

# **WebVRAM Administration Module User Guide**



**October 2020**

**Department of Veterans Affairs**

**Office of Information and Technology**

## Revision History

Date	Document Revision	Description	Author
10/22/2020	2.2	<p>Updated for WebVRAM Release 2.0 (Cerner Integration):</p> <ul style="list-style-type: none"> <li>• Updated Section <a href="#">1.2.2</a> (Assumptions). <ul style="list-style-type: none"> <li>○ Added user prerequisite to have local IT validate their Home VistA DIVISION field.</li> <li>○ Added information about standard Home VistA primary menu option.</li> </ul> </li> <li>• Added Cerner verbiage to Section <a href="#">2</a> (Software Summary).</li> <li>• Updated CPRS Tabs in Section <a href="#">4.2</a> (Add New User) to clarify the user should have COR or RPT tab, not both.</li> <li>• Added new Section <a href="#">4.7</a> (Standard Configuration for VistA Imaging Functionality) to explain VistA Imaging user setup.</li> <li>• Added new Section <a href="#">4.9.1</a> (User Log Cerner Messages).</li> <li>• Updated Section <a href="#">5.1.1</a> (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.</li> <li>• Updated <a href="#">Table 3</a> (User Profile Issues and VistA Data Anomalies) in Section <a href="#">5.1.2</a> (Common Problems and Resolutions with User Profiles and VistA Data Anomalies). <ul style="list-style-type: none"> <li>○ Added CPRS double security key conflict.</li> <li>○ Corrected Resolution for “User logs into WebVRAM successfully. Connections to remote sites through Reflection/CPRS end in ‘FAILED’ message.”</li> </ul> </li> </ul>	WebVRAM Project Team, VA Office of Information and Technology (OIT) Enterprise Program Management Office (EPMO)

Date	Document Revision	Description	Author
7/29/2020	2.1	<p>Updated for WebVRAM Release 1.3 (associated with VistA patch WEBG*1.0*3):</p> <ul style="list-style-type: none"> <li>• Added Section <a href="#">4.3</a> (Add Security Key Not Present in User's Home VistA – Audit Required).</li> <li>• Added Section <a href="#">4.6.4</a> (To Use the Tele-ICU Provider CPRS Timeout Option) to explain how to configure the user profile of a Tele-ICU provider to use the CPRS extended timeout value.</li> <li>• Changed title of Section <a href="#">4.8</a> (View/Edit User's Home VistA System and Active Directory Name).</li> </ul>	WebVRAM Project Team, VA OIT EP MO
5/12/2020	2.0	<p>Updated for WebVRAM Release 1.2 (associated with information-only patch WEBG*1.0*1):</p> <ul style="list-style-type: none"> <li>• Updated Section <a href="#">1.2.2</a> (Assumptions) to rephrase requirement for users to have the WEBG WEBVRAM GUI Secondary Menu Option in their Home VistA.</li> <li>• Updated Section <a href="#">1.2.6</a> (References and Resources) to change Rational to GitHub.</li> <li>• Rewrote entire Section <a href="#">3.2</a> (Information the Business Unit Administrator User Will Need).</li> <li>• Added Caution message to Section <a href="#">4.2</a> (Add New User), Step 5.</li> <li>• Revised Caution message in Section <a href="#">4.2</a> (Add New User), Step 6.</li> <li>• Changed heading to Section <a href="#">4.5</a> (Duplicate Users in Home VistA and Other VistA Data Anomalies) and added steps 6 and 7.</li> <li>• Added Section <a href="#">4.6</a> (Standard Configurations for CPRS Functionality) and subsections.</li> <li>• Changed heading to Section <a href="#">4.10</a> (Disable User Account) and edited first paragraph.</li> <li>• Edited Section <a href="#">5</a> (Troubleshooting):</li> </ul>	WebVRAM Project Team, VA OIT EP MO

Date	Document Revision	Description	Author
		<ul style="list-style-type: none"> <li>○ Added Section <a href="#">5.1.1</a> (Initial Checklist to Begin Troubleshooting User Access Issues).</li> <li>○ Added Section <a href="#">5.1.2</a> (Common Problems and Resolutions with User Profiles and VistA Data Anomalies).</li> <li>○ Added Section <a href="#">5.2</a> (Look Up a User's Home VistA Profile Information).</li> <li>● Changed captions for Figures 5, 6, 7, 8, 10, 11, 12, 15, 22, 23, 24, 25, 26, 27, 28, and 31 and associated cross-references.</li> <li>● Various minor formatting and verbiage changes.</li> </ul>	
12/4/2019	1.7	Updated to address comments from Health Product Support. Technical Writer review and edit.	WebVRAM Project Team, VA OIT EPMO
11/21/2019	1.6	Added clarity to different pathways for Business Unit Administrator and WebVRAM Administrator to add new user.	WebVRAM PMO Support
11/15/2019	1.5	Changed title of Section 2.1 to WebVRAM Roles and defined all user roles. Changed "Business Administrator" to "Business Unit Administrator" to match the names of Roles in the application. Corrected various entries "Admin" or "Administrative" to Administration to match the wording displayed in the application for consistency. Changes to Section 3.5 include updates to instructions and narrative on adding user based on the user role (Business Unit Administrator or WebVRAM Administrator).	WebVRAM PMO Support
10/18/2019	1.4	Added instructions for entering required VistA Profile data.	WebVRAM PMO Support
10/11/2019	1.3	Technical Writer review and edit.	WebVRAM Project Team, VA OIT EPMO
10/9/2019	1.2	Added content for Home VistA View/Change and View Logs functionality.	WebVRAM PMO Support

<b>Date</b>	<b>Document Revision</b>	<b>Description</b>	<b>Author</b>
10/7/2019	1.1	Reworked flow to match screen shots and added Duplicate User error process steps.	WebVRAM PMO Support
9/25/2019	1.0	Baseline document.	WebVRAM Project Team, VA OIT EPMO

# Table of Contents

<b>1. Introduction .....</b>	<b>1</b>
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.....	3
1.2.4. VA OIT Standard Disclaimers .....	3
1.2.4.1. Software Disclaimer .....	3
1.2.4.2. Documentation Disclaimer .....	3
1.2.5. Documentation Conventions .....	3
1.2.6. References and Resources.....	4
1.3. Enterprise Service Desk and Organizational Contacts.....	4
<b>2. Software Summary.....</b>	<b>5</b>
2.1. WebVRAM Roles .....	5
<b>3. Getting Started .....</b>	<b>6</b>
3.1. Business Unit Administrator User Setup .....	6
3.2. Information the Business Unit Administrator User Will Need.....	6
3.3. Logging into the WebVRAM Administration Module (WAM) .....	7
<b>4. Using the Application .....</b>	<b>11</b>
4.1. View / Edit User.....	11
4.2. Add New User .....	16
4.3. Add Security Key Not Present in User's Home VistA – Audit Required .....	23
4.4. Quick Delete of User Profile Entries .....	24
4.5. Duplicate Users in Home VistA and Other VistA Data Anomalies.....	25
4.6. Standard Configurations for CPRS Functionality .....	31
4.6.1. To Order Meds and Write Notes in CPRS.....	31
4.6.2. To Write CPRS Tele-ICU Notes at Chillicothe and Cleveland VA Medical Centers with a WebVRAM Connection .....	31
4.6.3. To Use CPRS Features as a Non-Physician Provider .....	32
4.6.4. To Use the Tele-ICU Provider CPRS Timeout Option.....	32
4.7. Standard Configuration for VistA Imaging Functionality .....	33
4.8. View/Edit User's Home VistA System and Active Directory Name.....	34
4.9. View User's Log .....	37
4.9.1. User Log Cerner Messages .....	39
4.10. Disable User Account.....	41
4.11. Exit System .....	41
<b>5. Troubleshooting.....</b>	<b>42</b>

5.1.	Special Instructions for Error Correction .....	42
5.1.1.	Initial Checklist to Begin Troubleshooting User Access Issues .....	42
5.1.2.	Common Problems and Resolutions with User Profiles and VistA Data Anomalies .....	45
5.2.	Look Up a User’s Home VistA Profile Information.....	49
<b>6.</b>	<b>Acronyms and Abbreviations .....</b>	<b>50</b>

## List of Figures

Figure 1:	WebVRAM Terms and Conditions for Usage Screen.....	7
Figure 2:	WebVRAM Login Screen .....	8
Figure 3:	WebVRAM Main Screen .....	9
Figure 4:	WebVRAM Administration Module Main Page.....	10
Figure 5:	Users Screen .....	11
Figure 6:	User Profile Screen .....	12
Figure 7:	VistA Sites Screen .....	13
Figure 8:	Administration Module Users Link.....	14
Figure 9:	Add/Remove Secondary Menu Options Screen.....	15
Figure 10:	Administration Module Business Units Links.....	16
Figure 11:	Business Unit Profile Screen.....	16
Figure 12:	Add User Screen.....	17
Figure 13:	User Lookup on Add User Screen.....	17
Figure 14:	User Not Found on Home VistA Error .....	18
Figure 15:	Add User Screen – Success Message .....	19
Figure 16:	VistA Profile Option .....	22
Figure 17:	VistA Profile Data Entry Fields .....	22
Figure 18:	Edit User Quick Delete Option .....	24
Figure 19:	Duplicate User Error Message .....	25
Figure 20:	WebVRAM Access Request Screen .....	26
Figure 21:	User Disabled Status .....	26
Figure 22:	User Profile Screen with Enable User Button.....	27
Figure 23:	User Profile Screen – Edit User Button .....	34
Figure 24:	Edit User Screen .....	35
Figure 25:	Edit User Screen – Home VistA Field Cleared .....	35
Figure 26:	Edit User Screen – Home VistA “Auto-Fill” Feature .....	36
Figure 27:	Edit User Screen – New Home VistA System Selected .....	36
Figure 28:	User Profile Screen – View Logs Button .....	37
Figure 29:	User Log Listing .....	37
Figure 30:	User Log Detail Listing .....	38
Figure 31:	Cerner Messages in User Log.....	40
Figure 32:	User Profile Screen – Disable User Button .....	41
Figure 33:	Unauthorized Access Error Message.....	42

## List of Tables

Table 1: Documentation Symbols and Descriptions .....	3
Table 2: Enterprise Service Desk Support Information.....	4
Table 3: User Profile Issues and VistA Data Anomalies.....	45
Table 4: Acronyms and Abbreviations.....	50

# 1. Introduction

The Web VistA Remote Access Management (WebVRAM) application solution 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 (Admin) Module Graphical User Interface (GUI) has been developed.

## 1.1. Purpose

The purpose of the WebVRAM Administration Module User Guide is to familiarize authorized users of the Administration Module (not the WebVRAM application) with the key features and navigational elements of the GUI. Additionally, this guide provides technical information to system administrators, IT support staff, and other authorized WebVRAM Administration Module users. The Administration Module GUI will be used to add new, business-authorized users of the WebVRAM application to the WUT. Adding new users will consist of entering a user profile via the GUI to create user data in the WUT. The WUT user profile allows the WebVRAM application user to login and access its functionality. A separate user guide exists for users of the WebVRAM application.

## 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 WebVRAM Administration Module User Guide are as follows:

- [1 Introduction](#)
- [2 Software Summary](#)
- [3 Getting Started](#)
- [4 Using the Application](#)
- [5 Troubleshooting](#)
- [6 Acronyms and Abbreviations](#)

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

## 1.2.2. Assumptions

This guide was written with assumptions as follows:

- WebVRAM Administration Module users are authorized by business line management to access the GUI for the purpose of recording user profiles in the WUT.
- User profile information for users of the WebVRAM application is provided by the user's business line management to those responsible for entering that user profile data through the Administration Module.
- Required local Security Keys are identified and incorporated into User Account Profiles by WebVRAM Administration Module users.
- Users of the WebVRAM application have current VA network access and an active local or "Home" VistA user profile.
- WebVRAM application users must have the WEBG WEBVRAM GUI Secondary Menu Option in their 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.**

- User must have a DIVISION value in their Home VistA profile. It must not be blank, and it must contain a correct value for the VA Division in which they are located. Local IT must verify the validity of this value in the user's Home VistA profile.



**IMPORTANT: The DIVISION field must be populated in the Home VistA profile to allow the user to connect to some remote VistA sites they are authorized to access.**

- The primary menu option at the user's Home VistA system is a standard VistA menu name (not a custom menu name). There are only three values that are accepted by remote locations across the enterprise:
  - XUSERTOOLS
  - PX PCE CLINICIAN MENU
  - NURSCL-MENU



**Most primary menus uploaded from the user's Home VistA profile into the WebVRAM profile will be customized for local use. These customized menus will not be recognized as valid at remote sites, causing the profile creation to fail ending in a terminated connection/failed synchronization at remote sites.**

- Administration Module users will only be responsible for entering application user profile data and will not be responsible for any WUT maintenance or WebVRAM application maintenance.

### 1.2.3. Coordination

WebVRAM Administration Module users must obtain approval from their respective WebVRAM application business owners/stakeholders to access and use the WebVRAM Administration Module to enter application user profile data into the WUT.

