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

March 2024
Department of Veterans Affairs
Office of Information and Technology

Revision History

Date	Revision	Description	Author
3/2/2024	10.0	Updates for Release 10.0 – Section 5.1.1 and Section 6 Table 3 – Clarified security key placement.	WebVRAM Project Team
12/14/2023	9.0	Updates for Release 9.0 – Section 2 – Updated bullet point to say that only the WebVRAM Administrator role can change Director information. Updated section 3.2 -new bullet point about Director approvals being required to add a new BUA.	WebVRAM Project Team
8/23/2023	8.1	Reviewed for patch 3*17 – No changes were required. This patch does not make any changes to GUI or user-facing components. Updated acronyms, minor formatting, and section 508 formatting.	WebVRAM Project Team
8/23/2023	8.0	Release 8.0 Changes: • Updated Month/date in cover page and footers • Section 3.3: Updated URL Section 3.4: Updated URL	WebVRAM Project Team
7/17/2023	7.0	Section 4.2 • Updated instructions on Add Business Unit window • Updated screenshot for Figure 6 Section 4.3 • Updated screenshot for Figure 7	WebVRAM Project Team
2/7/2023	7.0	Added Section 1.2.7: System Maintenance	WebVRAM Project Team
12/20/2022	6.2	Release 6.2 changes: • Updated date info on cover page • Updated date on footers area • Updated Screenshot for: o Figure 3 o Figure 12	WebVRAM Project Team
10/11/2022	6.0	Release 6 changes: • Updated date info on cover page • Updated date on footers area • Updated Figure 3 (screen shot) in Section 3.4	WebVRAM Project Team
9/5/2022	5.0.2	Updated Figure 2 (screen shot) in Section 3.4	WebVRAM Project Team
7/20/2022	5.0	Updated Figure 2 (screenshot) in Section 3.4	WebVRAM Project Team
7/8/2022	5.0	Removed all references to Internet Explorer browser as it is no longer supported.	WebVRAM Project Team
6/24/2022	5.0	Section 3.4: • Updates to instructions to reflect workflow related to PIV Login • Updated screenshots for Figures 1, 2 and 3	WebVRAM Project Team

4/12/2022	4.1	Update Section 4.2, added Step 8, new error message is displayed when a Business Unit Name already exist. Screenshot of error message added.	WebVRAM Project Team
4/5/2022	4.1	Updated Section 3.2., paragraph 1, WebVRAM Administrator Setup with specific instructions for requesting a new BU Admin be added to a BU.	WebVRAM Team, OIT DSO SPM.
3/4/2022	4.1	Added Section 3.1 (New Business Unit Process)	WebVRAM Team, VA Office of Information and Technology (OIT) Development, Security, and Operations (DevSecOps) Software Product Management (SPM)
2/25/2022	4.1	Updated and clarified Section 3.3 (Information the WebVRAM Administrator Will Need)	WebVRAM Team, VA Office of Information and Technology (OIT) Development, Security, and Operations (DevSecOps) Software Product Management (SPM)
12/9/2021	4.0	Updated for WebVRAM Release 4.0, (associated with informational VistA patch WEBG*3*5): • Updated verbiage in Section 1.8 (Software Summary) and Section 3.4 (Logging into the WebVRAM Administration Module) to add Microsoft Edge as a supported internet browser. • Replaced Figure 1 (WebVRAM Terms and Conditions for Usage Screen). • Replaced Figure 2 (WebVRAM Login Screen). • Deleted subsections under Section 4.4 (Custom Profile Values Required to Access CPRS Features at Certain Sites) and added hyperlink to WebVRAM Administration Module User Guide. • Updated steps 2, 3, and 4 in Section 5.1.1 (Initial Checklist to Begin Troubleshooting User Access Issues). • Added new Issue #1, edited Issue #6, updated Issue #16, and added new Issue #18 in Table 3 (User Profile Issues and VistA Data Anomalies). • Removed references to Fee Basis Claims System (FBCS) from Section 1.8 (Software Summary) and Appendix A (Appendix A – Acronyms and Abbreviations). • Added "WEBG" to Appendix A (Appendix A – Acronyms and Abbreviations).	WebVRAM Team, VA Office of Information and Technology (OIT) Development, Security, and Operations (DevSecOps) Software Product Management (SPM)

4/8/2021	3.0	Updated for WebVRAM Release 3.0 (associated with VistA patch WEBG*3*1):	WebVRAM Project Team, VA OIT Enterprise Program Management Office (EPMO)
		• Added Section 4.4 (Custom Profile Values Required to Access CPRS Features).	
		• Corrected User Class values for Chillicothe and Cleveland in step 8 of Section 5.1.1 (Initial Checklist to Begin Troubleshooting User Access Issues).	
		• Updated Table 3 (User Profile Issues and VistA Data Anomalies) in Section 6 (Common Problems and Resolutions with User Profiles and VistA Data Anomalies).	
		o Added Issue # column.	
		o Added step 3 to Issue 3.	
		o Edited step 3 under Issue 5.	
		o Edited Issue 7.	
		o Added Issues 14-16.	
		• Retitled Section 6 to Appendix A (Appendix A – Acronyms and Abbreviations).	
10/22/2020	2.0	Updated for WebVRAM Release 2.0 (EHR Integration):	WebVRAM Project Team, VA OIT EPMO
		• Updated Section 1.2.1 (Organization of the Manual).	
		• Added EHR verbiage to Section 1.8 (Software Summary).	
		• Organized subsections under new heading in Section 4 (Using the Application).	
		• Added Section 4.6 (Add Security Key Not Present in User's Home VistA – Audit Required).	
		• Updated Section 5.1.1 (Initial Checklist to Begin Troubleshooting User Access Issues) to clarify and add detail to the importance of matching the Home VistA profile data to the WebVRAM profile data.	
		• Updated Table 3 (User Profile Issues and VistA Data Anomalies) in Section 6 (Common Problems and Resolutions with User Profiles and VistA Data Anomalies).	
		o Added CPRS double security key conflict.	
		o Corrected Resolution for "User logs into WebVRAM successfully. Connections to remote sites through Reflection/CPRS end in 'FAILED' message."	
5/12/2020	1.0	Initial document publication for WebVRAM Release 1.2.	WebVRAM Project Team, VA OIT EPMO

Table of Contents

List of Figures

List of Tables

1. Introduction

The Web Veteran's Health Information Systems and Technology Architecture (VistA) Remote Access Management (WebVRAM) application enables synchronization of VistA account credentials by leveraging the VistA Station ID Callback (STIC) module 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 enjoy consistency in access to disparate VistA systems.

In April 2019, the WebVRAM Office of Information and Technology (OIT) management determined that user authentication for the application needed to be performed internal to the application itself, rather than utilizing an external authentication service. A redesign of the software became necessary and includes provision for a new WebVRAM User Table (WUT) to be retained in a Structured Query Language (SQL) database. To enter authorized application user profiles into the WUT, an Administration Module Graphical User Interface (GUI) was developed.

1.1. Purpose

This WebVRAM Administrator User Guide will familiarize authorized users with the process of adding new Business Units and assigning Business Unit Administrators as "managers" of the Business Units. Separate user guides exist for users of the WebVRAM application and for Business Unit Administrators explaining the steps to add authorized users to the application database; refer to the WebVRAM User Guide and the WebVRAM Administration Module User Guide on the Veteran's Affairs (VA) Document Library (VDL).

1.2. Document Orientation

The document orientation is shown below in Sections 1.2.1 through 1.5.

1.2.1. Organization of the Manual

The major sections of the WebVRAM Administrator User Guide are as follows:

- 1 Introduction
- 1.8 Software Summary
- 3 Getting Started
- 4 Using the Application
- 5 Troubleshooting

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

1.2.2. Assumptions

This guide was written with assumptions as follows:

- WebVRAM Administration Module users (Business Unit Administrators) are authorized by business line management to access the Graphical User Interface (GUI) for the purpose of recording user profiles in the WebVRAM User Table (WUT).

