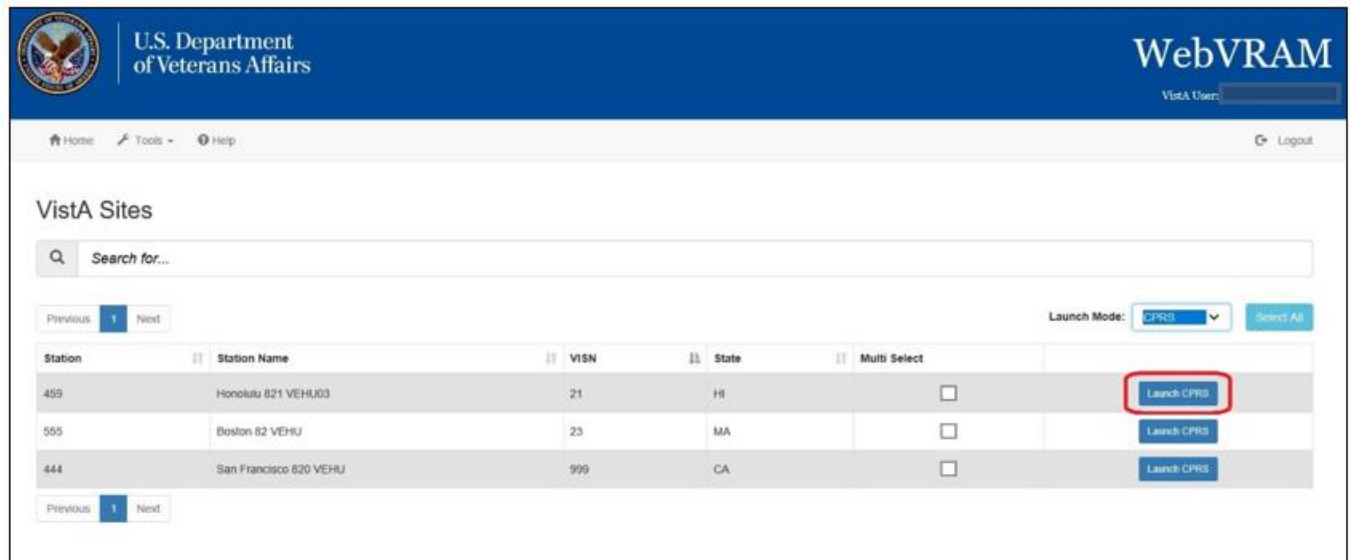
Figure 20: Reflection – Tile Vertical View



4.1.2. Launch Mode: CPRS

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

Figure 21: Launch CPRS Button



4. This version of WebVRAM is not integrated with the IAM Personal Identification Verification (PIV) 2-Factor Authentication (2FA) login process. When 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 22: CPRS Version Screen

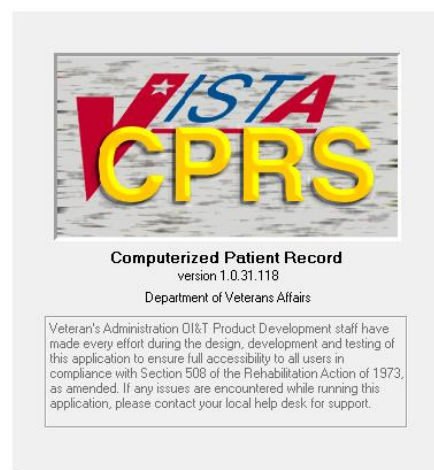
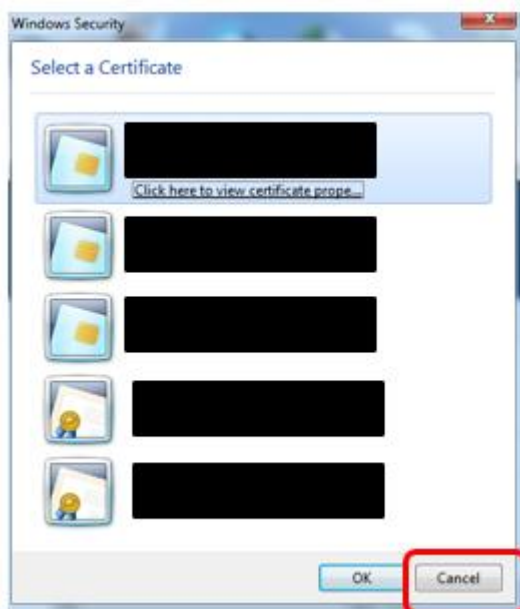