### 1.2.4. VA OIT Standard 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 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
	<b>NOTE:</b> Used to inform the reader of general information including references to additional reading material.
	<b>CAUTION:</b> Used to caution the reader to take special notice of critical information.

“Snapshots” of computer online displays (i.e., character-based screen captures/dialogs) and computer source code are shown in a non-proportional font and enclosed within a box. Also included are 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 – GitHub WebVRAM 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	1-855-673-4357 or Teletypewriter (TTY) 844-224-6186; <a href="mailto:nationalservicedeskair@va.gov">nationalservicedeskair@va.gov</a>
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. Software Summary

WebVRAM is a web-based, cloud-hosted application utilizing VA Enterprise Architecture and Design principles that facilitates user access to multiple remote VistA systems and applications such as Computerized Patient Record System (CPRS), Cerner PowerChart® Electronic Health Record (EHR), 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 GUI. The VA-approved web browser for accessing WebVRAM is Microsoft Internet Explorer (IE) version 11.0.

### 2.1. WebVRAM Roles

The WebVRAM Administration Module enables the management of users, profiles, assignment of users to business units, and report generation. There are three types of user roles:

- **WebVRAM User** – The WebVRAM User can only access designated remote VistA sites. The WebVRAM user can launch a remote session using Launch Reflection, Launch CPRS, or Launch Cerner from the sites listing page of the application. The WebVRAM user does not have access to the WebVRAM Administration Module.
- **Business Unit Administrator** – The Business Unit Administrator 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/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 to 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. WebVRAM Administrator is the highest access level.

## 3. Getting Started

### 3.1. Business Unit Administrator User Setup

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

1. The business unit determines and implements their process for approving users to access WebVRAM and determines which VistA remote sites they can access.
2. The business unit approves and designates one or more Business Unit Administrators authorized to add new users to the WebVRAM User Table (WUT).
3. A WebVRAM Administrator adds the Business Unit Administrator(s) to the WUT database and specifies which 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.

### 3.2. Information the Business Unit Administrator User Will Need

To add a new user, the Business Unit Administrator will need:

- Windows VA Username from the Global Address List (GAL) (e.g., vhaisl....)
- Home VistA system name(s) (e.g., Togus, ME; Connecticut HCS; etc.)
- VistA systems the user is authorized to access by their business line management
- A list of all current VistA accounts for the user, outside their Home VistA system, where they have active login credentials:



**These sites must NOT be added to the user's WebVRAM profile when it is created.** See Section [4.2 Add New User](#).

- In the event some user profile data does not automatically populate when added to the WebVRAM database, additional setup items from the user's Home VistA system may be needed to correctly set up a new user in WebVRAM:
  - User's VistA Secondary Menu Options
  - User's VistA Security Keys
  - User's VistA Title
  - User's VistA Service/Section
  - User's VistA User Class and Person Class



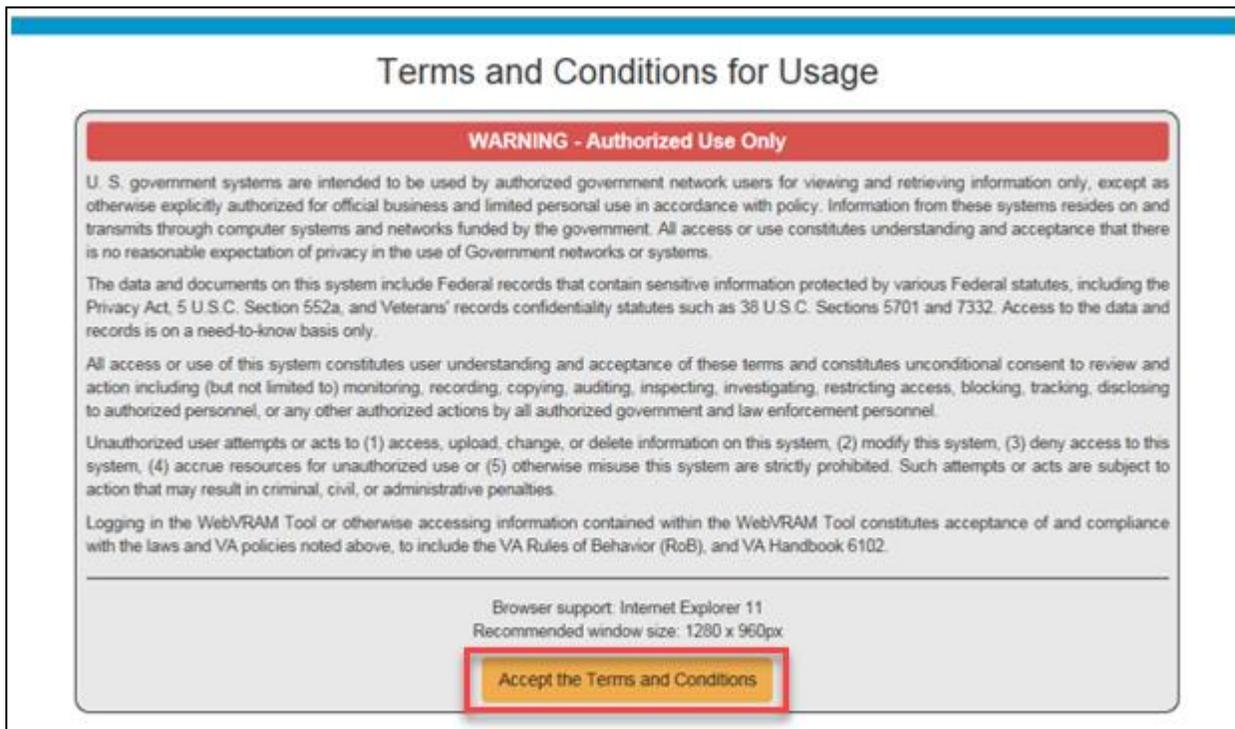
**IMPORTANT: The WEBG WEBVRAM GUI Secondary Menu Option was pushed to all existing VistA profiles on 3/21/2020. If the user's Home VistA profile was created prior to this date, they should already have the WEBG WEBVRAM GUI Secondary Menu Option. If the user's Home VistA profile was established AFTER 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.

### 3.3. Logging into the WebVRAM Administration Module (WAM)

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 1: WebVRAM Terms and Conditions for Usage Screen



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 2: WebVRAM Login Screen**

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

### Vista Login

Databases in the Enterprise Testing Service (ETS) Test Center (ETSIC) are to be used for testing only. They are never to be used for training, presentations, live demos. Even with de-identified databases there still are security and privacy concerns. Violations to this policy will result in appropriate disciplinary action as defined in Regulation (VMR 820(b)), removal of the database(s) and/or suspension/termination of access privileges. The data in this TEST system is protected by the same confidentiality regulations, statutes, and penalties for unauthorized disclosure as a production system.

```
821 / vritest  
  
RPC Hostname: [REDACTED]  
RPC Port: [REDACTED]  
Namespace: [REDACTED]
```

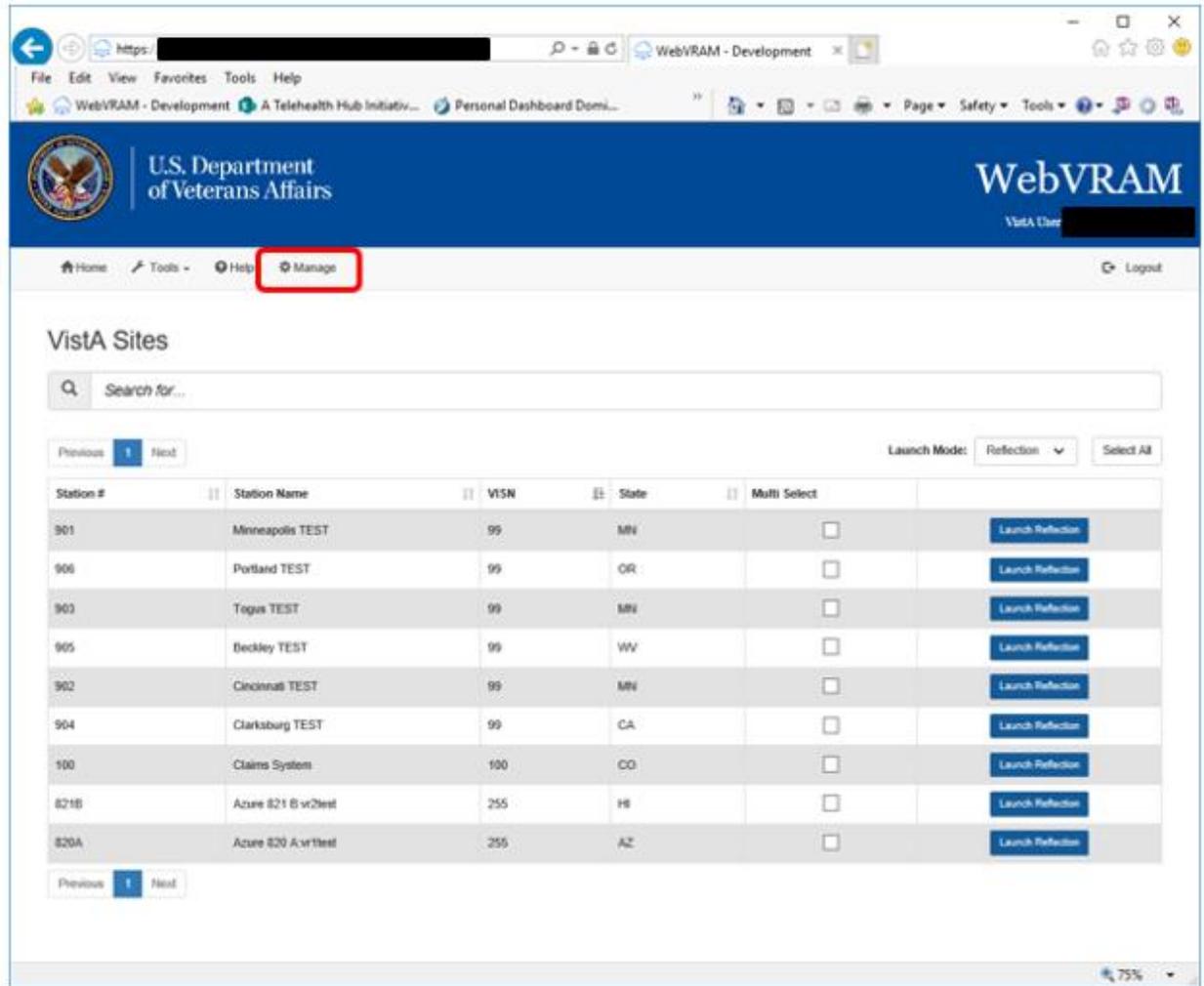
Access Code

Verify Code

Change Verify Code

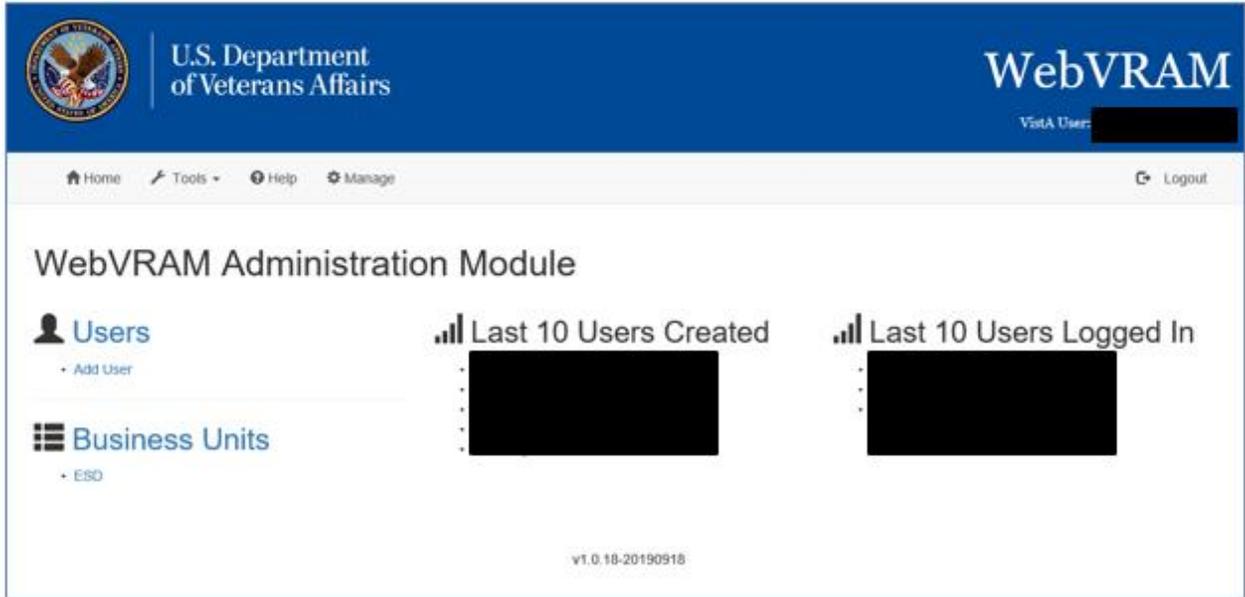
- The WebVRAM application's main page is displayed. Click on **Manage** from the menu bar along the top of the page.