- New Business Units requesting access to WebVRAM for authorized users have followed the Enterprise Service Desk (ESD) process for establishing a recognized Business Unit in the application database.

- New Business Units will provide the user profile information of the authorized Business Unit Administrators to be added as managers of those Business Units.

- WebVRAM application users must have the WEBG WEBVRAM GUI Secondary Menu Option in their local/"Home" VistA profile.

    IMPORTANT: The WEBG WEBVRAM GUI Secondary Menu Option is required for the user to be able to login to the WebVRAM application. The WEBG WEBVRAM GUI Secondary Menu Option was pushed to all existing VistA profiles on 3/21/2020. If the user's Home VistA profile was created prior to this date, they should already have the WEBG WEBVRAM GUI Secondary Menu Option. If the user's Home VistA profile was established AFTER 3/21/2020 or if that secondary menu option is missing for any reason, the user will need to submit a request to have local IT add the WEBG WEBVRAM GUI Secondary Menu Option to their Home VistA profile. Without that menu option, the user will NOT be able to login to WebVRAM.

- The primary menu option at the user's Home VistA system is a standard VistA menu name (not a custom menu name).

- WebVRAM Administrators will only be responsible for adding new Business Units and authorized Business Administrators and will not be responsible for any WUT maintenance or WebVRAM application maintenance.

1.2.3. Coordination

WebVRAM Administrators are assigned by the ESD Accounts Management Team to add new Business Units and managers of those Business Units into the WUT.

1.3. VA OIT Standard Disclaimers

1.3.1. 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 and 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.

1.3.2. 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.

1.4. 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 or dialogs) and computer source code are shown in a non-proportional font and enclosed within a box. The document also includes 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**.

1.5. References and Resources

- WebVRAM System Design Document
- WebVRAM User Stories and Backlog – JIRA WebVRAM Repository
- [WebVRAM Administration Module User Guide](#)
- [WebVRAM User Guide](#)

1.6. 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.

1.7. Enterprise Service Desk and Organizational Contacts

Enterprise Service Desk 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	Open a Tier 1 Service Now (SNOW) ticket with 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.

1.8. Software 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 applications such as Computerized Patient Record System (CPRS) and New VA Electronic Health Record (EHR), 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 GUI. The VA-approved web browser for accessing WebVRAM is Microsoft Edge version 91.0.864.67 or greater.

2. WebVRAM Roles

The WebVRAM Administration Module allows for the management of users, profiles, assignment of user to Business Units and report generation. There are three type of user roles:

- **WebVRAM User** – The WebVRAM User can only access designated remote VistA sites. The WebVRAM user can launch a remote VistA session using Launch Reflection, Launch CPRS, or Launch New VA EHR from the site listings page of the application. The WebVRAM user does not have access to the WebVRAM Administration Module.

- **Business Unit Administrator** – The Business Unit Administrator (BUA) has access to the WebVRAM Administration Module pages and can manage users within their assigned Business Unit. The Business Unit Administrator can create and add new users for the Business Unit to which they are assigned to manage and can only view or edit users within their Business Unit.

- **WebVRAM Administrator** – The WebVRAM Administrator has access to the WebVRAM Administration Module pages and has the highest user-level role. The WebVRAM Administrator can add new Business Units and can assign Business Unit Administrators as managers of a Business Unit. The WebVRAM Administrator can create, view, and edit users and Business Units, view log files, and pull reports sorted by Business Unit. Only the WebVRAM Administrator can add, update, and remove Business Unit Director information.

3. Getting Started

3.1. New Business Unit Process

Before users can access the WebVRAM application, they must have approval to do so from the Director (or equivalent) of their VISN, Hub, Regional or Enterprise organization and the Director of that organization must create and get approval for a Business Unit that is added to the WebVRAM database. The Director then assigns Business Unit staff to act as Business Unit Administrators (BUAs) who are charged with adding and maintaining profiles for new users added under that Business Unit in the WebVRAM database. The process for creating and obtaining approvals for a new Business Unit are found on a VA SharePoint site accessible to all VA staff on the VA network. Once the Business Unit is established, and BUAs are authorized, a WebVRAM Administrator can then add the Business Unit and associated BUAs into the WebVRAM database.

3.2. WebVRAM Administrator Setup

To access the WebVRAM Administration Module (WAM), the user follows these initial process steps:

1. With approval from the ESD Accounts Management Team, a newly assigned WebVRAM Administrator contacts an existing WebVRAM Administrator and requests their profile be setup in the WebVRAM User Table (WUT) with the role of WebVRAM Administrator. For Telehealth organizations, submit a request to the **Office of Community Care Help Desk (OCCHD)** via email to request the administrator profile be added to WebVRAM. For Non-Telehealth organizations, submit a Your Information Technology (YourIT) or VA Help Desk Service Now (SNOW) INCIDENT ticket and make certain it gets assigned to the **ESD Application Provisioning Group**. *Do not submit a REQUEST ticket which will take extra time to get assigned to the correct group for resolution.*

2. The newly assigned WebVRAM Administrator confirms their ability to login to the WebVRAM application, using their Home VistA Access and Verify codes, once their profile is successfully established in the WUT.

3. The Business Unit determines and implements their process for approving users to access WebVRAM and determines which VistA remote sites they can access.

4. The Business Unit approves and designates one or more BUAs authorized to add new users to the WUT.

5. A WebVRAM Administrator adds the BUA(s) to the WUT and specifies the Business Unit with which they are associated. Each Business Unit determines whether there are divisions that can be added as a Business Unit within the larger organization.

3.3. Information the WebVRAM Administrator Will Need

The WebVRAM Administrator will need:

- The name and abbreviation of the new Business Unit to be added to the WUT.

- Confirmation that the user has an active VistA user profile on their Home VistA production system. Until the user has a valid, active Home VistA user profile, they cannot access the WebVRAM application.

- *MANDATORY:* Confirmation that the user has the **WEBG WEBVRAM GUI** Secondary Menu option in their Home VistA user profile. This must be confirmed by the WebVRAM Administrator who is adding the new Business Unit Administrator to the WUT by using WebVRAM to login to the user's Home VistA site, performing a User Inquiry and verifying that they have this secondary menu option in their VistA profile. If the WebVRAM Administrator is not familiar with how to perform a User Inquiry in VistA, instructions can be found on page 25 of this guide in the *Resolution* column of Issue number 4. If this secondary menu option is not present in their Home VistA system user profile, instruct the user to

submit an Electronic Permission Access System (ePAS) request to have that menu option added to their VistA profile. Without that secondary menu option, the user will not be able to login to the application and will receive an "unauthorized user" error.

- The full name and VA Active Directory Global Address List (GAL) username (e.g. vhaisltestus) for the Business Unit Administrator(s) to be added as manager of the new Business Unit.

- Approval from the Business Unit Director of the Business Unit for the user to be granted access as a Business Unit Administrator.

3.4. Logging into the WebVRAM Administration Module

1. From the 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 select **Accept the Terms and Conditions** as shown below.

