

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



March 2024

Department of Veterans Affairs

Office of Information and Technology

Table 1: Abbreviated Revision History

Date	Document Revision	Description	Author
3/2/2024	10.0	Release 10.0 – Updated month/date in cover page and footers. Updated Section 1.1 for PIV login page link. Updated Section 7.1.3 Table 6: Profile Issues and VistA Data Anomalies Error messages. Updated Bootstrap references to version 5.3.2	WebVRAM Project Team
12/11/2023	9.0	Release 9.0 – Updated month/date in cover page and footers. Updated section 3.1 and section 4.1 to indicate only the WebVRAM Administrator role can update Director information. Updated Section 5.6.3 with a note regarding multiple BU and extended timeout. Added section 5.6.4 Extended Timeout details. Updated Section 7.1 with new support group name. Added text in section 7.1.3 to address AV Code expiration and PIV information. Updated Section 6 and Appendix B.	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 Graphical User Interface (GUI) or user-facing components. Updated acronyms, Section 508 formatting, corrected VistA file names and standard formatting.	WebVRAM Project Team
8/23/2023	8.0	Release 8.0: <ul style="list-style-type: none"> Updated Month/date in cover page and footers Section 5.5: Updated URL to Access Request page	WebVRAM Project Team
3/17/2023	7.0	Section 7.3.2: <ul style="list-style-type: none"> Updated description of how WebVRAM displays an active duplicate account issue Updated screenshot on Figure 38 Section 7.3.3 <ul style="list-style-type: none"> Update screenshot on figure 39 Section 7.3.3.1 Updates screenshot on figure 40	WebVRAM Project Team

Date	Document Revision	Description	Author
3/3/2023	7.0	Updated content of Section 6.1: Access Review Audit Updated Footer date Updated Cover page date	WebVRAM Project Team
2/7/2023	7.0	Added Section 2.7: System Maintenance	WebVRAM Project Team
12/20/2022	6.2	Release 6.2 <ul style="list-style-type: none"> Updated date info on cover page Updated date on footers area Updated screenshot to: <ul style="list-style-type: none"> Figure 3 Figure 5 Figure 7 Figure 24 	WebVRAM Project Team
10/31/2022	5.0.3	Release 5.0.3 Hotfix Added new section: 7.3.7. VistA Sites with Sub-Divisions sites	WebVRAM Project Team
10/11/2022	6.0	Section 4.3: <ul style="list-style-type: none"> Updated screenshot to Figure 3: WebVRAM Main Screen Section 5.2: <ul style="list-style-type: none"> Added Figure 17a: Warning Message – The user's Active Directory data is incomplete or missing Description of error message when Active Directory data missing 	WebVRAM Project Team
9/23/2022	6.0	Update to Section 7.1.2 and 7.3.6 , remove references to NTL SUP ADMIN group and replace with WebVRAM group.	WebVRAM Project Team
9/22/2022	6.0	Update to Section 7.1.2 : Submitting Help Desk Tickets for User Issues. Removed reference to contact OCCHID.	WebVRAM Project Team
9/8/2022	5.0.2	Update to Section 4.2. Added important info related to User Class: CONNECTOR PROXY	WebVRAM Project Team

Date	Document Revision	Description	Author
9/5/2022	5.0.2	Updated instructions on Section 2.3. Updated Figure 2 in Section 4.3 . Added figure 45 - Synchronization Successful Screen. Section 7.3.5: Added figure 45 - Synchronization Successful Screen	WebVRAM Project Team
8/2/2022	5.0	Added section on Access Review Audit, Section 6 with links to ESO SOPs. Also added Appendix C.	WebVRAM Team, VA OIT, DevSecOps, SPM
7/22/2022	5.0	Updated Figure 2 (screenshot) in Section 4.3	WebVRAM Team, VA OIT, DevSecOps, SPM
7/19/2022	5.0	Format changes to Section 2.2.2 as per Jira User Story WEB-1628	WebVRAM Team, VA OIT, DevSecOps, SPM
7/8/2022	5.0	Removed all references to Internet Explorer browser as it is no longer supported.	WebVRAM Team, VA OIT, DevSecOps, SPM
6/27/2022	5.0	Section 4.3 - Updated instructions to reflect PIV Login workflow. Updated screenshots for Figures 1 and 2. Section 5.2 – Updated instructions to reflect new error message in the Add User screen if the user's WEBG WEBVRAM GUI menu option is missing from their Home VistA site. Added screenshot of error message.	WebVRAM Team, VA OIT, DevSecOps, SPM

Date	Document Revision	Description	Author
5/12/2022	4.1	<p>Updated contents verbiage and screenshots to Section 7.3.3</p> <ul style="list-style-type: none"> • Removed references to the generic "Caution!" message • Replaced Figure 40: Edit Site Screen – IEN Mismatch • Replaced Figure 41: Edit Site Screen – SSN Conflict • Replaced Figure 42: Edit Site Screen – Same Access Code • Replaced Figure 43: Edit Site Screen – NPI Already Assigned 	WebVRAM Team, VA OIT, DevSecOps, SPM
4/12/2022	4.1	<p>Updated screenshots for:</p> <ul style="list-style-type: none"> • Figure 6: User Profile Screen • Figure 31: User Profile Screen – View Logs Button • Figure 32: User Log Listing 	WebVRAM Team, VA OIT, DevSecOps, SPM
4/8/2022	4.1	<p>Added a new menu option to Section 5.9 (Standard Configuration for VistA Imaging Functionality) needed at some sites for VistA Imaging to launch from CPRS. Also added a new warning to Section 5.10 (View/Edit User's Home VistA System and Active Directory Name).</p>	WebVRAM Team, VA OIT, DevSecOps, SPM
3/30/2022	4.1	<p>Added CPRS Photo DLL "Library not registered" error and resolution to Table 6</p>	WebVRAM Team, VA OIT, DevSecOps, SPM
3/7/2022	4.1	<p>Added Reflection "untrusted file location" error resolution to Table 6 (User Profile Issues and VistA Data Anomalies)</p>	WebVRAM Team, VA OIT, DevSecOps, SPM
2/24/2022	4.1	<p>Added Section 1 (Quick Start Guide)</p>	WebVRAM Team, VA OIT,

Date	Document Revision	Description	Author
			DevSecOps, SPM
2/15/2022	4.1	Updated Section 3.1 (Business Unit Setup) and Section 3.2 (Information Needed to Add Users to WebVRAM) with current information.	WebVRAM Team, VA OIT, DevSecOps, SPM
12/9/2021	4.0	<p>Updated for WebVRAM Release 4.0, (associated with informational VistA patch WEBG*3*5):</p> <ul style="list-style-type: none"> Added information to Section 2.5.1 (Assumptions). Updated verbiage in Section 2.5.2 (Coordination). Updated verbiage in Sections 3 (Software Summary) and 3.1 (WebVRAM Roles). Updated verbiage in Sections 4.1 (Business Unit Setup) and 4.2 (Information Needed to Add Users to). Updated Section 4.3 (Logging into the WAM) to add Microsoft Edge as a supported internet browser. Replaced Figure 2 (WebVRAM Login Screen). Rewrote Section 5.3 (Add Security Key Not Present in User's Home VistA). Edited steps 2, 3, and 5 and added step 7 in Section 5.5 (Existing User with Same Name in Home VistA and Other VistA Data Anomalies). Replaced Figure 26 (User Disabled Status – User Search Screen). Revised Sections 5.6.1 (To Order Meds and Write Notes in CPRS) and 5.6.2 (To Use CPRS Features as a Non-Physician Provider). Added new Section 5.7.1 (Site-specific CPRS Clinical Teams – Consults/Menus Access). Added White City, Sioux Falls, and Houston to Table 4 (Site-specific VistA Profile Values). 	WebVRAM Team, VA Office of Information and Technology (OIT)

Date	Document Revision	Description	Author
		<ul style="list-style-type: none"> Added information for Mental Health providers to Section 5.7.4 (To Access Provider CPRS Features at Biloxi). Added new Section 5.7.8 (To Author CPRS Notes at Houston). Added new Section 5.7.12 (To Access CPRS Oncology Notes at Sioux Falls). Added new Section 5.7.13 (To Access CPRS Notes at White City). Updated first and second paragraph of Section 5.7.14 (To Access Consults at New Jersey). Corrected step 3 of Section 5.8 (Access CPRS at Remote Sites Using CPRS Desktop Launcher); <i>a user MUST synchronize to a remote site using WebVRAM at least every 29 days to keep their VistA profile active at that site.</i> Updated steps 2, 3, and 4 in Section 7.1.1 (Initial Checklist to Begin Troubleshooting User Access Issues). Added new Section 7.1.2 (Submitting Help Desk Tickets for User Issues). Added new Issue #1 to Table 6 (User Profile Issues and VistA Data Anomalies) and renumbered all other issues. Edited Issue #6 ("User logs into WebVRAM successfully. Connections to remote sites through Reflection or CPRS end in 'FAILED' message") in Table 6 (User Profile Issues and VistA Data Anomalies). Added new Issue #18 to Table 6 (User Profile Issues and VistA Data Anomalies). Added WEBG to Appendix 0 (Appendix A – Acronyms and Abbreviations). 	

Table of Contents

1 Quick Start Guide.....	13
1.1 Login To WebVRAM	13
1.2 Gather New User Data	14
1.3 New Business Unit Process.....	14
1.4 Add New Users to the WAM	15
1.5 When a User Changes Locations – New Home VistA.....	15
2 Introduction.....	15
2.1 Purpose	16
2.2 Document Orientation.....	16
2.2.1 Organization of the Manual	16
2.2.2 Documentation Conventions.....	16
2.2.3 References and Resources	17
2.3 Login To WebVRAM	17
2.4 New Business Unit Process.....	19
2.5 Successful Upload Options	19
2.5.1 Assumptions.....	20
2.5.2 Coordination	22
2.5.3 VA OIT Standard Disclaimers	22
2.5.4 Software Disclaimer.....	22
2.5.5 Documentation Disclaimer	22
2.6 Enterprise Service Desk and Organizational Contacts	22
2.7 System Maintenance	23
3 Software Summary	23
3.1 WebVRAM Roles.....	23
4 Getting Started.....	24
4.1 Business Unit Setup	24
4.2 Information Needed to Add Users to WebVRAM	25
4.3 Logging into the WAM	26
5 Using the Application	28
5.1 View and Edit User	28
5.2 Add New User	32
5.3 Add Security Key Not Present in User’s Home VistA.....	45
5.4 Quick Delete of User Profile Entries.....	45

5.5	Existing User with Same Name in Home VistA and Other VistA Data Anomalies	46
5.6	Standard Configurations for CPRS Functionality	54
5.6.1	To Order Meds and Write Notes in CPRS	54
5.6.2	To Use CPRS Features as a Non-Physician Provider.....	55
5.6.3	Extended Timeout.....	55
5.7	Custom Profile Values or Site-specific Clinical Teams Required to Access Features at Certain Sites.....	57
5.7.1	Site-specific CPRS Clinical Teams – Consults/Menus Access	57
5.7.2	Summary of Site-specific VistA Profile Values.....	57
5.7.3	All VAMCs: Secondary Menu Required for Mental Health Clinical Reminders	61
5.7.4	To Access Provider CPRS Features at Biloxi.....	62
5.7.5	To Access Tele-ICU Notes at Chillicothe, OH.....	62
5.7.6	To Access Tele-ICU Notes at Cleveland, Ohio	62
5.7.7	To Access Progress Notes at Detroit.....	62
5.7.8	To Author CPRS Notes at Houston.....	62
5.7.9	Order Meds and Access Progress Notes at Northern California and San Francisco.....	63
5.7.10	To Sign CPRS Notes at Puget Sound	63
5.7.11	To Access VistA Scheduling at Puget Sound.....	63
5.7.12	To Access CPRS Oncology Notes at Sioux Falls	63
5.7.13	To Access CPRS Notes at White City.....	63
5.7.14	To Access Consults at New Jersey.....	63
5.8	Access CPRS at Remote Sites Using CPRS Desktop Launcher	66
5.9	Standard Configuration for VistA Imaging Functionality.....	67
5.10	View/Edit User’s Home VistA System and Active Directory Name.....	67
5.11	View User’s Log	70
5.11.1	User Log New VA EHR Messages	72
5.12	Disable User Account.....	74
5.13	Exit System	75
6	Access Review Audit.....	75
7	Troubleshooting.....	75
7.1	Special Instructions for Error Correction.....	75
7.1.1	Initial Checklist to Begin Troubleshooting User Access Issues.....	75
7.1.2	Submitting Help Desk Tickets for User Issues	77

7.1.3	Common Problems and Resolutions with User Profiles and VistA Data Anomalies.....	78
7.2	Look Up a User's Home VistA Profile Information	87
7.3	Duplicate Account Reconciliation.....	88
7.3.1	Detecting VistA User Account Conflicts – Block Site Access	88
7.3.2	Detecting VistA User Account Conflicts – User Profile VistA Sites.....	89
7.3.3	Viewing Duplicate Account Issues – Edit Site	89
7.3.4	Duplicate Accounts – IEN Mismatch	89
7.3.5	Resolving the IEN Mismatch	90
7.3.6	Duplicate Accounts – SSN Conflict	90
7.3.7	Resolving the SSN Conflict	91
7.3.8	Duplicate Accounts – Same Access Code.....	91
7.3.9	Resolving the Same Access Code Issue	92
7.3.10	Duplicate Accounts – NPI Number Already Assigned	93
7.3.11	Resolving the NPI Number Already Assigned Issue	94
7.3.12	Duplicate Account Issue – Detailed Logs – Error Message.....	94
7.3.13	Synchronization Successful Screen.....	94
7.3.14	Resolving Duplicate Account Issues.....	95
7.3.15	VistA Sites with Sub-Divisions sites	99
Appendix A – Acronyms and Abbreviations		100
Appendix B – Access Review Audit Memo.....		102

List of Figures

Figure 1: WebVRAM Terms and Conditions for Usage Screen	26
Figure 2: WebVRAM Login Screen	26
Figure 3: WebVRAM Main Screen	27
Figure 4: WebVRAM Administration Module Main Page	27
Figure 5: Users Screen	28
Figure 6: User Profile Screen	30
Figure 7: VistA Sites Screen.....	30
Figure 8: Administration Module Users Link	31
Figure 9: Add or Remove Secondary Menu Options Screen.....	32
Figure 10: Administration Module Business Units Links	33
Figure 11: Business Unit Profile Screen	33
Figure 12: Add User Screen.....	34
Figure 13: User Lookup on Add User Screen.....	35
Figure 14: User Not Found on Home VistA Error	35
Figure 15: WebVRAM Administration Module	36
Figure 16: Add User Screen – Success Message.....	37
Figure 17: Banner on Disabled User Profile – Business Unit Must Be Added	39
Figure 18: Warning Message – Business Unit Must Be Added	39
Figure 19: Warning Message –AD data is incomplete or missing.....	40
Figure 20: VistA Profile Edit Option.....	44
Figure 21: VistA Profile Data Entry Fields	44
Figure 22: VistA Profile Service Section Drop-down List	45
Figure 23: Edit User Quick Delete Option.....	46
Figure 24: Existing User with Same Name Error Message	47
Figure 25: WebVRAM Access Request Screen.....	48
Figure 26: User Disabled Status – User Search Screen.....	49
Figure 27: User Profile Screen with Enable User Button	49
Figure 28: User Profile Screen – Edit User Button.....	68
Figure 29: Edit User Screen	69
Figure 30: Edit User Screen – Home VistA Field Cleared	69
Figure 31: Edit User Screen – Home VistA “Auto-Fill” Feature.....	70
Figure 32: Edit User Screen – New Home VistA System Selected	70
Figure 33: User Profile Screen – View Logs Button.....	70
Figure 34: User Log Listing	71
Figure 35: Detailed Logs	72
Figure 36: New VA EHR Messages in User Log	73
Figure 37: User Profile Screen – Disable User Button	74
Figure 38: Unauthorized Access Error Message	76

Figure 39: VistA Sites Screen with Edit Site Button.....	88
Figure 40: User Profile VistA Sites Section with Duplicate Account Issues.....	89
Figure 41: User Profile VistA Sites Section with Pencil Icon to Edit Site.....	89
Figure 42: Edit Site Screen – IEN Mismatch	90
Figure 43: Edit Site Screen – SSN Conflict	91
Figure 44: Edit Site Screen – Same Access Code	92
Figure 45: Edit Site Screen – NPI Already Assigned.....	93
Figure 46: Detailed Logs – Failed Synchronization Due to Duplicate Account.....	94

List of Tables

Table 1: Abbreviated Revision History.....	1
Table 2: Documentation Symbols and Descriptions.....	17
Table 3: Enterprise Service Desk Support Information	22
Table 4: Site-specific VistA Profile Values.....	57
Table 5: Houston Custom User Class Values	62
Table 6: User Profile Issues and VistA Data Anomalies.....	78
Table 7: Acronyms and Abbreviations.....	100

1 Quick Start Guide

Congratulations and welcome to the WebVRAM Administration Module User Guide! As a Business Unit Administrator (BU Admin), your primary responsibilities are to add authorized user profiles to the WebVRAM database and to assist those users with their initial first connections using WebVRAM to the remote Veteran's Health Information Systems and Technology Architecture (Vista) sites they are authorized to access. The authorization for users to be added to the WebVRAM database comes from your Business Unit Director, who will also authorize you to act as a BU Admin for that Business Unit. See [Section 4.1](#), Business Unit Setup for more details surrounding this process. This Quick Start Guide provides the basic steps to follow to setup a new user in the WebVRAM User Table (database or WUT). More specific instructions are found in Sections [3.2](#) and [4.2](#).