**Figure 3: WebVRAM Main Screen**



5. The WebVRAM Administration Module Main Page is displayed.

Figure 4: WebVRAM Administration Module Main Page



## 4. Using the Application

### 4.1. View / Edit User

1. **Find User:** In many instances, the user will have recently requested a change to their existing WebVRAM User Profile. When a WebVRAM Administrator or a Business Unit Administrator user logs in to the WAM, they will be shown a display of the last 10 users to login to the system and may be able to select the user they need to edit. If the user is not in that list, click on the **Users** link on the left side of the WebVRAM Administration Module Main Page as shown in Figure 4. Clicking that link displays the WebVRAM Administration Module Users Screen as shown in Figure 5. Clicking on the **Next** button or the **page number** at the bottom of the screen will allow you to scroll through the user list. Or, you may click on the **Last Name** or **First Name** heading to sort the list alphabetically.

Figure 5: Users Screen

User #	AD Username	First Name	Last Name	Status	
5	VHAI	B	W	Enabled	View User
6	VACO	C	W	Enabled	View User
10	VHAC	P	W	Enabled	View User
14	VHAM	C	W	Enabled	View User
2	VHAM	C	U	Disabled	View User
1	VHAM	C	W	Enabled	View User
12	VHAC	F	T	Enabled	View User
9	VHAM	S	S	Enabled	View User
8	VHASL	K	S	Enabled	View User
19	vha	L	S	Enabled	View User

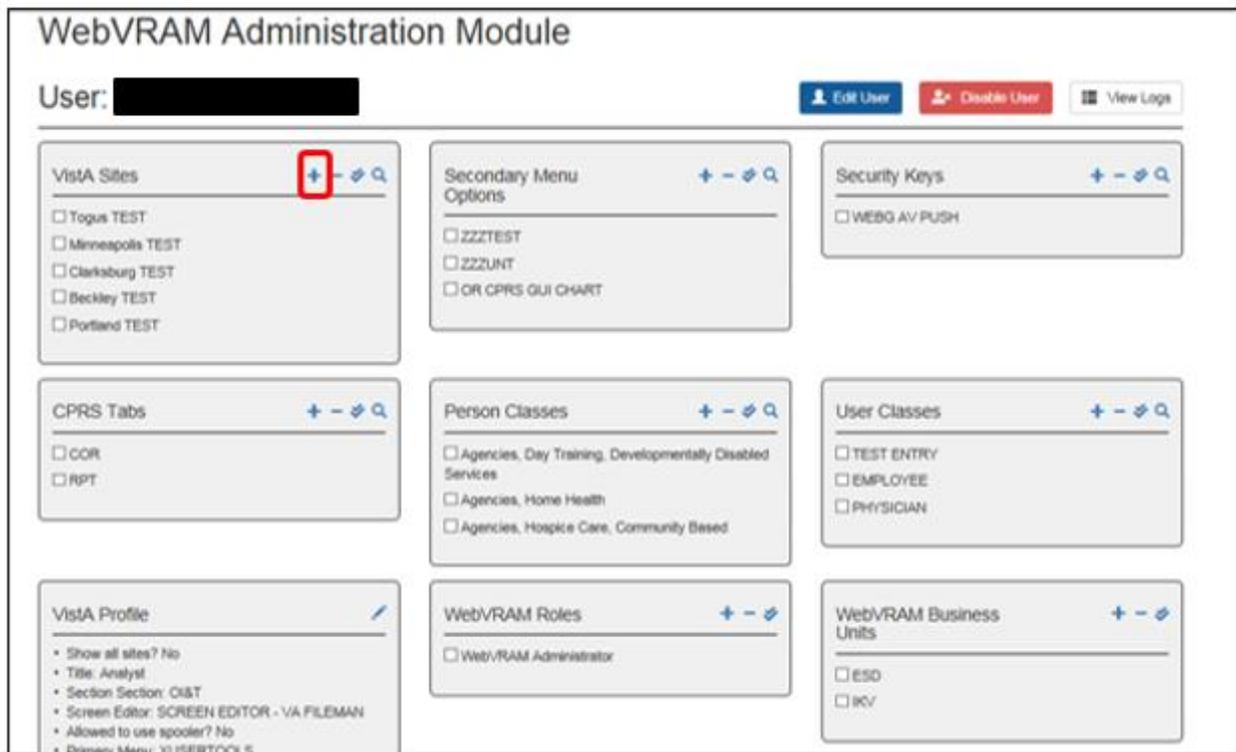
2. **Search Box:** In the box with the magnifying glass icon above the Users list, type the user's last name, or first name <space> last name, or Windows VA Username/Network ID. Windows VA Username may be the best search option to prevent seeing multiple users with the same or similar name. This search will start showing names of users matching the search criteria entered so that the correct user can be selected to edit.

3. **View User:** Once the user is identified, to edit the user, click on **View User** on the right side of the user's name as shown in Figure 5 above. This opens the WebVRAM Administration Module **User Profile Screen**, which provides an overview of the data elements that can be added or removed from a user's profile as shown in Figure 6: User Profile Screen. To add information for any given component, click on the "+" sign in each area. From this screen, user information listed here can be added or removed from the user profile.

Sections include:

- VistA Sites (remote VistA sites a user has been authorized to access)
- CPRS tabs
- Secondary Menu Options
- Security Keys
- Person Classes
- User Classes
- WebVRAM Roles – the roles the user will have in relation to the use of WebVRAM
- WebVRAM Business Units – assigning a Business Unit to the user
- VistA Profile

**Figure 6: User Profile Screen**



4. Clicking on the “+” sign in the VistA Sites option brings up the next screen, which displays remote VistA systems the user may connect to for work.

Figure 7: VistA Sites Screen

U.S. Department of Veterans Affairs

Home Tools Help Manage

WebVRAM Administration Module

User: [REDACTED] Edit User Disable User View Logs

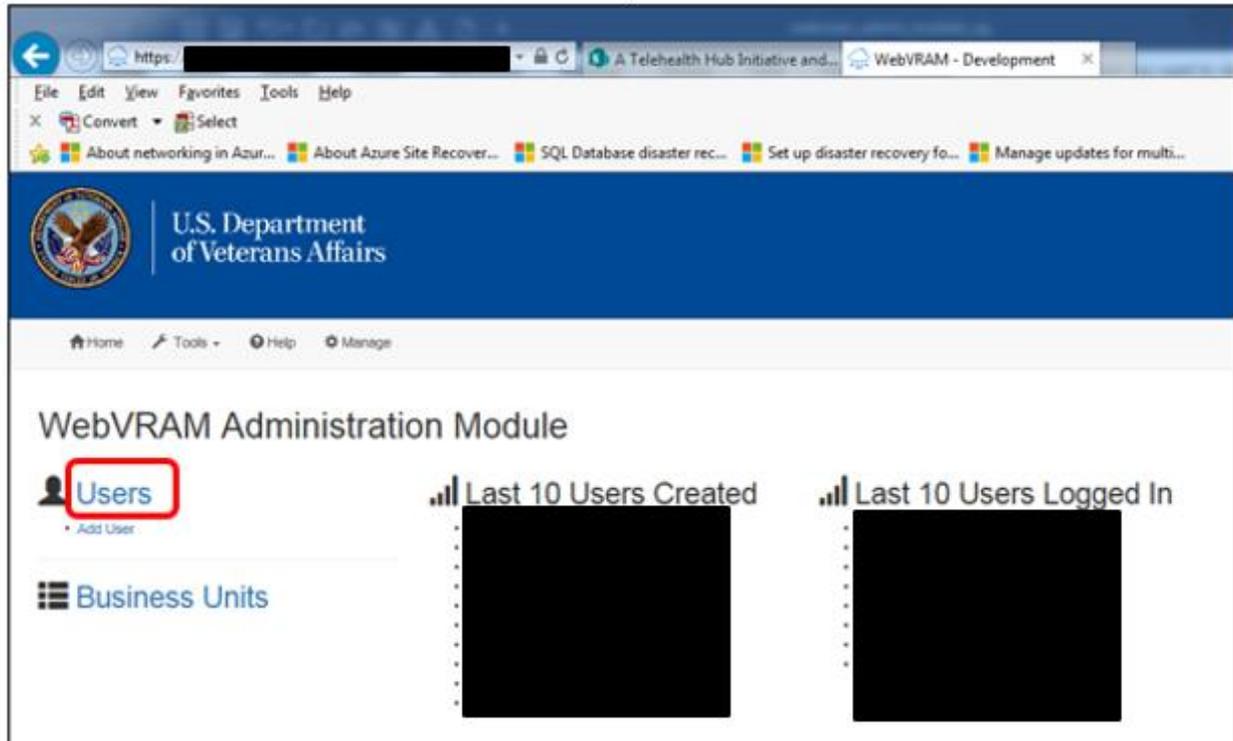
VistA Sites Add all sites Remove all sites

station #	Station Name	VISA	State	Test Site?	
741	Global Disability Examinations	741	CO	Yes	Add Site
821B	Azure 821 B:vr2test	255	HI	No	Remove Site
820B	Azure 820 B:vr2test	255	CA	No	Remove Site
820A	Azure 820 A:vr1test	255	AZ	No	Remove Site
200CORP	Veterans Benefits	100	CO	Yes	Add Site
100	Claims System	100	CO	Yes	Add Site
903	Togus TEST	99	MN	Yes	Add Site
906	Portland TEST	99	OR	Yes	Add Site
901	Minneapolis TEST	99	MN	Yes	Add Site

5. **Add/Remove VistA System(s) Selection Screen:** VistA sites approved by the user’s manager can be added to the user’s profile in this screen by clicking the **Add Site** button on the right side of the row corresponding to the VistA location. Sites can be removed from the user’s profile by clicking the **Remove Site** button on right side of the line of the site to be removed. If authorized, ALL VistA sites can be added to the user’s profile by clicking the **Add all sites** button. Once all sites are added to the user’s profile, selected VistA sites can be removed by searching for them using the search window, and then clicking on **Remove Site**.

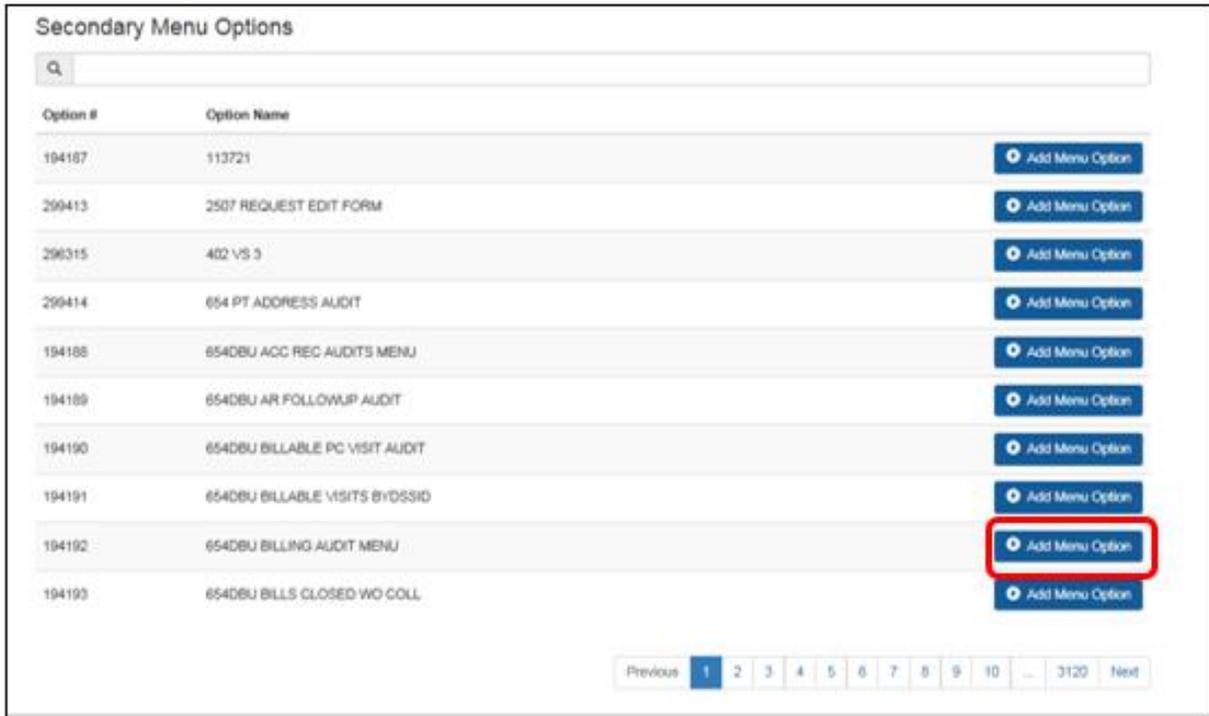
6. **Additional Edits:** After one area is edited for the user, to edit other components of that user, click on the user's name at the top of the page as shown in Figure 7 above, and the User Profile Screen will be shown again as seen in Figure 6. Select the component to edit and click the "+" sign to add or remove data.
7. Clicking on the **Users** link on the left side will open a longer user list displayed on a new page as shown above in Figure 5: Users Screen. You can also search for a user by entering a partial name in the search window.