Figure 1: WebVRAM Terms and Conditions for Usage Screen

3. The next web page displayed is the WebVRAM Login page. Select the "**Sign In with VA PIV Card**" button.

Figure 2: WebVRAM Login Screen using Personal Identity Verification (PIV) card
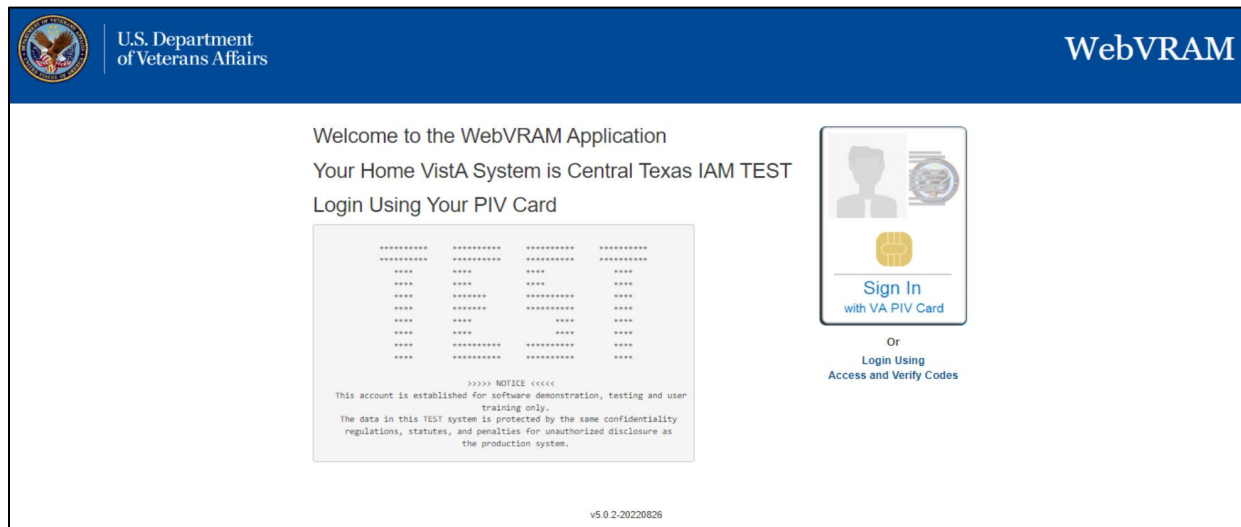
4. The **ActivClient** screen comes up, prompting the user to enter their Personal Identification Number (PIN). Enter PIN and select **OK**

5. The WebVRAM application's main page is displayed. Select **Manage** from the menu bar along the top of the page.

Figure 3: WebVRAM Main Screen
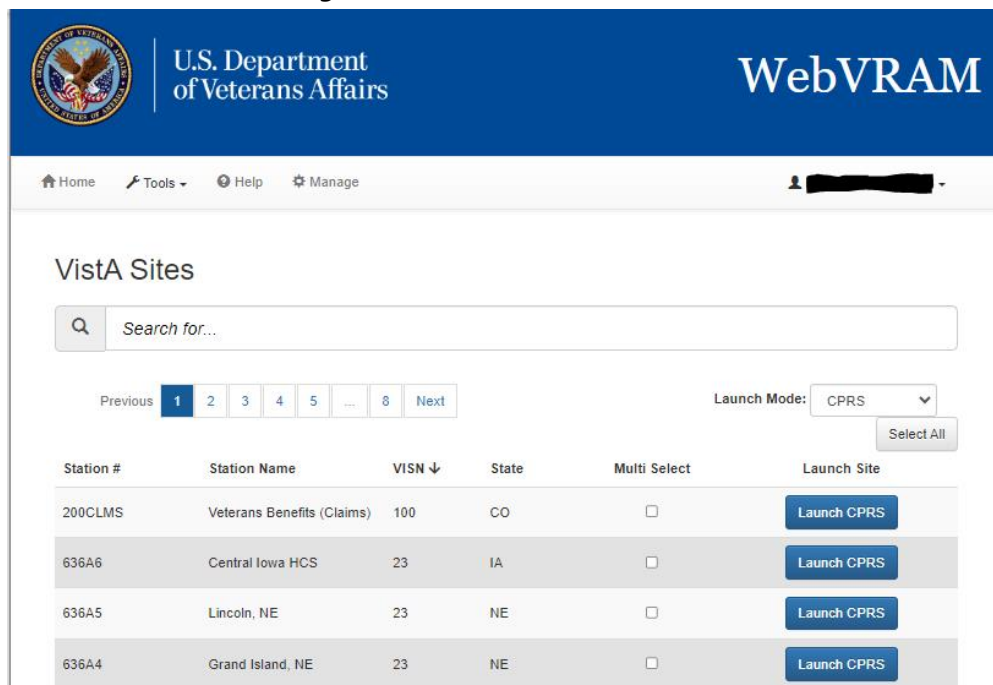
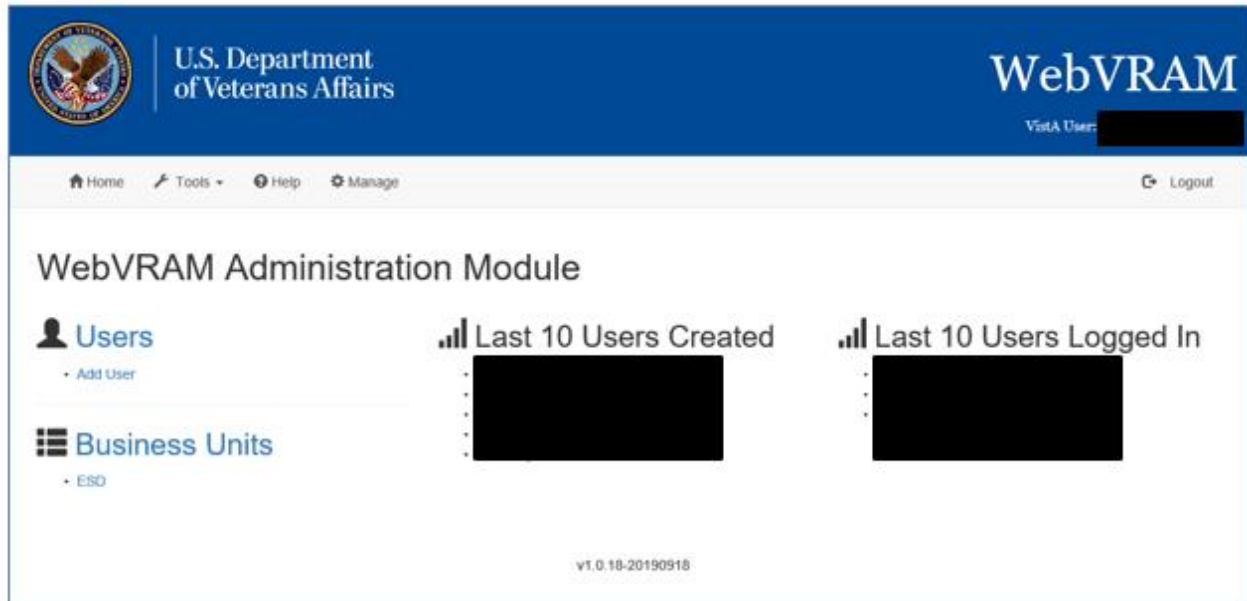6. The WebVRAM Administration Module Main Page is displayed.

Figure 4: WebVRAM Administration Module Main Page


4. Using the Application

4.1. Add BUA to the WebVRAM User Table

To add a Business Unit Administrator (BUA) to the WebVRAM User Table, follow the steps in the WebVRAM Administration Module User Guide. If you do not have a copy, one can be requested from the WebVRAM Project Team.

