

Web Veterans Health Information Systems and Technology Architecture Remote Access Management (WebVRAM) Deployment, Installation, Back-Out, and Rollback Guide (DIBRG)



December 2024

Department of Veterans Affairs

Office of Information and Technology

Revision History

Date	Document Version	Description	Author
12/14/2024	5.12	Initial document publication for WebVRAM 13.0	WebVRAM PMO Team
11/29/2024	5.11	Initial document publication for WebVRAM 12.0.2	WebVRAM PMO Team
10/4/2024	5.10	Initial document publication for WebVRAM 12.0.1	WebVRAM PMO Team
9/28/2024	5.9	Initial document publication for WebVRAM 12.0	WebVRAM PMO Team
9/24/2024	5.8	Initial document publication for WebVRAM 11.0.6	WebVRAM PMO Team
7/20/2024	5.7	Initial document publication for WebVRAM 11.0.5	WebVRAM PMO Team
7/13/2024	5.6	Initial document publication for WebVRAM Release 11.0.3	WebVRAM PMO Team
6/29/2024	5.5	Initial document publication for WebVRAM Release 11.0.2	WebVRAM PMO Team
5/24/2024	5.4	Initial document publication for WebVRAM Release 11.0.1	WebVRAM PMO Team
5/4/2024	5.3	Initial document publication for WebVRAM Release 11 Associated to VistA Information Patch WEBG*3*20.	WebVRAM PMO Team
4/12/2024	5.3	Initial document publication for WebVRAM Release 10.0.3	WebVRAM PMO Team
4/8/2024	5.2	Initial document publication for WebVRAM Release 10.0.2	WebVRAM PMO Team
3/12/2024	5.1	Initial document publication for WebVRAM Release 10.0.1	WebVRAM PMO Team
3/2/2024	5.0	Initial document publication for WebVRAM Release 10.0. Associated to VistA Information Patch WEBG*3*19.	WebVRAM PMO Team

Date	Document Version	Description	Author
12/16/2023	4.1	Initial document publication for WebVRAM Release 9.0. Associated to VistA Information Patch WEBG*3*16.	WebVRAM PMO Team
11/6/2023	4.0	Initial document publication for WebVRAM Release WEBG*3*17. Updated User Story list in Section 1. , No GUI changes were made, and no changes will be visible to users in this release. Implementation and Rollback are not impacted. References to Cerner replaced.	WebVRAM PMO Team
08/9/2023	3.1	Initial document publication for WebVRAM Release 8.0, associated with VistA Informational Patch WEBG*3*15.	WebVRAM PMO Team
04/1/2023	3.0	Initial document publication for WebVRAM Release 7.0, associated with VistA Informational Patch WEBG*3*11.	WebVRAM PMO Team
09/21/2022	2.1	Initial document publication for WebVRAM Release 6.0, associated with VistA Informational Patch WEBG*3*9. <ul style="list-style-type: none"> • Updated for 6.0. • Updated Table 4. • Updated Table 7. Updated Table 9	WebVRAM PMO Team
05/17/2022	2.0	Initial document publication for WebVRAM Release 5.0, associated with VistA Informational Patch WEBG*3*8. <ul style="list-style-type: none"> • Updated for 5.0. • Updated Figure 1 and Figure 2. • Updated Section 4.5 Installation Scripts updated.	WebVRAM PMO Team
04/12/2022	1.1	Initial document publication for WebVRAM Release 4.1, associated with VistA Informational Patch WEBG*3*7.	WebVRAM PMO Team

Date	Document Version	Description	Author
		Updates for 4.1.	
12/7/2021	1.0	<p>Initial document publication for WebVRAM Release 4.0, associated with VistA Informational Patch WEBG*3*5. Notable changes from WebVRAM 3.0 Deployment, Installation, Back-Out, and Rollback Guide (DIBRG):</p> <ul style="list-style-type: none"> • Updated Section 1 (Introduction). • Updated Table 2 (Deployment, Installation, Back-out, and Rollback Roles and Responsibilities). • Updated Section 3.1 (Timeline). • Removed references to Fee Basis Claims System (FBCS) from Table 5 (High-level Milestones) and Section 3.2.1 [Deployment Topology (Targeted Architecture)]. • Replaced Figure 1 (WebVRAM Physical Architecture and Environments). • Updated Section 3.3.3 (Software). • Updated verbiage in Section 3.3.4 (Communications). • Replaced “VA VIP Triad” with “VA PM and Business Owner” in Table 9 (Team Support Information/Role). • Updated Section 3.3.5 (Deployment/Installation/Back-Out Checklist). • Updated Section 4.2 (Platform Installation and Preparation). • Added Section 4.11 (CPRS Version Installation on Shared Directory). 	Office of Information and Technology (OIT) Development, Security, and Operations (DevSecOps) Software Product Management (SPM) WebVRAM Team

Date	Document Version	Description	Author
		<ul style="list-style-type: none">• Updated Section 5.2.2 (User Acceptance Testing).• Updated Section 5.4 (Back-Out Risks).	

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Guide (DIBRG) for new products going into the Veteran’s Affairs Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect particulars of these procedures at a single or at multiple locations.