**Figure 8: Administration Module Users Link**



8. **Updating the User Profile:** Edits to each area of the user profile can be performed by following a similar process for each component as shown in Figure 7 and here in Figure 9. To add an option, click the **Add <Option>** button on the right side of the option. To remove an option, click the **Remove <Option>** button on the right side if an option was added in error.

Figure 9: Add/Remove Secondary Menu Options Screen



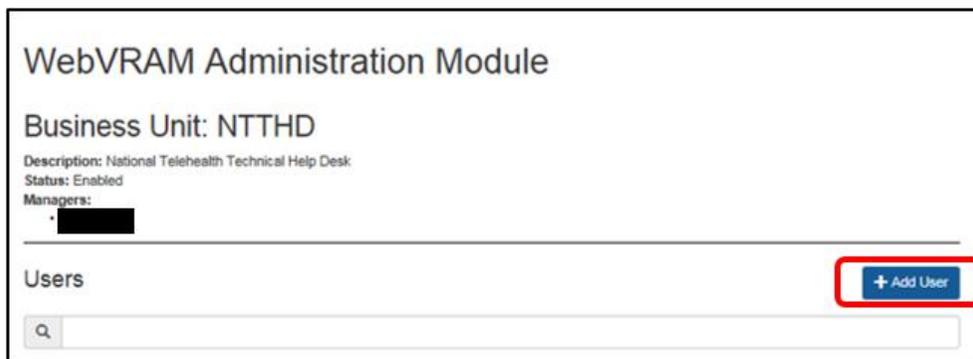
## 4.2. Add New User

The Business Unit Administrator can add new users to the Business Unit they are authorized to manage. To add a new user, click **Manage** on the toolbar. Under the **Business Units** heading, click on the **Business Unit abbreviation** and then click on **Add User** on the right side of the screen. See Figure 10 and Figure 11 below. After selecting these options, the Add User Screen is displayed.

**Figure 10: Administration Module Business Units Links**



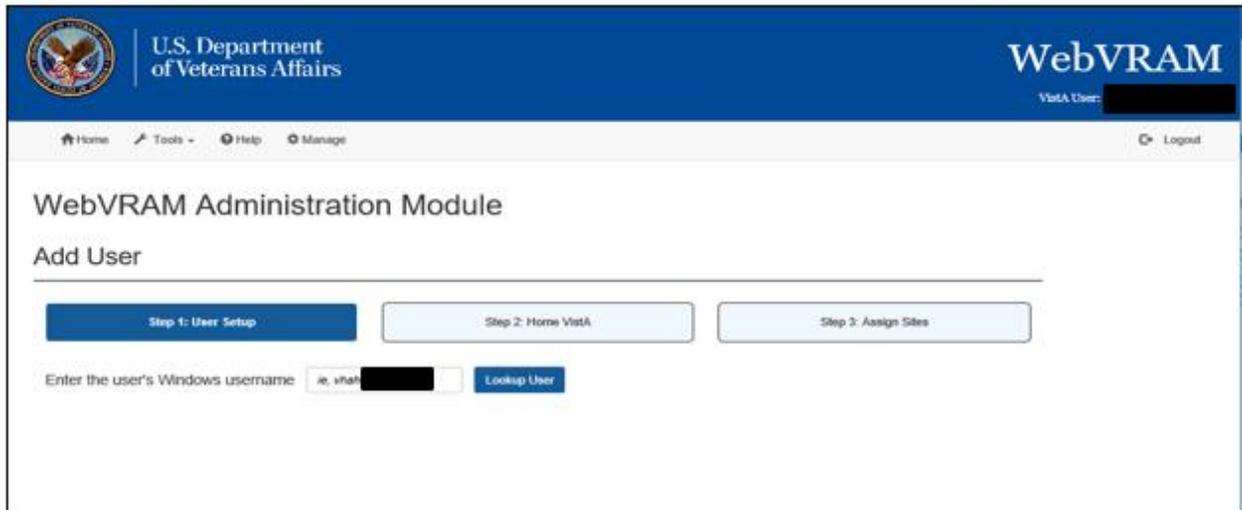
**Figure 11: Business Unit Profile Screen**



The Business Unit Administrator can add a user as outlined above using the “Business Unit” pathway, or they can simply click on the **Add User** link under the **Users** heading on the

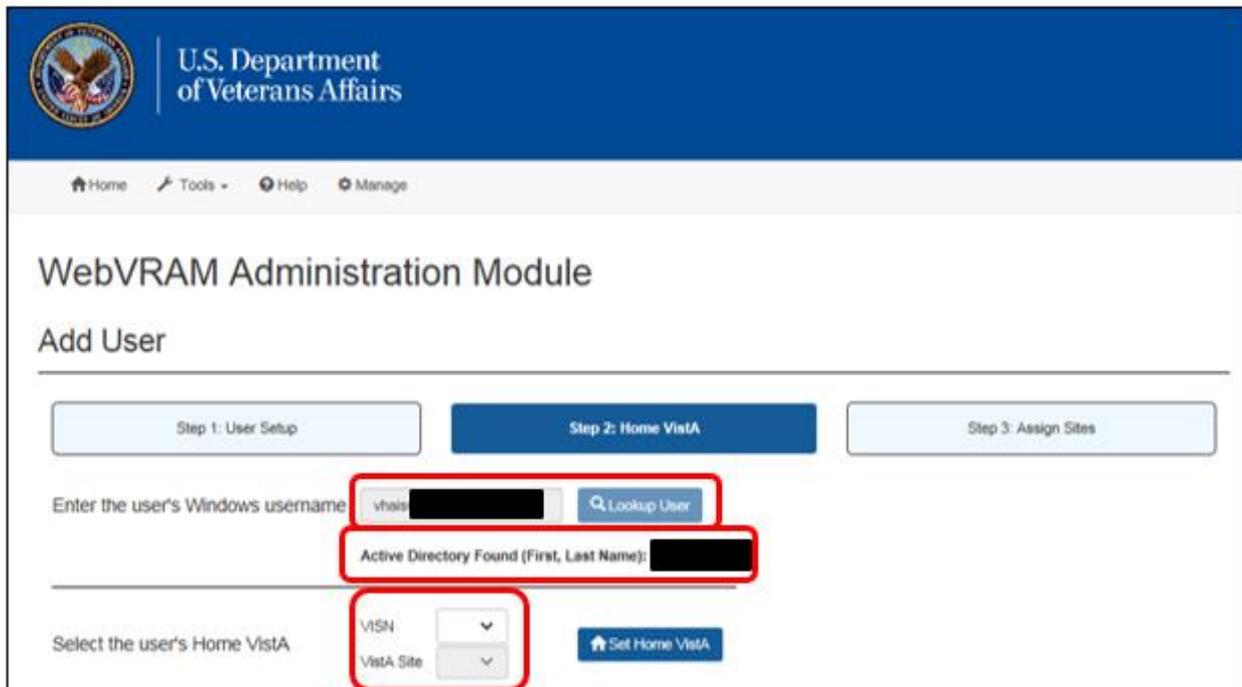
WebVRAM Administration Module Main Page. The Add User Screen is displayed, as shown in Figure 12 below.

**Figure 12: Add User Screen**



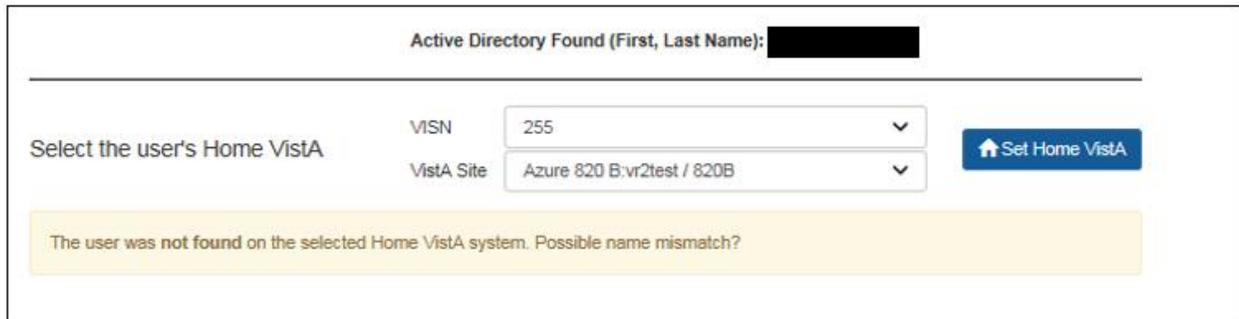
1. **Windows Username Search Box:** Search for a user to add to the WUT by typing their full Windows VA Username/Network ID in the **Enter the user's Windows username** search box and clicking on the **Lookup User** button.
  - a. If the user is found in the VA GAL/AD, the user's full name is returned and presented on the screen with a message prefix of "Active Directory Found (First, Last Name:)" as shown below.

**Figure 13: User Lookup on Add User Screen**



2. Verify the user found is the correct user. If so, select the user's VISN and associated Home VistA Site from the drop-down lists shown in Figure 7. If the user already exists in the WebVRAM User Table, the User Profile Screen will automatically appear as shown in Figure 6.
3. If the user does not have an active VistA account at the Home VistA Site selected, an error will appear indicating the user was not found on that VistA system. Unless the site was selected incorrectly, you will need to contact the user to confirm that they have an active VistA account and user profile established on their Home VistA system.

**Figure 14: User Not Found on Home VistA Error**



The screenshot shows a web interface for user management. At the top, it displays "Active Directory Found (First, Last Name):" followed by a redacted name. Below this, there are two dropdown menus: "VISN" with the value "255" and "VistA Site" with the value "Azure 820 B:vr2test / 820B". To the right of these dropdowns is a blue button labeled "Set Home VistA". Below the dropdowns, a yellow error message box contains the text: "The user was not found on the selected Home VistA system. Possible name mismatch?".

4. Once the Home VistA system is selected from the drop-down boxes, click the **Set Home VistA** button. If all user profile information is entered correctly in the user's Home VistA system, a "Success" message will display, as shown in Figure 15 below, and you can then add authorized VistA sites to the user profile by clicking on the **Add VistA Sites** button.  
Alternatively, the Administrator may choose to add another user at this point without first updating the VistA sites for this user, if the Administrator prefers to add all users first and update their profile information later. To proceed in this manner, click the **Add another user** button.

Figure 15: Add User Screen – Success Message

The screenshot shows the 'WebVRAM Administration Module' interface for adding a user. It features three progress steps: 'Step 1: User Setup', 'Step 2: Home Vista', and 'Step 3: Assign Sites', with 'Step 3' being the active step. Below the steps, there is a form for entering the user's Windows username and Active Directory details. A 'Lookup User' button is present. The 'Select the user's Home Vista' section includes dropdowns for 'VISN' (255) and 'Vista Site' (Azure 821 A:vr1test [DEV HOME VISTA] / 459), along with a 'Set Home Vista' button. A 'Success!' message states: 'WebVRAM is building the user's profile based on the Home Vista system, in the meantime - assign Vista sites to the user'. At the bottom, there are two buttons: 'Add Vista Sites' and 'Add another user', both highlighted with red boxes.

5. As shown in Figure 6, the following data elements should be added to each new user profile once the user has been added to the WUT, *if the Vista profile of the user is not accessible to the WebVRAM application for automatic retrieval of this data:*

- **Vista Sites (Remote)** – Add all Vista sites the user is approved to access to perform work. As shown in Figure 7, the user can have ALL Vista systems added to their profile if they are authorized to access all Vista sites across the VA enterprise.



**CAUTION:** If the user has an active Vista account at any site outside their local/Home Vista system, **DO NOT** add that site (or sites) to their WebVRAM profile. Instruct the user that they should **NOT** use WebVRAM to access those sites, where they have a current Vista login account, but should continue to access those accounts directly as they have been doing.

This is because WebVRAM retrieves the user's local Vista profile and pushes it to any remote system the user connects to using the application. It then overwrites any existing Vista account information the user had before that connection was made with the information in the user's Home Vista profile. WebVRAM was designed to connect users to remote Vista sites where they do **NOT** already have an active Vista account.

- **CPRS Tabs** – CPRS users will need the **COR** or **RPT** tab added to their profile. The user should have only one tab value and not both, and the value in the WebVRAM profile should be identical to the value in the user's Home Vista profile.
- **Secondary Menu Options** – Add any Secondary Menu Options required to use Vista applications when the user connects to remote Vista sites. For example, the

CPRS application requires the user to have the **OR CPRS GUI CHART** Secondary Menu Option in their user profile before CPRS can be launched.

- **Security Keys** – The **WEBG AV PUSH** security key MUST be added to the WebVRAM user profile. If not present, the user will not be able to completely synchronize to a remote VistA system, and when attempting to launch CPRS at a remote site, the user will receive an “Invalid Access/Verify Code Pair” error.