1.1 Login To WebVRAM

1. From Microsoft Edge browser, navigate to the WebVRAM home page at this link: WebVRAM Home Page You will see the **Terms and Conditions** page.
2. *BEFORE* you login, save the **Terms and Conditions** page as a favorite if you wish to quickly navigate to this page later. *DO NOT login and save the WebVRAM home page as a favorite link because navigating to that link will open the home page, but you will not be officially logged in and the application features will not work.*
3. Click Accept the Terms and Conditions button, then at the Login page, confirm that your Home Vista site is listed correctly, then enter your Home Vista Access and Verify codes to complete login to the application. (A link to the PIV login page is available for PIV card login.) *If the correct home Vista site is not listed on your login page, log an Office of Community Care Help Desk (OCCHD) (Telehealth business units) or Help Desk (non-Telehealth business units) ticket to ensure that your WebVRAM profile was setup based on your actual Home Vista user account. Enterprise Service Desk (ESD) tickets should be assigned to the ESD Application Provisioning Group.*
4. Your Home Page should list the Vista sites serviced by your Business Unit, which you should be able to access using WebVRAM. It is essential that you have access to all sites except your Home Vista site so you can trouble shoot user connection issues at those sites by viewing user profiles to triage reasons for failed connections or lack of access to Vista applications and features. If no Vista sites are listed on your home page, you will be able to edit your own user profile and add those sites to your profile. **Your Home Vista site will not be listed on your home page because you should never use WebVRAM to connect to your**

Home VistA system but should instead login directly to your Home VistA system. Specific instructions are provided later in the user guide, but the basic steps are listed here to add VistA sites to your WebVRAM profile.

- a. Click **Manage** on the Toolbar.
- b. Click the **Users** link on the WebVRAM Administration Module page.
- c. Search for your profile by entering your Veteran's Affairs (VA) Network Identification (ID) (Global Address List (GAL) ID; vhaissl...) or your last name in the search field.
- d. When you see your name in the list, click on the **View User** button on the right side of your information.
- e. In the VistA Sites section of your profile, click on the '+' sign to add VistA sites to your profile. Once added, click on the **Home** icon to confirm those sites are listed on your home page.

1.2 Gather New User Data

For each new user you add for your Business Unit to the WebVRAM Administration Module (WAM), you will need to collect the following data:

- The user's Windows Active Directory Username from the Global Address List (GAL) (e.g., vhaissl....)
- The Veteran's Integrated Service Network (VISN) the user resides in.
- The user's Home VistA system name within that VISN (e.g., Togus, ME; Connecticut Health Care System (HCS); etc.) and current VistA Access and Verify codes.
- The 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.

1.3 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 in a VA SharePoint site accessible to all VA staff on the VA network. Please contact the WebVRAM Team for this document. 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.

1.4 Add New Users to the WAM

1. Click on the **Manage** icon on the Toolbar.
2. Click on your Business Unit listed under the **Business Units** heading on the *WebVRAM Administration Module* page.
3. Click on the **Add User** button.
4. Enter the user's GAL Windows (Active Directory) username (vhaisl...) in the username field and click **Lookup User**.
5. Enter the user's VISN and Home Vista System and click the **Set Home Vista** button.
6. If the user's Home Vista account data uploads correctly into WebVRAM, you will see a *Success!* message at the bottom of the page.
7. Two options will be available after a successful upload: **Add Vista Sites** or **Add another user**. If you wish to update the user's profile you just added, click the **Add Vista Sites** button. If you wish to continue adding other users then update their profiles later, click the **Add another user button**.
8. *If Vista does not upload the user's profile data correctly, you will see no change in the screen or you may get an error message regarding duplicate accounts at the Home Vista site, or a "User Not Found" error. For these issues, refer to Section [5.2](#).*
9. For detailed instructions regarding specific user profile updates, refer to Section [5](#) of the user guide. To view a user's Home Vista profile, or to view remote profiles at sites the user connects to, refer to Section 7.2.

1.5 When a User Changes Locations – New Home Vista

When a user changes residence or begins working out of a new Vista site, the OLD Home Vista must be manually removed from the user's Vista Site list in their user profile. See Section [5.1](#) for details regarding this action. The new Home Vista location is then added to the user's profile. See Section [5.10](#).

2 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.

2.1 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, Information Technology (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.

2.2 Document Orientation

The document orientation is shown below in Sections 2.2.1 through 2.2.3.

2.2.1 Organization of the Manual

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



1. [Quick Start Guide](#)
2. [Introduction](#)
3. [Software Summary](#)
4. [Getting Started](#)
5. [Using the Application](#)
6. [Audits](#)
7. [Troubleshooting](#)

2.2.2 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 2: Documentation Symbols and Descriptions

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

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

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

2.2.3 References and Resources

- WebVRAM System Design Document
- WebVRAM Requirement Elaboration Document
- WebVRAM User Stories and Backlog – JIRA WebVRAM Project

2.3 Login To WebVRAM

1. From Microsoft Edge browser, navigate to the WebVRAM home page. You will see the Terms and Conditions page.
2. BEFORE you login, save the Terms and Conditions page as a favorite if you wish to quickly navigate to this page later. DO NOT login and save the WebVRAM home page as a favorite link because navigating to that link will open the home page, but you will not be officially logged in and the application features will not work.
3. Click Accept the Terms and Conditions button, then at the Login page, confirm that your Home VistA site is listed correctly, then enter your Home VistA Access and Verify codes to complete login to the application. If the correct home VistA site is not listed on your login page, log an OCCHD (Telehealth business units) or Help Desk (non-Telehealth business units) ticket to ensure that your WebVRAM profile was setup based on your actual Home VistA user account. ESD tickets should be assigned to the ESD Application Provisioning Group.

4. Your Home Page should list the VistA sites serviced by your Business Unit, which you should be able to access using WebVRAM. It is essential that you have access to all sites **except your Home VistA site** so you can trouble shoot user connection issues at those sites by viewing user profiles to triage reasons for failed connections or lack of access to VistA applications and features.



NOTE: If no VistA sites are listed on your home page, you will be able to edit your own user profile and add those sites to your profile.

Your Home VistA site will not be listed on your home page because you should never use WebVRAM to connect to your Home VistA system but should instead login directly to your Home VistA system. Specific instructions are provided later in the user guide, but the basic steps are listed here to add VistA sites to your WebVRAM profile.

5. Click Manage on the Toolbar.
6. Click the Users link on the WebVRAM Administration Module page.
7. Search for your profile by entering your VA Network ID (GAL ID; vhaisl...) or your last name in the search field.
8. When you see your name in the list, click on the View User button on the right side of your information.
9. In the VistA Sites section of your profile, click on the '+' sign to add VistA sites to your profile. Once added, click on the Home icon to confirm those sites are listed on your home page.
10. Gather New User Data
11. For each new user you add for your Business Unit to the WebVRAM Administration Module (WAM), you will need to collect the following data:
12. The user's Windows Active Directory Username from the Global Address List (GAL) (e.g., vhaisl....)
13. The VISN the user resides in.
14. The user's Home VistA system name within that VISN (e.g., Togus, ME; Connecticut HCS; etc.) and current VistA Access and Verify codes.
 - 14.1 The VistA systems the user is authorized to access by their business line management.
 - 14.2 A list of all current VistA accounts for the user, outside their Home VistA system, where they have active login credentials.

2.4 New Business Unit Process

1. 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.
2. 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 in this document 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. Add New Users to the WAM
4. Click on the Manage icon on the Toolbar.
5. Click on your Business Unit listed under the Business Units heading on the WebVRAM Administration Module page.
6. Click on the Add User button.
7. Enter the user's GAL Windows (Active Directory) username (vhaisl...) in the username field and click Lookup User.
8. Enter the user's VISN and Home Vista System and click the Set Home Vista button.
9. If the user's Home Vista account data uploads correctly into WebVRAM, you will see a Success! message at the bottom of the page.

2.5 Successful Upload Options

Two options will be available after a successful upload: Add Vista Sites or Add another user. If you wish to update the user's profile you just added, click the Add Vista Sites button. If you wish to continue adding other users then update their profiles later, click the Add another user button.

If Vista does not upload the user's profile data correctly, you will see no change in the screen or you may get an error message regarding duplicate accounts at the Home Vista site, or a "User Not Found" error. For these issues, refer to Section 5.2.

For detailed instructions regarding specific user profile updates, refer to Section 5 of the user guide. To view a user's Home Vista profile, or to view remote profiles at sites the user connects to, refer to Section 7.2.

- When a User Changes Locations – New Home Vista

- When a user changes residence or begins working out of a new VistA site, the OLD Home VistA must be manually removed from the user's VistA Site list in their user profile. See Section 5.1 for details regarding this action. The new Home VistA location is then added to the user's profile. See Section 5.10.

2.5.1 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 WebVRAM User Table (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. This menu does NOT need to be added to any user's WebVRAM profile. Authorized users can work with their local Automated Data Processing Application Coordinator (ADPAC) or submit an Electronic Permission Access System (ePAS) or National Automated Response System (NARS) request to have that menu option added to their Home VistA user profile.



IMPORTANT: The WEBG WEBVRAM GUI Secondary Menu Option is required in the Home VistA user profile 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 March 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 March 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.

- 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.
- The primary menu option in a user's Home VistA user profile may be a "custom" value created by local IT staff for ease of access at that site. These custom values are only "names," but they are built using standard VA menu options. Since these primary menus have a custom name, they are generally not recognized as valid by other VistA systems at other sites. For a WebVRAM user to successfully connect through WebVRAM to a remote VistA system outside their Home VistA system, the primary menu from their Home VistA profile should NOT be in their WebVRAM user profile.
- This custom primary menu will normally upload from the user's Home VistA profile automatically when a new user is added. If that Home VistA custom primary menu is left "as is" in the uploaded WebVRAM profile, their connection attempts to remote VistA sites they are authorized to access will fail. When adding a new user, **a standard VistA menu name** (not a custom menu name) **must be added to the user's WebVRAM user profile to replace any custom primary menus** that might have been uploaded from their Home VistA profile, or if the upload from VistA did not succeed, a standard menu must be added to their profile manually by their Business Unit Administrator.

There are only three values that are accepted by remote locations across the enterprise:

- **XUSERTOOLS**
- **PX PCE CLINICIAN MENU**
- **NURSCL-MENU**



IMPORTANT: 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. The user's log will have a "Menu tree rebuild for user failed" message at the end of the log for that connection, as discussed in Section [5.11](#) (View User's Log). One of the three primary menus listed above **MUST** be added the user's VistA Profile section of the WebVRAM User Profile; see Section [5.2](#), step 6 ([Primary Menu](#)).

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

2.5.2 Coordination

WebVRAM Administration Module users must obtain approval from their respective WebVRAM application business unit director/manager to access and use the WebVRAM Administration Module to enter application user profile data into the WUT. An email documenting approval from the director/manager should be archived and will be needed when the Administration Module user is added to WebVRAM as a Business Unit Administrator.

2.5.3 VA OIT Standard Disclaimers

2.5.4 Software Disclaimer

This software was developed at the Department of Veterans Affairs (VA) by employees of the Federal Government in the course of their official duties. Pursuant to title 17 Section 105 of the United States Code, this software is not subject to copyright protection and is in the public domain. VA assumes no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic. We would appreciate acknowledgement if the software is used. This software can be redistributed or modified freely if any derivative works bear some notice that they are derived from it, and any modified versions bear some notice that they have been modified.

2.5.5 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.

2.6 Enterprise Service Desk and Organizational Contacts

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

Table 3: Enterprise Service Desk Support Information

Name	Role	Org	Contact Info
OIT Enterprise Service Desk	Tier 1 Support	OIT	ESD Service Desk via YourIT.

Name	Role	Org	Contact Info
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.

2.7 System Maintenance

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

3 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 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 or CPRS sessions, with separate user profile login to each remote VistA/CPRS 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.

3.1 WebVRAM Roles

The WebVRAM Administration Module enables the management of users, profiles, and assignment of users to business units. 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 the New VA EHR 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 web 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 as managers to a business unit. The WebVRAM Administrator can create, view, and edit users and business units and can view log files. Only the WebVRAM Administrator can add, remove, or update Business Unit Director information. WebVRAM Administrator is the highest access level.

4 Getting Started

4.1 Business Unit Setup

To access the WAM, all users follow these initial process steps:

1. The Business Unit line management director (or equivalent) determines and implements their process for approving users to access WebVRAM and determines which VistA remote sites they can access. The VA business unit director will receive approval to set up a WebVRAM business unit and will work with the *ESD Application Provisioning Group* to add the business unit to the WebVRAM database. This process is described in the *Process to Add a New Business Unit to WebVRAM* document found in SharePoint. A form with approval of Business Unit Administrators or an email approval from the director will need to be maintained and attached to a Help Desk request to establish the Business Unit Administrators as described in Step 2.
2. The business unit approves and designates two or more Business Unit Administrators authorized to add new users to the WebVRAM User Table (WUT). The Business Unit Administrator will then need to submit a Help Desk Ticket assigned to the *ESD Application Provisioning Group* with a request to be added to the WebVRAM database as an Administrator for the specific Business Unit and attach the Business Unit director approval described in Step 1.
3. A WebVRAM Administrator from the *ESD Application Provisioning Group* adds the Business Unit Administrator(s) to the WUT database and specifies which Business Unit they will manage.
4. The WebVRAM Administrator adds or updates Business Unit Director name and email information if necessary for the Business Unit. Only a WebVRAM Administrator may add, change, or remove Business Unit Director information.

4.2 Information Needed to Add Users to WebVRAM

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

- The user's Windows Active Directory Username from the Global Address List (GAL) (e.g., vhaisl....)
- The VISN the user resides in.
- The user's Home VistA system name within that VISN (e.g., Togus, ME; Connecticut HCS; etc.) and current VistA Access and Verify codes.
- The 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:



CAUTION: These remote sites where a user has an existing VistA account must NOT be added to the user's WebVRAM profile when it is created. See Section [5.2 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 Person Class
 - User's User Class (if available)
 - User's VistA CPRS Tab (only one should be added even if they have two in their VistA profile. If they have both Clinical Orders Repository (COR) and Report (RPT), do NOT add the RPT tab to the user's WebVRAM profile.



IMPORTANT: User Class of CONNECTOR PROXY needs to be set in the WebVRAM user profile for all service accounts and bot accounts. Doing so will ensure that the service/bot account is excluded from Federal Information Security Management Act Office of Inspector General (FISMA OIG) report.

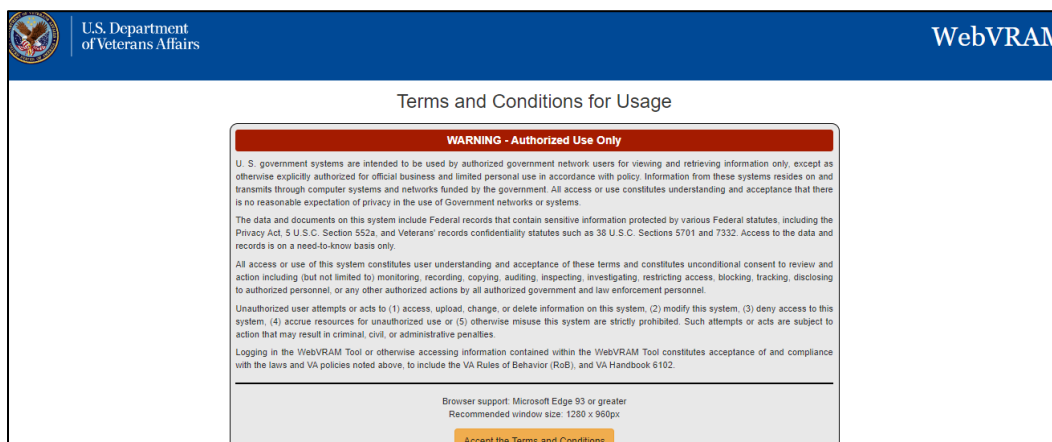
4.3 Logging into the WAM

1. From Microsoft Edge browser, navigate to the WebVRAM home page.
2. The Terms and Conditions web page will be the first page displayed.