4.2. Add Business Unit

1. Select the **Business Units** link on the WebVRAM Administration Module Main Page.

Figure 5: Administration Module Business Units Link
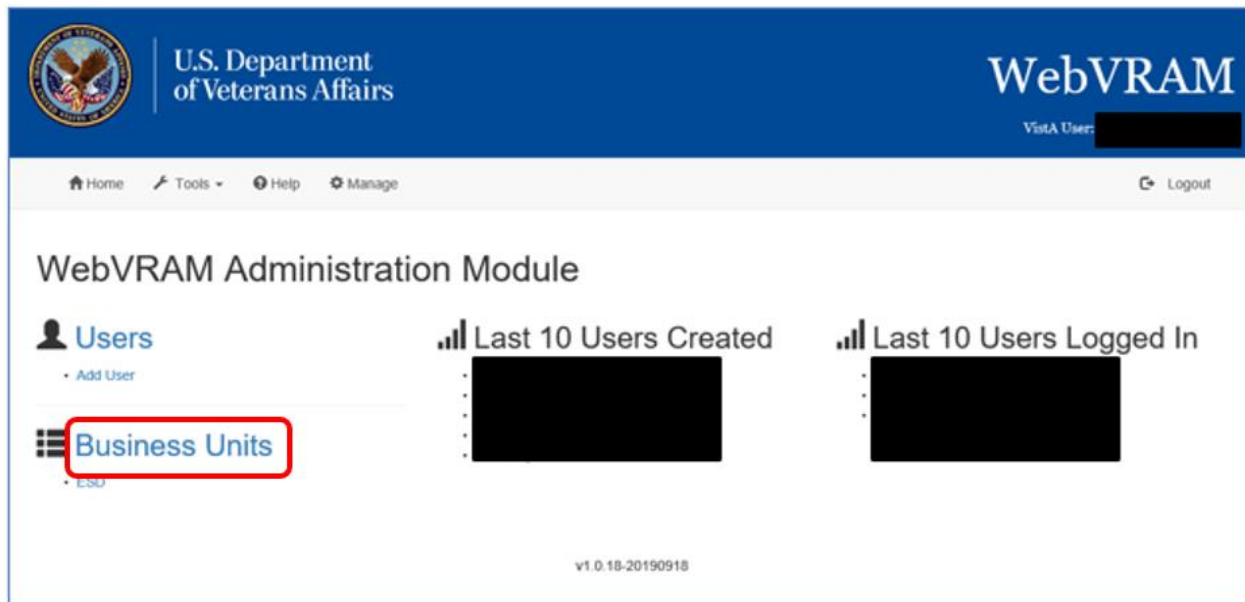
2. A list of Business Units is displayed along with summary information on the Business Units Screen. Select **Add Business Unit**.

Figure 6: Business Units Screen
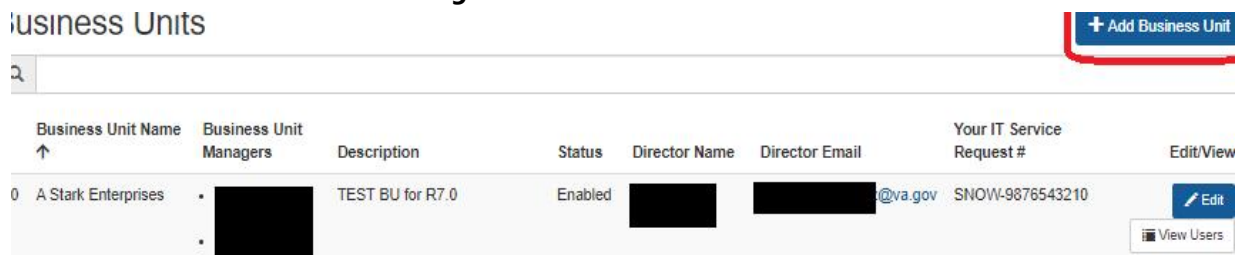
3. A new window pops up to allow creation of a new Business Unit and addition of BUA(s).

4. Business Unit Director Name

5. Business Unit Director VA Email

6. Your IT Service Request #

7. Enter the *abbreviation* of the Business Unit in the **Business Unit Name** field.

8. Enter a description or expansion of the abbreviation of the Business Unit in the **Business Unit Description** field.

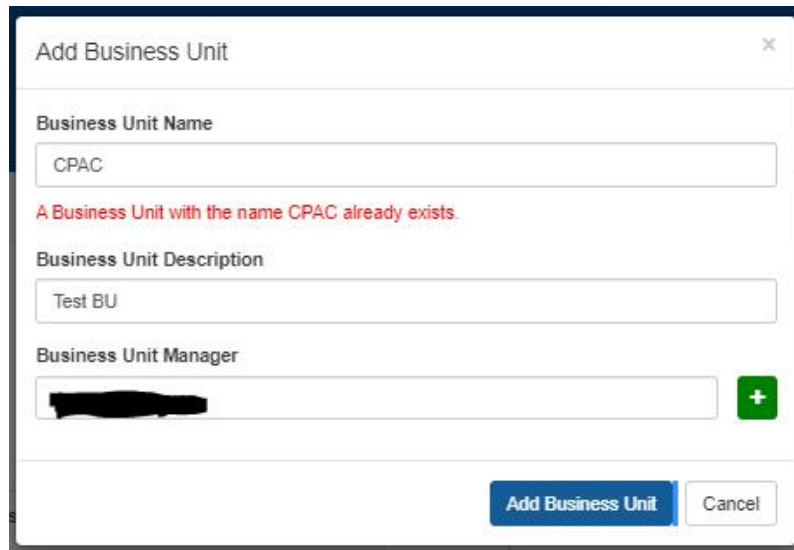9. Enter a partial name for the BUA in the **Business Unit Manager** field and choose the correct BUA to be added as manager from the drop-down list below the field. Additional BUAs can be added by clicking the "**+**" sign to the right of the field where the first BUA has been entered. A new field is displayed, and another BUA may be added. Repeat these steps until all BUAs have been added to the Business Unit.

10. Select the **Add Business Unit** button when all entries are completed. The new Business Unit is added to the list of all Business Units.

Figure 7: Add Business Unit Window

11. In the event a duplicate **Business Unit Name** is entered, an error message is displayed under the **Business Business Name** field to warn a Business Unit with the name "(example: CPAC)" already exists. See screenshot below:

Figure 8: Add Business Unit

4.3. Assign Business Unit to BUA Profile

After the Business Unit is set up and the BUA(s) have been added as managers to the Business Unit, assign the Business Unit to the BUA's WUT profile. Select **Manage** on the top toolbar, then select the **user** whose profile you need to edit.

NOTE: For instructions on how to find and select a user, refer to the WebVRAM Administration Module User Guide.

Figure 9: Administration Module Manage Button
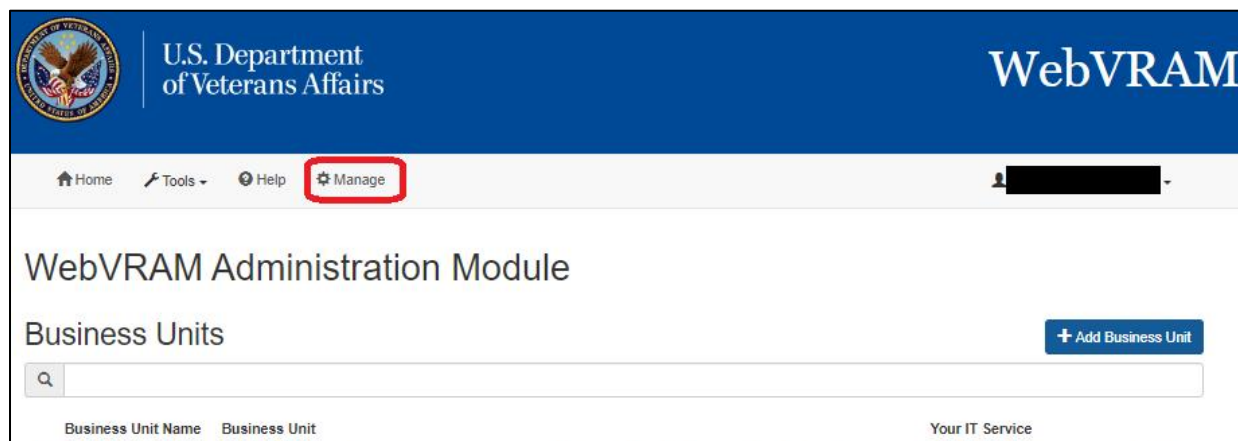
1. From the User Profile Screen, select the "**+**" sign on the **WebVRAM Business Units** option.

Figure 10: User Profile Screen
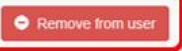
2. The Business Units Assignment Screen is displayed. Locate the Business Unit that the BUA will manage. Select the **Assign to user** button on the right side of the Business Unit row to add it to the BUA's profile. The button will change to **Remove from user** once the selection has been made, and the Business Unit is added to the profile.