Add other security keys that exist in the user’s VistA profile as needed. Also add security keys for site-specific applications that only exist at one or a few remote VistA sites if the user will need these keys to perform job responsibilities at those sites.

- **WebVRAM Roles** – Add the **WebVRAM User** role to the user’s profile.
- **WebVRAM Business Units** – If this data element is not automatically populated, add the appropriate business unit to the user’s profile by opening this widget and clicking **Assign to User** on the right side of the business unit to be added.

6. **MANDATORY:** Select or add the following data elements to the user profile. These elements are **mandatory**, and if not added, will cause access to WebVRAM to fail or will cause certain features of WebVRAM to fail. **They cannot be blank.** To edit these fields, from the User Profile Screen, click on the **pencil icon** in the top right corner of the **VistA Profile** box as shown in Figure 16. The data for each field to be selected/added is listed here and shown in Figure 17.

- **Title** – If not auto-populated, enter the user’s job title as recorded in their VistA profile, such as Nurse Practitioner, Benefits Clerk, Physician, Help Desk Technician, Psychiatrist, Analyst, etc.
- **Service Section** – If not auto-populated, enter the user’s VA Service Section, such as VHA, VACO, VBA, OIT, etc.
- **Screen Editor** – If not auto-populated, enter **SCREEN EDITOR – VA FILEMAN**. Some business units, such as Consolidated Patient Account Center (CPAC), use a different screen editor to perform job functions. Check with each user to verify the screen editor they should use.
- **Allowed to use spooler?** – Most users will not need to use the VistA spooler. Each business unit will need to determine which users require the spooler. The default value for this option is **No**. For users who need this VistA feature, select **Yes** from the drop-down menu.
- **Primary Menu** – If not auto-populated, ask the user to supply the name of their primary menu; the user may have to contact their local IT support staff to find out their primary menu. Once known, enter the user’s VistA Primary Menu name. This value must be a standard VistA menu name for the user’s primary menu on his/her local or Home VistA system.



**CAUTION: If the primary menu is not a standard VistA menu, the user will not be able to connect to remote VistA systems through WebVRAM; the**

**connection will fail with a “menu tree rebuild failure” error.** Menu names that start with **ZZ**, such as **ZZ CLINICIAN MAIN MENU**, are not VA standard menus and should not be entered in this field.

If the user’s Home VistA profile is successfully pulled into their WebVRAM profile when the user is first added, and the user’s primary menu is a custom menu, then the application will automatically add a standardized menu to the WebVRAM profile.

If the user’s profile does not auto-populate with the Home VistA values and/or is “blank” when first created, then the Business Unit Administrator should add a standardized menu based on the user’s job description as follows:

- Physician or Physician Assistant: **PX PCE CLINICIAN MENU**
- Nurse: **NURSCL-MENU**
- Non-Clinical User: **XUSERTOOLS**

After all edits have been made to the fields in this category, click the **Update VistA Profile** button at the bottom of the window. If updates should not be saved, click **Cancel**.



**NOTE:** Other options of the user profile should be updated automatically when the user logs in to the WebVRAM application for the first time. Upon initial login, WebVRAM checks the user’s Home VistA system and retrieves all keys, menu options, secondary menu options, and other profile elements to make up a complete user profile that will be replicated when the user logs into the remote site(s) via WebVRAM. If, after login, the user finds that secondary menu options and keys are not being passed to the remote sites they attempt to access, instruct them to open a Service Now (SNOW)/YourIT ticket to request help resolving the issue.

Figure 16: VistA Profile Option

The screenshot shows a web interface with two main panels. The top panel, titled "CPRS Tabs", contains two unchecked checkboxes: "RPT" and "COR". To the right of this panel are two other sections: "Person" with the text "No person" and "WebVR" with two unchecked checkboxes: "WebVR" and "Busines". The bottom panel, titled "VistA Profile", contains a list of profile settings: "Show all sites? No", "Title: Tester", "Section Section: VHA", "Screen Editor: SCREEN EDITOR - VA FILEMAN", "Allowed to use spooler? No", and "Primary Menu: MCARUSER". A red square highlights a blue pencil icon in the top right corner of the "VistA Profile" panel.

Figure 17: VistA Profile Data Entry Fields

The screenshot shows a "VistA Profile" data entry form. It contains several input fields: "Show All Sites?" with a dropdown menu set to "No"; "Title" with a text field containing "Tester"; "Service Section" with a text field containing "VHA"; "Screen Editor" with a text field containing "SCREEN EDITOR - VA FILEMAN"; "Allowed to use spooler?" with a dropdown menu set to "No"; and "Primary Menu" with a text field containing "MCARUSER". At the bottom of the form, there are two buttons: "Update VistA Profile" (highlighted with a red box) and "Cancel".

### 4.3. **Add Security Key Not Present in User’s Home VistA – Audit Required**



**CAUTION:** The procedures in this section do NOT apply to CPAC Business Unit Administrators, as they follow an established auditing policy/procedure 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 where the Security Keys do not exist in and are not added to the users’ Home VistA profiles.
  - a. Collate this data into a separate list for each Home VistA site, for users who share the same Home VistA system.
  - 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](#).

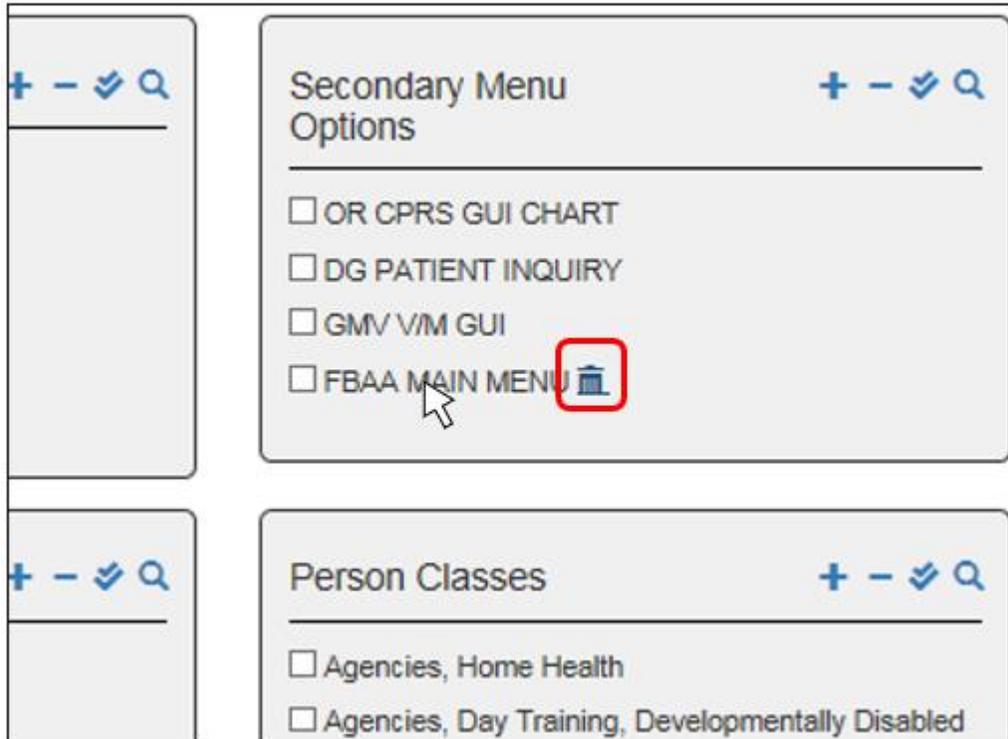


**NOTE:** The hyperlink above points to the VA intranet and will only work for authorized users connected to the VA network.

## 4.4. Quick Delete of User Profile Entries

If a user profile data element needs to be deleted, return to the User Profile Screen. For all categories of the user data except VistA Profile, hover the cursor over the item to be deleted and a trashcan icon will appear. Click the **trashcan icon**, and the element is deleted from the user's profile. There is no need to open or edit the category box. See Figure 18 below.

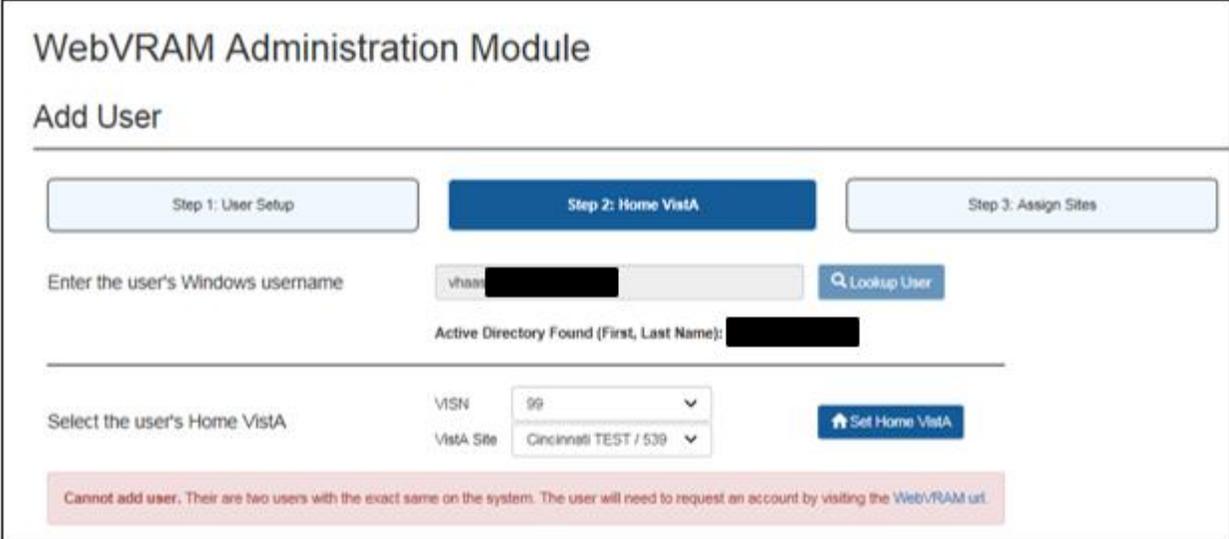
Figure 18: Edit User Quick Delete Option



## 4.5. Duplicate Users in Home VistA and Other VistA Data Anomalies

If a WebVRAM Administrator attempts to add a new user to the WUT through the WAM, and that user has a nearly identical profile to a user who already has a profile in the same Home VistA system, the following error will display as shown in Figure 19: “Cannot add user. There are two users with the exact same name on the Home VistA system. The user will need to request an account by visiting the [WebVRAM Access Request URL](#).”

**Figure 19: Duplicate User Error Message**



The screenshot shows the 'WebVRAM Administration Module' interface for adding a user. It features three steps: 'Step 1: User Setup', 'Step 2: Home VistA' (which is active), and 'Step 3: Assign Sites'. The 'Add User' section includes a text input for the user's Windows username, a 'Lookup User' button, and a field for the Active Directory Found (First, Last Name). Below this, there are dropdown menus for 'VISN' (set to '99') and 'Vista Site' (set to 'Cincinnati TEST / 539'), along with a 'Set Home VistA' button. A red error message at the bottom states: 'Cannot add user. There are two users with the exact same on the system. The user will need to request an account by visiting the WebVRAM url.'

1. Contact the user and instruct them to navigate to the URL above using the Internet Explorer browser. Once the user has accessed this URL, they will must complete the fields on that webpage, as shown below in Figure 20:
  - a. Select the correct **Business Unit** from the drop-down list.
  - b. Select the correct **VISN** from the drop-down list.
  - c. Select the local or **Home VistA** from the drop-down list.
  - d. Enter the Access and Verify codes used to access the Home (local) VistA system.
  - e. Click **Send Access Request**.

Figure 20: WebVRAM Access Request Screen

U.S. Department of Veterans Affairs

WebVRAM

## Access Request

To request access, complete the following steps in order:

1. Select your business unit
2. Select your VISN
3. Select your Home VistA system
4. Login using your Access and Verify Code

Business Unit: OCC

VISN: 99

Home VistA: Cincinnati TEST - 539

Access Code:

Verify Code:

[Send Access Request](#)

v1.0.19-20190925

75%

2. Once the user has successfully navigated to the page, entered all required information, and successfully sent the access request with no errors, login to the WebVRAM application and click on the **Manage** option on the toolbar. Select the user from the **Last 10 Users Created** or the **Last 10 Users to Login** or locate the user by entering the user's name in the search bar on the first page of the user list.
3. When the user is located and displayed for editing, the user's listing should show a **Status** of "Disabled" as shown below. Click on the **View User** button on the right side of the user listing. The User Profile Screen will appear.