Figure 23: PIV Select a Certificate Screen



5. The CPRS VistA Login screen appears. Enter your local VistA Access and Verify codes, then click **OK** to launch CPRS as shown below. At successful entry of those codes, the CPRS patient selection screen will appear.

Figure 24: CPRS Login Screen



4.1.2.1. 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 4.1.1.1, multiple CPRS sessions to different VistA sites can be performed by changing the **Launch Mode** as outlined in Section 4.1.2 above, then clicking the checkboxes in the **Multi Select** column. Clicking the **Launch Selected** button will then launch simultaneous multiple CPRS sessions.



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

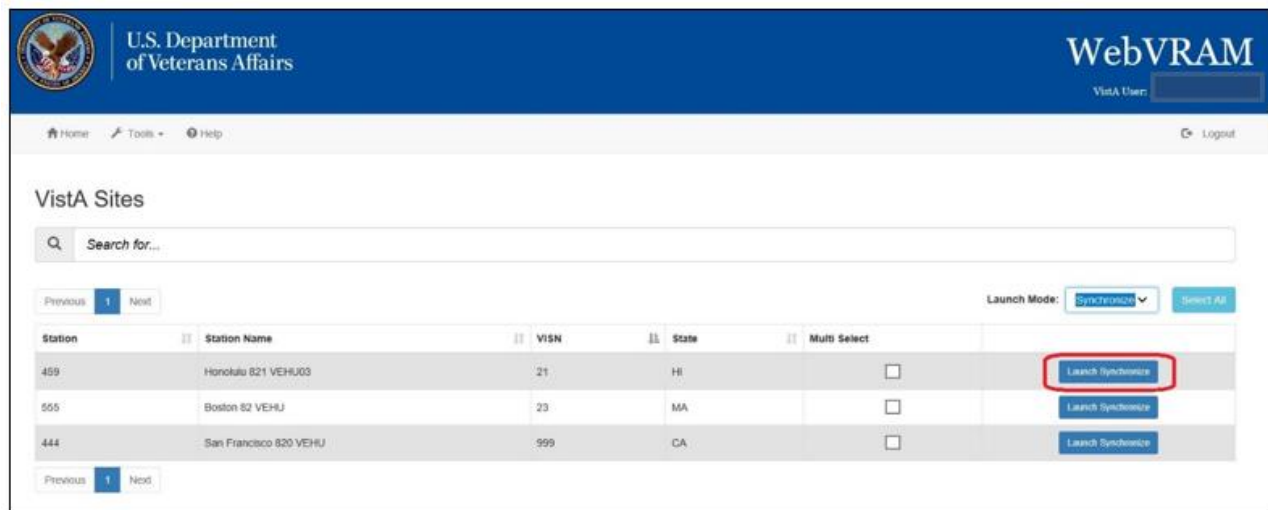
Also, the user may not be able to add Access and Verify codes to each login screen before one or more of them time out and must be relaunched. It is recommended that the user create a VistA “shortcut” Access/Verify (A/V) pair that can be copied and pasted into the Access Code field in each CPRS login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

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

4.1.3. Launch Mode: Synchronize

1. Login to WebVRAM.
2. From the WebVRAM home page, click on the Launch Mode dropdown and select **Synchronize**. Then select the Station Name of the remote VistA site to which to connect.
3. Click on the **Launch Synchronize** button.
4. WebVRAM will launch Synchronize to connect to the selected VistA site.
5. Synchronize updates and syncs up your personal information on the remote VistA system.