Figure 11: Business Units Assignment Screen – Assign to User Button
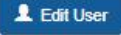
Figure 12: Business Units Assignment Screen – Remove from User Button
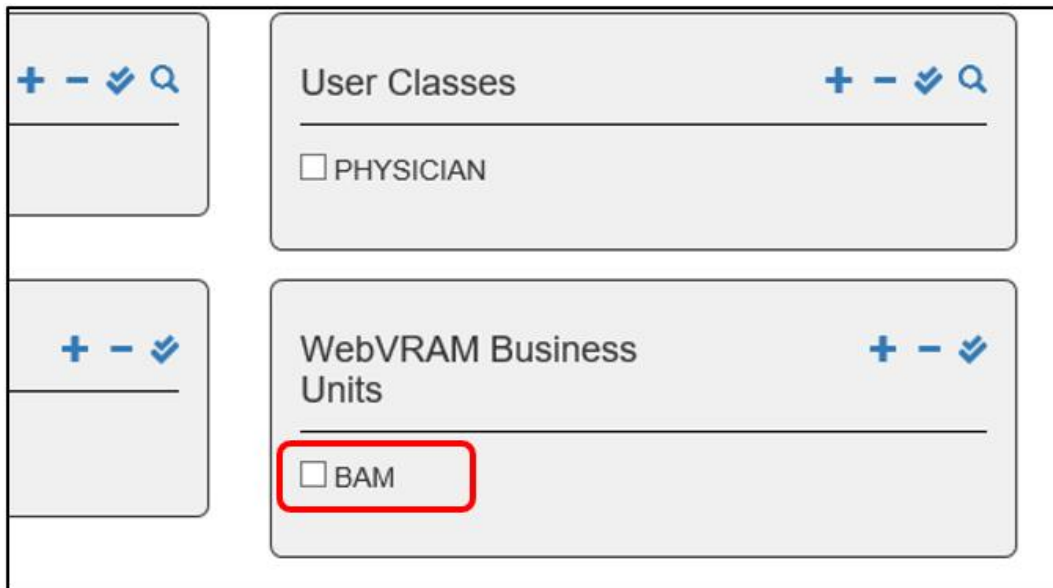
3. Select the **name** of the BUA next to the **User** label at the top of the Business Units Assignment Screen to return to the User Profile Screen.

Figure 13: Business Units Assignment Screen – User Name

4. Confirm the Business Unit was added successfully to the BUA's profile. The Business Unit should be listed under the **WebVRAM Business Units** option on the User Profile Screen.
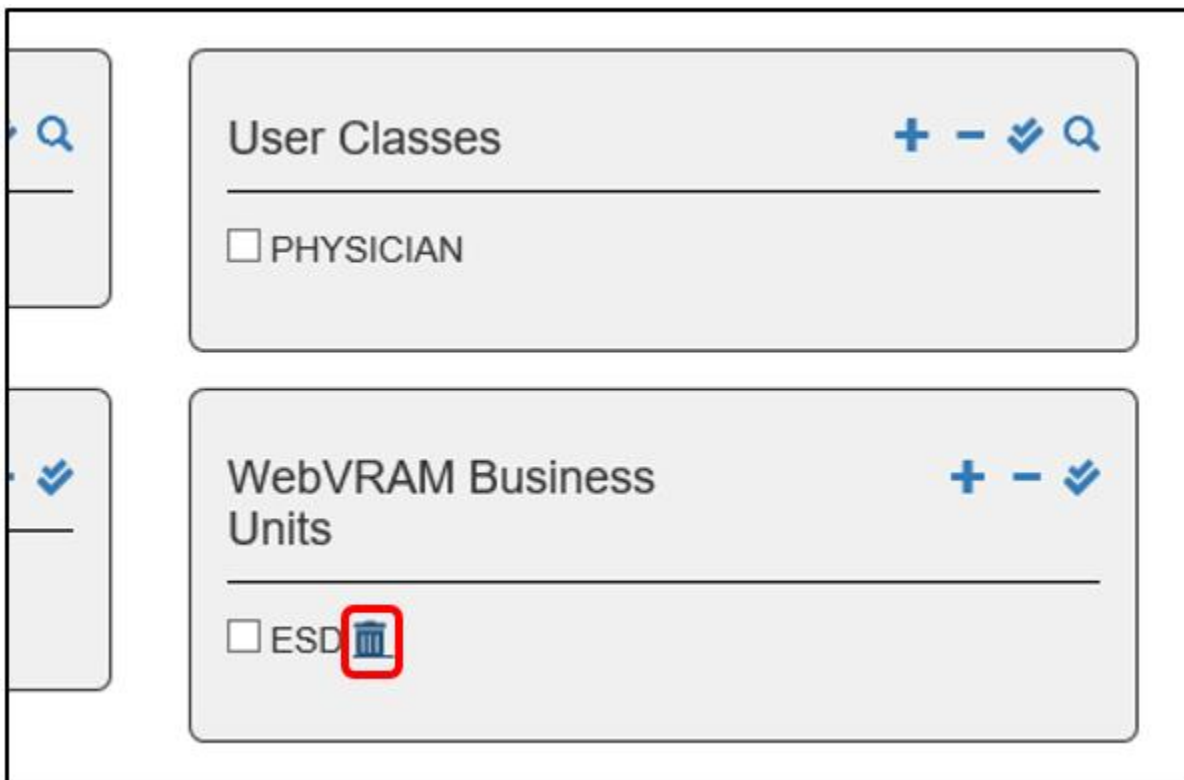
Figure 14: User Profile Screen – Confirm Business Unit Assignment

5. There are several ways to remove a Business Unit from a BUA's profile:

   a. Hover over the **Business Unit** on the WebVRAM Business Units option of the User Profile Screen and select the **trashcan icon**.

Figure 15: WebVRAM Business Units Profile Option – Trashcan Icon

b. Select the "**+**" sign on the WebVRAM Business Units option to reopen the Business Units Assignment Screen and select the **Remove from user** button shown in Figure 12.

4.4. Custom Profile Values Required to Access CPRS Features at Certain Sites

A few VA Medical Centers (VAMCs) or Health Care Systems (HCSs) elect to implement local business rules that require users to possess specific values in their VistA user profile in the NEW PERSON file (#200) in order to access certain CPRS features at those sites. These go beyond the standard secondary menu (e.g. OR CPRS GUI CHART) and keys (e.g. ORES, ORELSE, OREMAS, PROVIDER) needed to access those features in CPRS. These custom requirements are documented in the [WebVRAM Administration Module User Guide](#).

4.5. Disable BUA Account

When a BUA leaves the VA or changes positions to one that no longer requires the use of WebVRAM, the WebVRAM Administrator must disable their WebVRAM user profile. Navigate to the **User Profile Screen** and select the **Disable User** button on the top right above the user profile summary. Once this is done, the User Profile Screen will only show one button, **Enable User**, and the user will no longer be able to login to WebVRAM. User profiles are kept indefinitely in the WUT as directed by VA policy for retention of records.

NOTE: If a BUA leaves the VA, their Home VistA account will be "dis-usered," and login to the WebVRAM application will be prevented since they no longer have an active VistA account.