 **NOTE:** If a user wishes to add this link to your favorites, do so now and NOT after logging into the application when the user's home page is displayed. Using the "home page" favorite link later on will result in the WebVRAM features not working properly.

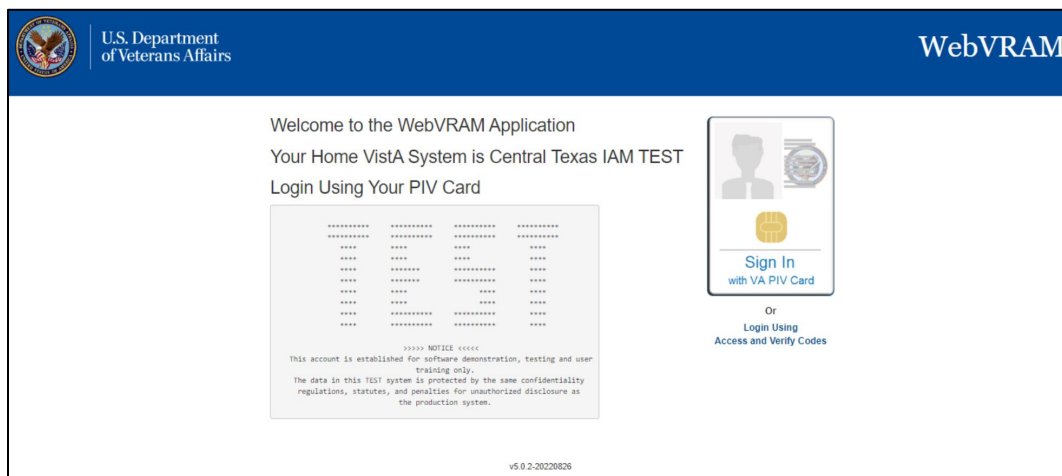
Read through the VA application use terms and conditions and click **Accept the Terms and Conditions** button as shown below.

Figure 1: WebVRAM Terms and Conditions for Usage Screen



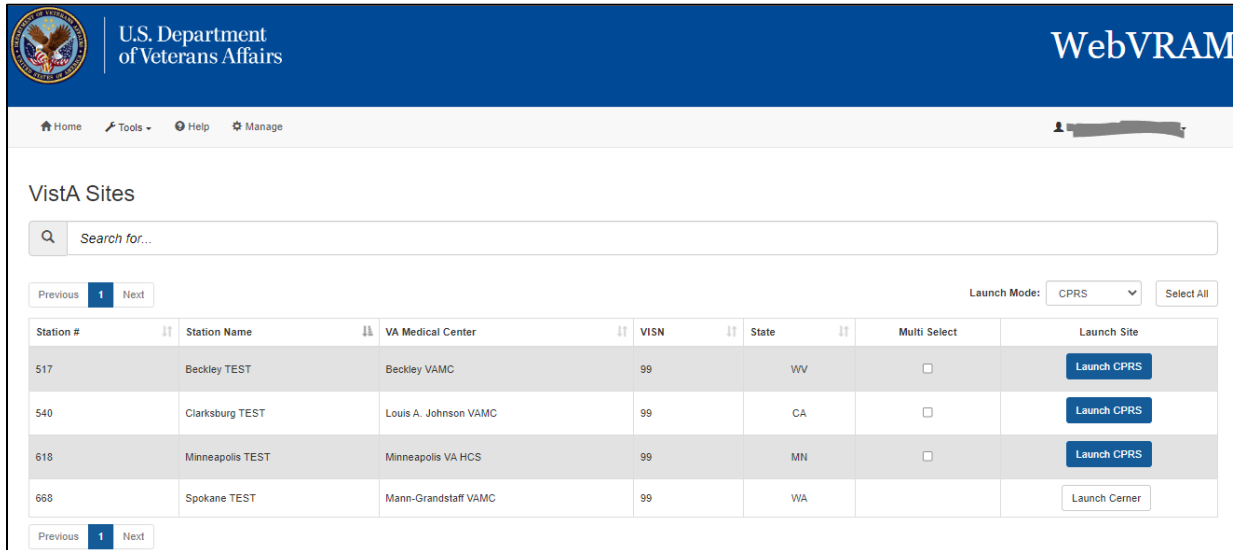
3. The next web page displayed is the WebVRAM Login page. Click on the **"Sign In with a VA Personal Identification and Verification PIV Card"** button.

Figure 2: WebVRAM Login Screen



4. The **ActivClient** screen comes up, prompting the user to enter their PIV's Personal Identification Number (PIN). Enter PIN and click **OK**
5. 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

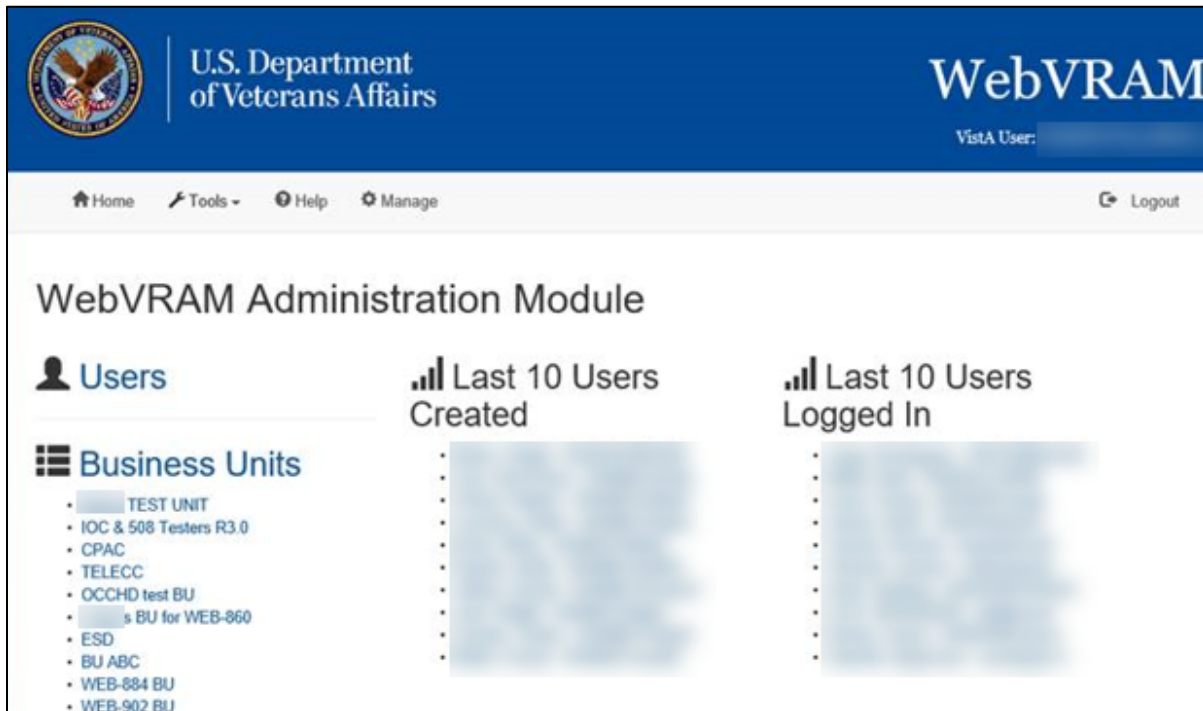


The screenshot shows the WebVRAM Main Screen. At the top is the U.S. Department of Veterans Affairs logo and the text "U.S. Department of Veterans Affairs" and "WebVRAM". Below the header is a navigation bar with "Home", "Tools", "Help", and "Manage". A user profile icon is on the right. The main content area is titled "VistA Sites" and contains a search bar with the placeholder "Search for...". Below the search bar are "Previous", "1", and "Next" buttons. To the right of the table is a "Launch Mode" dropdown set to "CPRS" and a "Select All" button. The table has columns: Station #, Station Name, VA Medical Center, VISN, State, Multi Select, and Launch Site. It lists four sites: Beckley TEST, Clarksburg TEST, Minneapolis TEST, and Spokane TEST. Each site has a "Launch CPRS" button. At the bottom of the table are "Previous", "1", and "Next" buttons.

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

6. The WebVRAM Administration Module Main Page is displayed.

Figure 4: WebVRAM Administration Module Main Page



The screenshot shows the WebVRAM Administration Module Main Page. At the top is the U.S. Department of Veterans Affairs logo and the text "U.S. Department of Veterans Affairs" and "WebVRAM". Below the header is a navigation bar with "Home", "Tools", "Help", and "Manage". A user profile icon is on the right. The main content area is titled "WebVRAM Administration Module". It features a "Users" section with a "Business Units" list: TEST UNIT, IOC & 508 Testers R3.0, CPAC, TELECC, OCCHD test BU, s BU for WEB-860, ESD, BU ABC, WEB-884 BU, and WEB-902 BU. To the right of the list are two charts: "Last 10 Users Created" and "Last 10 Users Logged In". At the bottom right is a "Logout" button.

5 Using the Application

5.1 View and 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	Business Unit	View User
68	[REDACTED]	[REDACTED]	[REDACTED]	Disabled	ESD	View User
110	[REDACTED]	[REDACTED]	[REDACTED]	Enabled	CPAC	View User
110	[REDACTED]	[REDACTED]	[REDACTED]	Enabled	VA TELECC - WEST	View User
110	[REDACTED]	[REDACTED]	[REDACTED]	Enabled	IOC & 508 Testers	View User
234	[REDACTED]	[REDACTED]	[REDACTED]	Enabled	ESD	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 or 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

WebVRAM Administration Module

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

Home Vista Site: Beckley TEST

Vista Sites

☐ Minneapolis TEST

☐ Cincinnati TEST

☐ Togus TEST

☐ Clarksburg TEST

☐ Spokane TEST

Secondary Menu Options

☐ DG PATIENT INQUIRY

☐ OR CPRS GUI CHART

☐ SROMENU

☐ WEBG WEBVRAM GUI

☐ YS BROKER1

☐ YSUSER

Security Keys

☐ WEBG AV PUSH

☐ MAGDISP ADMIN

☐ MAGDISP CLIN

☐ ORES

☐ PROVIDER

☐ PSB CPRS MED BUTTON

☐ SDMOB

☐ SDOB

☐ SCENI ENCOUNTER EDIT

CPRS Tabs

☐ COR

Person Classes

☐ Allopathic & Osteopathic Physicians, Psychiatry & Neurology

User Classes

☐ PHYSICIAN

Vista Profile

- Title: IT SPECIALIST
- Service/Section: REMOTE
- Screen Editor: SCREEN EDITOR - VA FILEMAN
- Allowed to use spooler? No
- Primary Menu: NURSCL-MENU

WebVRAM Roles

☐ WebVRAM User

☐ Business Unit Administrator

WebVRAM Business Units

☐ ESD

☐ BU ABC WEB-1107

☐ WEB-884 BU

- 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

WebVRAM

Home Tools Help Manage

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

Home Vista Site: Togus TEST (Maine VA HCS - Togus)

Vista Sites

[Add all sites](#) [Remove all sites](#)

Station #	Station Name	VA Medical Center	VISN	State	Test Site?	Action
517	Beckley TEST	Beckley VAMC	99	WV	No	Edit Site Remove Site Add Site
523	Boston IAM Test	Boston VA HCS	1	MA	Yes	Add Site
674	Central Texas IAM TEST	Central Texas Veterans HCS	99	TX	Yes	Add Site

- Add or 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**.


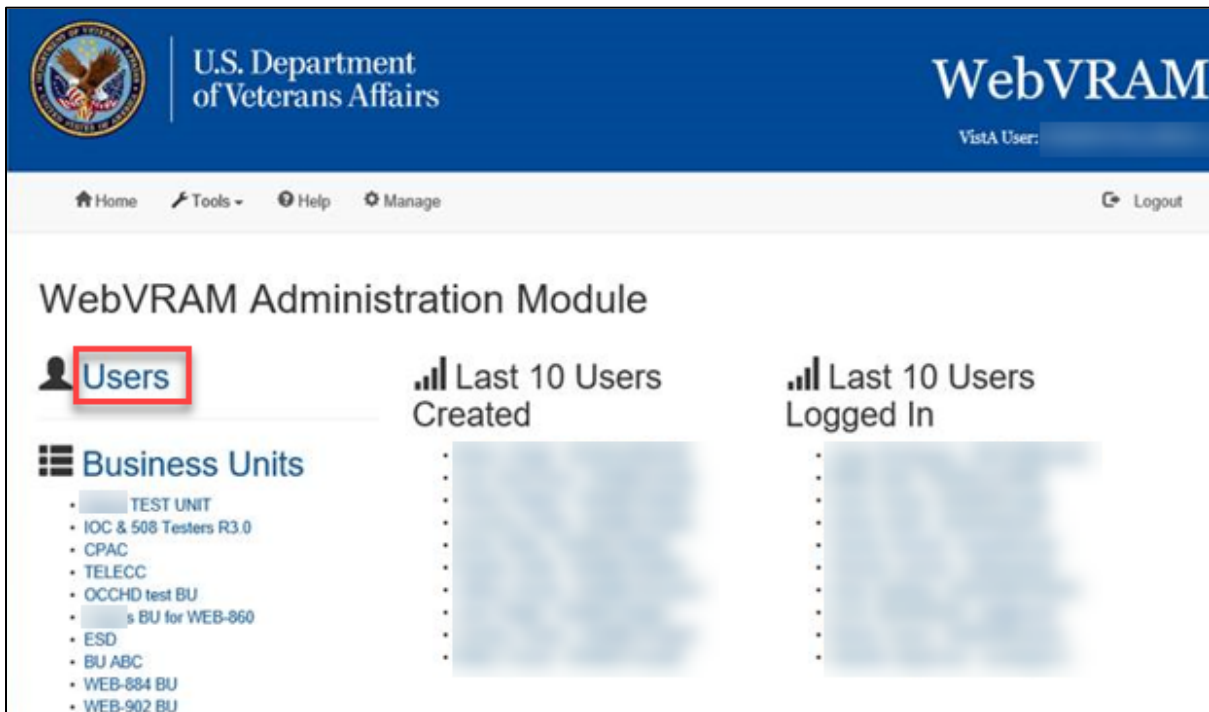
6.  **CAUTION: If the Edit Site button is displayed for any site, WebVRAM has detected potential duplicate VistA user account issues at the site, and the user will not be able to connect to the site. See Section 7.3 [Duplicate Account Reconciliation](#). Additional Edits:** After one area is edited for 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. When logged in as a WebVRAM Administrator, 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 or Remove Secondary Menu Options Screen

The screenshot shows a web interface titled "Secondary Menu Options". At the top is a search bar. Below it is a table with two columns: "Option #", "Option Name", and a third column containing "Add Menu Option" buttons. The table lists 10 options. The button for the 9th option, "654DBU BILLING AUDIT MENU", is highlighted with a red rectangle. At the bottom of the table is a pagination control with "Previous", "Next", and a series of numbered links (1-10) and a "3120" link.

Option #	Option Name	
194187	113721	Add Menu Option
299413	2507 REQUEST EDIT FORM	Add Menu Option
298315	402 VS 3	Add Menu Option
299414	654 PT ADDRESS AUDIT	Add Menu Option
194188	654DBU ACC REC AUDITS MENU	Add Menu Option
194189	654DBU AR FOLLOWUP AUDIT	Add Menu Option
194190	654DBU BILLABLE PC VISIT AUDIT	Add Menu Option
194191	654DBU BILLABLE VISITS BYDSSID	Add Menu Option
194192	654DBU BILLING AUDIT MENU	Add Menu Option
194193	654DBU BILLS CLOSED WO COLL	Add Menu Option

9. **Adding or Deleting WebVRAM Business Unit:** Any Business Unit Administrator can add a new business unit to a user profile or remove an existing business unit from a user profile by editing the WebVRAM Business Units section of the profile.