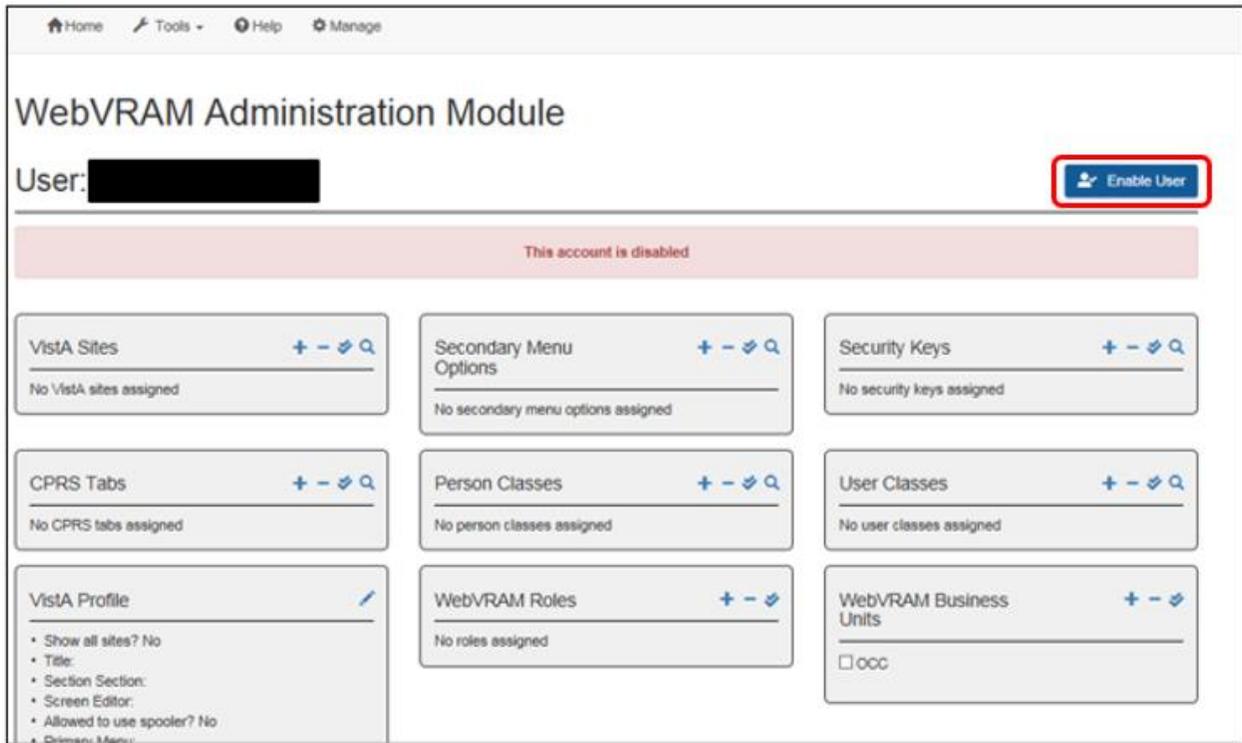
Figure 21: User Disabled Status

Status
Disabled

[View User](#)

- Click on the **Enable User** button on the top right of the User Profile Screen, as shown below.

**Figure 22: User Profile Screen with Enable User Button**



- The button on the top right of the screen changes from **Enable User** to **Disable User**. The user is now enabled for WebVRAM access. Contact the user with instructions to retry logging into the application. If they are unable to log in after these actions have been taken, ask the user to create a ticket using SNOW/YourIT or by calling the ESD.
- Ask the user to provide all aspects of their Home VistA user profile listed below. To discover this information, the user may need to contact local IT by creating a SNOW/YourIT ticket. Users who use the VistA roll-and-scroll screen will be aware that they can type in a common VistA menu option to find most of these values themselves, but there are some that are not displayed when using that VistA option. The option is the User Toolbox, and if the user has a Primary Menu that is NOT the User Toolbox, they can simply type **XUSERTOOLS** at any VistA menu prompt. They then select the **Display User Characteristics** option from that menu to view their user profile and record the values they see. Based on this information, update their WebVRAM user profile and add the role of “User” to their WebVRAM user profile.
  - CPRS Tabs
  - Secondary Menu Options
  - Security Keys
  - Person Class, User Class

- e. Vista Profile Information:
    - i. Title
    - ii. Section
    - iii. Screen Editor
    - iv. Allowed to use spooler
7. **KPA CPAC NSD MENU**: As a Business Unit Administrator, you should have the **KPA CPAC NSD MENU** Secondary Menu Option in your WebVRAM profile. If it is not there, you should be able to add it to your profile. This menu option will allow you to login to a user's Home VistA site and inquire to see their VistA profile values. This can be done if there is an urgent need and the user cannot obtain the values you need to add to their blank profile in an expeditious manner. The steps to use this option are as follows:
- a. If the **KPA CPAC NSD MENU** is not in your list of Secondary Menu Options, add it to your profile in the same way you would update any user profile.
  - b. Identify the user's Home VistA location by editing their user profile as shown below in Section [4.8](#) (View/Edit User's Home VistA System and Active Directory Name). There is no need to edit their Home VistA profile, so simply select **Cancel** once you have identified their Home VistA system.
  - c. Click the **Home** button on the toolbar to view the remote VistA sites you have in your **VistA Sites** list. If the user's Home VistA site is not in your list of VistA sites, add it to your profile in the same way you would update any user profile.
  - d. Click the **Home** button to return to your home screen and list of VistA sites. Locate the user's Home VistA site and click **Launch Reflection**.
  - e. After WebVRAM logs you into that VistA system, follow any prompts that require you to "Press Enter to Continue" until the cursor stops at a VistA "Select Option" menu prompt, as shown below.

```
Change my Division
Display User Characteristics
Edit User Characteristics
Electronic Signature Code Edit
Menu Templates ...
Spooler Menu ...
Switch UCI
TaskMan User
User Help

Select User's Toolbox Option: CPAC
```

VistA may not show the menu options, depending on the site parameters at each remote site. As long as the "Select Option" prompt is present, you can proceed.

- f. At the VistA menu prompt, type **CPAC** to navigate to the KPA CPAC NSD Menu.
- g. When the KPA CPAC NSD Menu prompt appears, type **USER** to select the User Inquiry option.

- h. At the next prompt, type the user's **Lastname,Firstname** and press <Enter>. If the user has a name similar to other users (e.g. Amy Smith), a list of users will be displayed to make a selection. Locate the user with the correct full name (middle initial, suffix, etc.) and type the **number** of that user to the right of the CHOOSE prompt. Press <Enter> *twice* at the DEVICE prompt.
- i. The user's profile information is displayed, as shown below. You can copy/paste the VistA values needed to build the WebVRAM user profile by highlighting the text displayed, **right-clicking** with your mouse, and selecting **Copy** from the drop-down. Press <Enter> to scroll through the entire profile to list all options.



**CAUTION: Do NOT use the keystroke combination of Ctrl+C to copy from the displayed text. VistA will terminate your session and you will have to start over.**

```

LNAME, FNAME MI  (#12404)
-----
Service/Section:  PULMONARY

ATTRIBUTES
-----
Creator .....***                               Date entered.....Feb 27, 1992
Mult Sign-on ...ALLOWED                         Fileman codes .....
Time-out .....900                               Type-ahead .....ALLOWED
Title .....STAFF PHYSICIAN                     Office Phone .....555-555-5555
Auto-Menu .....YES, MENUS GENERATED           Voice Pager .....
Last Sign-on ...Mar 31, 2020                    Digital Pager ..... 555-555-5555
Has a E-SIG ...Yes                              Write Med's .....YES
NPI .....*****                               Taxonomy .....207RP1001X
Person Class:  Allopathic & Osteopathic Physicians
                Internal Medicine
                Pulmonary Disease

Primary Menu:  ARL MD MENU                       Consolidated Practitioner's Menu

Secondary Menu(s)
-----
PCE  [PX PCE CLINICIAN MENU]                    PCE Clinician Menu
PEF  [IBDF PRINT OPTIONS]                       Print Options
DOC  [ZMD DOC2 MENU]                             Practitioner's Menu II
      [OR CPRS GUI CHART]                        CPRSChart version 1.0.31.118
CN   [GMRCZ SERVICE ACTION MENU]                Consult/Request Service Menu
      [MARPULMUSER]                              Pulmonary Menu
      [OOPS GUI SUPERVISOR MENU]                ASISTS GUI Supervisor Menu

(Context)
      [AJR CAIRO HAND-OFF]                       CAIRO Hand-off Tool
      [AXV ENG EQUIP LOAN]                       ZZAXV ENG EQUIP LOAN
      [DVBA CAPRI GUI]                           Capri GUI (Broker)
      [WEBG WEBVRAM GUI]                         WEBG WEBVRAM GUI

Keys Held
-----
      MAGDISP CLIN          MCKEYPFT          ORES          PROVIDER

Patient Selection
-----
Restrict?: NO
OE/RR List:

```

```

CPRS Access Tabs
-----
Name      Description                Effective   Expiration
-----
COR       CPRS GUI "core" tabs.           JUN 25,2002

CPRS Parameter info (User Specific)
-----
OR ADD ORDERS MENU:      ORZ GMENU CLINICIAN MEDICINE LIST MANAGER

Last used MailMan: 05/20/15@07:58
NEW messages: 346 (346 in the IN basket)

Office phone:
Fax:
Digital pager:

Mail Groups:
MED SVC DOCS                (Public)
PHYSICIANS                  (Public)

Type <Enter> to continue or '^' to exit:

Select NEW PERSON NAME:

```

- j. Once the required values are copied, they can be pasted into a Word document and then added into the WebVRAM profile.
  - i. Secondary menu option names to add to the WebVRAM user profile are the names in [brackets] displayed in the VistA profile list. Type the name as it appears in the brackets to add it to the WebVRAM profile.
  - ii. Add Menus, Keys, Person Class, User Class, and CPRS Tabs by clicking the “+” sign in each WebVRAM profile section. Either select the available option or search by name in the search bar for the option.



**IMPORTANT:** Be sure to add the WEBG AV PUSH Security Key to the user’s profile along with the other Security Keys from the user’s VistA profile.



**NOTE:** Some menu options are not standardized VistA menu options, and you will not find them in the WebVRAM options list. These local “custom” menus will often start with the letters ZZ, or some other combination of 2 or 3 letters before the actual menu name. These custom menus cannot be added to the WebVRAM user profile and would not be useable at the remote site anyway.

## 4.6. Standard Configurations for CPRS Functionality

For certain features to be available to clinicians within CPRS when accessing it at remote sites, the following WebVRAM configurations must be added to the WebVRAM user profile. These configurations will not necessarily be present in the user's Home VistA profile, and therefore they may not be added to the WebVRAM profile when it auto-populates as a new user is created.



**CAUTION:** The WebVRAM profile may occasionally pull **both** CPRS tabs from the VistA user profile, namely **COR** and **RPT**. If both values are present in the WebVRAM profile, **remove the RPT value and leave only the COR value**. If both values are passed to the remote site when a user connects through WebVRAM, CPRS will not function properly since the two tabs will be in conflict with each other. The CPRS RPT tab provides “read-only” access to the patient record.

### 4.6.1. To Order Meds and Write Notes in CPRS

#### Home VistA Profile:

- **AUTHORIZED TO ORDER MEDS** flag in File 200 set to “YES”

#### WebVRAM Profile:

- Security Key of **ORES** and **PROVIDER**
- CPRS Tabs: **COR**
- The **same Person Class** that exists in their Home VistA profile
- User Class of **PHYSICIAN**

### 4.6.2. To Write CPRS Tele-ICU Notes at Chillicothe and Cleveland VA Medical Centers with a WebVRAM Connection

#### WebVRAM Profile:

- User Classes: **Internist** and **Tele-Health Staff** must both be added

### 4.6.3. To Use CPRS Features as a Non-Physician Provider

Some clinicians need to write notes and order certain medications in CPRS but do not need the other “physician authorized” features. The following profile configuration is recommended:

#### Home VistA Profile:

- **AUTHORIZED TO ORDER MEDS** flag in File 200 set to “YES”

#### WebVRAM Profile:

- Security Key of **ORELSE** and **PROVIDER**
- CPRS Tabs: **COR**
- The **same Person Class** that exists in their Home VistA profile
- User Class of **NURSE** or **NURSE PRACTITIONER** (whichever one best matches the Person Class)

### 4.6.4. To Use the Tele-ICU Provider CPRS Timeout Option

Tele-ICU providers have been authorized by VA to set values in their VistA user profile that will prevent CPRS sessions from timing out for up to 6 hours (equal to 360 minutes or 21,600 seconds). These local values are passed by WebVRAM to remote sites to enable remote ICU patient monitoring without CPRS timing out. The following values must be set for all Tele-ICU providers requiring this extended CPRS timeout option.



**NOTE:** Home VistA profile values must be set by the user’s local IT staff. An Electronic Permission Access System (ePAS) request may be required to make updates if these values do not already exist for the user.

#### Home VistA Profile:

- **TIMED READ** (user profile timeout value) set to **21600** via FileMan edit (File 200 – NEW PERSON file; Field = TIMED READ)
- **ORWOR TIMEOUT CHART** set to **21600** in the user’s parameters (File 8989.5 – PARAMETERS file)

#### WebVRAM Profile:

- **Service/Section** set to **TELE-ICU**

## **4.7. Standard Configuration for VistA Imaging Functionality**

Clinical users of WebVRAM can launch VistA Imaging from CPRS after establishing a remote connection through WebVRAM, if the following Secondary Menus and Security Key are authorized and present in the user's Home VistA profile and WebVRAM profile.