Figure 16: User Profile Screen – Disable User Button
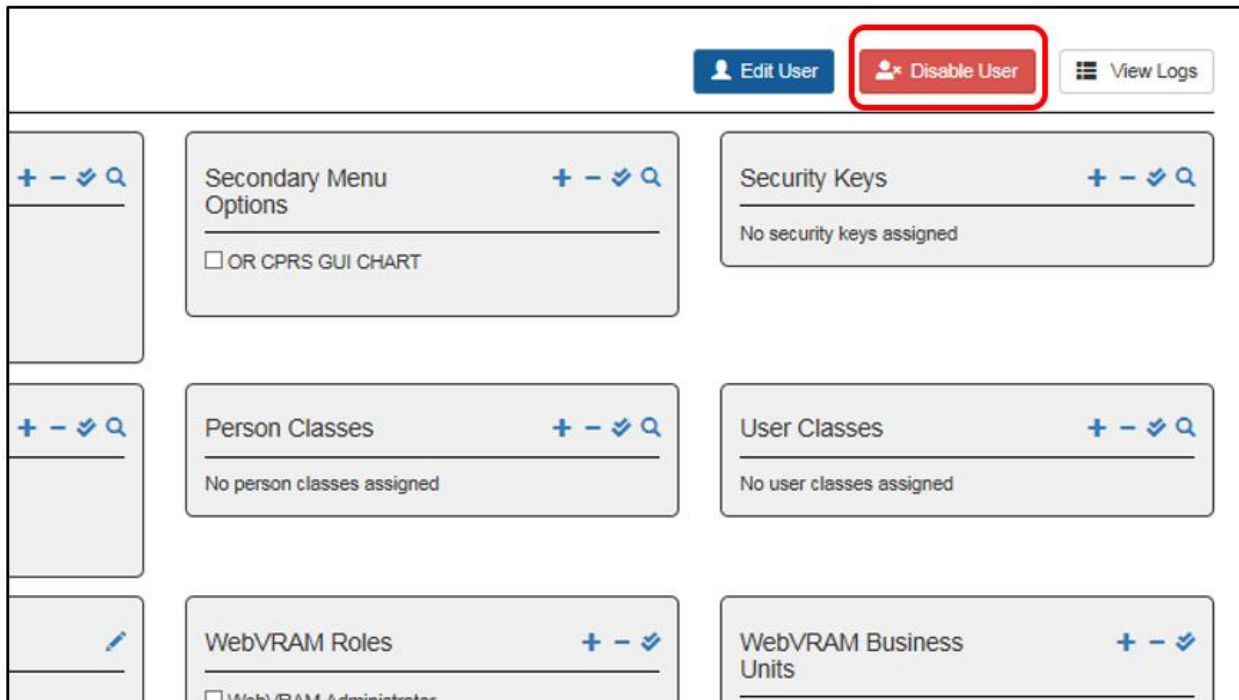
4.6. Add Security Key Not Present in User's Home VistA – Audit Required

⚠️ **CAUTION: The procedures in this section do NOT apply to Consolidated Patient Account Center (CPAC) Business Unit Administrators, as they follow an established auditing policy specific to their Business Unit.**

If a Business Unit Administrator adds a Security Key to a user's WebVRAM profile that **does not** exist in the user's Home VistA profile, the Business Unit Administrator **must** take the following steps to comply with VA Security Policy and Procedure surrounding monthly profile audits:

1. Generate a monthly list of all users granted new Security Keys <u>where the Security Keys do not exist in and are not added to the users' Home VistA profiles</u>.

   a. Collate this data into a separate list for each Home VistA site, <u>for users who share the same Home VistA system</u>.

   b. In these lists, designate all the remote sites these users access via WebVRAM [i.e. sites where the new Security Key(s) will be pushed and added to the remote user profile with each WebVRAM connection].

   c. Note the Security Key(s) that have been added for each user in each list. This can be done in a spreadsheet.

2. Contact the Information System Security Officer (ISSO) at the user's Home VistA system and request a copy of the local monthly audit performed on the users identified in Step 1.

3. For each remote site identified in Step 1, send the list of users to each remote site's ISSO via email with a communication stating they "have reviewed the users listed for audit purposes for the month of [FILL IN MONTH]." Also attach the local monthly audit received from the user's Home VistA ISSO obtained in Step 2.

This process will result in two lists sent to each user's remote site ISSO:

- A monthly list of users granted new Security Keys in WebVRAM where the Security Keys do not exist in the users' Home VistA profiles.

- A copy of the local Home VistA audit performed by those users' local ISSO(s).

There is no "standard" template for creating this report. Follow the instructions in Step 1 to identify data to be included in the report.

The ISSO for each site can be found using the VA ISSO Locator.

ℹ **NOTE:** The hyperlink above points to the VA intranet and will only work for authorized users connected to the VA network.

4.7. Exit System

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

5. Troubleshooting

For troubleshooting, please contact the Enterprise Service Desk (ESD) at 1-855-673-4357, log a ticket, and request escalation of the ticket to Tier 3 support.

5.1. Special Instructions for Error Correction

5.1.1. Initial Checklist to Begin Troubleshooting User Access Issues

1. Does the user have a **WebVRAM profile**?

   a. If YES, go to step 2.

   b. If NO, they will receive the "Unauthorized Access" error after clicking on the Accept the Terms and Conditions button when accessing the application URL. Add the user profile to WebVRAM.

Figure 17: Unauthorized Access Error Message
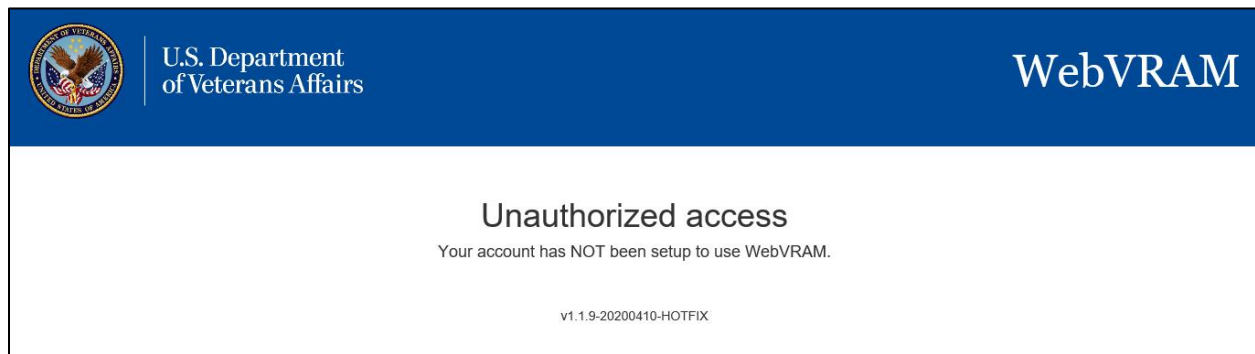
2. Does the user have the **WEBG WEBVRAM GUI Secondary Menu Option** in their Home VistA profile?

   a. If NOT, the user will receive an error that says: "Your Access or Verify Code is invalid in your home VistA Profile *(<Home VistA>).* Please contact your Local IT or ESD Help Desk to reset your access and verify codes. The WebVRAM Team cannot change these codes."

   The error message contains a link to the YourIT SNOW ticket creation page for INC tickets. Report an Issue - yourIT Service Portal (va.gov)" error. Instruct the user to submit an ePAS request to have local IT add the WEBG WEBVRAM GUI Secondary Menu Option to their Home VistA profile.

3. Does the user profile have the **WEBG AV PUSH Security Key**?

   a. If NOT, add the WEBG AV PUSH Security Key to the WebVRAM user profile. **DO NOT ADD THIS KEY TO THE HOME VISTA PROFILE!**

4. If the user has CPRS Tab = **COR**, then the user may also need the following security keys in the WebVRAM user profile:

   a. **OR CPRS GUI CHART** Secondary Menu Option.

   b. **ORES** (for physicians) or **ORELSE** (for nurses and clinical support staff).

   c. **PROVIDER** Security Key for physicians and some nurses.

   ℹ️ NOTE: PROVIDER Security Key is for clinicians authorized to enter orders. The need for the PROVIDER key should be determined by the Business Unit Director in coordination with local and enterprise security officers.

   REFERENCE: [CPRS Technical Manual](), Electronic Signature section.

   ⚠️ CAUTION: The menus and keys in a user's WebVRAM profile must match those in the user's Home VistA profile. Menus and keys are

provided at the local level based on ePAS approvals for the user's role, based on VA policy.