5.2 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

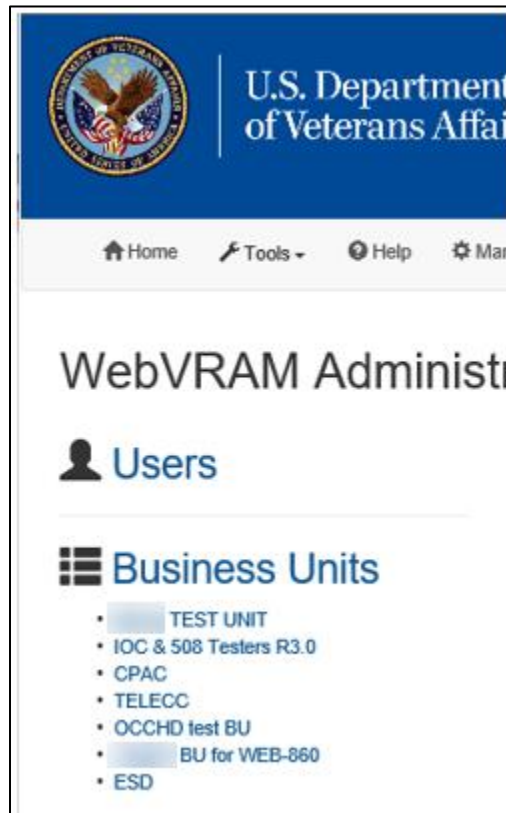
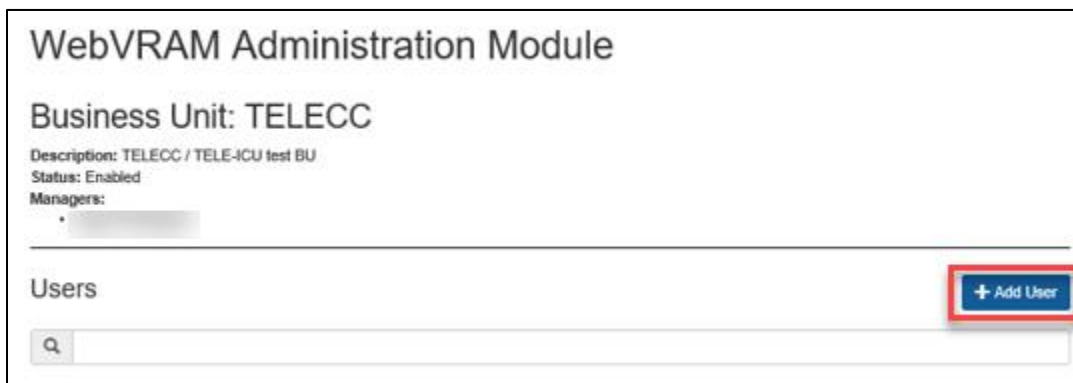
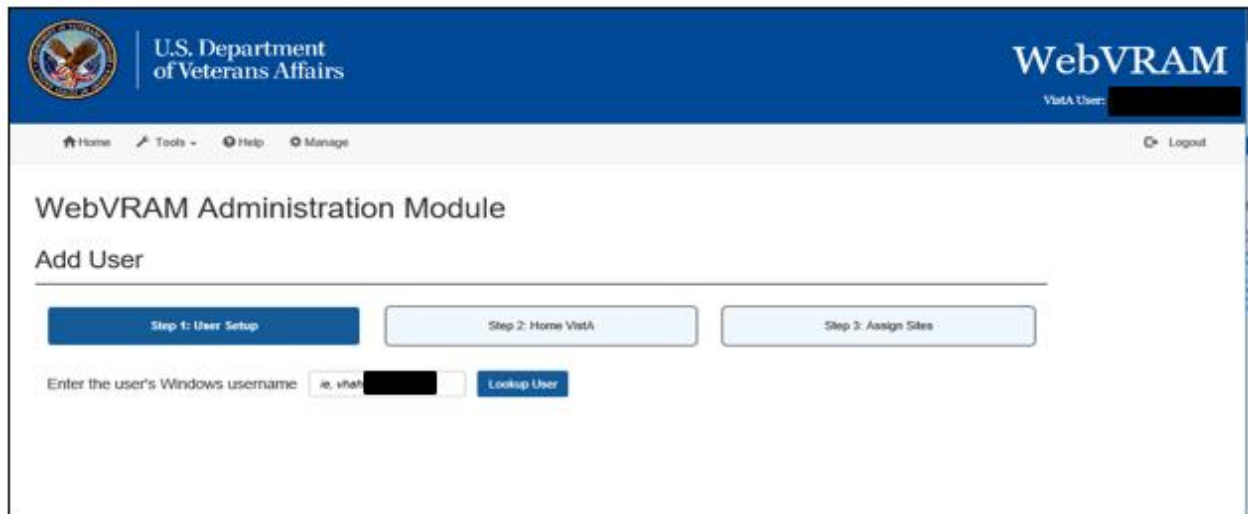


Figure 11: Business Unit Profile Screen



After clicking on the **Add User** button, the Add User Screen is displayed, as shown in Figure 12 below.

Figure 12: Add User Screen



The screenshot displays the 'Add User' screen within the WebVRAM Administration Module. The interface includes a top navigation bar with the U.S. Department of Veterans Affairs logo and 'WebVRAM' branding. Below the navigation bar, the main content area is titled 'WebVRAM Administration Module' and 'Add User'. The screen shows a three-step process: Step 1: User Setup (active), Step 2: Home VistA, and Step 3: Assign Sites. Below the steps, there is a text input field labeled 'Enter the user's Windows username' with a placeholder 'ie, vha' and a 'Lookup User' button.

1. **Windows Username Search Box:** Search for a user to add to the WUT by typing their full Windows VA Username or 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 Global Address List or Active Directory (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

4. If the WEBG WEBVRAM GUI menu does not exist in the user's local Home VistA site profile, a specific error message will be displayed indicating the "WEBG WEBVRAM GUI menu option needs to be added to the local VistA profile." To

resolve this, the user needs to submit a Service Now (SNOW) Ticket to have WEBG WEBVRAM GUI added to their Home Vista's Secondary Menu Options.

Figure 15: WebVRAM Administration Module

5. 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 16 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.



CAUTION: Occasionally, the user's Vista profile will not upload automatically from the user's Home Vista system. There are various database rules within Vista that may cause this to happen. If this occurs, a blank, disabled user profile will be added to WebVRAM. The profile must be populated with the Home Vista profile data. The first data element that must be added before the rest of the profile can be populated is the user's business unit. This is a mandatory entry for all user profiles.

Figure 16: Add User Screen – Success Message

WebVRAM Administration Module

Add User

Step 1: User Setup

Step 2: Home Vista

Step 3: Assign Sites

Enter the user's Windows username Lookup User

Active Directory Found (First, Last Name):

Select the user's Home Vista

VISA

Vista Site

Set Home Vista

Success!

WebVRAM is building the user's profile based on the Home Vista system, in the meantime - assign Vista sites to the user

Add Vista Sites OR Add another user

- 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.**

i NOTE: For instructions on finding the user's Home Vista profile data, see Section [5.5](#) (Existing User with Same Name in Home Vista and Other Vista Data Anomalies), Step 8 KPA CPAC NSD MENU. Any Business Unit Administrator may access the Home Vista site of a user to view their Vista profile data unless the Home Vista site of the Business Unit Administrator is the same as the user's Home Vista site. If this is the case, the Business Unit Administrator may either log an Enterprise Service Desk ticket requesting the user's Vista profile data, or they may ask another Business Unit Administrator for assistance in obtaining the user's Vista profile information.

- **WebVRAM Business Units – A business unit must be added to the user profile before any other data can be added. This is a mandatory field that must be populated.** This is indicated by a warning message near the top of the profile as shown in Figure 17 below. If the Business Unit Administrator tries to enable the account without first adding the business unit to the profile, a pop-up error message will display as shown in Figure 18. 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.

Figure 17: Banner on Disabled User Profile – Business Unit Must Be Added

WebVRAM Administration Module

User:

Edit User Enable User View Logs

This account is disabled

A Business Unit must be added to this user's profile before you can populate any other profile data.
Please remove UNKNOWN add a Business Unit to this user now before updating any other information.

Vista Sites

+ - 🔍

☐ Azure 821 B.vr2test
☐ Azure 820 A.vr1test

Secondary Menu Options

+ - 🔍

No secondary menu options assigned

Security Keys

+ - 🔍

No security keys assigned

CPRS Tabs

+ - 🔍

No CPRS tabs assigned

Person Classes

+ - 🔍

No person classes assigned

User Classes

+ - 🔍

No user classes assigned

Vista Profile

✎

- Title:
- Service/Section:
- Screen Editor:
- Allowed to use spooler? No
- Primary Menu:

WebVRAM Roles

+ - 🔍

☐ WebVRAM Administrator

WebVRAM Business Units

+ - 🔍

☐ UNKNOWN

Figure 18: Warning Message – Business Unit Must Be Added

Home Tools Help Manage

WebVRAM Administration Module

User:

This account is disabled

A Business Unit must be added to this user's profile before you can populate any other profile data.
Please remove UNKNOWN add a Business Unit to this user now before updating any other information.

Vista Sites

+ - 🔍

☐ Azure 821 B.vr2test
☐ Azure 820 A.vr1test

Secondary Menu Options

+ - 🔍

No secondary menu options assigned

Security Keys

+ - 🔍

No security keys assigned

CPRS Tabs

+ - 🔍

No CPRS tabs assigned

Person Classes

+ - 🔍

No person classes assigned

User Classes

+ - 🔍

No user classes assigned

Vista Profile

✎

- Title:
- Service/Section:
- Screen Editor:
- Allowed to use spooler? No
- Primary Menu:

WebVRAM Roles

+ - 🔍

☐ WebVRAM Administrator

WebVRAM Business Units

+ - 🔍

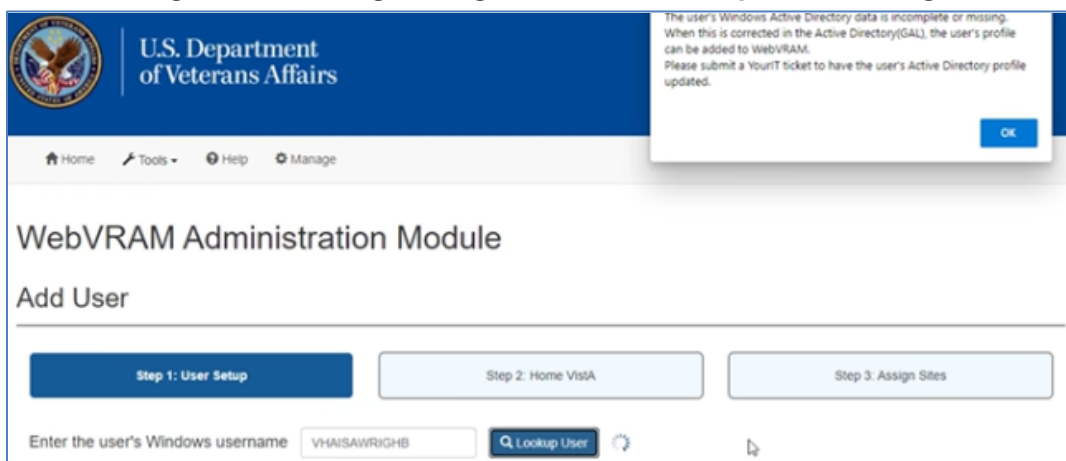
☐ UNKNOWN

Update Business Unit

A Business Unit must be added to this user's profile before you can populate any other profile data.
Please remove UNKNOWN add a Business Unit to this user now before updating any other information.

Cancel

Figure 19: Warning Message –AD data is incomplete or missing



The error message is displayed during the Add User process when WebVRAM detects Active Directory data is missing from Active Directory. Under the circumstance, WebVRAM is not able to complete the Add User process. The message instructs the BU Admin to submit a yourIT ticket to have the user's Active Directory profile updated. The error message reads "The user's Windows Active Directory data is incomplete or missing. When this is corrected in the Active

directory (GAL), the user's profile can be added to WebVRAM. Please submit a YourIT ticket to have the user's Active Directory profile updated."

- **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.



CAUTION: If the Edit Site button is displayed for any site, WebVRAM has detected potential duplicate VistA user account issues at the site, and the user will not be able to connect to the site. See Section 7.3 [Duplicate Account Reconciliation](#).

- **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 and 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.

7. **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 20. The data for each field to be selected or added is listed here and shown in Figure 21.

- **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** – This is a drop-down list field (see Figure 22 below). Select the user’s VA Service Section, such as CPAC NATIONAL, MEDICAL SERVICE Office of Information and Technology (OIT), Telemedicine Intensive Care Unit (TELE-ICU), 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 their 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 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 20: VistA Profile Edit Option

CPRS Tabs + - 🔍

☐ COR

VistA Profile 

- Title: CPAC NSD TECH
- Service/Section: REMOTE
- Screen Editor: SCREEN EDITOR - VA FILEMAN
- Allowed to use spooler? No
- Primary Menu: NURS-RN

Figure 21: VistA Profile Data Entry Fields

VistA Profile

Title CPAC NSD TECH

Service Section OI&T ▼

Screen Editor SCREEN EDITOR - VA FILEMAN

Allowed to use spooler? No ▼

Primary Menu R2CPAC IT

Update VistA Profile Cancel

Figure 22: VistA Profile Service Section Drop-down List

The screenshot shows the 'VistA Profile' configuration window. On the left, there are fields for 'Title', 'Service Section' (highlighted with a red box), 'Screen Editor', 'Allowed to use spooler?' (set to 'No'), and 'Primary Menu' (set to 'NURS-RN'). On the right, a drop-down list is open, displaying a list of service sections. The 'REMOTE' option is highlighted in blue. At the bottom right, there are 'Update VistA Profile' and 'Cancel' buttons.

Service Section
AMBULATORY CARE
CLINICAL INFORMATICS SERVICE
CPAC CENTRAL PLAINS
CPAC FLORIDA/CARIBBEAN
CPAC MID ATLANTIC
CPAC MID SOUTH
CPAC NATIONAL
CPAC NORTH CENTRAL
CPAC NORTH EAST
CPAC WEST
DENTAL SERVICE
ENTERPRISE SERVICE DESK
HIM PROGRAM OFFICE
MEDICAL SERVICE
MENTAL HEALTH & BEHAVIORAL SC.
OCC DELIVERY OPS
OCC HELP DESK
OI&T
PHARMACY SERVICE
RADIOLOGY SERVICE
REMOTE
SUPPLY CHAIN
TELE-ICU
UNKNOWN
VA CENTRAL OFFICE

5.3 Add Security Key Not Present in User's Home VistA

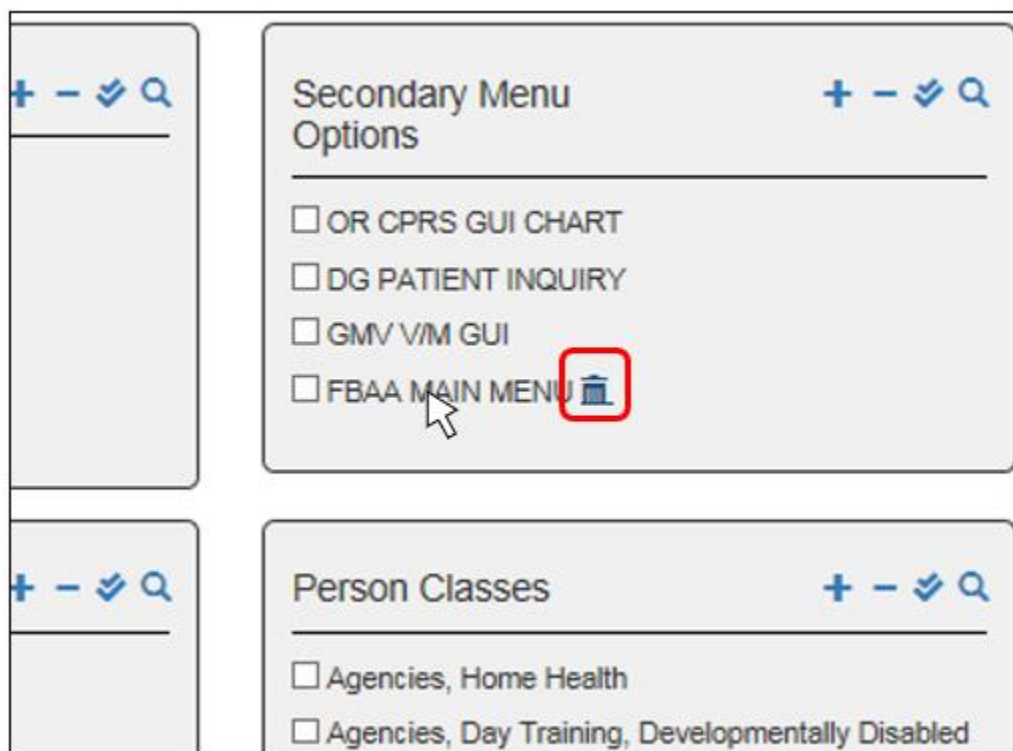
A Business Unit Administrator may need to add a custom Secondary Menu or Security Key to a user's WebVRAM profile that **cannot be added to** the user's Home VistA profile. This will be necessary at times for the user to access certain VistA/CPRS features at a specific remote site where the Menu or Key is required to perform their VA-directed job duties at that site. This will not cause issues at other remote sites where this custom Menu/Key does not exist as it will not recognize the Menu/Key as valid, and it will not be added to that site's VistA profile for that user by WebVRAM when they connect using the application.

5.4 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 23 below.

Figure 23: Edit User Quick Delete Option



5.5 Existing User with Same Name 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 24: "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 page."