Table of Contents

1. Introduction	1
1.1. Purpose	2
1.2. Dependencies	2
1.3. Constraints	3
2. Roles and Responsibilities	4
3. Deployment	6
3.1. Timeline	7
3.2. Site Readiness Assessment	8
3.2.1. Deployment Topology (Targeted Architecture)	9
3.2.2. Site Information (Locations, Deployment Recipients)	12
3.2.3. Site Preparation	12
3.3. Resources	12
3.3.1. Facility Specifics	12
3.3.2. Hardware	13
3.3.3. Software	13
3.3.4. Communications	14
3.3.5. Deployment/Installation/Back-Out Checklist	15
4. Installation	15
4.1. Pre-installation and System Requirements	16
4.1.1. VistA Patch Installation	16
4.2. Platform Installation and Preparation	16
4.3. Database Creation	16
4.4. Installation Scripts	16
4.5. Cron Scripts	16
4.6. Access Requirements and Skills Needed for the Installation	17
4.7. Installation Procedure	17
4.8. Installation Verification Procedure	17
4.9. System Configuration	17
4.10. Database Tuning	18
4.11. CPRS Version Installation on Shared Directory	18
5. Back-Out Procedure	18
5.1. Back-Out Strategy	19
5.2. Back-Out Considerations	19
5.2.1. Load Testing	19
5.2.2. User Acceptance Testing	20
5.3. Back-Out Criteria	20

5.4. Back-Out Risks	20
5.5. Authority for Back-Out	20
5.6. Back-Out Procedure	20
5.7. Back-Out Verification Procedure	21
6. Rollback Procedure	21
6.1. Rollback Considerations	21
6.2. Rollback Criteria	21
6.3. Rollback Risks	21
6.4. Authority for Rollback	22
6.5. Rollback Procedure	22
6.6. Rollback Verification Procedure	22

List of Figures

Figure 1: WebVRAM Physical Architecture and Environments.....	9
Figure 2: WebVRAM Single Production String.....	18
Figure 3: WebVRAM Home Page.....	21

List of Tables

Table 1: Release Contents.....	1
Table 2: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities	4
Table 3: General Roles and Responsibilities.....	5
Table 4: Code Deployment Responsibilities.....	6
Table 5: High-level Milestones	7
Table 6: Facility-specific Features	12
Table 7: Hardware Specifications.....	13
Table 8: Software Specifications.....	13
Table 9: Team Support Information/Role.....	14
Table 10: Deployment/Installation/Back-out Checklist	15

1. Introduction

This document describes how to deploy and install the Web VistA Remote Access Management (WebVRAM) product, as well as how to back-out the product and rollback to a previous version or data set. This document is a companion to the project charter and management plan for this effort.

WebVRAM Release 13.0 Content:

These software changes listed below, include defect remediations. These along with a general regression test of the application will be validated during this Initial Operating Capabilities (IOC) testing cycle.

Table 1: Release Contents

Jira No.	Type	Description
WEB-5832	Initiative	WebVRAM R13.0
WEB-4571	Epic	BU Director Ack Phase 1
WEB-8023	Epic	BU Director Ack Phase 2
WEB-8024	Epic	Remote Site Refresh Phase 1
WEB-8025	Epic	Upgrade ASP.NET Core MVC
WEB-4163	Story	Upgrade ASP.NET Core MVC to the newest version before November 12, 2024
WEB-5010	Story	Business Unit Director Acknowledgement - Email Reminders
WEB-5011	Story	Business Unit Director Acknowledgement - Report
WEB-5208	Story	Enhancement: WebVRAM System Access Report - Create a new role for WebVRAM - WebVRAM_Product_Owner
WEB-5597	Story	WebVRAM should not change the termination date in VistA user profiles
WEB-5599	Story	Keep the termination date at remote VistAs synchronized with the termination date at the home VistA
WEB-5600	Story	WebVRAM needs to refresh the last login date at all remote VistA sites when a user logs into WebVRAM
WEB-5605	Story	Remote Site Refresh VET-HOME Updates
WEB-5607	Story	Remote Site Refresh Site List Page Column Changes
WEB-7968	Story	WebVRAM GitHub CodeQL Implementation in GHES
WEB-8245	Story	WebVRAM GitHub CodeQL Implementation in GHES - Part 2
WEB-4932	Bug	PROD: When selecting between A/V and PIV login method, page display of Message of the Day box inconsistent
WEB-5724	Bug	After Removing BU Admins from a BU, screen fails to refresh correctly.
WEB-5788	Bug	DEV / Expected error message not being displayed in the "Login-IAM" page
WEB-6073	Bug	Edit Business Unit: WebVRAM should not allow addition of BUA with disabled account

WEB-6074	Bug	First time login to WebVRAM by New Users: Update eSignature Code - window not closing
WEB-6670	Bug	Users who have never logged into WebVRAM need to be disabled after 30 days of inactivity by the automated daily process.
WEB-7616	Bug	Create new BU in PREPROD - Error condition while creating new BU

1.1. Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the WebVRAM solution, will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2. Dependencies

Dependencies include:

- Secure Shell (SSH) communications protocol is required at regional VistA systems or individual VistA instances where the application is intended to be used.
- VistA sites must support use of Remote Procedure Call (RPC) Broker v1.1 component.
- Successful use of WebVRAM to access remote VistA systems requires:
 - Remote VistA system must be accessible via VA Wide Area Network (WAN) resources.
 - Implementation of Local Security Keys must be communicated and incorporated into the WebVRAM user profile where impact to assigned menus or options exist.
 - Remote VistA system configuration changes impacting connectivity (i.e. port, protocol, initial logon prompt) must be communicated and incorporated into the WebVRAM system USER TABLE.
 - Remote application entry must be configured in the remote VistA system.
 - Specific WebVRAM VistA Security Keys must be stored in the remote VistA system.
- Synchronization of the User Account Profile is required for WebVRAM to function.
- Synchronization of User Account credentials is required for VistA Graphical User Interface (GUI) Application usage by WebVRAM users.