Figure 25: Launch Synchronize Button



4.2. Changing Verify Code

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

1. From your Internet Explorer browser, navigate to the [WebVRAM home page](#).
2. The Terms and Conditions web page is displayed. Click **Accept the Terms and Conditions**.
3. The Login page is displayed.
4. Enter your local VistA Access and Verify Codes and click the **Change Verify Code** checkbox.
5. Click **Login**.

Figure 26: WebVRAM Login – Change Verify Code



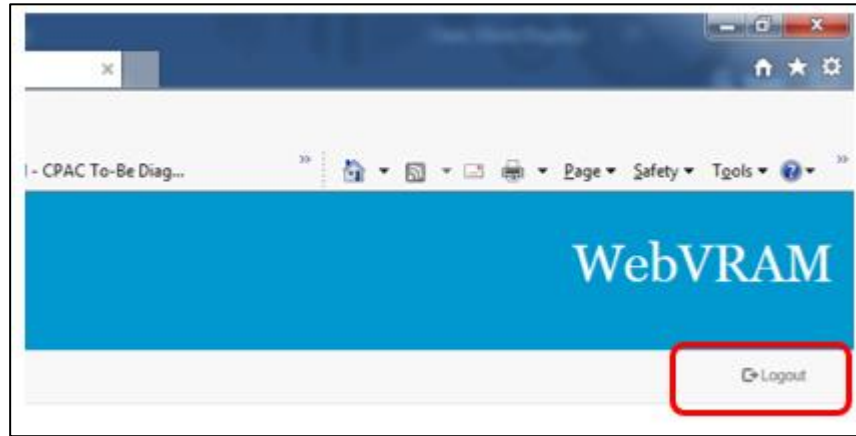
The screenshot shows the WebVRAM login interface. At the top is a blue header with the U.S. Department of Veterans Affairs logo on the left and the text "U.S. Department of Veterans Affairs" and "WebVRAM" on the right. Below the header is a white area containing the "VistA Login" section. This section includes a text box with a disclaimer about the Enterprise Testing Service (ETS) Test Center (ETSTC) and a "Login" button. To the right of the text box is a "VistA Login" form with fields for "Access Code" and "Verify Code", both masked with asterisks. Below these fields is a checkbox labeled "Change Verify Code" which is checked, and a "Login" button. A red rectangle highlights the "Change Verify Code" checkbox and the "Login" button.

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

4.3. Exit System

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

Figure 27: WebVRAM Logout



5. Troubleshooting

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

5.1. Special Instructions for Error Correction

5.1.1. 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 Administrator.

5.1.2. Reflection Fails to Launch

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

5.1.3. Other Errors

For all other errors encountered during use of the WebVRAM application, create a ticket through YourIT or phone the ESD.



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 YourIT ticket or phoning the ESD.

6. 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
CPAC	Consolidated Patient Account Center
CPRS	Computerized Patient Record System (CPRS)
ESD	Enterprise Service Desk
FBCS	Fee Basis Claim System
FPO	Field Program Office
GUI	Graphical User Interface
IAM	Identify and Access Management
NPI	National Provider Identifier
OIT	Office of Information and Technology
PII	Personally Identifiable Information
PIV	Personal Identification Verification
RPC	Remote Procedure Call
SDD	System Design Document
SNOW	Service Now, also called YourIT
SQL	Structured Query Language
SSO	Single Sign On
STIC	Station ID Callback Module
URL	Uniform Resource Locator
VHA	Veterans Health Administration
VM	Virtual Machine
VPN	Virtual Private Network
VRAM	VistA Remote Access Management
WebVRAM	Web VistA Remote Access Management