Figure 24: Existing User with Same Name Error Message

The screenshot displays 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'. In Step 2, the user has entered a Windows username 'vhaas' and clicked 'Look up User'. The system found an 'Active Directory Found (First, Last Name): [redacted]'. Below this, the user has selected '99' for VISN and 'Cincinnati TEST / 539' for VistA Site, and clicked 'Set Home VistA'. 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 Microsoft Edge browser. Once the user has accessed this URL, they will must complete the fields on that webpage, as shown below in Figure 25:
 - 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 their Home (local) VistA system.
 - e. Click **Send Access Request**.

Figure 25: WebVRAM Access Request Screen



The screenshot shows the 'Access Request' screen of the WebVRAM application. At the top, there is a blue header with the U.S. Department of Veterans Affairs logo on the left, the text 'U.S. Department of Veterans Affairs' in the center, and 'WebVRAM' on the right. Below the header, the title 'Access Request' is displayed. A sub-header states: 'To request access, complete the following steps in order:'. A numbered list follows: 1. Select your business unit, 2. Select your VISN, 3. Select your Home VistA system, and 4. Login using your Access and Verify Code. The form contains five input fields: 'Business Unit' (dropdown menu showing 'OCC'), 'VISN' (dropdown menu showing '99'), 'Home VistA' (dropdown menu showing 'Cincinnati TEST - 539'), 'Access Code' (text input field), and 'Verify Code' (text input field). Below these fields is a blue button labeled 'Send Access Request'. At the bottom center, the version number 'v1.0.19-20190925' is displayed. In the bottom right corner, there is a zoom icon and the text '75%'.

2. Once the user has navigated to the page, entered all required information, and successfully sent the access request with no errors by receiving a "success" message, 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.




- When the user is located and displayed for editing, the user's profile page or the listing from the search page should show a **Status** of "Disabled" as shown below. From the user search page listing, click the **View User** button on the right side of the user listing. The User Profile Screen will appear.

Figure 26: User Disabled Status – User Search Screen

WebVRAM Administration Module

Users

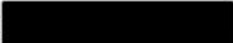
Q


User #	AD Username	First Name	Last Name ↓	Status	Business Unit	View User
68				Disabled	ESD	 View User
110				Enabled	CPAC	 View User
110				Enabled	VA TELECC - WEST	 View User

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

Figure 27: User Profile Screen with Enable User Button

WebVRAM Administration Module

User: 

 Enable User

This account is disabled

Vista Sites

+ - 🔍

No Vista sites assigned

Secondary Menu Options

+ - 🔍

No secondary menu options assigned

Security Keys

+ - 🔍

No security keys assigned

CPRS Tabs

+ - 🔍

No CPRS tabs assigned

Person Classes

+ - 🔍

No person classes assigned

User Classes

+ - 🔍

No user classes assigned

Vista Profile

✎

- Show all sites? No
- Title:
- Section Section:
- Screen Editor:
- Allowed to use spooler? No
- Delimited Menu:

WebVRAM Roles

+ - 🔍

No roles assigned

WebVRAM Business Units

+ - 🔍

☐ occ

- 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 log into the application using their Home Vista Access and Verify codes. 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.

6. 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.
 - a. CPRS Tabs
 - b. Secondary Menu Options
 - c. Security Keys
 - d. Person Class, User Class
 - e. Vista Profile Information:
 - i. Title
 - ii. Screen Editor
 - iii. Allowed to use spooler
7. The Service Section value must be manually added to any user profile whether it automatically uploads from VistA or comes across as a blank profile. This can be done by selecting a value from the drop-down option in the Service Section of the VistA Profile component of the user profile as shown in [Figure 22](#) above.
8. **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 5.10](#) (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 and 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
    [MCARPULMUSER]              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.

5.6 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.

5.6.1 To Order Meds and Write Notes in CPRS

Home VistA Profile (recommended):

- **AUTHORIZED TO WRITE MED ORDERS** field (#53.1) in the NEW PERSON file (#200) set to “YES”
- Security Keys of **ORES** and **PROVIDER**
- CPRS Tabs: **COR**

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** and **PROVIDER**

5.6.2 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 WRITE MED ORDERS** field (#53.1) in the NEW PERSON file (#200) set to “YES”
- Security Key of **ORELSE** and **PROVIDER**
- CPRS Tabs: **COR**

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)



NOTE: The business owner of the WebVRAM application does not dictate policy regarding the assignment of CPRS Security Keys and Tabs. The configurations above are only recommendations. The WebVRAM profile values **MUST BE IDENTICAL** to the Home VistA profile values and should be determined for each user based on VA and line management policy.

5.6.3 Extended Timeout

WebVRAM allows extended timeout for users who meet one of the following criteria:

- BU is one of the following Business Units and TIMED READ and ORWOR TIMEOUT CHART are set to 21,600 secs:
 - V10 TELECC (May be member of multiple business units)
 - VA TELECC – WEST (May be member of multiple business units)
 - V23 CCC
 - VISN 20 VA Health Connect
 - VISN 12 CCC

- VISON 5 Pharmacy VA Health Connect
- BU is "V21 Clinical Contact Center" and TIMED READ and ORWOR TIMEOUT CHART is set to 14,400 secs.

Home VistA Profile:

- **TIMED READ** (# OF SECONDS) field (#200.1) in the NEW PERSON file (#200) user profile timeout value set to **21600** via FileMan edit.
- **ORWOR TIMEOUT CHART** field (#200.19) set to **21600** via FileMan in the NEW PERSON file (#200).
- Home VistA profile values must be set by the user's local IT staff. An ePAS request may be required to make updates if these values do not already exist for the user.

Extended Timeout Disallowed for non-approved users

WebVRAM disallows extended timeout when TIMED READ or ORWOR TIMEOUT CHART are set to a value greater than 900 seconds, the user belongs to one business unit and the BU is not authorized extended timeout. In this case, WebVRAM will pass 900 seconds to the remote VistA sites for TIMED READ and ORWOR TIMEOUT CHART and will print the following warning in the synchronization log: **"This user is assigned to a business unit that does not allow extended timeout. For this reason, time out has been reduced to 900 seconds"**



NOTE: If a user belonging to multiple business units and is granted an extended timeout, an error message will be shown saying: **"This user belongs to multiple business units. For this reason, the user is not allowed to have an extended time out. Time out has been reduced to 900 seconds."** This does not apply to TeleCritical Care providers with Business Units set to V10 TELECC or VA TELECC – WEST, since they are always allowed extended timeout, even if they belong to multiple business units.




NOTE: Users who belong to multiple Business Units are not eligible to have Extended Timeout. If a user requires Extended Timeout, that user should be removed from all but the one business unit where Extended Timeout is required. This does not apply to TeleCritical Care providers with Business Units set to V10 TELECC or VA TELECC – WEST, since they are always allowed extended timeout, even if they belong to multiple business units.

5.7 Custom Profile Values or Site-specific Clinical Teams Required to Access 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 NEW PERSON file (#200) in order to access certain CPRS or other VistA 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 listed in this section.

5.7.1 Site-specific CPRS Clinical Teams – Consults/Menus Access

Some VAMCs require a clinician to belong to a Clinical Team at that site before they can access CPRS consults or certain CPRS order menus. When a provider is unable to access consults or CPRS order menus at one of these sites, but can access all other CPRS features, the Clinical Application Coordinator (CAC) at that site will need to be contacted to arrange for the provider to be added to the correct team, or to identify which site-specific user parameters are needed to access these CPRS features. A national CAC directory can be found on the VHA National CAC Roster SharePoint site.

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

5.7.2 Summary of Site-specific VistA Profile Values

The table below provides a quick-reference summary of site-specific VistA profile values; the business rules are described in more detail in the following subsections.

Table 4: Site-specific VistA Profile Values

Site	Provider Type / Activity	Title	User Class	Service - Section
Biloxi, Mississippi	Providers requiring access to all CPRS provider features and notifications	Not applicable	<ul style="list-style-type: none">PROVIDERCR PC PROV	Not applicable
Chillicothe, Ohio	Tele-ICU providers writing CPRS Tele-ICU Notes	Not applicable	Tele-Health Staff	Not applicable

Site	Provider Type / Activity	Title	User Class	Service - Section
Cleveland, Ohio	Tele-ICU providers writing CPRS Tele-ICU Notes	Not applicable	INTERNIST	Not applicable
Detroit, Michigan	Providers needing to access all features of CPRS Progress Notes	Not applicable	<ul style="list-style-type: none"> • PROVIDER • CLINICAL COORDINATOR • NURSE (for Registered Nurses and Nurse Practitioners) 	Not applicable
Houston	Providers needing to author CPRS notes	Role: <ul style="list-style-type: none"> • MD/Physician • Physician Assistant • Nurse Practitioner • Nurse/RN • LPN/LVN • Psychologist • Social Worker 	User Class: <ul style="list-style-type: none"> • PHYSICIAN • PHYSICIAN ASSISTANT • NURSE PRACTITIONER • NURSE • NURSE LICENSED PRACTICAL • PSYCHOLOGIST • SOCIAL WORKER 	Not applicable
Northern California and San Francisco	Providers placing orders and writing progress notes in CPRS	Not applicable	Not applicable	MEDICAL SERVICE
Puget Sound HCS	Providers / Schedulers signing CPRS notes	Not applicable	HPM CSC ADMIN	Not applicable
Puget Sound HCS	Schedulers needing to access VistA Scheduling features	Not applicable	DOCUMENTATION ASSISTANT	Not applicable
Sioux Falls	Tele-oncologists needing access to CPRS oncology notes	Not applicable	PGX AUTHORIZED STAFF	Not applicable

Site	Provider Type / Activity	Title	User Class	Service - Section
White City	Providers needing access to CPRS notes	Not applicable	MEDICAL CLERK, PROVIDER, Additional Signer	Not applicable
New Jersey ¹	Physicians connecting to New Jersey HCS: Person Class (Provider Type) containing "Allopathic" but Specialization value does NOT contain "Psychiatry" or "Psych/Mental" or "Neuro"	PHYSICIAN	PHYSICIAN	AMBULATORY CARE
New Jersey ¹	Nurses connecting to New Jersey HCS: Person Class (Provider Type) containing "Nursing" but Specialization value does NOT contain "Psychiatry" or "Psych/Mental" or "Neuro"	NURSE	NURSE	AMBULATORY CARE

¹ Specified profile values are automatically substituted when the user connects to New Jersey HCS using WebVRAM.

Site	Provider Type / Activity	Title	User Class	Service - Section
New Jersey ¹	Physician Assistants/Nurse Practitioners connecting to New Jersey HCS: Person Class (Provider Type) containing "Physician Assistants" but Specialization value does NOT contain "Psychiatry" or "Psych/Mental" or "Neuro"	NURSE PRACTITIONER	NURSE PRACTITIONER and PROVIDER NOTE: Both values are required.	AMBULATORY CARE
New Jersey ¹	Psychiatrists connecting to New Jersey HCS: Person Class (Provider Type) containing "Allopathic" and CLASSIFICATION (not Specialization) = "Psychiatry and Neurology"	PSYCHIATRIST	PSYCHIATRIST	MENTAL HEALTH and BEHAVIORAL SC. NOTE: Service Section includes the period as written above.
New Jersey ¹	Behavioral/mental health providers connecting to New Jersey HCS: Person Class (Provider Type) containing "Behavioral"	PSYCHOLOGIST	STAFF PSYCHOLOGIST	MENTAL HEALTH and BEHAVIORAL SC. NOTE: Service Section the period as written above.

Site	Provider Type / Activity	Title	User Class	Service - Section
New Jersey ¹	Mental health nurses connecting to New Jersey HCS: Person Class (Provider Type) containing "Nursing" and Specialization value that DOES contain "Psychiatry" or "Psych/Mental" or "Neuro"	NURSE	NURSE	MENTAL HEALTH and BEHAVIORAL SC. NOTE: Service Section includes the period as written above.
New Jersey ¹	Mental health Physician Assistants/Nurse Practitioners connecting to New Jersey HCS: Person Class (Provider Type) containing "Physician Assistants" and Specialization value DOES contain "Psychiatry" or "Psych/Mental" or "Neuro"	NURSE PRACTITIONER	NURSE PRACTITIONER and PROVIDER NOTE: Both values are required.	MENTAL HEALTH and BEHAVIORAL SC. NOTE: Service Section the period as written above.

5.7.3 All VAMCs: Secondary Menu Required for Mental Health Clinical Reminders

To access Mental Health Clinical Reminders at **all** VAMCs, the user must have a Secondary Menu of **YS BROKER1** in both their Home VistA profile and their WebVRAM profile. If they can launch the Mental Health Assistant (MHA) from CPRS at some sites, and not others, the user may need to have the current version of the YS_MHA_A_XE10.dll installed on their Government Furnished Equipment (GFE)

workstation. If that does not resolve the issue, the site where the MHA app is not launching from CPRS may require a custom User Class, Service Section, etc. to access the app. If this occurs, submit a help desk INCIDENT ticket, and make certain it gets assigned to the WebVRAM Group to add the custom value to the WebVRAM database so it can be added to the user profile.

5.7.4 To Access Provider CPRS Features at Biloxi

Providers requiring access to all CPRS provider features and notifications at Biloxi, MS, must have the following User Class values in their WebVRAM profile:

- **PROVIDER**
- **CR PC PROV**

To allow Mental Health providers to access CPRS mental health features, the following User Class value must be added to their WebVRAM Profile:

- **CR MH OPT USER**

5.7.5 To Access Tele-ICU Notes at Chillicothe, OH

Tele-ICU providers needing to access CPRS Tele-ICU Progress Notes at Chillicothe, OH, must have a User Class value of **Tele-Health Staff**.

5.7.6 To Access Tele-ICU Notes at Cleveland, Ohio

Tele-ICU providers needing to access CPRS Tele-ICU Progress Notes at Cleveland, OH, must have a User Class value of **INTERNIST**.

5.7.7 To Access Progress Notes at Detroit

Providers needing to access all features of CPRS Progress Notes at Detroit VAMC must have the following User Class values in their WebVRAM profile:

- **PROVIDER**
- **CLINICAL COORDINATOR**
- **NURSE** (for Registered Nurses and Nurse Practitioners)

5.7.8 To Author CPRS Notes at Houston

Providers needing to author CPRS notes at Houston will need the following User Class values in their WebVRAM profile, based on their provider role.

Table 5: Houston Custom User Class Values

Role	User Class
MD/Physician	PHYSICIAN

Role	User Class
Physician Assistant	PHYSICIAN ASSISTANT
Nurse Practitioner	NURSE PRACTITIONER
Nurse/RN	NURSE
LPN/LVN	NURSE LICENSED PRACTICAL
Psychologist	PSYCHOLOGIST
Social Worker	SOCIAL WORKER

5.7.9 Order Meds and Access Progress Notes at Northern California and San Francisco

Providers needing to order medications and create/update progress notes in CPRS at Northern California and San Francisco must have a Service Section value of **MEDICAL SERVICE**.

5.7.10 To Sign CPRS Notes at Puget Sound

Providers/Schedulers signing CPRS notes at Puget Sound HCS must have a User Class value of **HPM CSC ADMIN** in their WebVRAM profile.

5.7.11 To Access VistA Scheduling at Puget Sound

Schedulers needing to access VistA Scheduling features at Puget Sound HCS must have a User Class value of **DOCUMENTATION ASSISTANT** in their WebVRAM profile.

5.7.12 To Access CPRS Oncology Notes at Sioux Falls

Tele-oncologists needing access to CPRS oncology notes at Sioux Falls must have the User Class value of **PGX AUTHORIZED STAFF** in their WebVRAM profile.

5.7.13 To Access CPRS Notes at White City

Providers needing access to CPRS notes at White City must have three User Class values in their WebVRAM profile: **MEDICAL CLERK**, **PROVIDER** and **Additional Signer**.

5.7.14 To Access Consults at New Jersey

Providers needing to view consults, and specifically mental health consults, at New Jersey HCS must have the following values based on their clinical role. At this time, these

values must be manually added to the provider's WebVRAM profile before they synchronize through WebVRAM to do work at New Jersey.



NOTE: In a future release, these values will be automatically added to the user profile that is transmitted to the New Jersey VistA profile when the user connects to that site using WebVRAM. These values will be transmitted in place of any other values the user may have in their existing VistA and WebVRAM profiles, but only when New Jersey is accessed remotely through the application. WebVRAM will substitute these values in real-time when these users synchronize to the New Jersey HCS.