- Hypertext Transfer Protocol Secure (HTTPS) is used by WebVRAM to launch user connections to external applications by directing the user to the Uniform Resource Locator (URL) specific to the applications.

1.3. Constraints

There are no additional constraints to this project.

2. Roles and Responsibilities

Table 2: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

ID	Team	Phase / Role	Tasks
1	Project Team and Development Team	Deployment	Plan and schedule deployment (including orchestration with vendors).
2	Development Team	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.
3	Enterprise Operations (EO)	Deployment	Test for operational readiness.
4	Development Team	Deployment	Execute deployment.
5	Development Team	Installation	Plan and schedule installation.
6	Project Team/Hosting Team	Installation	Ensure Authority to Operate and that certificate authority security documentation is in place.
7	Development Team	Back-out	Confirm availability of back-out instructions and back-out strategy (the criteria that trigger a back-out).
8	Enterprise Support Desk (ESD)/Development Team	Post Deployment	Provide hardware, software and system support.

This section describes the teams who perform the steps described in this plan. Representatives from the teams listed in the following table perform deployment and

installation activities. This phase begins after the solution design (including deployment topology) is complete. Design activities are not included in this phase.

Table 3: General Roles and Responsibilities

Team	Tasks / Responsibilities
ESD Team	<ul style="list-style-type: none"> • Receive and process incoming incidents via Service Now Ticket. • Determine incident types and capture all relevant incident data. • Create developer user accounts. • Troubleshoot and resolve basic issues.
VA Project Team	<ul style="list-style-type: none"> • Liaison between the Development Team and the ESD Team. • Facilitate deployment and issue resolution. • Identify and submit issues to the VA Product Manager.
WebVRAM Development Team	<ul style="list-style-type: none"> • Develop and deploy the application between environments. • Provide Tier 3 support for application issues. • Identify and submit issues to the VA Product Manager.

Table 4: Code Deployment Responsibilities

Team	Phase	Role
WebVRAM Development Team	Planning	<ul style="list-style-type: none"> Finalize development increment and code compilation instructions. Provide listing of developer accounts.
WebVRAM Project Team	Planning	<ul style="list-style-type: none"> Schedule Software Quality Assurance (SQA) and Initial Operating Capability (IOC) testers and support all aspects of IOC Testing preparation.
WebVRAM Development Team	Prepare for Deployment	<ul style="list-style-type: none"> Freeze all development activities. Request secure and technical code reviews. Resolve internal Quality Assurance testing defects/issues and IOC Testing defects/issues.
WebVRAM Project Team	Execute Deployment	<ul style="list-style-type: none"> Coordinate deployment support by maintaining the bridge and managing all involved stakeholders. Conduct IOC Testing activities.
WebVRAM Development Team	Execute Deployment	<ul style="list-style-type: none"> Work with Project Team to resolve issues. Deploy final increment version from DEVTEST to PREPROD. Deploy final version of code from PREPROD to PROD.
WebVRAM Project Team	Validation and Go-Live	<ul style="list-style-type: none"> Validate that the PROD environment functions as expected.
Development Team	Validation and Go-Live	<ul style="list-style-type: none"> Execute rollback, if necessary. Provide Tier 3 support as required.

3. Deployment

The deployment is planned as a single rollout.

This section provides the schedule and milestones for the deployment.

This DIBRG identifies processes and procedures to promote the WebVRAM system into the Production environment. The WebVRAM system is web-based and is deployed using

files containing configuration information rather than code package objects moved directly from one environment to another.

3.1. Timeline

The deployment and installation will run for approximately one day, as depicted in the master deployment schedule for WebVRAM.

The high-level project schedule, as reported in VA Product Line Accountability and Reporting System (VA PARS), is included below:

Table 5: High-level Milestones

Milestones	Target Date
WebVRAM Project Initiation	10/26/2018
Increment 1 – VA Enterprise Cloud Setup/System Integration Testing	1/22/2019
Increment 2 – WebVRAM Single Sign-on to Vista	4/4/2019
Increment 3 – Redesign of WebVRAM	6/28/2019
Increment 4 – IOC and Production Release (Redesign)	9/27/2019
Increment 5 – Two Factor Authentication (2FA) Development	12/18/2019
Increment 6 – Production Hot Fix	3/18/2020
Increment 7 – Reflection Macro Software Development, Consolidated Patient Account Center (CPAC) Migration, and Defect Resolution	6/17/2020
Increment 8 – Defects, Platform Upgrade and Team Foundation Server (TFS) Migration to GitHub	9/16/2020
Increment 9 – WebVRAM Integration with Cerner Features	12/16/2020
Increment 10 – Information Sys Security Officer Enhancement/Security Key Notification and Two Factor Authentication	3/17/2021
Increment 11 – Information Sys Security Officer Enhancement/Security Key Notification and 2FA Part 2 (Disabled Users Report)	6/16/2021
Increment 12 – Disabled User Report, 2FA, Support for Microsoft Edge, PASS Computerized Patient Record System Orders List	9/15/2021
Increment 14 – Implement Microsoft Edge Browser Support	12/15/2021
Increment 15 - Authentication and Security enhancements. Disabled User report enhancements, Cerner Migration Support.	3/16/2022