5. Does the user need to add (write) Progress Notes to the patient chart in CPRS? If YES, the user must have:

   a. **ORES, ORELSE** and **PROVIDER** Security Keys (PROVIDER key may be required at some VistA sites). The Security Keys are stored in the KEY subfield (#.01) in the KEYS subfile (#51) of the NEW PERSON file (#200).

   b. Home VistA Person Class and User Class values:

   i. If the user is a physician, the **PERSON CLASS** subfield (#.01) in the **PERSON CLASS** multiple (#8932.1) in the **NEW PERSON** file (#200) needs to **match** the user's Home VistA.

   ii. If the user is a nurse clinician, Person Class might be **Physician Assistant**, and User Class may need two values – **PHYSICIAN ASSISTANT and PROVIDER**.

6. Does the user need to assign themselves as Primary Provider to an Encounter in CPRS? If YES, the user must have:

   a. Their Home VistA Person Class and User Class values.

   b. The **USER CLASS** subfield (#.01) in the **USER CLASS** multiple (#9.5) in the **NEW PERSON** file (#200)value of **PROVIDER** should be present in their Home VistA profile and reflected in their WebVRAM profile.

7. Does the user need to order Meds as a physician? If YES, the user must have:

   a. **Home VistA Profile:**

   b. **AUTHORIZED TO WRITE MED ORDERS** field (#53.1) in the **NEW PERSON** file (#200) set to "YES"

   c. **WebVRAM Profile:**

   i. Security Keys of **ORES** and **PROVIDER**. The Security Keys are stored in the KEY subfield (#.01) in the KEYS subfile (#51) of the NEW PERSON file (#200).

   ii. CPRS Tabs: **COR**.

   iii. The **same** Person Class that exists in their Home VistA profile. the **PERSON CLASS** subfield (#.01) in the **PERSON CLASS** multiple (#8932.1) in the **NEW PERSON** file (#200) needs to **match** the user's Home VistA.

   d. User Class of **PHYSICIAN** and **PROVIDER** (See step 6b above). The **USER CLASS** subfield (#.01) in the **USER CLASS** multiple (#9.5) in the **NEW PERSON** file (#200) value of **PROVIDER** should be present in their Home VistA profile and reflected in their WebVRAM profile.

8. Does the user need to write CPRS Tele-ICU Notes at Chillicothe or Cleveland, or both VAMCs? If YES, the user must have:

   a. **WebVRAM Profile:**

      i. For Chillicothe, User Class of **Tele-Health Staff**. The **USER CLASS** subfield (#.01) in the **USER CLASS** multiple (#9.5) in the **NEW PERSON** file (#200) value of **Tele-Health Staff** needs to match the user's home VistA.

      ii. For Cleveland, User Class of **INTERNIST**. The **USER CLASS** subfield (#.01) in the **USER CLASS** multiple (#9.5) in the **NEW PERSON** file (#200) value of **INTERNIST** needs to match the user's home VistA.

6. Common Problems and Resolutions with User Profiles and VistA Data Anomalies

Table 3: User Profile Issues and VistA Data Anomalies

Issue #	Issue	Cause	Resolution
1.	User launches CPRS but receives an "Invalid Access and Verify" code error when logging into CPRS.	The **WEBG AV PUSH** Security Key is missing from the user's WebVRAM profile.	Add the **WEBG AV PUSH** Security Key to the user's WebVRAM profile. **DO NOT ADD THIS KEY TO THE HOME VISTA PROFILE!**
2.	User is unable to order controlled substance medications at remote sites accessed through WebVRAM.	The provider is not configured to prescribe controlled substances at the remote site. If a provider prescribes controlled substances at a site where the provider **already has permissions to do so** after connecting to the site through WebVRAM, this process will work correctly.	This functionality works in accordance with the business process. Configuration is required at the remote site to assign the provider permissions to prescribe controlled substances where appropriate. The user should work with their business management and local IT to make configuration changes at the remote site in accordance with VA and Drug Enforcement Administration (DEA) policy.

Issue #	Issue	Cause	Resolution
3.	User is unable to login to WebVRAM; receives "Unauthorized User No Profile" error.	WEBG WEVBRAM GUI Secondary Menu Option is missing from VistA profile.	Instruct the user to submit an ePAS request to add **WEBG WEBVRAM GUI Secondary Menu Option** to their Home VistA profile.

Issue #	Issue	Cause	Resolution
4.	Unable to login to WebVRAM; receives "Invalid Access or Verify Code" error.	1. WEBG WEVBRAM GUI Secondary Menu Option is missing from VistA profile. 2. Access and Verify codes need to be reset in user's Home VistA system. 3. A user may have duplicate VistA profiles in their Home VistA system which confuses the VistA authentication process. The "Invalid Access or Verify Code" error is sent to WebVRAM by the Home VistA system.	1. Instruct the user to submit an ePAS request to add **WEBG WEBVRAM GUI Secondary Menu Option** to their Home VistA profile. 2. Instruct the user to create a SNOW YourIT ticket to have local IT reset **BOTH their Access and Verify codes**. They will need to login to their local VistA and change their Verify code, then login to WebVRAM with the new Access and Verify code pair. 3. Check the user's Home VistA site to see if they have more than one active profile using the **KPA CPAC NSD MENU** secondary menu option (refer to the [WebVRAM Administration Module User Guide](#)). Use WebVRAM to connect to the user's Home VistA system and type "**CPAC**" at the first VistA menu prompt, followed by "**USER**" at the next prompt. Type the user's [Last name, First initials of first name]. If the user has two identical or nearly identical profiles, submit an ESD ticket on behalf of the user to have the duplicate profile with the least amount of data (e.g. menus, keys, person class, etc.) dis-usered or terminated in their Home VistA system.

Issue #	Issue	Cause	Resolution
5.	User can log in to WebVRAM but receives 'Invalid Access and Verify Code' error when launching Reflection or CPRS.	WEBG AV PUSH Security Key is missing from user profile.	Add **WEBG AV PUSH Security Key** to the WebVRAM user profile. **DO NOT ADD THIS KEY TO THE HOME VISTA PROFILE!**

6.	User logs into WebVRAM successfully. Connections to remote sites through Reflection or CPRS end in "FAILED" message.	1. Specifically, if the log shows a "**Menu tree rebuild for user failed**" error: A non-standard Primary Menu was pulled from VistA profile into WebVRAM profile. VistA customization across the enterprise results in non-standard Primary Menus, and the remote site does not recognize the custom menu and refuses to build the user profile due to rules violation.
		
		2. A non-standard Service Section value came from local VistA profile.
		
		3. Keystroke errors in WebVRAM VistA Profile parameters.
			1. For all users who are NOT assigned to a Business Unit of "CPAC" or a Business Unit that starts with "Office of Community Care (OCC)...," replace user's custom menu with a standard menu based on user role:
			  a. Role: Non-Clinical User **XUSERTOOLS**
			  b. Role: Physician User **PX PCE CLINICIAN MENU**
			  c. Role: Nurse User **NURSCL-MENU**
			CPAC or OCC Business Unit users have custom menus assigned by the VRAM team. Contact the Business Unit Administrators of these Business Units to deal with any WebVRAM Primary Menu issues for these users.
			2. Replace Service Section with MEDICAL SERVICE unless the user is with a CPAC or Office of Community Care (OCC) Business Unit.
			3. Check all VistA profile values in the WebVRAM VistA Profile section (bottom left side of profile) to ensure there are no spelling errors.

Issue #	Issue	Cause	Resolution
7.	User's connection to remote site FAILS and log shows "User's access [or verify] code already belongs to another user on <VAMC Name> site. Synchronization Failed."	User has identical Home VistA Access or Verify code to another user at remote site.	User must contact local IT: 1. If Access code is identical, both Access and Verify codes need to be reset. User then logs in directly to Home VistA and changes Verify code to one of their choosing. 2. If only Verify code is identical, only Verify code needs to be reset. User logs in directly to Home VistA and changes their Verify code.