- Providers with New Jersey HCS in their VistA Site list and a Home VistA Person Class (Provider Type) containing "Allopathic" who do NOT have a Specialization value containing "Psychiatry" or "Psych/Mental" or "Neuro" (e.g. Person Class #93) shall have the following values transmitted to the New Jersey HCS instead of the existing WebVRAM profile values:
 - Title: **PHYSICIAN**
 - User Class: **PHYSICIAN**
 - Service Section : **AMBULATORY CARE**
- Providers with New Jersey HCS in their VistA Site list and a Home VistA Person Class (Provider Type) containing "Nursing" who do NOT have a Specialization value containing "Psychiatry" or "Psych/Mental" or "Neuro" (e.g. Person Class #443) shall have the following values transmitted to the New Jersey HCS instead of the existing WebVRAM profile values:
 - Title: **NURSE**
 - User Class: **NURSE**
 - Service Section : **AMBULATORY CARE**
- Providers with New Jersey HCS in their VistA Site list and a Home VistA Person Class (Provider Type) containing "Physician Assistants" who do NOT have a Specialization value containing "Psychiatry" or "Psych/Mental" or "Neuro" (e.g. Person Class #541) shall have the following values transmitted to the New Jersey HCS instead of the existing WebVRAM profile values:
 - Title: **NURSE PRACTITIONER**
 - User Class: **NURSE PRACTITIONER** and **PROVIDER**
 - **NOTE:** Both values are required.
 - Service Section : **AMBULATORY CARE**

- Providers with New Jersey HCS in their VistA Site list and a Home VistA Person Class (Provider Type) containing "Allopathic" and who DO have a CLASSIFICATION (not Specialization) of "Psychiatry and Neurology" (e.g. Person Class #25) shall have the following values transmitted to the New Jersey HCS instead of the existing WebVRAM profile values:
 - Title: **PSYCHIATRIST**
 - User Class: **PSYCHIATRIST**
 - Service Section : **MENTAL HEALTH and BEHAVIORAL SC.**
 - **NOTE:** Service Section includes the period as written above.
- Providers with New Jersey HCS in their VistA Site list, and a home VistA Person Class (Provider Type) containing "Behavioral" (e.g. Person Class #295) shall have the following values transmitted to the New Jersey HCS instead of the existing WebVRAM profile values:
 - Title: **PSYCHOLOGIST**
 - User Class: **STAFF PSYCHOLOGIST**
 - Service Section : **MENTAL HEALTH and BEHAVIORAL SC.**
 - **NOTE:** Service Section includes the period as written above.
- Providers with New Jersey HCS in their VistA Site list and a Home VistA Person Class (Provider Type) containing "Nursing" who DO have a Specialization value containing "Psychiatry" or "Psych/Mental" or "Neuro" (e.g. Person Class #473) shall have the following values transmitted to the New Jersey HCS instead of the existing WebVRAM profile values:
 - Title: **NURSE**
 - User Class: **NURSE**
 - Service Section : **MENTAL HEALTH and BEHAVIORAL SC.**
 - **NOTE:** Service Section includes the period as written above.
- Providers with New Jersey HCS in their VistA Site list and a Home VistA Person Class (Provider Type) containing "Physician Assistants" who DO have a Specialization value containing "Psychiatry" or "Psych/Mental" or "Neuro" (e.g. Person Class #556) shall have the following values transmitted to the New Jersey HCS instead of the existing WebVRAM profile values:
 - Title: **NURSE PRACTITIONER**
 - User Class: **NURSE PRACTITIONER and PROVIDER**

- **NOTE:** Both values are required.
- Service Section : **MENTAL HEALTH and BEHAVIORAL SC.**
 - **NOTE:** Service Section includes the period as written above.

5.8 Access CPRS at Remote Sites Using CPRS Desktop Launcher

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

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

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

1. The VistA profile established at the remote site when the user connects through WebVRAM the first time will be terminated on day 31 after that synchronization event.
2. On day 31 after that synchronization, if the user does not synchronize to the remote site using WebVRAM on that day and tries to use only the CPRS Desktop Launcher to access patient records at that remote site, their CPRS login will be denied, and they will not be able to open CPRS at that site. This is because their VistA profile at that site will have been terminated at the end of the day before, and CPRS will not allow user access to the patient record at that site with a terminated VistA profile.
3. **If a user wishes to use only the CPRS Desktop Launcher and not WebVRAM to access patient records at the remote site, they MUST synchronize to that remote site using WebVRAM at least every 29 days to keep their VistA profile active at that site.** Performing a synchronization to the remote site to

update the user's VistA profile, and resetting a new 30-day expiration cycle, only takes a few seconds in WebVRAM and can be accomplished by selecting the **Synchronize** option from the Launch Mode drop-down, and then clicking the **Launch Synchronize** button associated with the remote site. It is NOT necessary to launch CPRS at the remote site and then login to CPRS to reset the VistA profile 30-day expiration date. **This must be done at least every 29 days for each remote site the user accesses to continue using the CPRS Desktop Launcher to work with patient records at those sites.**



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

5.9 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
- R2MAGCWP GUI RPC

Security Key

- MAGDISP CLIN

5.10 View/Edit User's Home VistA System and Active Directory Name

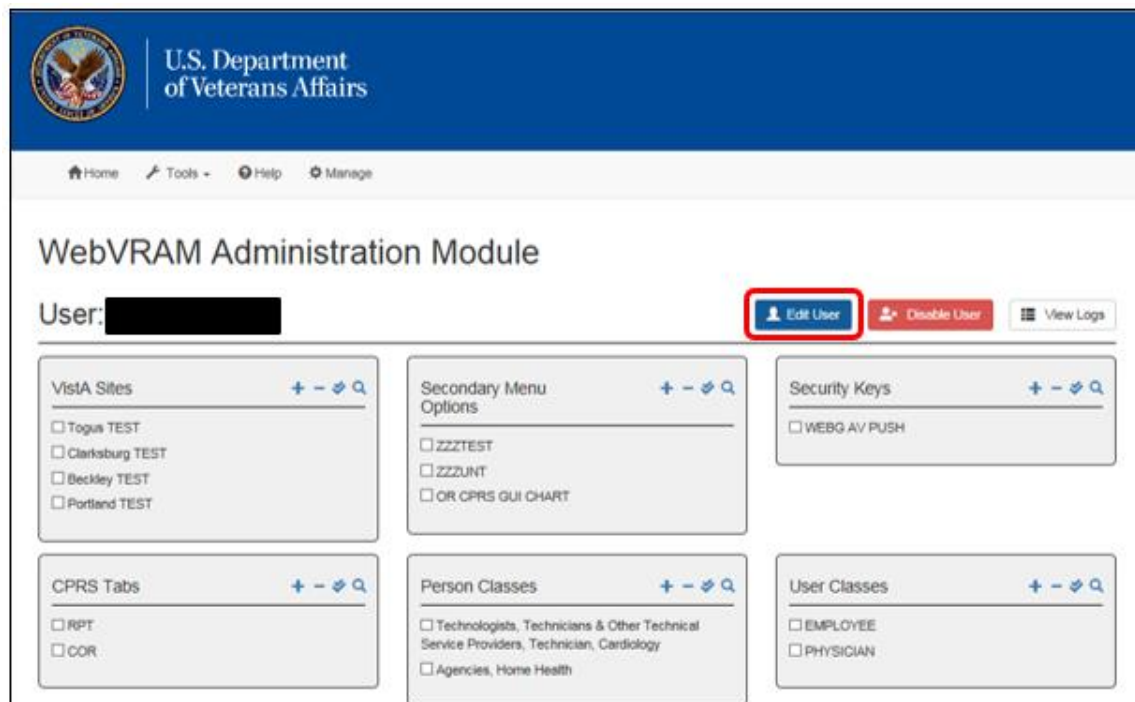


CAUTION: When a user changes locations and is assigned a new Home VistA System profile (account), their Windows Active Directory ID (GAL) will also usually be changed. If their Active Directory ID changes, you must wait at least 48 hours after that change occurs to proceed with the steps in this section. Also – and most important – the user's FULL NAME (Last Name, First Name, and Middle Initial/Middle Name) must match EXACTLY in the new Home VistA user profile, in the Windows Active Directory (GAL) and in the WebVRAM user profile (only Last Name and First 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 28: 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 29: Edit User Screen

The screenshot shows the 'WebVRAM Administration Module' interface. At the top, there's a navigation bar with 'Home', 'Tools', 'Help', and 'Manage'. Below this, the 'User:' field is followed by a redacted name. To the right are buttons for 'Edit User', 'Disable User', and 'View Logs'. The main section is titled 'Edit User' and contains a warning box: 'Proceed w/ Caution! Changing these settings may break the user's WebVRAM account.' Below the warning is a form with fields for 'First Name' (B), 'Last Name' (W), 'Active Directory (Windows) Username' (VHAIS), 'VA Email Address' (empty), and 'Home VistA' (Cincinnati TEST). The 'Home VistA' field has a red 'X' button highlighted with a red box. At the bottom of the form are 'Update User' and 'Cancel' buttons.

Figure 30: Edit User Screen – Home VistA Field Cleared

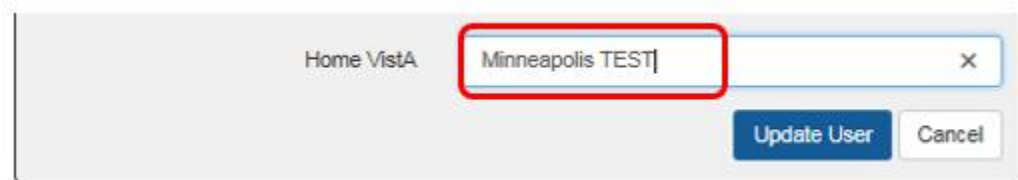
This is a close-up of the 'Home VistA' field from the previous screenshot. The field is now empty, and the red 'X' button is no longer visible. The field is highlighted with a red box. The 'Update User' and 'Cancel' buttons are still visible at the bottom.

- Figure 31 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 32.

Figure 31: Edit User Screen – Home VistA “Auto-Fill” Feature



Figure 32: 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) must also be changed in the **Edit User** component of their profile as shown above.
- The user will have been assigned a new set of Access and Verify codes. After all above steps have been completed, instruct the user to login to WebVRAM using their new Home VistA Access and Verify codes.

5.11 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 33: User Profile Screen – View Logs Button

WebVRAM Administration Module



User: [REDACTED]

Home VistA Site: Beckley TEST

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

Vista Sites	Secondary Menu Options	Security Keys
<input type="checkbox"/> Minneapolis TEST <input type="checkbox"/> Cincinnati TEST	<input type="checkbox"/> DG PATIENT INQUIRY <input type="checkbox"/> JOB CRRS GUICHAST	<input type="checkbox"/> WEBG AV PUSH <input type="checkbox"/> MAGDISP ADMIN

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 34 provides an overview of the user log and the **View Details** button.

Figure 34: User Log Listing

WebVRAM Administration Module

User: [REDACTED]

Edit User

Disable User

View Logs

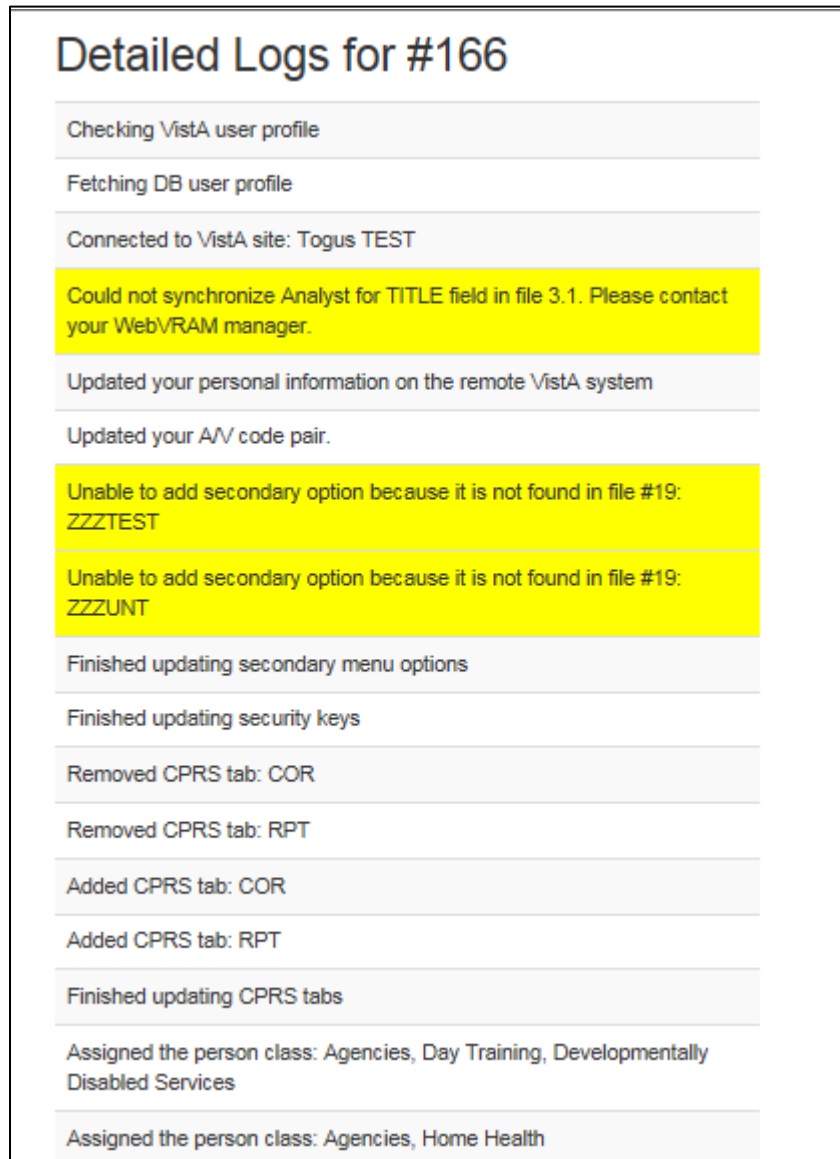
Home VistA Site: Cincinnati TEST

Logs

Log #	Start ☺	Stop ☺	VistA Site	Summary	Action
3628	Wed, Apr 13, 2022 11:54 AM	Wed, Apr 13, 2022 11:54 AM	Clarksburg TEST	Warning	View Details
3627	Tue, Apr 12, 2022 9:03 AM	Tue, Apr 12, 2022 9:03 AM	Beckley TEST	Failed	View Details
3626	Tue, Apr 12, 2022 8:45 AM	Tue, Apr 12, 2022 8:45 AM	Minneapolis TEST	Warning	View Details
3625	Tue, Apr 12, 2022 8:41 AM	Tue, Apr 12, 2022 8:41 AM	Multiple Sites	Warning	View Details
3624	Tue, Apr 12, 2022 8:36 AM	Tue, Apr 12, 2022 8:36 AM	Minneapolis TEST	Warning	View Details
3623	Mon, Apr 11, 2022 2:21 PM	Mon, Apr 11, 2022 2:22 PM	Clarksburg TEST	Warning	View Details

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

Figure 35: Detailed Logs



5.11.1 User Log New VA EHR Messages

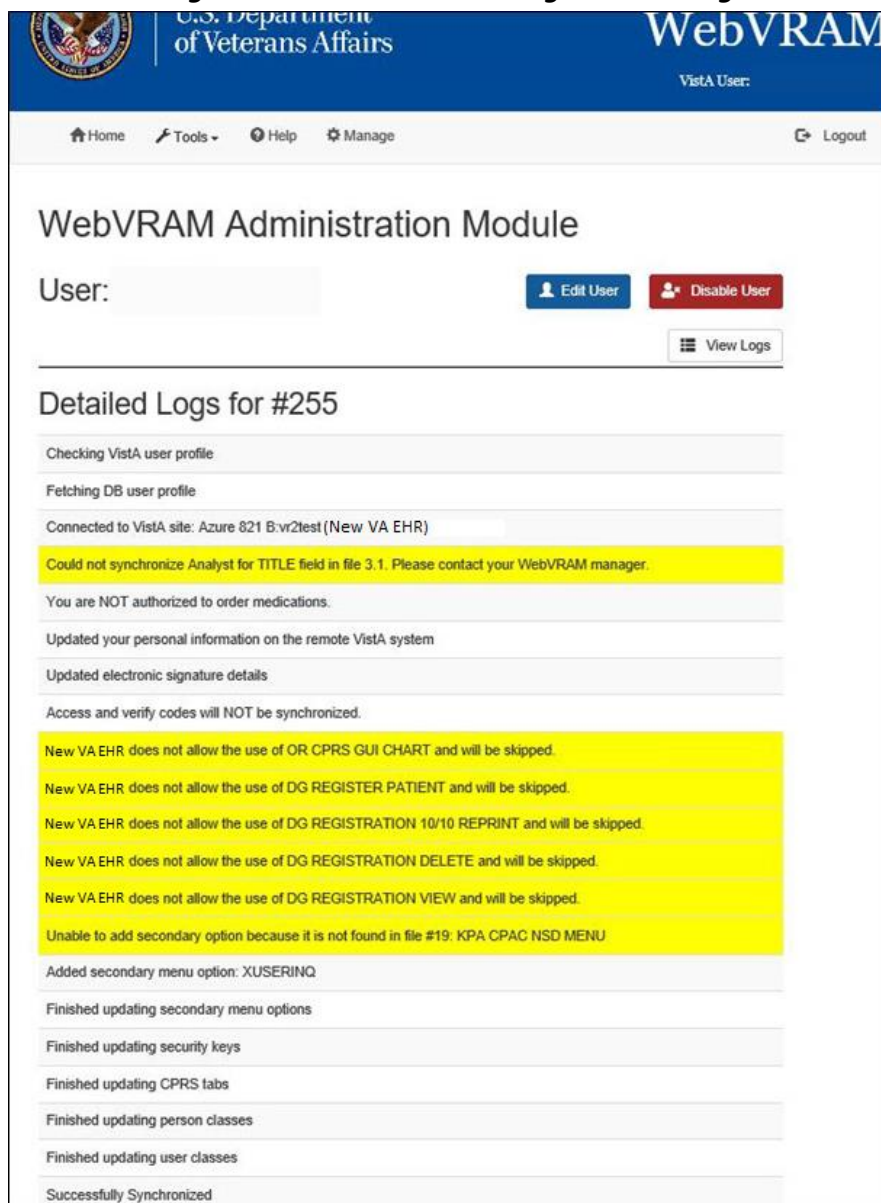
If a site is using New VA EHR , the site listings page displays the **Launch** New VA EHR button alongside the existing **Launch CPRS** or **Launch Reflection** button. Since the initial New VA EHR rollout will not replace all VistA functions, the user can still access certain VistA functions at New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

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

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

Figure 36 provides an example of the user log after synchronizing to a New VA HER site.