Milestones	Target Date
Increment 16 - Least Privileged Access (LPA), Pass CPRS Order LIST values to remote sites.	6/15/2022
Increment 17 - Retire IE11, User mgt Least Privileged Access Pass CPRS order list values Health Connect S/S.	9/14/2022
Increment 18 - Display Business Unit (BU) and BU Admin to regular users, Active Directory Data missing error message; Add new service section called "Veterans Integrated Service Network (VISN) 7 Network Clinical Resource Hub (CRH)"	12/14/2022
Increment 19 - Increment 19: Release 6.2 and 7.0 Features and Hotfixes	4/15/2023
Increment 20 - Increment 20: Updates for Release 7.0 and Release 8.0.	6/14/2023
Increment 21 - Increment 21: Updates for Releases 7.2, Release 8.0 and fixes.	9/13/2023
Increment 22 - Update for Release 8.0, Release 9.0, and hotfixes.	12/15/2023
Increment 23 – Updates for Release 9.0, Release 10.0, and hotfixes	3/15/2024
Increment 24 – Updates for Release 10.0, Release 11.0, 12.0 and hotfixes	6/15/2024
Increment 25 – Updates for Release 11.0, 12.0, 13.0 and hotfixes	9/13/2024
Increment 26 – Updates for Releases 13.0, 14.0, 15.0 and Hotfixes	12/13/2024

3.2. Site Readiness Assessment

This section discusses the locations that will receive the WebVRAM deployment. Topology determinations are made by the project architect and lead developer and vetted with the Strategic Technology Alignment Team (STAT) and Product Manager during the design phase as appropriate.

If applicable, IOC Testing arranged through a Memorandum of Understanding (MOU) with each testing site will be coordinated with the Area Manager and designated Vista Applications Division Supervisor. Site readiness will be assessed prior to and during IOC Testing in the site Pre-production and Production environments.

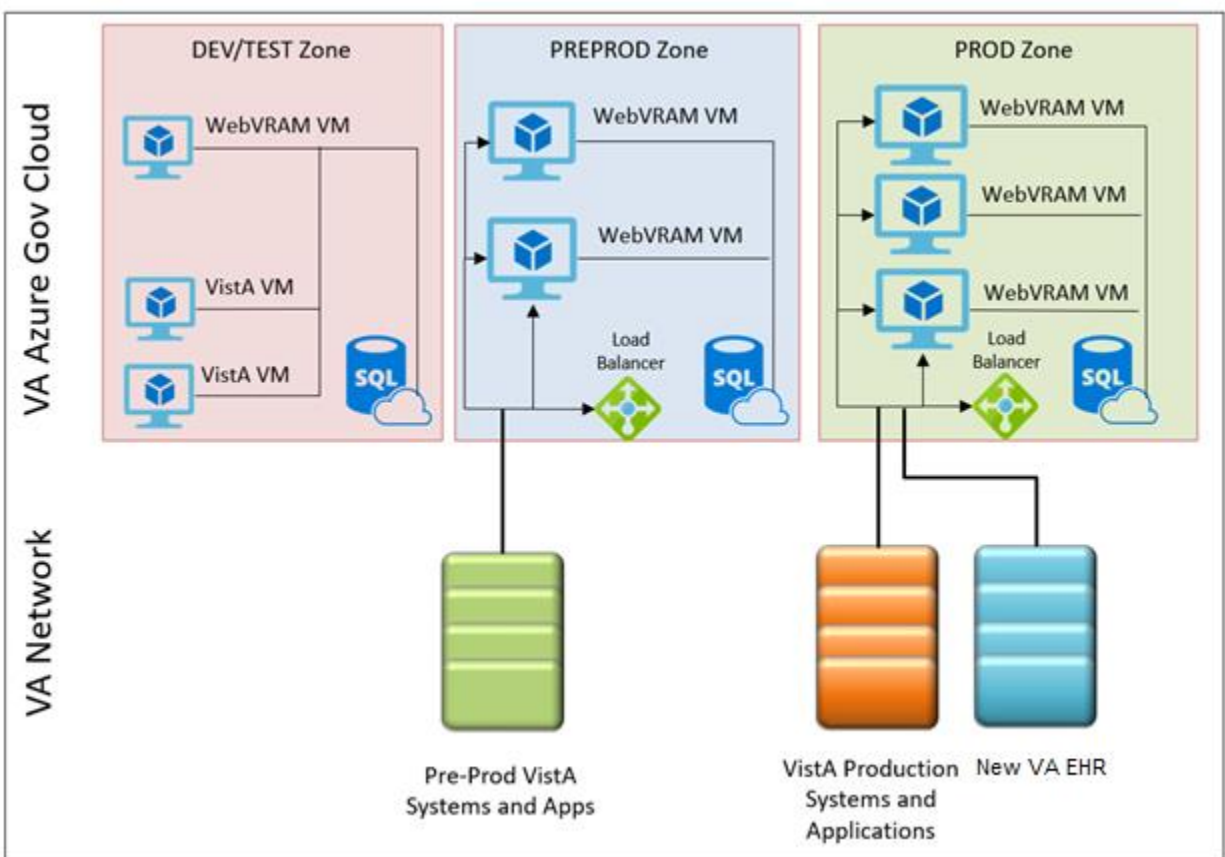
3.2.1. Deployment Topology (Targeted Architecture)

Deployment will be conducted through web client in a DEVTEST, Pre-production (PREPROD), and Production (PROD) environment administered by the Development Team.

The WebVRAM system is web-based and is deployed using files containing configuration information rather than code package objects moved directly from one environment to another.

Figure 1 outlines the physical architecture for deployment of the application from development through national release.