### **Secondary Menus**

- MAG WINDOWS
- MAGT TELEREADER MENU

### **Security Key**

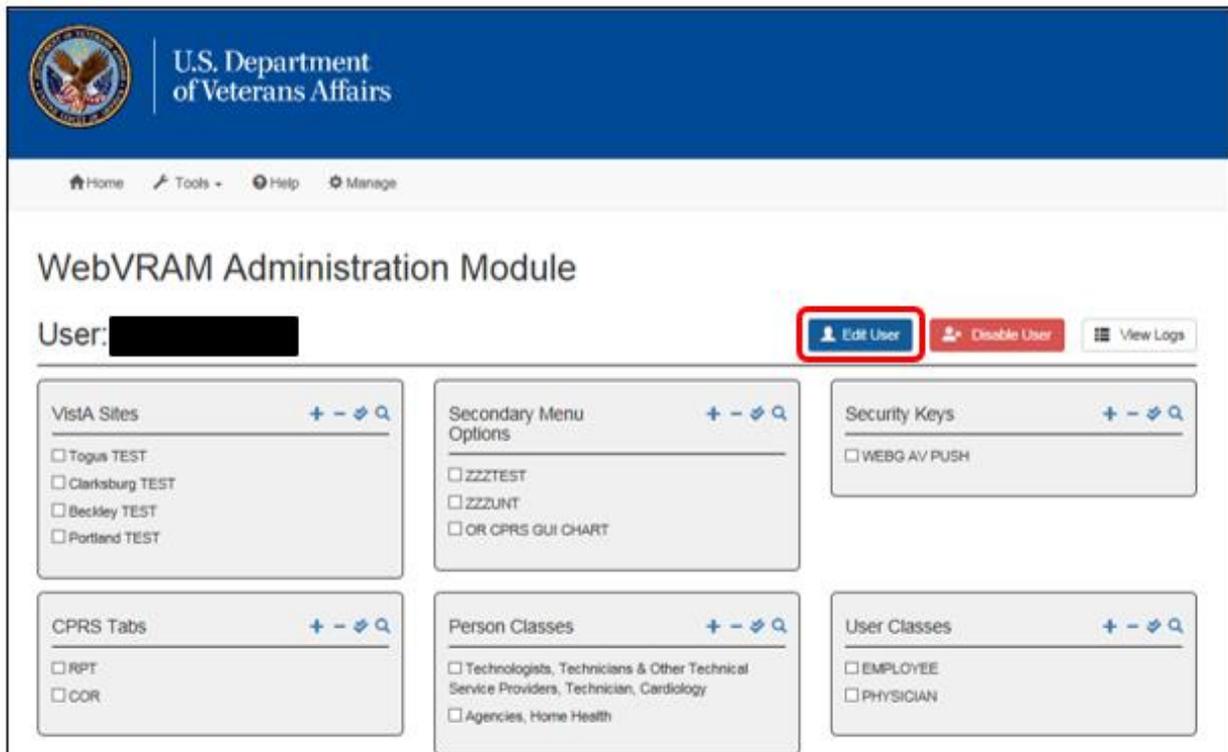
- MAGDISP CLIN

## 4.8. View/Edit User's Home VistA System and Active Directory Name

To view a user's Home VistA System setting, or to change the Home VistA System assignment in cases of the user relocating to another medical center, health care system, or VA office, perform the steps outlined here.

1. On the toolbar, click **Manage**. Select a user from one of the “most recent” lists, or if the user is not listed, click **Users** on the left side of the screen, then search for the desired user as shown in Figure 5: Users Screen.
2. From the user's data overview screen, click **Edit User**, as shown below.

Figure 23: User Profile Screen – Edit User Button



3. The Edit User Screen appears and displays the user's key data. In the "Home VistA" field, click the "X" to in the right side of the box, then type a few characters of the new Home VistA system into the box, as shown below.

**Figure 24: Edit User Screen**

Home Tools Help Manage

## WebVRAM Administration Module

User: [REDACTED] [Edit User](#) [Disable User](#) [View Logs](#)

### Edit User

**Proceed w/Caution!**  
Changing these settings may break the user's WebVRAM account.

First Name	B [REDACTED]
Last Name	W [REDACTED]
Active Directory (Windows) Username	VHAIS [REDACTED]
VA Email Address	
Home VistA	Cincinnati TEST <input type="button" value="X"/>

[Update User](#) [Cancel](#)

**Figure 25: Edit User Screen – Home VistA Field Cleared**

VA Email Address

Home VistA

[Update User](#) [Cancel](#)

- Figure 26 displays the auto-fill feature for the Home VistA box, which provides options for the new Home VistA system until the correct option is displayed in a text box below the Home VistA box. Type a *partial name* of the desired new Home VistA system. In the example below, typing “min” brings up the **Minneapolis TEST** option, which can be added to the Home VistA field. Clicking on the option box presented with the correct full name of the VistA site to be added will populate the Home VistA field with that information, as shown in Figure 27.

**Figure 26: Edit User Screen – Home VistA “Auto-Fill” Feature**



**Figure 27: Edit User Screen – New Home VistA System Selected**

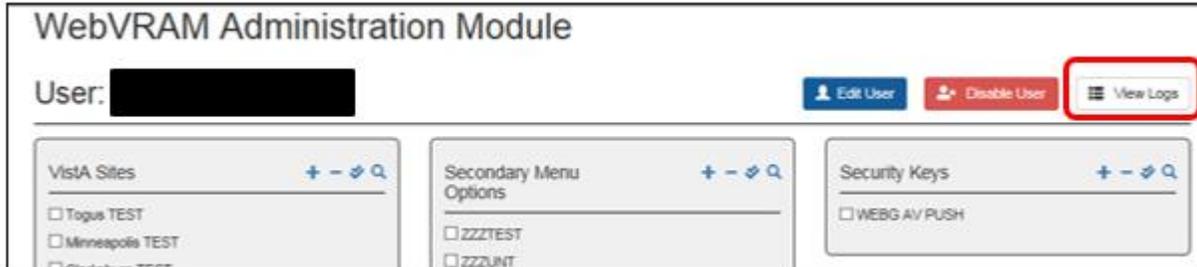


- If the user has experienced a recent name change, the user’s name and VA Active Directory Username (Windows VA Username/Network ID) can also be changed in the **Edit User** component of their profile.

## 4.9. View User's Log

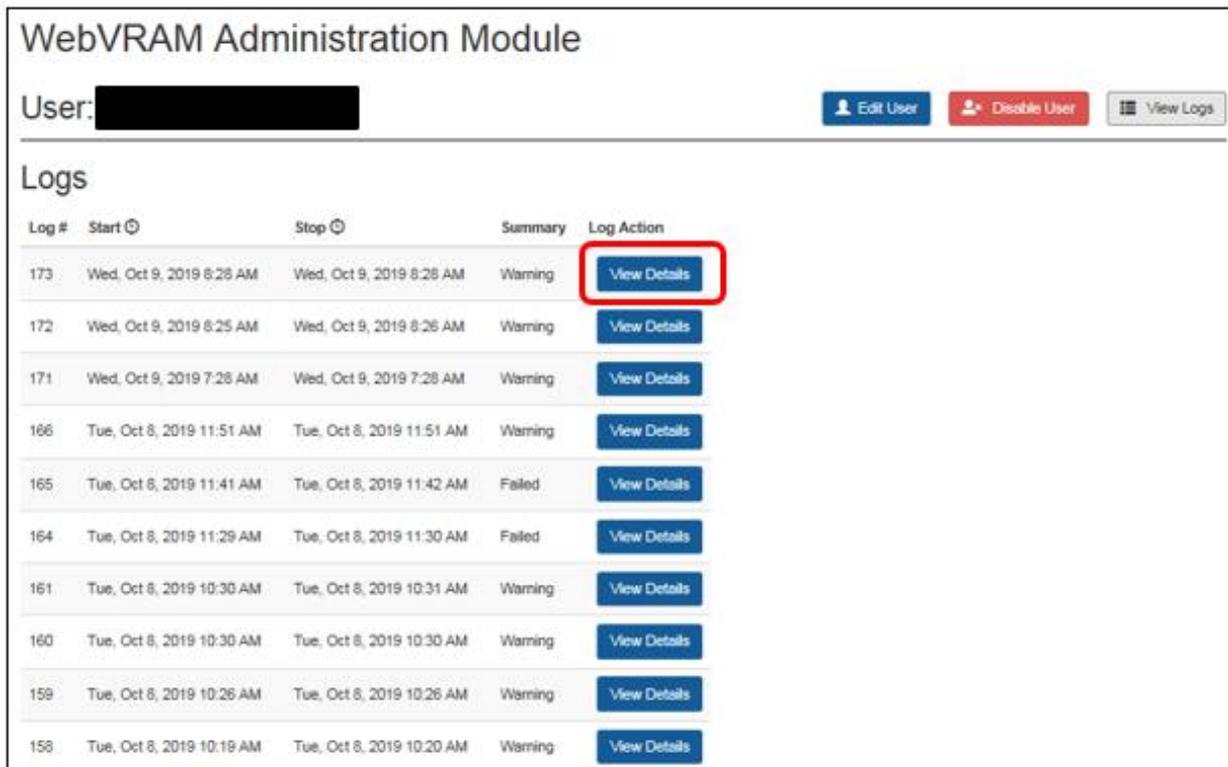
A log of the user's activity on the system can be viewed from the WAM by clicking on the **View Logs** button at the top right of the User Profile Screen.

**Figure 28: User Profile Screen – View Logs Button**



A listing of the user's activity is presented, and the details of each user transaction can be viewed by clicking the **View Details** button to the right of each transaction entry. Figure 29 provides an overview of the user log and the **View Details** button.

**Figure 29: User Log Listing**



The figure below provides an example of the user transaction activity details, as captured in this log.

**Figure 30: User Log Detail Listing**

Detailed Logs for #166

- Checking VistA user profile
- Fetching DB user profile
- Connected to VistA site: Togus TEST
- Could not synchronize Analyst for TITLE field in file 3.1. Please contact your WebVRAM manager.
- Updated your personal information on the remote VistA system
- Updated your A/V code pair.
- Unable to add secondary option because it is not found in file #19: ZZZTEST
- Unable to add secondary option because it is not found in file #19: ZZZUNT
- Finished updating secondary menu options
- Finished updating security keys
- Removed CPRS tab: COR
- Removed CPRS tab: RPT
- Added CPRS tab: COR
- Added CPRS tab: RPT
- Finished updating CPRS tabs
- Assigned the person class: Agencies, Day Training, Developmentally Disabled Services
- Assigned the person class: Agencies, Home Health

### 4.9.1. User Log Cerner Messages

If a site is using Cerner EHR, the site listings page displays the **Launch Cerner** button alongside the existing **Launch CPRS** or **Launch Reflection** button. Since the initial Cerner rollout will not replace all VistA functions, the user can still access certain VistA functions at Cerner sites as he/she did previously.



**NOTE:** WebVRAM will pass menus and security keys for active VistA functions to remote Cerner sites but will not pass menus and security keys for VistA functions that have been replaced by Cerner.

After synchronizing to a Cerner site, the User Log Detail Listing will include messages about menus and security keys that were not passed to the Cerner site due to those VistA functions being replaced by Cerner and deemed inactive at that site. For example, “Cerner does not allow the use of OR CPRS GUI CHART and will be skipped.”

[Figure 31](#) provides an example of the user log after synchronizing to a Cerner site.

Figure 31: Cerner Messages in User Log

The screenshot displays the WebVRAM Administration Module interface. At the top, there is a header for the U.S. Department of Veterans Affairs and the WebVRAM logo. Below the header is a navigation bar with links for Home, Tools, Help, and Manage, and a Logout button. The main content area is titled "WebVRAM Administration Module" and shows a user profile for "User: #255" with buttons for "Edit User", "Disable User", and "View Logs".