Figure 36: New VA EHR Messages in User Log



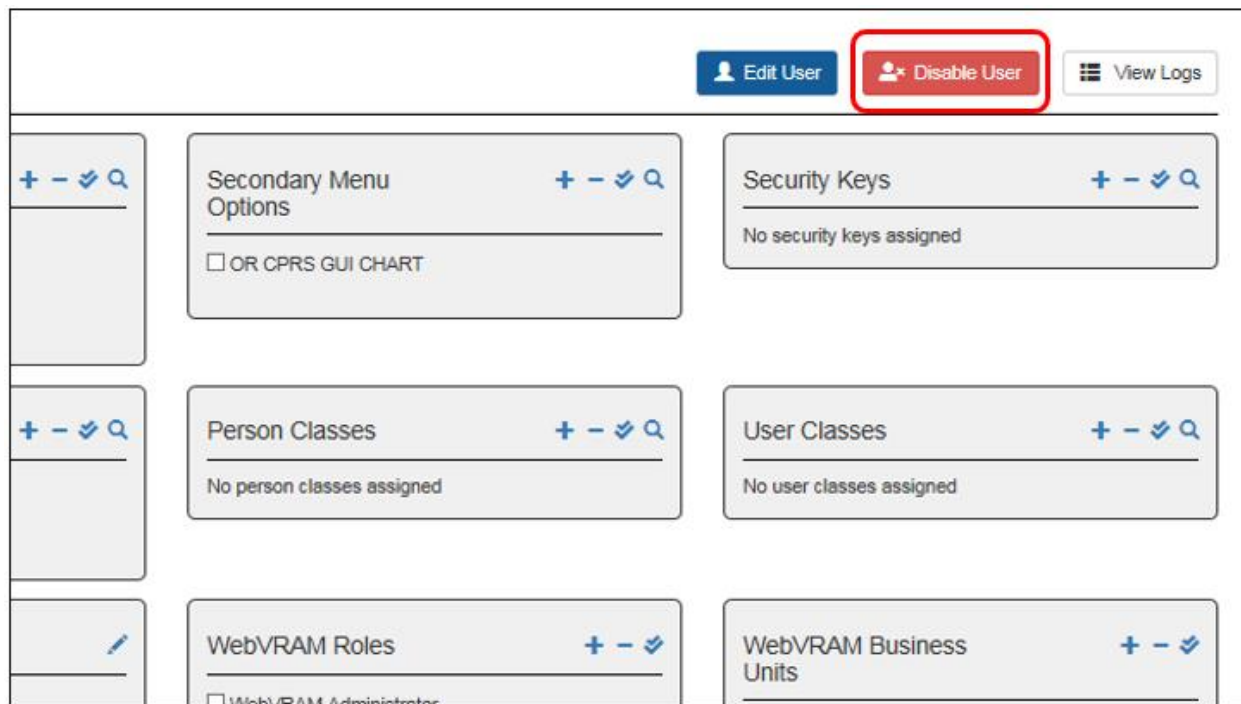
5.12 Disable User Account

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 37 below. Once this is done, the User Profile Screen will only show one button, **Enable User**, as shown in Figure 27, 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 dis-used flag turned "on" at each remote site where the user is no longer authorized to access VistA.

Figure 37: User Profile Screen – Disable User Button



5.13 Exit System

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

6 Access Review Audit

On a quarterly basis, Business Unit Administrators must perform an Access Review Audit for their Business Unit.

This audit requires that Business Unit Administrators (1) identify users who have left the VA, (2) identify users who have not been disabled by an automated tool due to 90 days of inactivity, and (3) identify users who have changed positions and no longer require the use of WebVRAM. The Business Unit Administrator must disable the WebVRAM user profile of these users following the instructions in section 5.12 entitled "Disable User Account."

This audit also requires that Business Unit Administrators review the menus and keys assigned to each user to determine if menus or keys need to be changed or revoked.

Once the audit has been completed, the Business Unit Administrator needs to fill out the General Account Review memo provided in Appendix B and upload it to the appropriate subfolder under the MS Teams Access Review Audit Memo folder.

There is a subfolder for every quarterly audit under the main folder. The WebVRAM Business Unit Administrator needs to upload the General Account Review memo to the appropriate subfolder according to the month and year of the current audit.

Please note that only one audit memo needs to be provided per Business Unit and that only the completed General Account Review memo itself is needed..

7 Troubleshooting

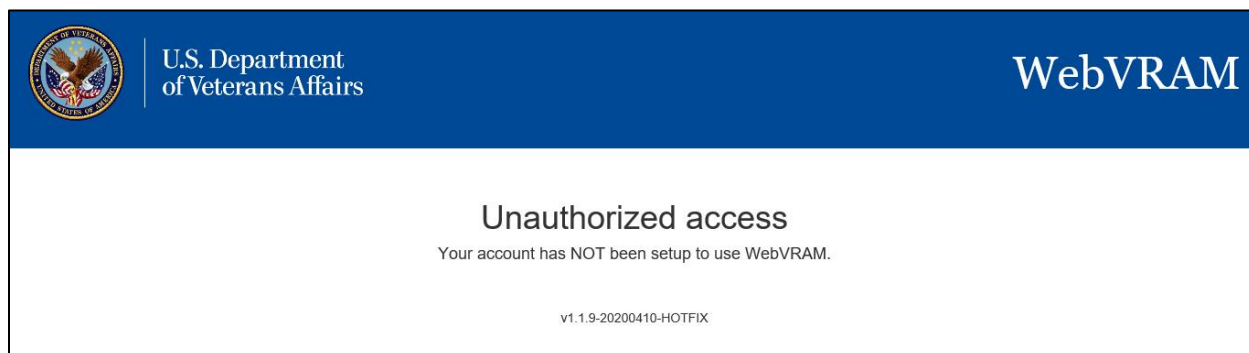
For troubleshooting, users may contact the Enterprise Service Desk (ESD) by phone or by entering a SNOW (YourIT) ticket to receive Tier 1-3 support.

7.1 Special Instructions for Error Correction

7.1.1 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 38: Unauthorized Access Error Message



2. Does the user have the **WEBG WEBVRAM GUI Secondary Menu Option** in their Home VistA profile?
 - 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!**
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. This Security Key does NOT need to be added to their Home VistA profile and serves no purpose if added to that 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 for physicians and some nurses.



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 or 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 WRITE MED ORDERS** field (#53.1) in the NEW PERSON 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 or Cleveland VAMCs or both? If YES, the user must have:
 - a. **WebVRAM Profile:**
 - i. For Chillicothe, User Class of **Tele-Health Staff**.
 - ii. For Cleveland, User Class of **INTERNIST**.

7.1.2 Submitting Help Desk Tickets for User Issues

If a user experience any of the following issues, have them submit a help desk ticket through Service Now (SNOW) or YourIT or call the Enterprise Service Desk (ESD) at 855-

673-4357. ESD Tier 1 agents have a knowledge base and experience to resolve these issues.

- Need to configure Reflection to allow multiple simultaneous sessions for a single VistA location.
- Error message "not a valid Access and Verify Code pair" when launching CPRS in WebVRAM.
- Issues with the Computerized Patient Record System (CPRS) including the following:
 - Unable to log into CPRS when launched from WebVRAM.
 - Unable to view patient records in CPRS.
 - Unable to write orders in CPRS.
 - Unable to access CPRS while connected through VPN or Citrix.
 - CPRS Reminders are not working.
 - Need to set MS Edge default home page to open WebVRAM.

For more complicated issues than those already listed, have the user submit (or submit on behalf of the user) an ESD ticket and assign the ticket to the **SPM.Health.PCS.Sub_4.WebVRAM** group which provides Tier 2 support and can resolve complex issues in a timely manner. **Be certain that this assignment is made when the ticket is logged.** Sometimes a Tier 1 ESD agent will assign the ticket to the user's local IT staff who does not know how to resolve WebVRAM issues, which will delay resolution of the problem.

The next section contains a list of common problems and resolutions for those problems that you as a Business Unit Administrator can resolve or can work with local IT staff to resolve.

7.1.3 Common Problems and Resolutions with User Profiles and VistA Data Anomalies

Table 6: 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!

Issue #	Issue	Cause	Resolution
2.	User is unable to order controlled substance medications at remote sites accessed through WebVRAM.	<p>The provider is not configured to prescribe controlled substances at the remote site.</p> <p>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.</p>	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.
3.	User is unable to login to WebVRAM; receives "Unauthorized User/No Profile" error.	WEBG WEBVRAM 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 "Your Access or Verify Code is invalid in your home VistA Profile (<Home VistA Name>). Please contact your Local IT or ESD Help Desk to reset your access and verify codes. The WebVRAM Team cannot change these codes." error. A link to the YourIT/SNOW portal is included in the error message to create an INC ticket.	<ol style="list-style-type: none"> 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. 4. A user's Access and Verify Code may have expired. A user who logs in with PIV card must still keep their Access and Verify Codes up to date. 	<ol style="list-style-type: none"> 1. Instruct the user to submit an ePAS request to add WEBG WEBVRAM GUI Secondary Menu Option to their Home VistA profile. A screenshot of the error is helpful for the support team. 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 (follow the instructions in Section 5.5, Step 8). 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 a SNOW (YourIT) ticket on behalf of the user to have the duplicate profile with the least amount of data (e.g. menus, keys, person class, etc.) disused 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.	<ol style="list-style-type: none"> 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. A non-standard Service Section value came from local VistA profile. Keystroke errors in WebVRAM VistA Profile parameters. 	<ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> Role: Non-Clinical User / XUSERTOOLS Role: Physician User / PX PCE CLINICIAN MENU 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. Replace Service Section with MEDICAL SERVICE unless the user is with a CPAC or Office of Community Care (OCC) Business Unit. 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.	<p>User must contact local IT:</p> <ol style="list-style-type: none"> 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.

<p>8.</p>	<p>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.</p>	<ol style="list-style-type: none"> 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. 	<ol style="list-style-type: none"> 1. Add correct User Class and Person Class values in WebVRAM profile. Suggested values for Physician (values for other clinical providers will vary): <ol style="list-style-type: none"> 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 to the right of the Person Class field, remove the expiration date of the Person Class shown in the new window, and click 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.	<ol style="list-style-type: none"> 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. 	<ol style="list-style-type: none"> 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 Social Security Number (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.
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	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.

Issue #	Issue	Cause	Resolution
		creating the WebVRAM user profile.	
12.	User logs out of WebVRAM and is returned to the Terms/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.
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.

Issue #	Issue	Cause	Resolution
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.	See Section 5.7.14 .
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 (see Section 5.10). 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. See Section 5.2 , step 6 (Primary Menu).
19.	User receives "File is in an untrusted location " error when launching Reflection from WebVRAM.	The "Open files only from trusted locations" box is checked in Reflection. This is an optional setting that needs to be disabled.	Have the user open Reflection Workspace on their workstation, access the Settings for the application, select Specify Trusted Locations then <u>uncheck</u> the Open files only from trusted locations box.
20.	Library not registered error when launching CPRS at remote site.	A DLL file is not installed on the user's workstation that is required by a Class 3 product that is not used at all VAMC sites.	The user must log a help desk ticket and request installation of the CPRS Photo DLL on their workstation. Once installed, this error will not occur.

7.2 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 5.5 (Existing User with Same Name in Home Vista and Other Vista Data Anomalies), Step 8 KPA CPAC NSD MENU.

7.3 Duplicate Account Reconciliation

The Duplicate Account Reconciliation feature is an enhancement that will check for duplicate Vista profiles at a remote Vista site that may interfere with a user's attempt to synchronize, add, or update Vista profile data at the remote site.

7.3.1 Detecting Vista User Account Conflicts – Block Site Access

During user provisioning, the Business Unit Administrator may add individual or multiple Vista sites to a user's profile, or the Business Unit Administrator may click the **Add all sites** button. When a site is added, WebVRAM will detect if there is a duplicate account conflict at the newly added remote Vista site(s). The Vista Sites Screen will display an **Edit Site** button for each site where WebVRAM detects duplicate profiles, and the remote sites with duplicate Vista user profiles will not be available for user access.

Figure 39: Vista Sites Screen with Edit Site Button

WebVRAM Administration Module

User: [Edit User] [Disable User] [View Logs]

Vista Sites [Add all sites] [Remove all sites]

Q

Station #	Station Name	VISION	State	Test Site?	Action
821B	Azure 821 B:vr2test	255	HI	Yes	[Add Site]
459	Azure 821 A:vr1test [DEV HOME VISTA]	255	OR	Yes	[Add Site]
820B	Azure 820 B:vr2test	255	CA	Yes	[Add Site]
820A	Azure 820 A:vr1test	255	AZ	Yes	[Add Site]
402	Togus TEST	99	MN	No	[Edit Site] [Remove Site]
668	Spokane TEST	99	WA	Yes	[Add Site]
648	Portland TEST	99	OR	Yes	[Add Site]
618	Minneapolis TEST	99	MN	No	[Edit Site] [Remove Site]
540	Clarksburg TEST	99	CA	No	[Edit Site] [Remove Site]
517	Beckley TEST	99	WV	No	[Remove Site]
101	TEST	90	HI	Yes	[Add Site]

The VistA Sites Screen will show an **Edit Site** button to identify sites where user access is blocked due to potential duplicate VistA accounts; these sites are not added to the user's VistA Sites screen in WebVRAM.

7.3.2 Detecting VistA User Account Conflicts – User Profile VistA Sites

From the User Profile Screen, the VistA Sites section lists the VistA sites assigned to the WebVRAM user. The section will display the site names with a RED triangular icon to the left of the site name to indicate the status of a VistA site with an active duplicate account issue.

Figure 40: User Profile VistA Sites Section with Duplicate Account Issues



7.3.3 Viewing Duplicate Account Issues – Edit Site

From the User Profile Screen, the VistA Sites section lists the VistA sites assigned to the WebVRAM user. In this section, click on the **pencil icon** next to the site name to view duplicate account discrepancies detected by WebVRAM. The Edit Site Screen will appear.

Figure 41: User Profile VistA Sites Section with Pencil Icon to Edit Site



7.3.4 Duplicate Accounts – IEN Mismatch

The following is an example of a duplicate account issue due to Internal Entry Number (IEN) mismatch.

Figure 42: Edit Site Screen – IEN Mismatch

The screenshot shows a web interface titled "VistA Site: Clarksburg TEST". It contains a form with the following fields and values:

VistA Site: Clarksburg TEST	
Expected User IEN	123455
Date Duplicate Found	2023-03-17T19:58:43+00:00
Duplicate Data Dump	Expected User IEN: 123455. Actual User IEN: 1129647
<div><button>Update VistA Site</button><button>Cancel</button></div>	

The figure above displays a duplicate account issue detected at the “Clarksburg TEST” VistA site. The screen displays the **Expected User IEN** text field with the expected IEN value shown.

Date Duplicate Found is displayed.

Duplicate Data Dump lists the Expected User IEN and Actual User IEN:

- Expected User IEN: 123455
- Actual User IEN: 1129647

The screen includes buttons to **Update VistA Site** or **Cancel**.

7.3.5 Resolving the IEN Mismatch

To correct this issue, enter the Actual User IEN number from the error message (e.g. 1129647) into the **Expected User IEN** field at the top of the error message and click the **Update VistA Site** button.



CAUTION: Only edit the Expected User IEN when attempting to resolve a duplicate account issue. Changing this value incorrectly will break the user’s account on the remote VistA system.

7.3.6 Duplicate Accounts – SSN Conflict

The following is an example of a duplicate account issue due to an SSN already assigned to another user. The **Expected User IEN** field is blank, and the SSN conflict message is

displayed. Open a SNOW (YourIT) ticket and assign it to the user's local IT group to resolve the conflict.