Figure 1: WebVRAM Physical Architecture and Environments



The WebVRAM Administrative Module (WAM) with a GUI front-end provides an automated method of obtaining business user profile information to populate the WebVRAM USER TABLE to create the WebVRAM user profile. The business stakeholders provide the user's basic information, which is used by the WAM to query the user's local VistA instance(s) to gather their VistA user profile.

NOTE: Provisioned users who routinely perform work at more than one VA location will have a WebVRAM user profile consisting of a superset of all authorized VistA menus and keys from all locations.

WebVRAM communicates within its internal DEVTEST, PREPROD, and PRODUCTION environments through Transmission Control Protocol (TCP) connections defined by specifically authorized Internet Protocol (IP) addresses and ports.

In the DEVTEST environment, Application Windows Operating System (OS) Virtual Machines (VMs) communicate with two Linux OS VMs, which host the four VistA database instances used for development and testing of the application. The application also communicates through a TCP/IP connection with its DEVTEST Structured Query Language SQL database. Connections to testers' VA workstations for application testing are initiated through instantiation of the WebVRAM DEVTEST URL. The tester's VistA user profile is fabricated to replicate the necessary VistA menus, keys, user/person class, and electronic signature code to fully test WebVRAM functionality. This "testing" user profile is stored in the WebVRAM USER TABLE on the DEVTEST SQL database. All tester Personally Identifiable Information (PII) data is fabricated and has no relation to the tester's actual demographic or personal data.

In the PREPROD environment, WebVRAM Windows OS application VMs communicate with IOC site Pre-production (Test) VistAs, Pre-production Computerized Patient Record System (CPRS) instances, and Pre-production VA's New Electronic Health Record (EHR) Electronic Health Record (VA's New EHR) instances to accommodate required Pre-production testing. All Transfer Control Protocol (TCP connections use authorized Internet Protocol (IP) and ports and are considered on-premises connections, as all applications and databases reside within the VA network. The application also communicates through a TCP/IP connection with its PREPROD SQL database. Connections to testers' VA workstations for application testing are initiated through instantiation of the WebVRAM PREPROD URL. The IOC tester's user profile is retrieved by the WebVRAM Pre-production application version, and the local tester's VistA profile data is pulled from the tester's IOC Pre-production VistA NEW PERSON FILE to create the WebVRAM user profile stored in the Pre-production WebVRAM USER TABLE.

When a user presents a PIV card, the Identity and Access Managements (IAM/Windows Active Directory (AD) Service confirms a user's current VA network access status to ensure complete user verification. When presenting Access and Verify codes at user login, the VistA Station ID Callback (STIC) Remote Procedure Call (RPC) verifies that the user has current, active VistA credentials and permissions. The WebVRAM application then retrieves the following data from the local VistA files listed for the user:

- 200 – NEW PERSON
- 19 – OPTION

- 19.1 – SECURITY KEY
- 201 – PRIMARY MENU OPTION
- 203 – SECONDARY MENU OPTIONS
- 51 – KEYS
- 53.1 – AUTHORIZED TO ORDER MEDS
- 9.2 – TERMINATION DATE
- 200.04 – MULTIPLE SIGN-ON
- 200.18 – AUTO SIGN-ON
- 7 – DISUSER
- 20.4 – ELECTRONIC SIGNATURE CODE
- 20.3 – SIGNATURE BLOCK TITLE
- 20.2 – SIGNATURE BLOCK PRINTED NAME
- PERSON CLASS
- USER CLASS
- 8 – TITLE
- SERVICE/SECTION
- DEGREE
- NATIONAL PROVIDER IDENTIFIER (NPI)
- NPI STATUS
- 200.1 – TIMED READ
 - If the existing visited site value < 900, the value is set to 900; otherwise, no action is taken.
 - Some business units have approval from WebVRAM's ISO, ISSO and Authorizing Official for TIMED READ greater than 900.
- 8989.5 – ORWOR TIMEOUT CHART
- 4 – INSTITUTION FILE
- 4.014 – INSTITUTION ASSOCIATIONS

The connections established between the WebVRAM PROD environment and VA Network Production Vista, CPRS, and VA's New EHR instances also utilize authorized TCP/IP connections through specified ports. The application communicates through a TCP/IP connection with its PROD SQL database. User login is facilitated through the

WebVRAM PROD URL. At user login, the user's VistA profile data is pulled from the user's local IOC Production VistA NEW PERSON fixed to create the WebVRAM user profile stored in the Production WebVRAM USER TABLE. If the user is directed by line management and authorized to perform work at more than one VistA on a daily or routine basis, each VistA instance is queried to create a superset of that user's VistA profile containing all menus, keys, user/person class and electronic signature code data. The user's "Home" VistA Access/Verify codes are kept in the WebVRAM user profile and passed to remote VistA systems the user is authorized to access.

All application-to-VistA communications will be facilitated through RPC Broker protocol. User-to-application connections utilize web protocol, in keeping with VA Enterprise Design Patterns.

3.2.2.Site Information (Locations, Deployment Recipients)

The WebVRAM system is web-based and is deployed using files containing configuration information rather than code package objects moved directly from one environment to another.

3.2.3.Site Preparation

For WebVRAM Release 4.1, both VistA patch WEBG*1*0 and WEBG*1*3 must be installed at all VistA sites. This was accomplished when WebVRAM 1.3 was nationally released; there should be no sites that still require the installation of these patches. The web application will sustain software changes and be deployed into the Production instances in the Azure Cloud. This release requires WEBG*3*13 and WEBG*3*17 to be installed at all VistA sites.

3.3. Resources

This section describes hardware, software, and facilities required for the WebVRAM deployment and installation.