Issue #	Issue	Cause	Resolution
8.	Clinician User, while accessing remote site, is unable to add themselves as Primary Provider to a CPRS Encounter. Clinical User unable to order meds at remote site in CPRS.	1. User missing the ORES and PROVIDER keys in their Home VistA and WebVRAM profiles. 2. User's Person Class has an expiration date which was pushed to the remote site. The user may have a new Person Class in their Home VistA system with a more current expiration date. Check the Home VistA profile to confirm this. 3. User may need User Class of PHYSICIAN and PROVIDER added to their Home VistA and WebVRAM profile. 4. Northern California and San Francisco require a Service Section value of MEDICAL SERVICE to enable CPRS orders and notes to function.	1. Add correct User Class and Person Class values in WebVRAM profile. Suggested values for Physician (values for other clinical providers will vary): a. User Class: PHYSICIAN b. Person Class: Person Class value from the user's Home VistA system. 2. Edit the user's Person Class in WebVRAM by clicking on the Pencil Icon next to the Person Class field, remove the expiration date, and select the **Update Person Class** button. Have the user submit an ePAS ticket to have the Home VistA Person Class expiration date removed or updated. If it is updated, add the new expiration date to the WebVRAM corresponding Person Class. 3. Some sites require User Class values to enable ordering and note creation signing features in CPRS. Add User Class values of PHYSICIAN and PROVIDER to the user's Home VistA and WebVRAM profile. ePAS may be needed to add the values to the Home VistA system. 4. Add the value of MEDICAL SERVICE to the user's Service Section field in the WebVRAM profile. The home VistA Service Section value does not need to be changed.

Issue #	Issue	Cause	Resolution
9.	"User Not Found" when assigning Home VistA to user profile in WebVRAM.	1. User may have an inactive VistA account on their Home VistA system due to inactivity. 2. User's Active Directory [Global Address List (GAL)] full name does not match the VistA profile name exactly and VistA will not allow the user's profile to be accessed at their local site.	1. Check to ensure the local VistA account is active. If it is, instruct the user to submit an ePAS request to reactivate their Home VistA account. 2. Contact local IT and have the user's VistA name changed to EXACTLY match the GAL name, including the use of upper and lower cases. That seems to be an easier change than trying to change the GAL name to match VistA.
10.	"Cannot Add User...(Duplicate VistA Names)"	User has two nearly identical profiles on their Home VistA system; same SSN.	A URL appears with this error message. Send URL to user with instructions to complete the fields in the form at that URL. The fields are listed in the WebVRAM Admin Module Guide. Once user has done this, follow User Guide to "reactivate" their WebVRAM profile. Unfortunately, all VistA profile information must then be manually added. An enhancement is on the development backlog to add a "VistA Refresh" button to pull current VistA data into the WebVRAM profile.

Issue #	Issue	Cause	Resolution
11.	User Profile is added to WebVRAM, but all VistA Profile data is blank.	**PREVENTION: Have users check their VistA Profile BEFORE adding them as a new user**. It may take longer to add VistA profile data to WebVRAM, which also might result in typos and further failed connection attempts, than to have local IT remove duplicate entries before creating the WebVRAM user profile.	Ask the user to list their VistA profile with the User Toolbox and identify duplicate entries. Instruct the user to submit a SNOW YourIT ticket to have local IT remove the duplicate entry. Since the WebVRAM profile is already created, VistA profile data must be manually entered. A "VistA Refresh" button is under development.
12.	User logs out of WebVRAM and returned to the Terms and Conditions page. User attempts another login and receives "Invalid Access and Verify Codes" error.	MS Edge browser does not persist cookies due to VA policy.	Have the user refresh or close their browser and login again.
13.	User fails to connect to a remote site. In the User Log, the failed error states, "User's VistA profile is incomplete. Insufficient information to allow visiting: **Missing Station Number**."	The user is missing or has multiple values in the **Division field** of their Home VistA profile.	Have the user submit a SNOW YourIT ticket to work with local IT to have a default value added to the **Division** field in their Home VistA profile. Or if the user has multiple values in the Division field, ask local IT to remove all but one of the values.

Issue #	Issue	Cause	Resolution
14.	Clinical User has issues with CPRS features working at some remote sites but not working at other remote sites.	User has two CPRS Security Keys. They either have ORES and ORELSE, or they have ORES and OREMAS keys. More than one security key will cause conflicts with CPRS functionality.	If the user is a physician, psychologist, radiologist, or physician assistant, remove the **ORELSE** or **OREMAS** keys. Leave only the **ORES** key.
15.	User cannot access **Mental Health** Clinical Reminders in CPRS and receives the error "Application context has not been created! RPC info ORUTL4DLL (completed)."	User is missing the **YS BROKER1** Secondary Menu option in their Home VistA and WebVRAM profiles.	Have the user submit an ePAS request to add the **YS BROKER1** Secondary Menu option to their Home VistA profile and add that same value to their WebVRAM profile.
16.	User unable to access Clinical Reminders at New Jersey VAMC.	User must have specific values in the Title, Service Section, and User Class fields.	Refer to "Custom Profile Values or Site-specific Clinical Teams Required to Access Features at Certain Sites" section of the [WebVRAM Administration Module User Guide]().
17.	User's name changes (e.g. new last name) and they receive the "Your Account has NOT been setup to use WebVRAM" error when logging in.	The user's Active Directory ID in the WebVRAM database no longer matches the Active Directory ID in the GAL, so the VA authentication check fails when logging in.	From the Edit User Screen, update the user's **WebVRAM Active Directory (Windows) Username** to match the new Active Directory ID in the GAL. **NOTE:** Name changes in the VA Active Directory can take 24-48 hours to propagate through the network, and it may take that long for a successful login to WebVRAM to occur after changes are made.

Issue #	Issue	Cause	Resolution
18.	User cannot synchronize to a remote site and receives a "**Fatal Error: Synchronization Failed**" message.	Check the user's log by viewing the user profile and clicking the **View Logs** button. If you see a "**Menu tree rebuild for user failed**" message near the bottom of the log file, the user is missing one of the three standard Primary Menus that are recognized at all VistA sites as valid.	If the user has one of the three standard Primary Menus in their profile, replace it with one of the other three Primary Menu values. If the user has a local custom Primary Menu name in their Primary Menu field of their profile, replace it with one of the three standard Primary Menu values. CPAC or OCC Business Unit users have custom menus assigned by the VRAM team. Contact the Business Unit Administrators of these Business Units to deal with any WebVRAM Primary Menu issues for these users.
19.	User receives this error when connecting to any remote site: Fatal Error: BSE ERROR – ADDRESS FOR STN "XYZ" NOT FOUND. User failed to login using BSE. Unable to connect to VistA site <name of site>. ***Note: "XYZ" = the user's Home VistA Station #.***	The user's home VistA profile is either missing a value in the DIVISION field or that field contains an incorrect value.	Have the user log a Help Desk ticket, assigned to their local IT Staff, to have their user profile DIVISION field populated with the correct value. Then have them retry to connect to remote sites through WebVRAM.

A. Appendix A – Acronyms and Abbreviations

Acronyms and definitions are provided throughout the document with first use. Commonly used product-related acronyms are also collected in the table below.

Table 4: Acronyms and Abbreviations

Term	Definition
AD	Active Directory
BUA	Business Unit Administrator
New VA EHR	VA Standardized Electronic Health Record
CPAC	Consolidated Patient Account Center
CPRS	Computerized Patient Record System
DEA	Drug Enforcement Agency
EHR	Electronic Health Record
ePAS	Electronic Permission Access System
ESD	Enterprise Service Desk
FPO	Field Program Office
GAL	Global Address List
GUI	Graphical User Interface
HCS	Health Care System (large multi-site medical center)
IAM	Identity and Access Management
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
NPI	National Provider Identifier
OCC	Office of Community Care
OCCHD	Office of Community Care Help Desk
OIT	Office of Information and Technology
PHI	Protected Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identification and Validation

Term	Definition
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
VA	Veterans' Affairs
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
YourIT	Your Information Technology