Figure 43: Edit Site Screen – SSN Conflict

The screenshot shows a web interface titled "VistA Site: Togus TEST". It contains a form with the following elements:

- Expected User IEN**: A text input field that is currently blank.
- Date Duplicate Found**: A label next to the date "2021-03-02T20:28:15+00:00".
- Duplicate Data Dump**: A label next to a message: "There is a conflict with your existing SSN which is already assigned to the user IEN205425".
- Buttons**: Two buttons at the bottom right, "Update VistA Site" (in blue) and "Cancel" (in white).

The figure above displays a duplicate account issue detected at the "Togus TEST" VistA site. The screen displays the **Expected User IEN** text field as blank.

Date Duplicate Found is displayed.

Duplicate Data Dump displays the message, "**There is a conflict with your existing SSN which is already assigned to the user IEN205425.**"

The screen includes buttons to **Update VistA Site** or **Cancel**.

7.3.7 Resolving the SSN Conflict

To correct this issue, open a SNOW (YourIT) ticket and assign it to the user's local IT group. See Section 7.3.14 (Resolving Duplicate Account Issues) below.

After the conflict is resolved, contact the user and ask them to confirm they are able to connect to the remote VistA site.

7.3.8 Duplicate Accounts – Same Access Code

The following is an example of a duplicate account issue where the user has the same Access Code as another user with a different IEN. The **Expected User IEN** field is blank,

and the “same access code” error message is displayed. Open a SNOW (YourIT) ticket and assign it to the user’s local IT group to resolve this issue.

Figure 44: Edit Site Screen – Same Access Code

The screenshot shows a web interface for editing a VistA site. The title is "VistA Site: Minneapolis TEST". Below the title is a form with the following fields and content:

Expected User IEN	<input type="text"/>
Date Duplicate Found	2021-03-03T13:51:28+00:00
Duplicate Data Dump	User IEN 45102 has the same access code as User IEN 438884
<div><button>Update VistA Site</button><button>Cancel</button></div>	

The figure above displays a duplicate account issue detected at the “Minneapolis TEST” VistA site. The screen displays the **Expected User IEN** text field as blank.

Date Duplicate Found is displayed.

Duplicate Data Dump displays the message, “**User IEN 45102 has the same access code as User IEN 438884.**”

The screen includes buttons to **Update VistA Site** or **Cancel**.

7.3.9 Resolving the Same Access Code Issue

Since all VistA systems use the same algorithm to generate Access Codes and there is no central software to create and store Access Codes, occasionally the same code is assigned to more than one user at more than one site. If this error message is displayed, open a SNOW (YourIT) ticket to request the user’s Access Code be reset in their Home VistA profile. The user will also need to change their new temporary Verify Code to a code of their choosing once a new Access Code has been assigned. After the new Access and Verify Codes have been established, ask the user to login to WebVRAM and confirm they are now able to connect to the remote VistA site.

i NOTE: If, after the user’s Access Code is changed, the user’s connection attempt to the same remote site still fails, edit that site in the user’s profile and type the **Actual User IEN** number shown in the Duplicate Data Dump message into the **Expected User IEN** field, then click the **Update VistA Site** button as shown in Figure 42 above. After this change is made, have the user reconnect to the remote site, and the Access Code conflict should be resolved resulting in a successful connection attempt.

7.3.10 Duplicate Accounts – NPI Number Already Assigned

When a provider connects to a remote site where they have an existing account, and that account has their National Provider Identifier (NPI) number assigned to it, that account usually does not have the provider's SSN assigned to it. In this case, when WebVRAM makes a connection to this remote site, it passes the NPI and SSN with the request to update or add a VistA account profile to that site. VistA cannot find the same SSN in the existing account and creates a duplicate account with the new WebVRAM profile request. However, the synchronization fails because VistA will only allow the NPI to belong to one account, and it terminates the connection as it cannot accept the NPI and assign it to the new WebVRAM account. A partial WebVRAM account profile is created, but the connection to the remote site will continue to fail.

The following is an example of a duplicate account issue where the user's NPI is already assigned to another VistA account with a different IEN. The **Expected User IEN** field is blank, and the "NPI conflict" error message is displayed. Open a SNOW (YourIT) ticket and assign it to the user's local IT group to resolve this issue.

Figure 45: Edit Site Screen – NPI Already Assigned

The screenshot shows a web interface titled "VistA Site: Northern Indiana HCS". It contains a form with the following elements:

- Expected User IEN**: A text input field that is currently blank.
- Date Duplicate Found**: A label next to the date "2021-04-13T16:51:20+00:00".
- Duplicate Data Dump**: A label next to a message: "There is a conflict with your existing NPI (XXXXXXXXXX) which is already assigned to the user IEN 387787".
- Buttons**: Two buttons at the bottom right, "Update VistA Site" (in blue) and "Cancel" (in white).

The figure above displays a duplicate account issue detected at the "Northern Indiana HCS" VistA site. The screen displays the **Expected User IEN** text field as blank.

Date Duplicate Found is displayed.

Duplicate Data Dump displays the message, "There is a conflict with your existing NPI (XXXXXXXXXX) which is already assigned to the user IEN 387787."

The screen includes buttons to **Update VistA Site** or **Cancel**.

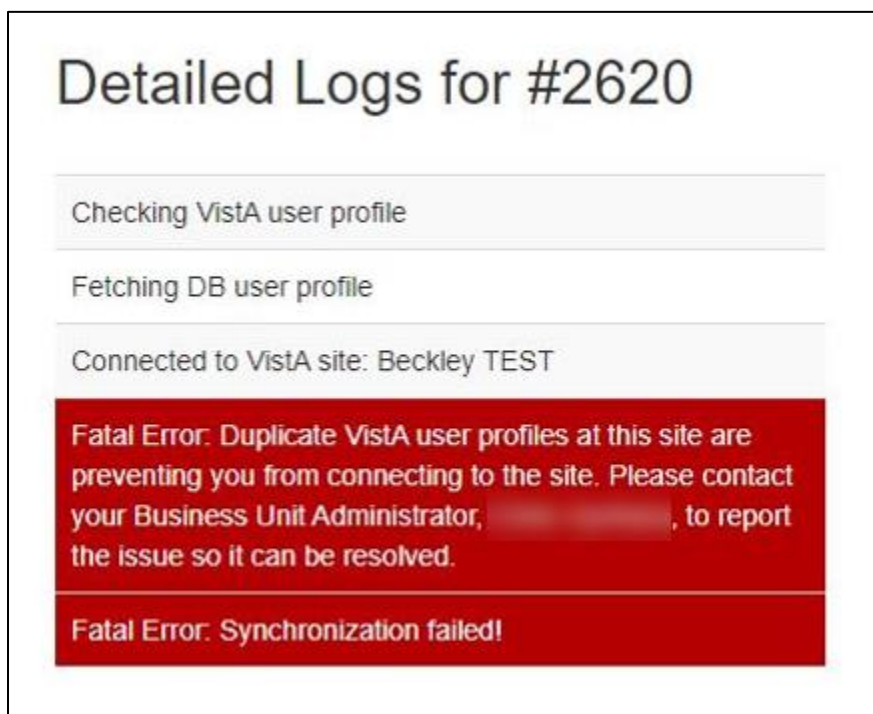
7.3.11 Resolving the NPI Number Already Assigned Issue

To resolve this issue, follow the process outlined in [Section 7.3.14, Step 7a](#), below. Open a SNOW (YourIT) ticket to have local IT verify that the VistA profile containing the NPI also contains the same SSN in the user's Home VistA profile. If it does not, request that local IT add or update the SSN in the VistA profile containing the NPI to match the SSN from the user's Home VistA profile. Request that all other duplicate profiles be disused or terminated.

7.3.12 Duplicate Account Issue – Detailed Logs – Error Message

When a user fails to connect to a remote VistA site due to a duplicate account issue, the error is captured in the user's Detailed Logs (see [Section 5.11 View User's Log](#)). Example logs are included below.

Figure 46: Detailed Logs – Failed Synchronization Due to Duplicate Account

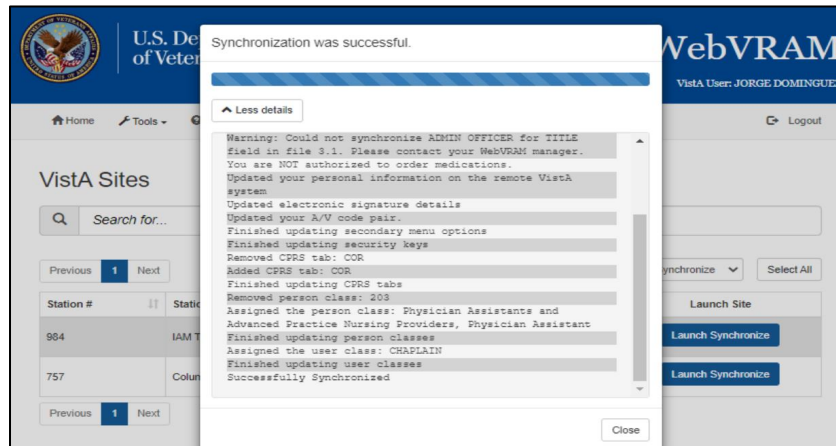


This synchronization failure error indicates a duplicate VistA account is detected at the remote site with a message instructing the user to “contact your Business Unit Administrator.”

7.3.13 Synchronization Successful Screen

When a user presses the Synchronize button, a successful synchronization will return a message stating the “Synchronization was successful” as shown below:

Figure 45: Synchronization was successful – VistA Sites screen



7.3.14 Resolving Duplicate Account Issues

Some duplicate account issues may require creating a SNOW (YourIT) ticket to get assistance from local IT staff at the remote site. Follow the steps below to gather information about duplicate accounts using VistA (see example screen capture below).

1. Using WebVRAM, Launch Reflection connection to the remote site and perform a user inquiry to view the duplicate profiles. Once logged into VistA at the remote site, enter the command **CPAC** at the first menu prompt.
2. Enter **USER** at the next menu prompt.
3. At the "Select NEW PERSON NAME" prompt, enter the **user's last name followed by a comma, and the first 2 letters of their first name**. Multiple selections of user profiles should be displayed.
4. Enter the **number** of the first duplicate profile in the list you are provided and view the profile.
5. After entering past the last line of the profile, the "Select NEW PERSON NAME" prompt will reappear. Press the **<up arrow>** key until the lastname,partial first name entry you made earlier comes up, then press **<Enter>**. View the profile detail for the second profile in the list by selecting the number next to it.
6. If there are more than two profiles, repeat step 5 for each additional profile.

Example VistA User Inquiry to Identify Duplicate Profiles

Good afternoon [LAST NAME, FIRST NAME]
You last signed on today at 13:57

Select PCE Clinician Menu <TEST ACCOUNT> Option: **CPAC** NSD Menu

Select CPAC NSD Menu <TEST ACCOUNT> Option: **USER** Inquiry

Select NEW PERSON NAME: **DUCK,DON**

1 DUCK,DONALD IT SPECIALIST
2 DUCK,DONALD R
3 DUCK,DONELLE
CHOOSE 1-3: **1** DUCK,DONALD IT SPECIALIST

DEVICE: **<Enter>** HOME(CRT) Right Margin: 80// **<Enter>**
DUCK,DONALD (#1107032)

Service Section : OIT

ATTRIBUTES

CreatorMOUSE, MINNIE Date entered.....Mar 11, 2021
Mult Sign-on ... Fileman codes@
Time-out Type-ahead
TitleIT SPECIALIST Office Phone4104414058
Auto-MenuYES, MENUS GENERATED Voice Pager
Last Sign-on ...Mar 11, 2021 Digital Pager
Has a E-SIG ...Yes Write Med's
NPI 1334374398 Taxonomy 207R00000X
Person Class: Allopathic and Osteopathic Physicians
Internal Medicine

Primary Menu: EVE Systems Manager Menu

Secondary Menu(s)

[DVBA CAPRI GUI] Capri GUI (Broker)
[MAG WINDOWS] All MAG* RPC's
[WEBG WEBVRAM GUI] WEBG WEBVRAM GUI

Keys Held

MAGDISPCLIN XUPROGMODE

Patient Selection

Restrict?:
OE/RR List:

CPRS Access Tabs

CPRS Parameter info (User Specific)

No Mailbox for this user. <Enter>

Select NEW PERSON NAME: <Up Arrow> <Enter>

NOTE: Pressing the up arrow key once brings "1" into the command line.
Pressing it again brings "DUCK,DON" into the command line.

1 DUCK,DONALD IT SPECIALIST
2 DUCK,DONALD R
3 DUCK,DONELLE
CHOOSE 1-3: 2 DUCK,DONALD IT SPECIALIST

DEVICE: <Enter> HOME(CRT) Right Margin: 80// <Enter>
DUCK,DONALD (#952389)

Service Section : OIT

Creator Date entered.....Jul 22, 2020
A/C changed V/C changed

Mult Sign-on ... Fileman codes
Time-out Type-ahead
TitleX*OTHER Office Phone
Auto-Menu Room
Voice Pager
Last Sign-on ...Jan 27, 2021 Digital Pager
Has a E-SIGNo Write Med's
Person Class:
NPI

Primary Menu:
Secondary Menu(s)

[JLV WEB SERVICES] JLV GUI Menu Option

Keys Held

Patient Selection

Restrict?:
OE/RR List:

CPRS Access Tabs

CPRS Parameter info (User Specific)

No Mailbox for this user.

7. For each profile viewed using the steps above:
 - a. If the user is a provider:
 - i. Identify which profile contains the provider's **NPI**. Note the VistA number to the right of the user's name (in parenthesis) for this profile.
 - ii. Have local IT verify that the SSN of this profile contains the same SSN in the user's Home VistA profile. If it does not, request that local IT add or update the SSN in this profile to match the SSN from the user's Home VistA profile. Request that all other duplicate profiles be dis-used or terminated.
 - b. If the user is NOT a provider:
 - i. Request that local IT dis-user/terminate all profiles that contain the least amount of data; these profiles will not contain all menus or keys and may include an incorrect Person Class (if applicable), the wrong primary menu, etc.
 - ii. Ask local IT to confirm that the remaining "active" profile contains the same SSN as the SSN in the user's Home VistA profile.
8. When step 7 is done, unblock the site for the user in WebVRAM and ask them to reconnect to that site using the application.
9. If, after executing all steps above, the user still has an issue connecting to the remote site, **use SNOW (YourIT) to submit an Incident to ESD** for the issue and assign it to the **WebVRAM** group.
 - a. Re-block the remote site for user access in WebVRAM.
 - b. Notify the user via email that the issue is not yet resolved yet and that an ESD ticket has been opened requesting assistance from the WebVRAM team.
 - c. Once the ESD ticket is resolved, unblock the site in WebVRAM for the user and contact the user with a request to retry access at that site using the application.
 - d. Repeat step 9 if the user still has connection issues at the remote site.

7.3.15 VistA Sites with Sub-Divisions sites

When creating an account for a new user, WebVRAM will not allow the assignment of a Sub Division site as the Home VistA. The Business Unit Administrator needs to select the Primary VistA as the user's Home VistA during account creation.

Example: WebVRAM will not allow Lincoln, Nebraska, station 636A5 to be selected as the user's Home VistA. The Business Unit Admin needs to select Central Plains HCS (station 636) as the user's Home VistA.

For user's who already have a Sub Division set as the Home VistA, WebVRAM will display the following warning during synchronization: "VistA Station XXXXX is a division of the Home VistA Station XXX in file #4.014. Azure 821 A:vr1test (DEV HOME VISTA) Division profile not updated to prevent change to home VistA user profile." (This would only happen when syncing between a Home VistA child division to the parent or a Home VistA parent to a child division. This warning doesn't prevent a user from launching Reflections or CPRS, it will only display the warning. Syncing to a remote that is not a division will continue to work as expected.)

If this warning is displayed, the user needs to contact their Business Unit Admin and request that the Home VistA field in their user profile be changed to the Primary VistA System. In the previous example, Lincoln, Nebraska, station 636A5, would be replaced with Central Plans HCS, station 636, by the Business Unit Admin.

Appendix A – 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 7: Acronyms and Abbreviations

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

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

Appendix B – Access Review Audit Memo

WebVRAM General Account Review

Department of Veterans Affairs

Date: <enter today's date>

From: <enter your name>

WebVRAM Business Unit:<enter the name of your business unit>

Subj: Quarterly Access Review

To: Information System Security Officer

A review of active WebVRAM users under my Business Unit has been completed. Users who have left the VA or have changed positions to one that no longer requires the use of WebVRAM have been identified and their WebVRAM user profile has been disabled.

A review of menus and key assignments for all WebVRAM users under my Business Unit has also been completed. The necessary revisions have been made and current assignments are appropriate for each employee's job responsibilities with separation of duties and least privilege taken into consideration.