3.3.1.Facility Specifics

WebVRAM will deploy on a cloud-hosted environment. There are six VistA patches from prior WebVRAM releases that should be installed at sites before installing this release.

Table 6: Facility-specific Features

Site	Space/Room	Features Needed	Other
IOC	Minimal	VistA Patch WEBG*1*0, WEBG*1*3, WEBG*3*11, WEBG*3*12, WEBG_3*13, and WEBG*3*21 patches installed in Pre-production accounts.	N/A

Site	Space/Room	Features Needed	Other
Enterprise VistA Sites	Minimal	VistA Patch WEBG*1*0, WEBG*1*3, WEBG*3*11, WEBG*3*12, WEBG*3*13, WEBG*3*17, and WEBG*3*21 patches installed in Production accounts.	N/A

3.3.2. Hardware

WebVRAM will be supported by the existing Azure cloud-hosted environments. See Section 3.2.1 Deployment Topology (Targeted Architecture) for hardware topology.

Table 7: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Windows Virtual Machine (VM) – 3 each	DS3	Version 2	4 cores (14GB RAM) w/ 1 P10 (128GB) managed premium OS Volume	Microsoft Azure	N/A
SQL Database	Gen5	vCore	2 cores (14GB RAM) Business Critical Tier w/ 150GB Data Storage	Microsoft Azure	N/A
Load Balancer	Basic	IPv4	Private with back-end connections to 3 application VMs	Microsoft Azure	N/A

Please see Section 2 Roles and Responsibilities for details about who is responsible for preparing the site to meet these hardware specifications.

3.3.3. Software

WebVRAM will be utilizing approved existing software listed on the VA Technical Reference Model (TRM).

Table 8: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other Notes
RPC-BSE	N/A	1.1	TCP M-based server	VA Infrastructure	N/A

Required Software	Make	Version	Configuration	Manufacturer	Other Notes
			connection enabler	and Security Services	
ASP.NET Core	N/A	8.0.6	Application run-time support	Microsoft	N/A
.NET Framework	N/A	8.0.6	Framework which runs Active Server Pages (ASP).NET	Microsoft	N/A
Bootstrap	N/A	5.3.2	Mobile application development toolkit	Bootstrap Core Team	N/A
Visual Studio 2022 Enterprise w/ Azure Components	N/A	2022	Code development tool	Microsoft	N/A
VA Fortify Static Code Analyzer (SCA) and Apps 22.x.x for Windows x64 w/Visual Studio Plugin	N/A	22.2.1	Secure code scan tool	Micro Focus	N/A
Angular 17+	N/A		GUI rendering tool	Open Source	N/A

3.3.4. Communications

A virtual meeting will be held for all team members involved with WebVRAM deployment. All parties involved and/or invested in WebVRAM deployment will receive status emails throughout the deployment activities.

Table 9: Team Support Information/Role

Team Support Information	Role
Communication Lead <i>Scheduled</i>	Serves as the main communication and coordination point of contact on behalf of the application to provide regular status updates and issue escalation.

Team Support Information	Role
SQA Tester(s) <i>Scheduled</i>	Performs testing to verify that application is functioning as expected.
Development <i>On Call</i>	Development resources are typically on-call for Production deployments, unless they are required to serve as advisory resources during the release activities.
VA PM and Business Owner <i>On Call</i>	Perform a Critical Decision review of the application to approve national release if all release requirements are met.
VA Business Point of Contact (POC) <i>On Call</i>	Engage Business Contacts if decisions need to be made regarding Production issues.
Development Team <i>Scheduled</i>	Application Support contacts are scheduled to perform Production code releases and infrastructure changes.
Product Support <i>On Call</i>	Product Support contacts are scheduled to assist with VistA patch distribution or are otherwise scheduled to be on call.
VA Enterprise Cloud (VAEC) Cloud Operations Management (COMS) Team <i>Scheduled</i>	Typically, on-call support for infrastructure issue troubleshooting and resolution.

3.3.5. Deployment/Installation/Back-Out Checklist

Table 10: Deployment/Installation/Back-out Checklist

Activity	Day	Time	Responsible Individual
Deploy	September 28, 2024	Approx. 9 p.m. Eastern Time	Development Team Member
Install	September 28, 2024	Approx. 9 p.m. Eastern Time	Development Team Member
Back-Out	September 28, 2024	As needed	Development Team Member

4. Installation

4.1. Pre-installation and System Requirements

System requirements are tracked in the Backlog in the Jira WebVRAM repository.

4.1.1. VistA Patch Installation

Sites must have four VistA patches installed prior to installing this release of WebVRAM; see **Section 3.3.1** for details.

4.2. Platform Installation and Preparation

Planned deployment will occur Saturdays during off hours, beginning around 9 p.m. Eastern. Software installation is expected to take approx. 1-3 hours, ending by midnight Eastern. Most deployments can be performed without any downtime. If downtime is anticipated, it will be communicated to users at least three days in advance.

Production defect repairs and/or emergency software updates may occur as needed on weekdays. Any downtime associated with these deployments will be communicated to users at least three days in advance. Download and Extract Files

The WebVRAM system is web-based and is deployed using files containing configuration information rather than code package objects moved directly from one environment to another.

For the identified extract files, refer to the "webvram_files_list.txt" text file located in the env_depl_impl folder in the GitHub WebVRAM product repository.

The WebVRAM Source Code can be found in the GitHub WebVRAM code repository.

NOTE: The hyperlinks above link to the VA intranet and will only work for authorized users connected to the VA network.