### Detailed Logs for #255

- Checking VistA user profile
- Fetching DB user profile
- Connected to VistA site: Azure 821 B:vr2test (CERNER)
- Could not synchronize Analyst for TITLE field in file 3.1. Please contact your WebVRAM manager.
- You are NOT authorized to order medications.
- Updated your personal information on the remote VistA system
- Updated electronic signature details
- Access and verify codes will NOT be synchronized.
- Cerner does not allow the use of OR CPRS GUI CHART and will be skipped.
- Cerner does not allow the use of DG REGISTER PATIENT and will be skipped.
- Cerner does not allow the use of DG REGISTRATION 10/10 REPRINT and will be skipped.
- Cerner does not allow the use of DG REGISTRATION DELETE and will be skipped.
- Cerner does not allow the use of DG REGISTRATION VIEW and will be skipped.
- Unable to add secondary option because it is not found in file #19: KPA CPAC NSD MENU
- Added secondary menu option: XUSERINQ
- Finished updating secondary menu options
- Finished updating security keys
- Finished updating CPRS tabs
- Finished updating person classes
- Finished updating user classes
- Successfully Synchronized

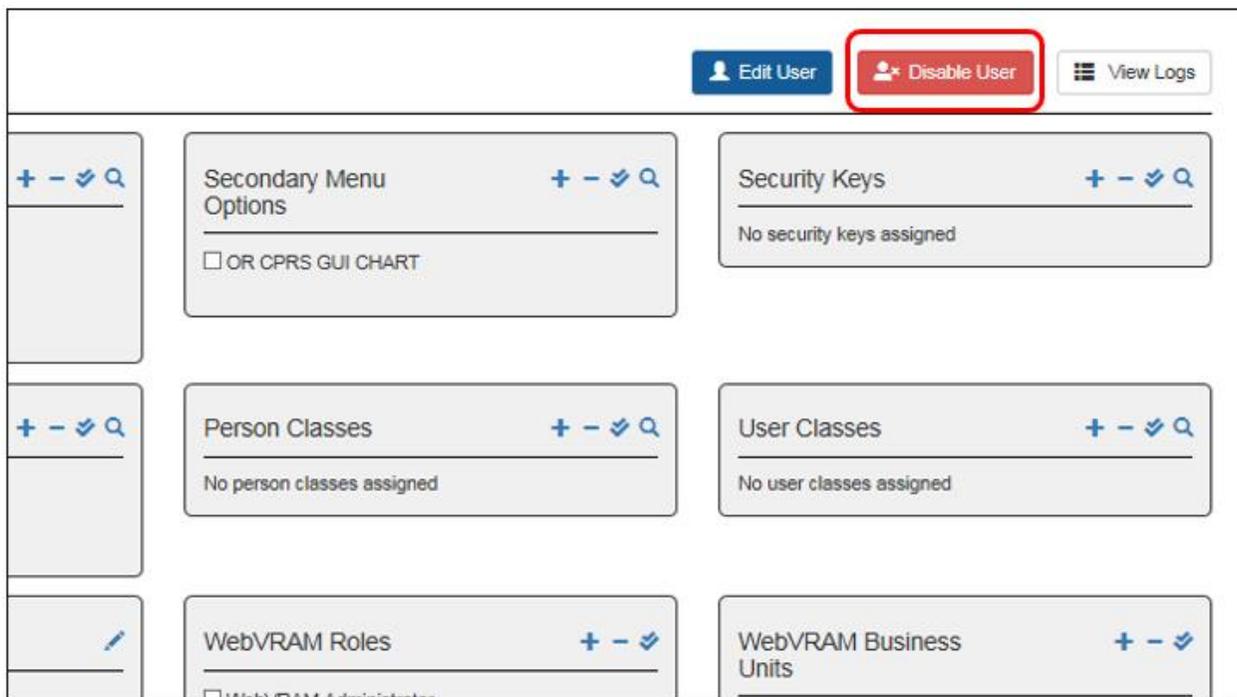
## 4.10. Disable User Account

When a user leaves the VA or changes positions to one that no longer requires the use of WebVRAM, the Business Unit Administrator must disable their WebVRAM user profile. Navigate to the **User Profile Screen** and click the **Disable User** button on the top right above the user profile summary, as shown in Figure 32 below. Once this is done, the User Profile Screen will only show one button, **Enable User**, as shown in Figure 22, and the user will not be able to login to WebVRAM.



**CAUTION: Each business unit is responsible for working with local IT support to disable the remote site VistA system account(s) the user has established through the use of WebVRAM.** Remote site VistA user profiles established electronically through WebVRAM have a set expiration of 30 days; the remote site VistA user profile will expire if the user does not access or login to that remote site within that timeframe. If the VistA user profile established at a remote site through WebVRAM is active when the user's WebVRAM profile is disabled, then the VistA user profile needs to have the disused flag turned "on" at each remote site where the user is no longer authorized to access VistA.

Figure 32: User Profile Screen – Disable User Button



## 4.11. Exit System

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

## 5. Troubleshooting

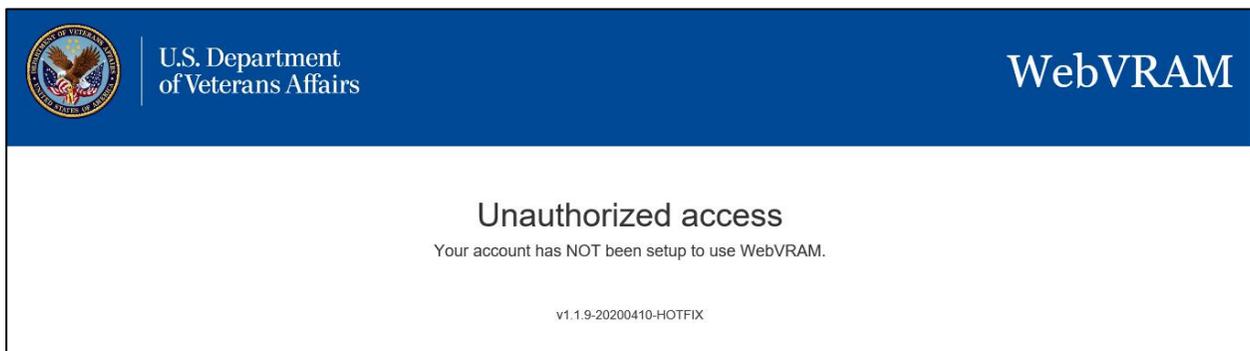
For troubleshooting, users may contact the Enterprise Service Desk (ESD) at 1-855-673-4357 or by entering a SNOW/YourIT ticket to receive Tier 1-3 support.

### 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 33: Unauthorized Access Error Message



2. Did the **WEBG WEBVRAM GUI Secondary Menu Option** propagate from their VistA profile into WebVRAM?
  - a. If NOT, the user will receive an “Invalid Access/Verify Codes” error. Instruct the user to submit an Electronic Permission Access System (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.

4. If the user has the CPRS Tab = **COR**, then they should also have the following items *at a minimum* in their 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.



**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).
  - b. Home VistA Person Class and User Class values:
    - i. If the user is a physician, Person Class 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 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:**
    - i. **AUTHORIZED TO ORDER MEDS** flag in File 200 set to "YES."
  - b. **WebVRAM Profile:**
    - i. Security Keys of **ORES** and **PROVIDER**.
    - ii. CPRS Tabs: **COR**.
    - iii. The **same** Person Class that exists in their Home VistA profile.
    - iv. User Class of **PHYSICIAN** and **PROVIDER** (see step 4c above).

8. Does the user need to write CPRS Tele-ICU Notes at Chillicothe and/or Cleveland VAMCs? If YES, the user must have:
  - a. **WebVRAM Profile:**
    - i. For Chillicothe, User Class of **Internist**.
    - ii. For Cleveland, User Class of **Tele-Health Staff**.

## 5.1.2. Common Problems and Resolutions with User Profiles and VistA Data Anomalies

Table 3: User Profile Issues and VistA Data Anomalies

Issue	Cause	Resolution
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 <b>already has permissions to do so</b> 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.
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 <b>WEBG WEBVRAM GUI Secondary Menu Option</b> to their Home VistA profile.
Unable to login to WebVRAM; receives "Invalid Access or Verify Code" error.	<ol style="list-style-type: none"> <li>1. WEBG WEVBRAM GUI Secondary Menu Option is missing from VistA profile.</li> <li>2. Access and Verify codes need to be reset in user's Home VistA system.</li> </ol>	<ol style="list-style-type: none"> <li>1. Instruct the user to submit an ePAS request to add <b>WEBG WEBVRAM GUI Secondary Menu Option</b> to their Home VistA profile.</li> <li>2. Instruct the user to create a SNOW/YourIT ticket to have local IT reset <b>BOTH their Access and Verify codes</b>. 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.</li> </ol>
User can log in to WebVRAM but receives 'Invalid Access/Verify Code' error when launching Reflection or CPRS.	WEBG AV PUSH Security Key is missing from user profile.	Add <b>WEBG AV PUSH Security Key</b> to the WebVRAM user profile.

Issue	Cause	Resolution
<p>User logs into WebVRAM successfully. Connections to remote sites through Reflection/CPRS end in "FAILED" message.</p>	<ol style="list-style-type: none"> <li>1. 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.</li> <li>2. A non-standard Service/Section value came from local VistA profile.</li> <li>3. Keystroke errors in WebVRAM VistA Profile parameters.</li> </ol>	<ol style="list-style-type: none"> <li>1. Replace User's Custom Menu with a Standard menu based on user role: <ol style="list-style-type: none"> <li>a. Role: Non-Clinical User / <b>XUSERTOOLS</b></li> <li>b. Role: Physician User / <b>PX PCE CLINICIAN MENU</b></li> <li>c. Role: Nurse User / <b>NURSCL-MENU</b></li> </ol> </li> <li>2. Replace Service/Section with <b>MEDICAL SERVICE unless the user is with a CPAC or Office of Community Care (OCC) Business Unit.</b></li> <li>3. Double-check all WebVRAM VistA Profile entries for typos.</li> </ol>
<p>User's connection to remote site FAILS and log shows "User's access [or verify] code already belongs to another user on &lt;VAMC Name&gt; site. Synchronization Failed."</p>	<p>User has identical Home VistA Access or Verify code to another user at remote site.</p>	<p>User must contact local IT:</p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>

Issue	Cause	Resolution
<p>Clinician User, while accessing remote site, is unable to add themselves as Primary Provider to a CPRS Encounter (1 and 2).</p> <p>Clinical User unable to order meds at remote site in CPRS (2).</p>	<ol style="list-style-type: none"> <li>1. Incorrect or missing User Class and Person Class values in VistA and/or WebVRAM Profile.</li> <li>2. User's Person Class had an expired Person Class EFFECTIVE DATE initially pushed to the remote site, resulting in an incorrectly translated value, even if the date was brought current.</li> </ol>	<ol style="list-style-type: none"> <li>1. Add correct User Class and Person Class values in WebVRAM profile. Suggested values for <b>Physician</b> (values for other clinical providers will vary): <ol style="list-style-type: none"> <li>a. User Class: <b>PHYSICIAN</b></li> <li>b. Person Class: <b>VASCULAR NEUROLOGY # 202</b></li> </ol> </li> <li>2. A WebVRAM code update will be released soon to overcome the VistA translation and profile data update problem.</li> </ol>
<p>"User Not Found" when assigning Home VistA to user profile in WebVRAM.</p>	<ol style="list-style-type: none"> <li>1. User may have an inactive VistA account on their Home VistA system due to inactivity.</li> <li>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.</li> </ol>	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>

Issue	Cause	Resolution
<p>“Cannot Add User...(Duplicate VistA Names)”</p>	<p>User has two nearly identical profiles on their Home VistA system; same SSN.</p>	<p>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.</p>
<p>User Profile is added to WebVRAM, but all VistA Profile data is blank.</p>	<p><b>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.</b></p>	<p>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.</p>
<p>User logs out of WebVRAM and is returned to the Terms/Conditions page. User attempts another login and receives “Invalid Access/Verify Codes” error.</p>	<p>Internet Explorer does not persist cookies due to VA policy.</p>	<p>Have the user refresh or close their browser and login again.</p>
<p>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: <b>Missing Station Number.</b>”</p>	<p>The user is missing or has multiple values in the <b>Division field</b> of their Home VistA profile.</p>	<p>Have the user submit a SNOW/YourIT ticket to work with local IT to have a default value added to the <b>Division</b> 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.</p>

Issue	Cause	Resolution
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 <b>ORELSE</b> or <b>OREMAS</b> keys. Leave only the <b>ORES</b> key.

## 5.2. Look Up a User’s Home VistA Profile Information

As a Business Unit Administrator, you should have the **KPA CPAC NSD MENU** Secondary Menu Option in your WebVRAM profile. If it is not there, you should be able to add it to your profile. This menu option will allow you to login to a user’s Home VistA site and inquire to see their VistA profile values. This can be done if there is an urgent need and the user cannot obtain the values you need to add to their blank profile in an expeditious manner. Follow the instructions in Section [4.5](#) (Duplicate Users in Home VistA and Other VistA Data Anomalies), Step 7 KPA CPAC NSD MENU.

## 6. Acronyms and Abbreviations

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

**Table 4: Acronyms and Abbreviations**

<b>Term</b>	<b>Definition</b>
AD	Active Directory
BUA	Business Unit Administrator
CPAC	Consolidated Patient Account Center
CPRS	Computerized Patient Record System
EHR	Electronic Health Record
ESD	Enterprise Service Desk
FBCS	Fee Basis Claim System
FPO	Field Program Office
GAL	Global Address List
GUI	Graphical User Interface
IAM	Identify and Access Management
NPI	National Provider Identifier
OCC	Office of Community Care
OIT	Office of Information and Technology
PHI	Protected Health Information
PII	Personally Identifiable Information
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
VDL	VA Document Library
VHA	Veterans Health Administration
VM	Virtual Machine
VPN	Virtual Private Network
VRAM	Vista Remote Access Management

<b>Term</b>	<b>Definition</b>
WAM	WebVRAM Administration Module
WebVRAM	Web VistA Remote Access Management
WUT	WebVRAM User Table