4.3. Database Creation

This section is not applicable.

4.4. Installation Scripts

The WebVRAM system uses two PowerShell scripts to deploy the application. The first script is run by a developer and is used to package a copy of the application after it has been built and then send it to the target server. The second script is run by a developer on the target server and will perform the steps outlined in section 4.8 Installation Procedure.

4.5. Cron Scripts

There are no Cron scripts for this installation. (A Cron script is a term for a routine or script that runs chronologically (i.e. runs on a regular timetable.)

4.6. Access Requirements and Skills Needed for the Installation

To complete the installation:

- Basic system administration skills are needed.
- Access to the web server is required.
- Permission is needed to:
 - Start/Stop the web server.
 - Update WebVRAM web application files.

4.7. Installation Procedure

The Installation Procedure is as follows:

1. Stop the web server.
2. Copy the WebVRAM files to the configured web application folder.
3. Configure the WebVRAM application to use the appropriate database.
4. Start the web server.

4.8. Installation Verification Procedure

Visit the web application at its WebVRAM Homepage:

1. Login using credentials.
2. Test drive the application.
3. Check the application logs for any errors.

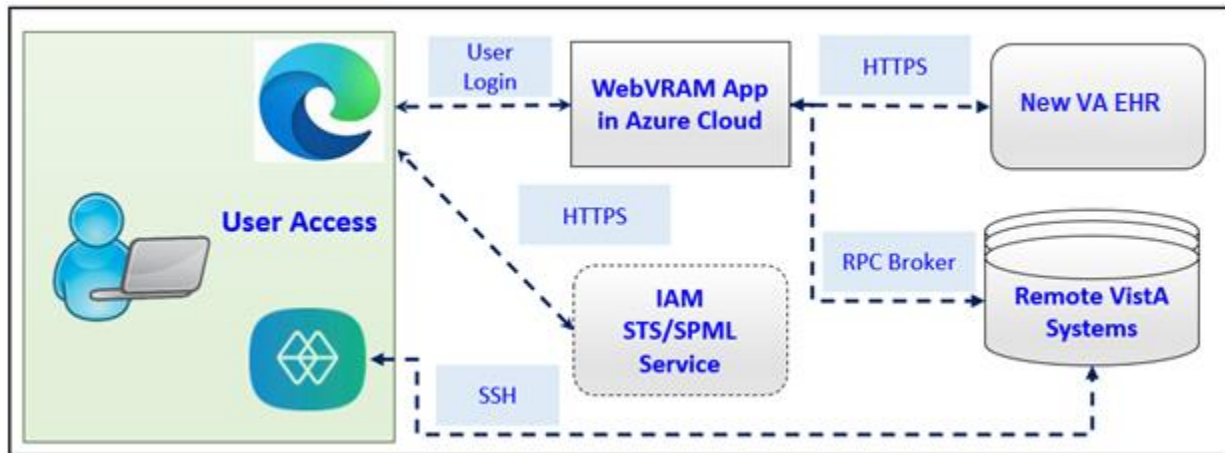
4.9. System Configuration

Figure 2: WebVRAM Single Production String shows the configuration of a single Production string to the extent that it is known. A full Production aspect of the application will involve multiple users and VistA sessions through several cloud subnets.

The user logs in to the WebVRAM web application located in the Azure cloud. The application utilizes the Station ID Callback RPC, or IAM Security Token Service / Services Provisioning Markup Language (STS/SPML) Service to perform user authentication. The WebVRAM application connects to CPRS instances using VistA Sentillion and connects to remote VistA systems via RPC Broker. The user uses Micro Focus Reflection to

connect to remote VistA systems via SSH. The application launches a connection to the VA's New EHR PIV Login URL.

Figure 2: WebVRAM Single Production String



4.10. Database Tuning

This section is not applicable.

4.11. CPRS Version Installation on Shared Directory

WebVRAM detects which version of the VA Computerized Patient Record System (CPRS) is required at each VistA location and launches that version on the user's desktop. To launch the correct set of executables, the latest production versions are added to a national Share Directory where the application can obtain and launch the correct version of CPRS software for the user. The CPRS team notifies the WebVRAM team when they are planning a new production version deployment of the application.

The procedures for downloading and adding the latest CPRS version executables are described in Standard Operating Procedure (SOP) *CPRS – Downloading Latest Version For WebVRAM National Directory* on the SOPs folder on the WebVRAM SharePoint site.

NOTE: The hyperlink above will navigate to sites on the VA intranet and will only work for authorized users connected to the VA network.

5. Back-Out Procedure

Back-out pertains to a return to the last known good operational state of the software and appropriate platform settings. Should a rollback of this deployment occur, the software will be removed from the appropriate platform.

5.1. Back-Out Strategy

Back-out and rollback are highly intertwined. The same high-level procedure is in place for both back-out and rollback. The back-out and rollback strategy for a project begins at the time of application deployment. Back-out and rollback procedure will bring the system back to the functionality of the previous release. The steps below describe, at a general level, what should be included in the procedure for back-out/rollback:

1. At the time of system deployment, create a complete backup of the system and store it on a separate machine.
2. Proceed with application-specific system deployment steps. If the system fails during deployment, perform a system rollback using the system backup created in step 1.
3. Perform thorough and comprehensive testing to ensure the integrity and functionality of the system.
4. Perform a system backup once the system is deemed stable and ready for users and store it on a separate machine. Once users begin working on the system, regularly create system backups and store them on another machine.
5. If system failure occurs after users are on the system, perform a system rollback using the system backup created in step 4.
6. Any client machines may need to clear their web browser cache before they will see the effects of the system rollback.

The strategy above provides assurance against fault and a guaranteed rollback position in the event of an undiagnosed fault. At times, however, there may be a reason to not rollback the complete solution migration and instead only rollback a portion of it. Some potential reasons for this include:

- The fault is easily identified and localized in a single software component which is deemed non-essential.
- The fault is not identified during initial release testing, but only after the solution is in use in Production and a complete database restore is no longer an option.
- The backup file is corrupted or lost.

In such cases, alternate approaches may be taken to restore the system to its previous state, although each approach will be dependent on the situational specifics.

5.2. Back-Out Considerations

5.2.1. Load Testing

Load testing is a performance test that subjects the system to varying workloads to measure and evaluate the performance behaviors and abilities of the system to continue to function properly under these different workloads. Load testing determines and ensures that the system functions properly beyond the expected maximum workload. Additionally, load testing evaluates the performance characteristics (e.g., response times, transaction rates, and other time-sensitive issues).

5.2.2. User Acceptance Testing

Pre-production Software Quality Assurance (SQA) testing performed by the WebVRAM project team was completed on March 2, 2023. IOC Testing was conducted in March 2023.

Business/Product Owner approval for national release will be obtained prior to the scheduled release.

5.3. Back-Out Criteria

The criteria for a back-out are:

- The fault is easily identified and localized in a single software component that has been deemed non-essential.
- The fault is not identified during initial release testing, but only after the solution is in use in Production, and a complete database restore is no longer an option.
- The backup file is corrupted or lost.

5.4. Back-Out Risks

There are no risks to backing out the WebVRAM product. The previous release would still be available to all users after a back-out of the new release is performed. If applicable, a VistA patch back-out across the enterprise would not affect the web application functionality.

5.5. Authority for Back-Out

Authority for back-out should be provided by the VA Product Manager.

5.6. Back-Out Procedure

The Back-Out Procedure is as follows:

1. Stop the web server.
2. Remove the WebVRAM files to the configured web application folder.
3. Remove the configuration of the WebVRAM application from the appropriate database.

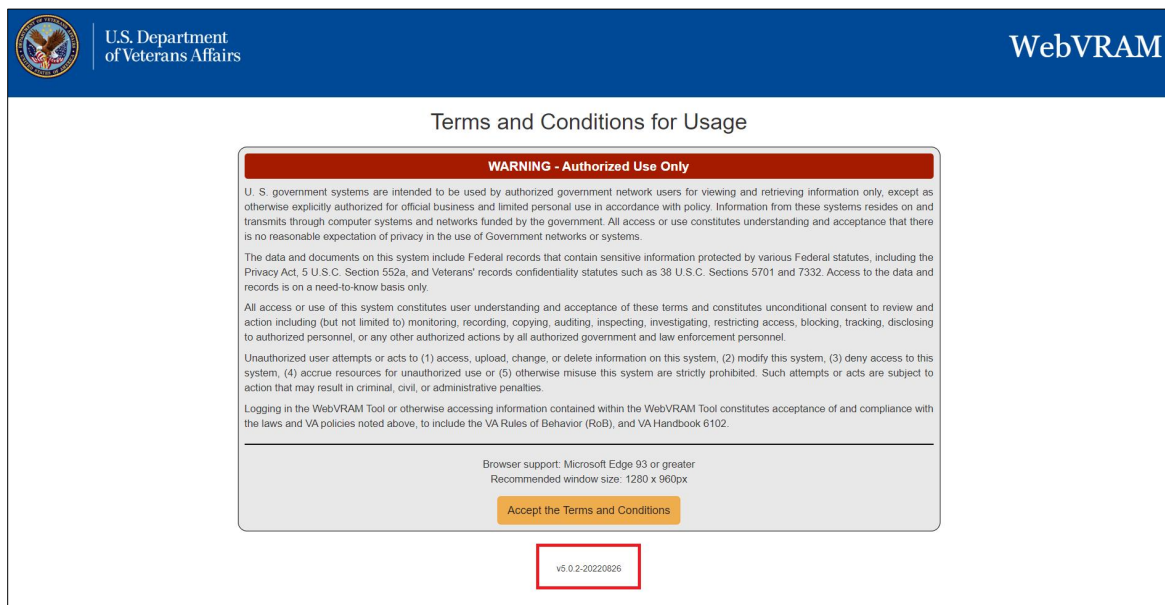
4. Start the web server.

5.7. Back-Out Verification Procedure

To verify back-out:

1. Visit the web application at its WebVRAM Homepage.
2. Locate the version information at the bottom of the page.
3. Check the application logs for any errors.
4. Test the application for all features and functionality. Report any negative findings to ESD for triage and potential defect repair.

Figure 3: WebVRAM Home Page



6. Rollback Procedure

This section describes the processes necessary to perform the Rollback Procedure.

6.1. Rollback Considerations

Business Owner approval will decide viability to proceed.

6.2. Rollback Criteria

Restore backup of Production environment taken prior to deployment.

6.3. Rollback Risks

No risks have been identified.

6.4. Authority for Rollback

Authority for rollback should be provided by the VA Project Manager (PM).

6.5. Rollback Procedure

A member of the Development Team will be assigned to this deployment. Rollback to the previous version of software will occur automatically after the back-out procedure outlined above in Section 5.6 is implemented.

6.6. Rollback Verification Procedure

After a back-out procedure has been performed, the WebVRAM product will be rolled back to the previous version in the Production environment. Verification of the prior version is outlined above in Section 5.7.